

Lucent Technologies
Bell Labs Innovations



Lucent Security Management Server

Release 9.1

Reports, Alarms, and Logs

260-100-019R9.1
Issue 1
July 2006

Copyright © 2006 Lucent Technologies. All Rights Reserved.

This material is protected by the copyright laws of the United States and other countries. It may not be reproduced, distributed, or altered in any fashion by any entity (either internal or external to Lucent Technologies), except in accordance with applicable agreements, contracts or licensing, without the express written consent of Lucent Technologies and the business management owner of the material.

Trademarks

All trademarks and service marks specified herein are owned by their respective companies.

Contents

About this information product

Purpose	xix
Who Should Read This Book	xix
What is in This Book	xix
What is Not in This Book	xxii
Supported Brick devices	xxii
Where to Find Technical Support	xxiii
How to comment	xxiii

1 Introduction to LSMS Logs

Overview	1-1
What are LSMS Logs?	1-2
Log Files	1-4

2 LSMS Log Viewer

Overview	2-1
Display the Log Viewer	2-2
Log Window Modes	2-9
Log Window Menus	2-11
Log Window Column Headings	2-12
Real Time Tab	2-13
History Tab	2-15

	Log Detail Window	2-17
	Log Viewer Filters Window	2-18
	Set the Help Facility	2-23
	Find Text Function	2-24
3	Types of LSMS Logs	
	Administrative Events Log	3-1
	Session Log	3-3
	Proactive Monitoring Log	3-7
	User Authentication Log	3-11
4	Introduction to Alarms	
	Overview	4-1
	What are Events, Alarm Triggers and Actions?	4-3
	Console Alarms Window	4-7
	Using the Wizard	4-9
5	Configuring Alarm Actions	
	Overview	5-1
	Configure a New Alarm Action	5-2
	Configuring the Direct Page Action	5-5
	Configuring the E-mail Action	5-9
	Configuring the SNMP Trap Action	5-12
	Configuring the Syslog Action	5-14
	Maintaining Actions	5-18
6	Configuring Alarm Triggers	
	Overview	6-1
	Configuring Triggers	6-3
	Alarm Code Trigger	6-7

<i>Brick</i> [®] Error Trigger	6-11
Brick Failover Event Trigger	6-14
<i>Brick</i> [®] ICM Trigger	6-17
<i>Brick</i> [®] Interface Lost Trigger	6-18
<i>Brick</i> [™] Lost Trigger	6-21
Brick Proactive Monitoring Trigger	6-25
<i>Brick</i> [®] SLA Round Trip Delay Alarm Trigger	6-30
VPN proactive Monitoring Trigger	6-31
LAN-to-LAN Tunnel Lost Trigger	6-38
LAN-to-LAN Tunnel UP Trigger	6-41
Local Presence Map Pool Trigger	6-44
LSMS Error Trigger	6-47
LSMS Status Change Trigger	6-50
LSMS Proactive Monitoring Trigger	6-52
QoS Alarm Triggers	6-57
Unauthorized LSMS Login Attempt Trigger	6-59
User Authentication Trigger	6-62
Maintaining Triggers	6-65
7 Configuring TL1 Alarms	
Overview	7-1
Configure TL1 Alarms	7-2
8 Introduction to LSMS Reports	
Overview	8-1
Types of LSMS Reports	8-2
Configuration Assistant Reports Settings	8-3
Report logic	8-5

9	Administrative Events Report	
	Overview	9-1
	To Generate an Administrative Events Report	9-2
	Administrative Events Report Output	9-12
10	Sessions Logged Report	
	Overview	10-1
	To Generate a Sessions Logged Report	10-2
	Sessions Logged Report Output	10-16
11	Closed Session Details Report	
	Overview	11-1
	To Generate a Closed Session Details Report	11-2
	Closed Session Details Report Output	11-23
12	Alarms Logged Report	
	Overview	12-1
	To Generate an Alarms Logged Report	12-2
	Alarms Logged Report Output	12-17
13	User Authentication Report	
	Overview	13-1
	To Generate a User Authentication Report	13-2
	User Authentication Report Output	13-14
14	WebTrends Reports	
	Overview	14-1
	Preparing the Environment	14-2
	Web Trends Configuration	14-5
	WebTrends Reports	14-14

A	SNMP	
	Overview	A-1
	What are SNMP Traps?	A-2
	What is the SNMP Agent?	A-9
	How to Collect Data from the LSMS	A-15
B	Alarm Code Rules	
	Overview	B-1
	Analyze Security Events First	B-2
	How to Create the Alarm Code Rules	B-3
C	Proactive Monitoring Trigger Parameters	
	Overview	C-1
	What are the Brick Proactive Monitoring Parameters?	C-2
	What are the LSMS Proactive Monitoring Parameters?	C-5
D	Proactive Monitoring Subtypes	
	Overview	D-1
	Brick Data	D-2
	Brick Interface Generic	D-4
	Brick Interface Ethernet	D-5
	LSMS Auditing	D-6
	Authentication Firewall	D-7
	Local Map Pool	D-8
	QoS Statistics	D-9
	SLA Statistics	D-10
	Brick VPN Data	D-11
E	Log Field Formats	
	Overview	E-1

	Record Header	E-2
	Log Record Types	E-4
F	Filterable Log Fields	
	Overview	F-1
	Filterable Log Fields	F-2
G	Log Field Syntax	
	Overview	G-1
	Log Field Syntax	G-2
H	Log File Sizing Guidelines	
	Administrative Events Log Sizing Guidelines	H-1
	Session Log Sizing Guidelines	H-2
	Promon Log Sizing Guidelines	H-3
	User Authentication Log Sizing Guidelines	H-4
	VPN Log Sizing Guidelines	H-5
I	Transferring Log Files via FTP	
	Overview	I-1
	Scheduling Log Transfer	I-4
	Creating FTP Scripts	I-7
	Post Log Transfer	I-10
	Using FTP Logs	I-11
	Troubleshooting Log Transfer	I-13
J	Pre-Configured Reports	
	Overview	J-1
	Closed Session Details Reports	J-2
	Administrative Events Reports	J-3
	Run a Pre-Configured Report	J-5

Run Multiple Reports J-6

Index

List of tables

About this information product

1	Part 1: LSMS Logs	xx
2	Part 2: LSMS Alarms	xx
3	Part 3: LSMS Reports	xx
4	Appendices	xxi

List of figures

1	Introduction to LSMS Logs	
1-1	Configuration Assistant Log File Entries	1-6
2	LSMS Log Viewer	
2-1	Log Viewer Menu	2-3
2-2	Log Viewer	2-4
2-3	LSMS Log Viewer With All Log Windows Open	2-5
2-4	LSMS Log Viewer File Menu	2-6
2-5	LSMS Log Viewer Window Menu	2-7
2-6	LSMS Log Window Real Time Tab (Session Log)	2-9
2-7	LSMS Log Window History Tab (Session Log)	2-9
2-8	LSMS Log Window Format Menu	2-11
2-9	Promon Log Window Column Headings	2-12
2-10	Session Log Window Column Headings	2-12
2-11	Log Window Real Time Tab Buttons	2-13
2-12	Log Window Real Time Tab Action Menu	2-13
2-13	Log Window History Tab Action Menu	2-15
2-14	Log Window History Tab Paging Buttons	2-15
2-15	Log Window Tool Tip Prompt	2-17
2-16	Log Window Detail Window	2-17
2-17	Log Viewer Filters Window	2-18

2-18	Filter Editor Window	2-19
2-19	Log Filter Parameters	2-20
2-20	IS/IS NOT Drop-down List	2-21
2-21	Find and Highlight Window	2-24

3 Types of LSMS Logs

3-1	Administrative Events Log Sample Record	3-1
3-2	Administrative Events Log Viewer	3-2
3-3	Session Log Sample Record	3-3
3-4	Session Log Viewer	3-4
3-5	Proactive Monitoring Log Sample Record	3-7
3-6	Proactive Monitoring Log Viewer	3-9
3-7	User Authentication Log Sample Record	3-11
3-8	User Authentication Log Viewer	3-12

4 Introduction to Alarms

4-1	Alarm Bell Icon	4-7
4-2	Console Alarms window	4-7
4-3	Wizard Buttons	4-9

5 Configuring Alarm Actions

5-1	LSMS Navigator Folder Panel	5-2
5-2	Alarm Action Wizard	5-3
5-3	Action Wizard Action Type Drop-down List	5-4
5-4	Direct Page Action	5-6
5-5	E-mail Action	5-10
5-6	SNMP Trap Action	5-12
5-7	Syslog Action	5-16

6 Configuring Alarm Triggers

6-1	LSMS Navigator Folder Panel	6-3
6-2	Alarm Trigger Editor	6-4
6-3	Alarm Trigger Editor Trigger Type Drop-down List	6-5
6-4	Alarm Trigger Editor Alarm Status Drop-down	6-5
6-5	Alarm Trigger Editor Alarm Code Trigger Parameters	6-8
6-6	Alarm Trigger Editor Brick Error Trigger Parameters	6-11
6-7	Alarm Trigger Brick Failover Event Trigger Parameters	6-14
6-8	Alarm Trigger Editor Brick Interface Lost Parameters	6-18
6-9	Alarm Trigger Editor Brick Lost Parameters	6-22
6-10	Alarm Trigger Editor Brick Proactive Monitoring Trigger Parameters	6-26
6-11	Select Threshold Values Window	6-27
6-12	Brick Proactive Monitoring Parameters Drop-down	6-28
6-13	Alarm Trigger Editor VPN Proactive Monitoring Trigger Parameters	6-32
6-14	VPN Proactive Monitoring Threshold Value Panel	6-33
6-15	Add New Threshold Window	6-34
6-16	VPN Proactive Monitoring PM Parameter Drop-Down List	6-34
6-17	VPN Proactive Monitoring Wizard (Group)	6-35
6-18	VPN Proactive Monitoring Wizard (Zone)	6-36
6-19	VPN Proactive Monitoring Wizard (Action)	6-37
6-20	Alarm Trigger Editor LAN-to-LAN tunnel Lost Parameters	6-39
6-21	Alarm Trigger Editor LAN-to-LAN tunnel Lost Parameters	6-41
6-22	Alarm Trigger Editor Local Presence Map Pool Trigger Parameters	6-45
6-23	Alarm Trigger Editor LSMS Error Trigger Parameters	6-48
6-24	Alarm Trigger Editor LSMS Status Change Trigger Parameters	6-50
6-25	Alarm Trigger Editor LSMS Proactive Monitoring Trigger Parameters	6-53
6-26	Select Threshold Values Window	6-54

6-27	LSMS Proactive Monitoring Parameters Drop-down List	6-55
6-28	Alarm Trigger Editor Unauthorized Login Attempt Trigger Parameters	6-60
6-29	Alarm Trigger Editor User Authentication Trigger Parameters	6-62
7	Configuring TL1 Alarms	
7-1	LSMS Navigator Folder Panel	7-2
7-2	TL11 Alarm Wizard	7-3
7-3	TL11 Alarm Wizard - NMA Parameters	7-4
7-4	TL11 Alarm Wizard - Brick Lost Parameters	7-6
7-5	TL11 Alarm Wizard - Brick Interface Lost Parameters	7-8
7-6	TL11 Alarm Wizard - Brick Failover Parameters	7-10
7-7	TL11 Alarm Wizard - Select Group	7-12
7-8	TL11 Alarm Wizard - Brick Interface Lost Parameters	7-13
8	Introduction to LSMS Reports	
8-1	Configuration Assistant Reports Parameters	8-3
9	Administrative Events Report	
9-1	Administrative Events Report Editor (Source/Events tab)	9-3
9-2	Administrative Events Editor (Text Search tab)	9-5
9-3	Administrative Events Editor (Columns tab)	9-6
9-4	Administrative Events Editor (Sorting tab)	9-8
9-5	Administrative Events Log Report	9-13
10	Sessions Logged Report	
10-1	Sessions Logged Editor (Sessions Logged tab)	10-3
10-2	Sessions Logged Editor (Bricks/Zones tab)	10-5
10-3	Sessions Logged Editor (Sessions Logged tab)	10-8
10-4	Sessions Logged Editor (Text Search tab)	10-10
10-5	Sessions Logged Editor (Columns tab)	10-11

10-6	Sessions Logged Editor (Sorting tab)	10-12
11	Closed Session Details Report	
11-1	Closed Session Details Editor (Host tab)	11-3
11-2	Closed Session Details Editor (Bricks/Zones tab)	11-5
11-3	Closed Session Details Editor (Host tab)	11-8
11-4	Closed Session Details Editor (Protocol tab)	11-10
11-5	Closed Session Details Editor (VPN tab)	11-12
11-6	Closed Session Details Editor (Proxy tab)	11-14
11-7	Closed Session Details Editor (Miscellaneous tab)	11-16
11-8	Closed Session Details Editor (Columns tab)	11-18
11-9	Closed Session Details Report (Part A)	11-24
12	Alarms Logged Report	
12-1	Alarms Logged Editor (Alarms Logged tab)	12-3
12-2	Alarms Logged Editor (Bricks/Zones tab)	12-5
12-3	Alarms Logged Editor (Alarms Logged tab)	12-8
12-4	Alarms Logged Editor (Text tab)	12-10
12-5	Alarms Logged Editor (Columns tab)	12-11
12-6	Alarms Logged Editor (Sorting tab)	12-13
12-7	Alarms Logged Report	12-18
13	User Authentication Report	
13-1	User Auth Editor (User Auth tab)	13-3
13-2	User Auth Editor (Columns tab)	13-8
13-3	User Auth Editor (Sorting tab)	13-10
13-4	User Authentication Report	13-15
14	WebTrends Reports	
14-1	Environmental Variables	14-3

14-2	Edit User Variable	14-4
14-3	Webtrends Scheduler	14-6
14-4	Add Scheduled Event Window	14-8
14-5	Webtrends Scheduler	14-9
14-6	DOS Window (Start Now)	14-10
14-7	Title, Log File Format Window	14-12

I Transferring Log Files via FTP

I-1	Log Transfer Parameter in Configuration Assistant	I-2
I-2	Example schedTables.txt File (Windows NT)	I-5
I-3	Example schedTables.txt File (Solaris)	I-5
I-4	Sample PKZIP Compression Script (Windows NT)	I-7
I-5	Sample PKZIP Compression Script (Unix)	I-8
I-6	Sample GZIP Compression Script (Windows NT)	I-8
I-7	Sample GZIP Compression Script (Unix)	I-9
I-8	ftplog.txt on Windows NT	I-11
I-9	ftplog.txt on Solaris	I-12

About this information product

Purpose

Welcome to the *Reports, Alarms, and Logs Guide*. This manual explains how to use log files, configure triggers and actions to generate alarms, and compile and view reports.

Who Should Read This Book

The *Reports, Alarms, and Logs Guide* is intended to be read by network administrators who will be using the LSMS application to:

- Use logs to monitor trends in the network
- Set up triggers and actions to be notified of system events
- Generate and view reports to analyze network traffic and for troubleshooting

In the terminology used by the LSMS, these administrators are referred to as LSMS Administrators and Group Administrators, depending on the privileges they have been given when their profiles were created.

What is in This Book

The *Reports, Alarms, and Logs Guide* explains the five log files and how to use these log files to monitor trends in the network.

It also explains how to configure triggers and actions so that Administrators are notified of network events. Procedures for generating and memorizing reports to analyze network traffic passing through one or more Lucent VPN Firewall *Bricks*® are also included.

The *Reports, Alarms, and Logs Guide* is divided into three sections, followed by a series of appendices. The following tables briefly explain what is in each chapter and appendix:

Table 1 Part 1: LSMS Logs

Chapter	Purpose
2. Introduction to LSMS Logs	This chapter explains the five log files, how log rollover works, and the Halt All Traffic feature.
3. LSMS Log Viewers	This chapter describes operation of the LSMS Log Viewer and its associated filtering.
4. Types of LSMS Logs	This chapter describes the five types of LSMS logs.

Table 2 Part 2: LSMS Alarms

Chapter	Purpose
5. Introduction to Alarms	This chapter provides basic information about LSMS alarms.
6. Configuring Alarm Actions	This chapter describes the four alarm actions that can be configured to launch upon receipt of an alarm trigger.
7. Configuring Alarm Triggers	This chapter describes various types of triggers that can be set to initiate alarm actions.

Table 3 Part 3: LSMS Reports

Chapter	Purpose
8. Introduction to LSMS Reports	This chapter provides basic information about LSMS reports.
9. Administrative Events Report	This chapter explains how to generate an Administrative Events Report to monitor events such as successful logins, logouts, creation of devices, zones, rulesets, etc.
10. Sessions Logged Report	This chapter explains how to generate a Sessions Logged Report to analyze network trends and to identify potential security problems.
11. Closed Session Details Report	This chapter explains how to generate a Closed Session Detail Report to monitor traffic through one or more Brick devices.
12. Alarms Logged Report	This chapter explains how to generate an Alarms Logged Report to produce a historical record of alarms generated by any installed Brick device or Real-Secure detector.

Table 3 Part 3: LSMS Reports (continued)

Chapter	Purpose
13. User Authentication Report	This chapter explains how to generate a User Authentication Report to view and analyze users who are authorized to access hosts protected by a Brick device or connected to a Brick device via a tunnel.
14. WebTrends Reports	This chapter explains how to generate WebTrends reports from LSMS session log files.

Table 4 Appendices

Appendix	Purpose
A. SNMP	This Appendix explains how to load the MIB files on a Network Management Station and how to create rules if a Brick device resides between the LSMS and the Network Management System (NMS).
B. Alarm Code Rules	This Appendix explains how to create rules with an alarm code so that an alarm is generated. It assumes the Alarm Code trigger has already been configured.
C. Proactive Monitoring Trigger Parameters	This appendix comprehensively explains the Proactive Monitoring parameters that can be used when configuring a Brick or LSMS Proactive Monitoring alarm.
D. Proactive Monitoring Subtypes	This appendix explains the fields contained in the seven subtypes that can be written to a Proactive Monitoring log record.
E. Log Field Formats	This appendix lists and explains the formats used in the LSMS logs and reports.
F. Filterable Log Fields	This appendix describes the meaning and syntax of each of the log fields that can be used to trigger an alarm or action.
G. Log Field Syntax	This appendix elaborates on the definition of each particular log field syntax.
H. Transferring Log Files via FTP	This appendix explains how to set up automated transfer of log files to long term storage areas.
I. Log File Sizing Guidelines	This appendix describes how to assess the amount of space required for each of the five logs based on network traffic and other factors.
J. Preconfigured Reports	This appendix explains the pre-configured reports that are created when the LSMS application is installed.

What is Not in This Book

If you are looking for information on any of the following topics, you should refer to the *LSMS Administration Guide*:

- How to log on and off the LSMS
- How to connect a Brick device to your network and configure the Brick device so that it communicates with the LSMS
- How to configure RealSecure detectors and set up LSMS failover
- How to create groups and set up additional Administrator accounts

These and other topics are covered in the *LSMS Administration Guide*. Since these topics pertain primarily to the set up and administration of the hardware, we recommend that you read the *Administration Guide* — and perform all required tasks — before you approach the *LSMS Policy Guide*, which includes the following topics:

- How to set up and manage security policy including rulesets, host groups, network address translation, application filters, etc.
- How to set up Brick devices to proxy incoming and outgoing SMTP, FTP, and HTTP sessions
- How to set up user authentication and digital certificates
- How to setup LAN-to-LAN tunnels and how to configure a Brick device or router to serve as the endpoint of a client tunnel

Supported Brick devices

The following available Brick models are supported by the current LSMS release:

- Model 20 Brick device
- Model 50 Brick device
- Model 150 Brick device
- Model 350 Brick device
- Model 1100/1100A Brick device
- Model 700 Brick device
- Model 1200 Standard and HS Brick devices

Some of the above Brick device models require a specific patch of the current LSMS release in order to be fully supported. For details about the LSMS patch release required for a specific Brick device model, refer to the *User's Guide* for the Brick device model or check out the **VPN Firewall Portfolio** link on the following website for specific LSMS patch release information: <http://www.lucent.com/security/>

Where to Find Technical Support

Technical assistance and additional information can be acquired by telephone or e-mail. If you require technical assistance, first collect information that technical support staff can use to diagnose the problem. This includes:

- Software version of the LSMS.
- Model number and serial number of the Brick.
- Platform the LSMS runs on (Windows or Solaris).
- Description of problem.
- Layout of your network. For example, is the Brick connected to a device such as a hub or router? Is the Brick operating as a bridge or is it using static routes? What are the Brick ports connected to? What is the IP address range and VBA for each zone? What is the security policy for each port?

After gathering the information, contact Lucent Security Customer Care at 1-866-LUCENT-8.

How to comment

To comment on this information product, go to the [Online Comment Form](http://www.lucent-info.com/comments/enus/) (<http://www.lucent-info.com/comments/enus/>) or email your comments to the Comments Hotline (comments@lucent.com).

1 Introduction to LSMS Logs

Overview

Purpose

Lucent Secure Compute Servers (LSCSs), or simply known as Compute Servers, are introduced in Release 8.0. They are identical to LSMSs, except that they do not have their own database. The primary purpose of an LSCS is to collect log data. Therefore, in this chapter, the term "LSMS" refers to both an LSMS and Compute Server.

The chapters in this section explain how to use the LSMS Log Viewer and the five logs that are provided with the LSMS. These logs can be used by Administrators to monitor traffic through one or more *Bricks*[®], track important administrative events, view statistics about the internal operations of the system, and perform a number of troubleshooting activities.

For troubleshooting, real-time data is the most useful tool. Only the LSMS Log Viewer provides the administrator with a window on activity as it happens. The Log Viewer also allows you to apply filters and combinations of filters to restrict the content of the messages it displays to those that apply to your current area of interest. The Detail window feature provides the ability to examine the details of a single log entry with all the fields clearly labeled. You can double-click any entry in a Log Viewer to display the Detail window.

The standalone Log Viewer can only be run directly on the LSMS or LSCS. Reports can be run on the LSMS or from a remote machine. Reports cannot be run from Compute Servers. The real-time functionality of the standalone Log Viewer can be accessed on the LSMS Navigator under the following menu selections:

Contents

What are LSMS Logs?	1-2
Log Files	1-4



What are LSMS Logs?

Overview

The LSMS application includes an audit server that monitors various aspects of LSMS and Brick operations and stores that information in logs that reside on the LSMS host.

You can view the contents of the logs by using one of the five Log Viewer windows, explained in [Chapter 2, “LSMS Log Viewer”](#).

When viewing the logs, you can view the logs in their entirety, or you can enter certain filtering criteria so that only specific information is displayed. The Log Viewer Filter Window and the Filter Editor are also discussed in [Chapter 2, “LSMS Log Viewer”](#).

Logs

The audit information collected by the LSMS is stored in five separate logs. These logs are:

- *Administrative Events Log*
The Administrative Events Log contains information about a variety of administrative events, including Bricks lost, policies loaded, error messages and alarms triggered and delivered. Also referred to as simply “the Event Log,” it is an important troubleshooting tool.
- *Proactive Monitoring (Promon) Log*
The Proactive Monitoring Log contains records that provide statistical information about the internal operations of the LSMS/LSCS and the *Bricks*® it is managing. This information allows high level monitoring of resources to identify usage patterns.
- *Session Log*
The Session Log contains Brick session records, which record network activity through the ports of the Bricks that the LSMS is managing. Application filter audit information is also stored in this log.
- *User Authentication Log*
The User Authentication Log contains messages that record successful or unsuccessful user authentication requests to the LSMS or other external servers, such as RADIUS or Secure ID servers.
- *VPN Log*
The VPN Log contains records that pertain to all VPN tunnel transactions including all errors, events, and messages. The information allows easier debugging of VPN tunnel problems.

Uses

In addition to providing Administrators with information about the operation of the LSMS and Brick, the logs also serve as the basis for the alarm and reporting subsystems.

The alarm and reporting subsystems are described below.

- *Alarms Subsystem*
The alarm subsystem monitors the logs for the occurrence of events that are configured in an alarm (e.g., *Brick*[®] Lost). If such an event occurs, the alarm is triggered and an Administrator is notified in a number of configurable ways, for example, by e-mail, by page, or by an SNMP trap sent to a network management station.
For details, see “Overview” (p. 7-1) and Chapter 6, “Configuring Alarm Triggers”, later in this guide.
- *Reports Subsystem*
The reports subsystem uses the logs from all LSMSs and Compute Servers to filter and present network information in a user-friendly format. The information in a report can be used to analyze patterns of network traffic and for troubleshooting purposes.
For details, see Chapter 8, “Introduction to LSMS Reports”, through Chapter 13, “User Authentication Report”.

LSMS Logs and Spreadsheets

Using the log files as the basis, you can create management or summary reports for further study and analysis with a spreadsheet application such as Microsoft Excel.



Log Files

Overview

The audit data in each log is accumulated in log files that are stored on the LSMS/LSCS host. The number of files in each log depends upon the amount of auditing that the LSMS is performing.

Log File Location

The table below indicates where the files for each log are located, if you chose the default installation path, on both the Windows and Solaris platforms:

Log	Windows NT	Solaris
Session	\users\isms\lmf\log\sessions	/opt/isms/lmf/log/sessions
Proactive Monitoring	\users\isms\lmf\log\promon	/opt/isms/lmf/log/promon
User Authentication	\users\isms\lmf\log\userauth	/opt/isms/lmf/log/userauth
Administrative Events	\users\isms\lmf\log\adminevents	/opt/isms/lmf/log/adminevents
VPN	\users\isms\lmf\log\vpn	/opt/isms/lmf/log/vpn

Log File Names

For each of the five logs, the first "loggable" event or activity that occurs each day causes a new log file to be created. The name of this file, and each file that is created throughout the remainder of the day, reflects the date and time the file was created.

The format of the name is:

YYYY-MM-DD-hh-mm-ss.log

where:

YYYY = year (four digits)

MM = month (01-12)

DD = day (01-31)

HH = hours (00-23)

mm = minutes (00-59)

ss = seconds (00-59)

The name of the first log file on any given day is made up of the year, month, and day. For example, the following would be the name of the first log file created on June 16, 2001:

2001-06-16-.log

If other log files are created during the day, their names would include the hour as well as the year, month, and day. Thus, if the second file created on June 16, 2001, was created at 1 pm, it would have this name:

2001-06-16-13-.log

If another log file is created before the hour is up, its name would consist of the year, month, day, hour, and minute. Therefore, if the third file created on June 16, 2001, was created at 1:30 pm, it would have this name:

2001-06-16-13-30-.log

Finally, if another log file is created before the minute is up, its name would be made up of the year, month, day, hour, and second, in the format shown below:

2001-06-16-13-30-45.log

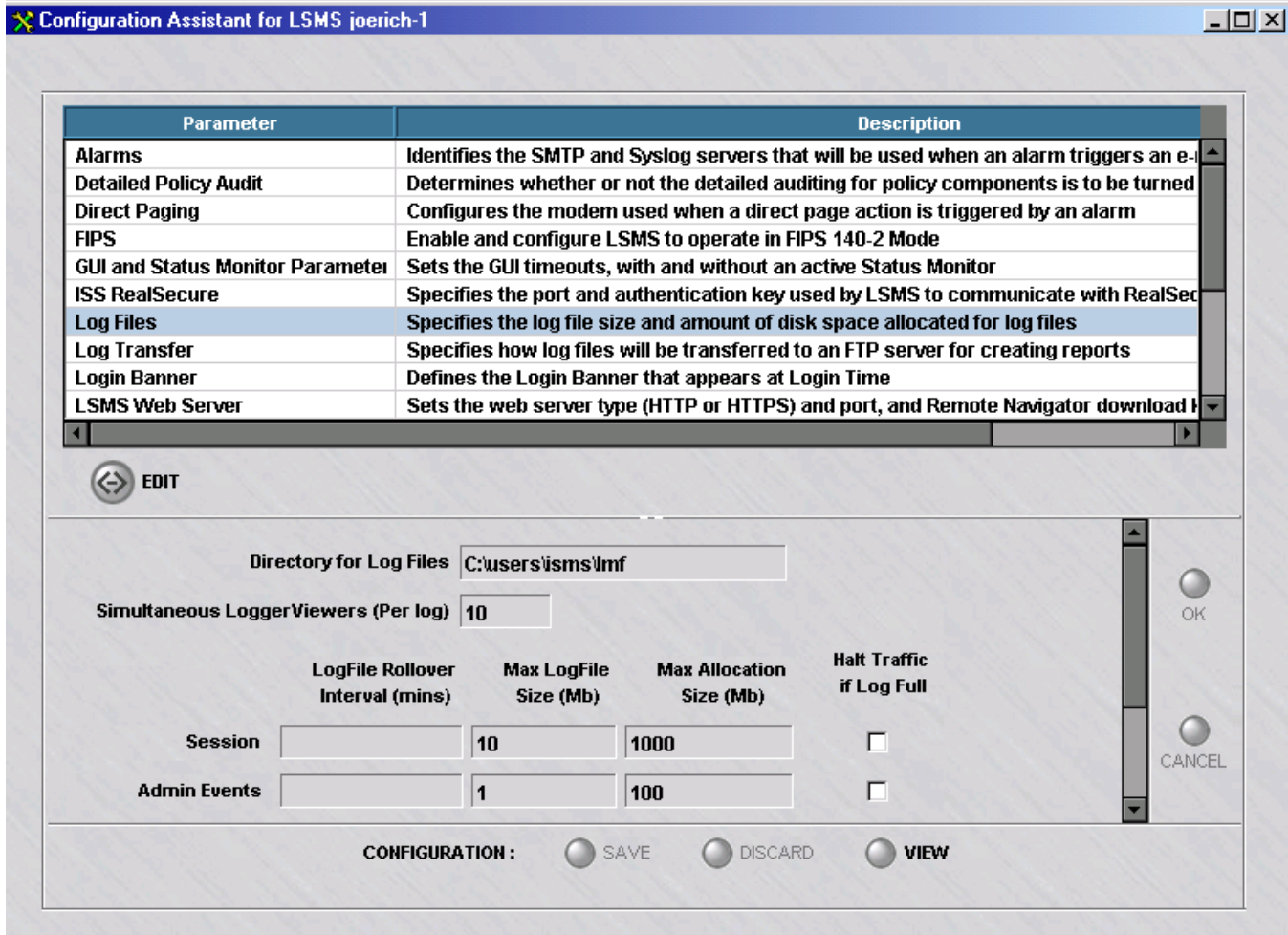
Important! The dash that appears before the *.log* in each file name has been added by the LSMS to ensure that the files display in the proper order. You may ignore it.

Log File Size

New log files are created whenever an existing log file reaches its maximum size or after the configured rollover interval. The maximum size and the rollover interval of the log files for each log is set using the Configuration Assistant. See Chapter 10, Using the Configuration Assistant in the *LSMS Administration Guide* for details on the

Configuration Assistant. [Figure 1-1, “Configuration Assistant Log File Entries”](#) (p. 1-6) shows the Configuration Assistant Log Files settings.

Figure 1-1 Configuration Assistant Log File Entries



The table below shows the default maximum file size and maximum disk allocation for each of the five logs. The time interval-based log file rotation is disabled, by default.

See [Appendix H, “Log File Sizing Guidelines”](#) for details on calculating appropriate log file sizes for your requirements.

Log	Maximum File Size	Maximum Disk Allocation
Session	10 Mb	1000 Mb
Administrative Events	1 Mb	100 Mb
Proactive Monitoring	10 Mb	200 Mb

Log	Maximum File Size	Maximum Disk Allocation
User Authentication	1 Mb	100 Mb
VPN	1 Mb	100 Mb

Halt All Traffic If Log Full

It is important that you allocate enough disk space for each log to accommodate the log files that are created. In [“Administrative Events Log” \(p. 3-1\)](#), we provide guidelines for determining how much space to allocate for each type of log.

If the disk space that was allocated for a particular log is exhausted, the LSMS will begin to delete old log files, beginning with the oldest, to make room for new ones.

Since this can cause you to lose important log records that may be necessary for troubleshooting or recovery purposes, you can prevent the old files from being deleted by checking the **Halt Traffic if Log Full** checkbox in the Configuration Assistant (see [Figure 1-1, “Configuration Assistant Log File Entries” \(p. 1-6\)](#)). This checkbox appears next to each log, so you can turn this feature on and off for each log.

For each Brick that will be generating log data, you must also check the **Halt All Traffic if Audit Fails** checkbox when initially configuring the Brick. If this has not been done for a Brick, edit the Brick’s configuration and click the checkbox. See Chapter 5, *Maintaining a Brick® Configuration* in the *LSMS Administration Guide* for instructions on editing a Brick configuration.

If you make any changes to a checkbox setting, you have to restart the logger service.

How it Works: If a log is about to be deleted due to lack of disk space, the logger subsystem checks to see if the **Halt Traffic if Log Full** checkbox for the log has been checked in the Configuration Assistant. If the checkbox is checked, the log is not deleted and the Bricks are disconnected from the LSMS.

When a Brick is disconnected from the LSMS and the **Halt All Traffic if Audit Fails** is checked on the Options tab of the Brick Editor for that Brick, then the Brick will not pass any more traffic until it reconnects to the logger on the LSMS.

Generate an Alarm: If you want to be notified when the allocation for a log file is approaching maximum capacity, and network traffic will soon stop because **Halt Traffic if Log Full** has been enabled, you can configure one of these alarm trigger types:

- **A Proactive Monitoring trigger** to monitor the amount of space left. This trigger would provide notification so the problem could be rectified before it escalates into a catastrophic scenario.
- An LSMS **Error trigger** configured with the error code: E4017 All Traffic Halted. This trigger is *not* proactive, only retroactive. It would provide a warning that a problem has already occurred and should be corrected, since traffic through the Brick will be halted until the log space is freed.

See [Chapter 6, “Configuring Alarm Triggers”](#) in this guide for details on how to configure these triggers.



2 LSMS Log Viewer

Overview

Purpose

This chapter explains how to use the LSMS Log Viewer. The purpose of the Log Viewer is to enable an administrator to view the five logs that are provided with the LSMS. These logs are: an Event Log, a Proactive Monitoring (Promon) Log, a Session Log, a VPN Log and a User Authentication Event Log. These logs can be viewed real-time or historically.

Contents

Display the Log Viewer	2-2
Log Window Modes	2-9
Log Window Menus	2-11
Log Window Column Headings	2-12
Real Time Tab	2-13
History Tab	2-15
Log Detail Window	2-17
Log Viewer Filters Window	2-18
Set the Help Facility	2-23
Find Text Function	2-24



Display the Log Viewer

Overview

The Log Viewer can be displayed locally from the LSMS/LSCS host or remotely, using the LSMS Remote Navigator. The following explains how to display the Log Viewer locally on both the Windows and Solaris platforms, and remotely using the LSMS Remote Navigator.

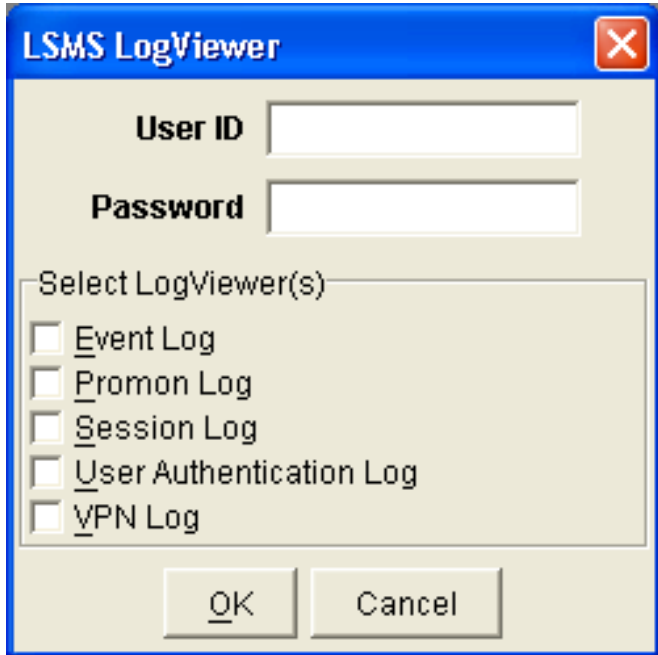
Display the Log Viewer Locally (Windows)

To display the Log Viewer from an LSMS host running Windows, follow the steps below:

- 1 Click the **Start** button on the Windows taskbar, and select:
Programs ► Lucent Security Management Server ► LSMS LogViewer

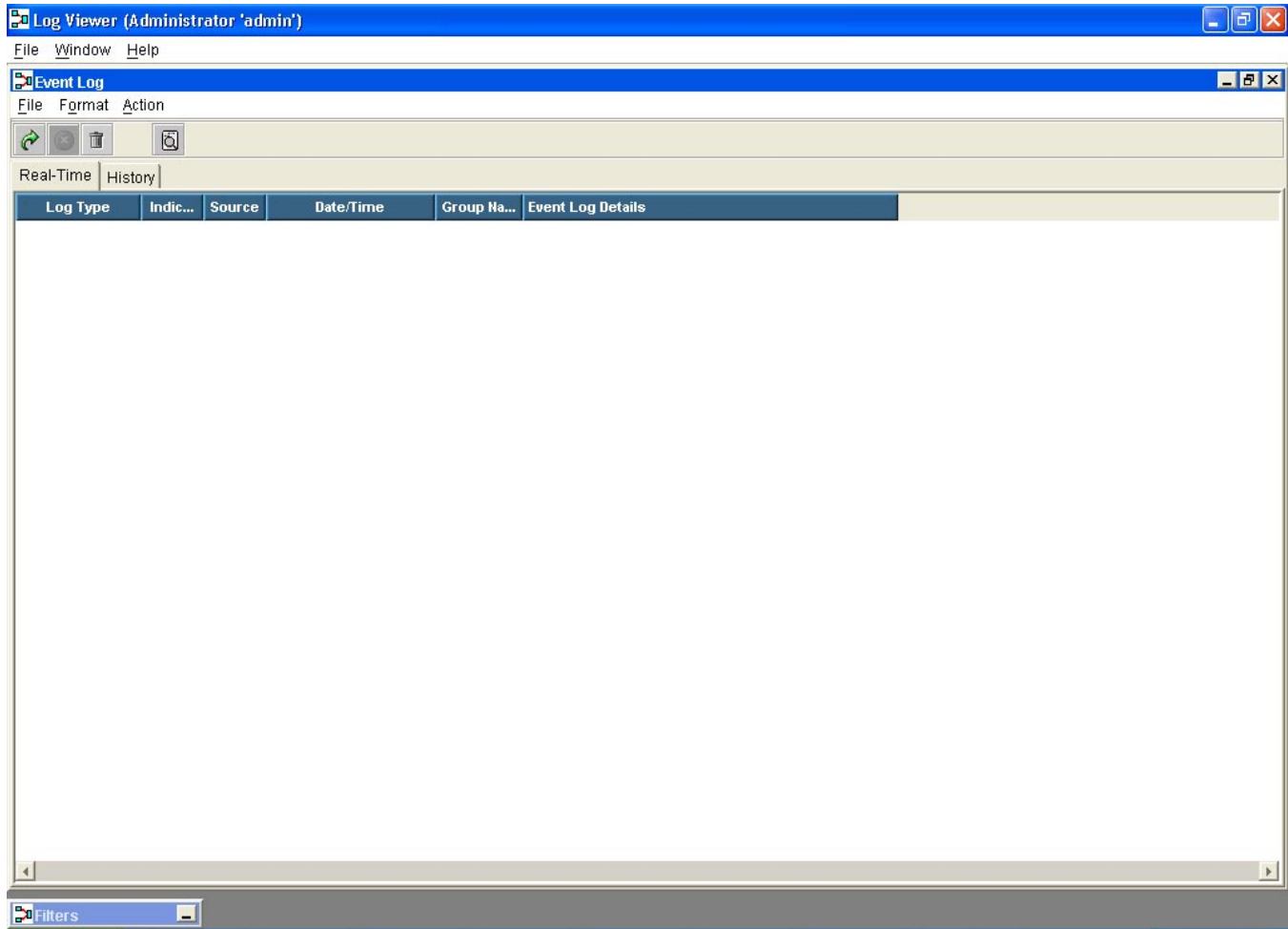
The Log Viewer menu will appear. It is shown in [Figure 2-1, “Log Viewer Menu”](#) (p. 2-3).

Figure 2-1 Log Viewer Menu



- 2 Select the log(s) you want to view and click the **OK** button. You may select up to five logs. The Log Viewer will appear with the first log you selected displayed. [Figure 2-2, “Log Viewer”](#) (p. 2-4) shows the Log Viewer with the Event Log displayed.

Figure 2-2 Log Viewer



Only one log will appear in the Log Viewer at any one time. If you selected more than one log, you can switch to one of the other logs you selected by opening the **Window** menu and selecting the log. All logs that are open are shown in the Window menu.

END OF STEPS

Display the Log Viewer Locally (Solaris)

To display the Log Viewer from an LSMS host running Solaris, follow the steps below:

- 1 Make the installation directory (usually */opt/isms/lmf*) the present working directory.
- 2 From the Solaris command line, enter:

```
./LogViewer
```

The Log Viewer window will appear. It is shown in [Figure 2-3, “LSMS Log Viewer With All Log Windows Open”](#) (p. 2-5).

Figure 2-3 LSMS Log Viewer With All Log Windows Open

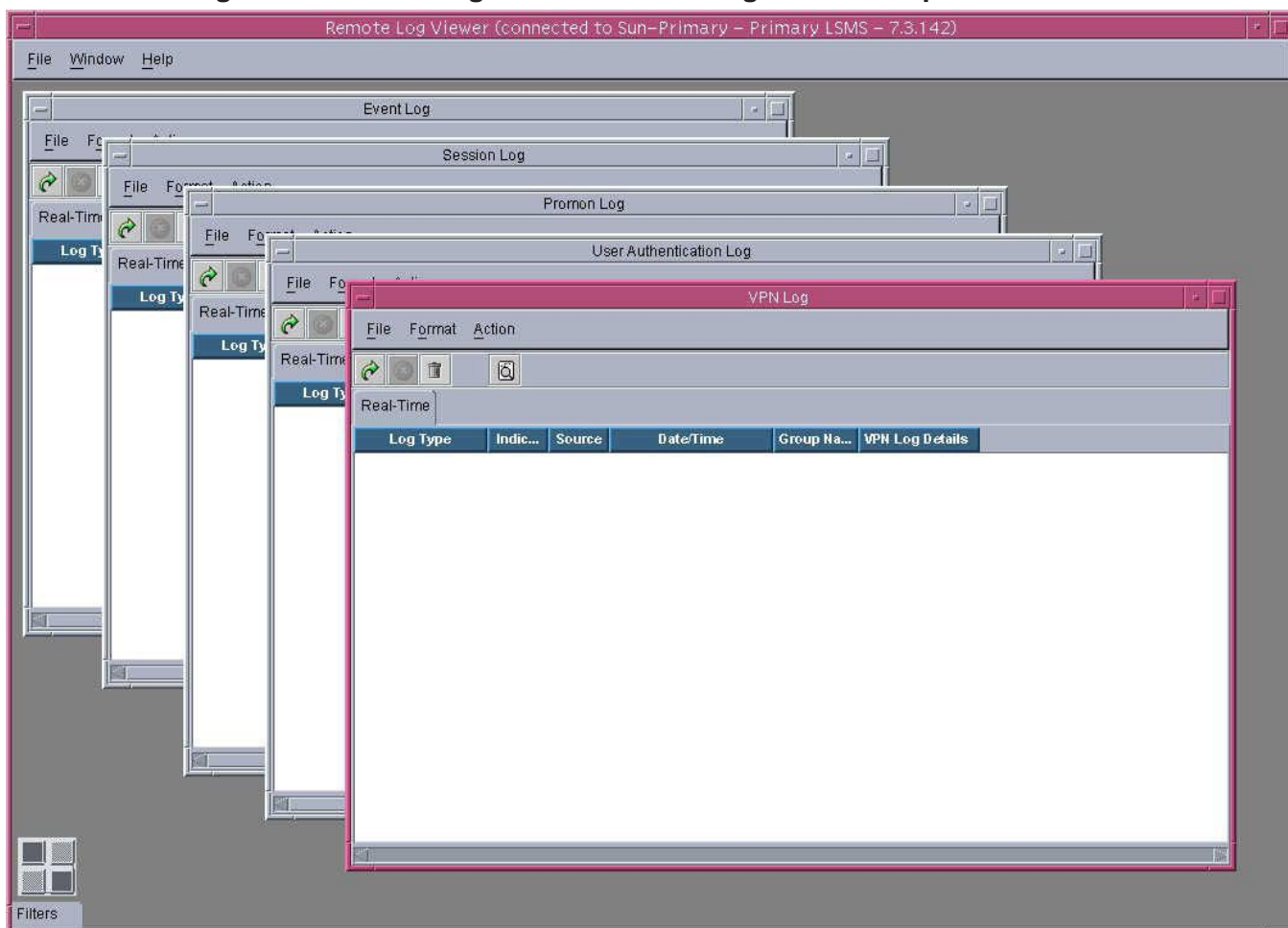


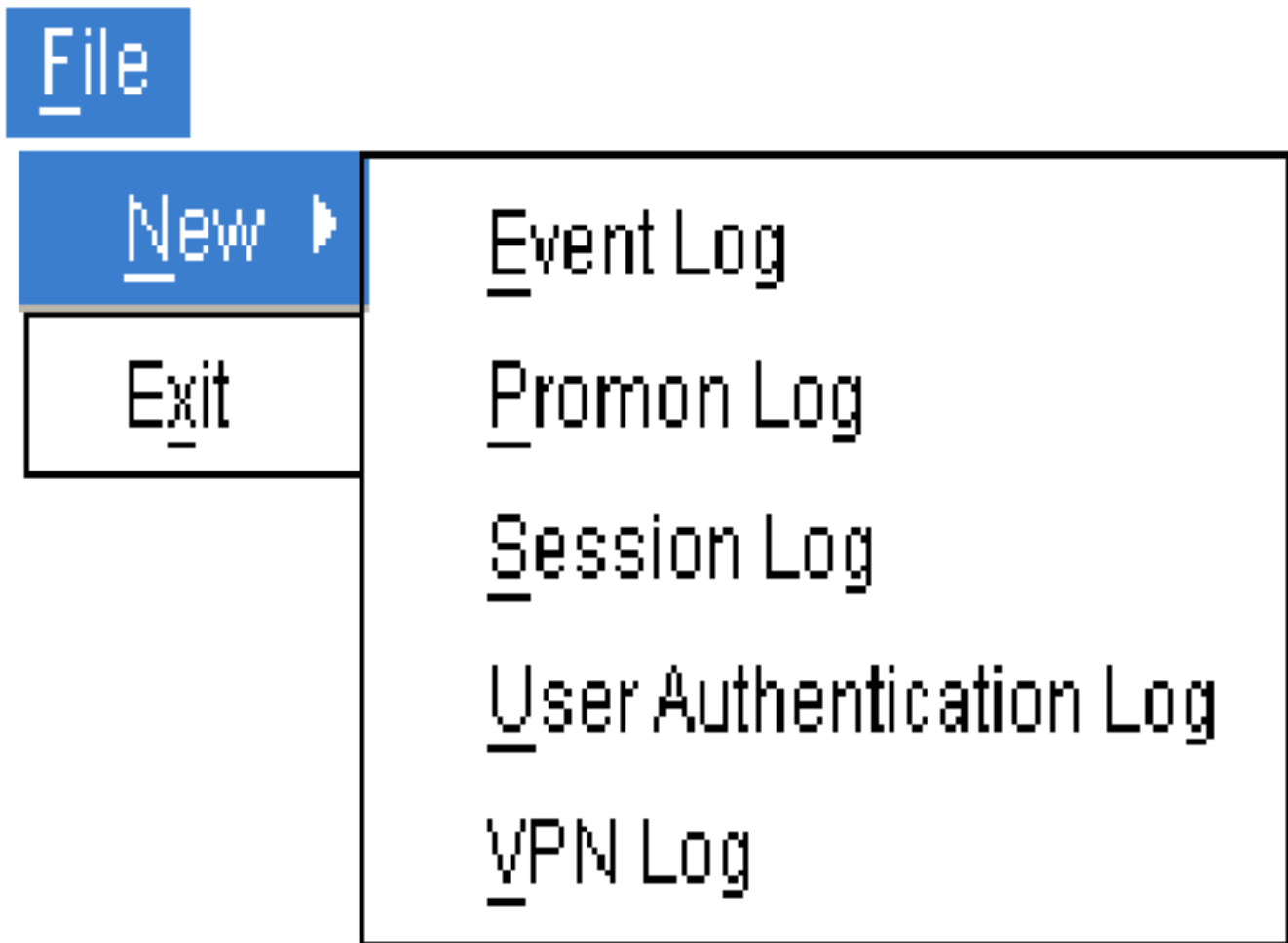
Figure 2-3, “LSMS Log Viewer With All Log Windows Open” (p. 2-5) shows all five Log Windows open as well as the **Log Viewer Filters** window. The **Filters** window

always opens, but only those Log Windows that you checked on the Log Viewer menu open.

The Log Viewer Filters window can be minimized, but it cannot be closed.

The Log Viewer's **File** menu allows you to open additional Log Windows after you've launched the Log Viewer. Only one instance of each Log Window type can be open at a time however. The menu selections for each Log Window type are grayed out if the corresponding window is already open.

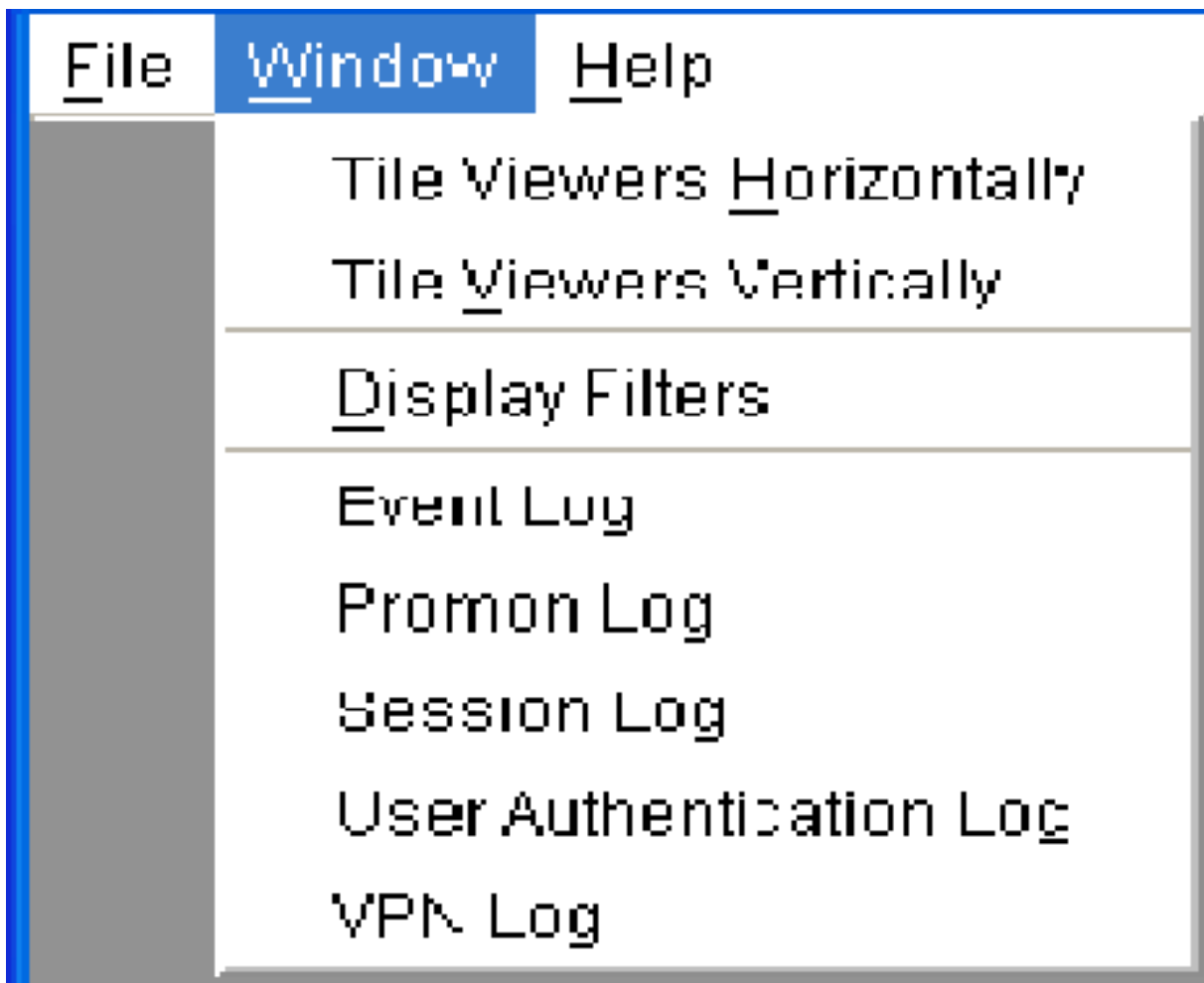
Figure 2-4 LSMS Log Viewer File Menu



The Log Viewer **Window** menu displays a menu entry for each window that is currently open. Clicking the entry for a specific Log Window brings that window to the front of the Log Viewer. The **Display Filters** menu selection works in a similar

fashion, but since the Filters window is always open, this menu entry is never grayed out.

Figure 2-5 LSMS Log Viewer Window Menu



END OF STEPS

Display the Log Viewer Remotely

LSMS Administrators may display the Log Viewer remotely using the LSMS Remote Navigator. Follow the steps below:

-
- 1 Open the LSMS Remote Navigator and log into the LSMS.
-

- 2 From any LSMS window, open the Utilities window and select

System Utilities ► LSMS Log Viewer

The LSMS Log Viewer menu will appear (see [Figure 2-1, “Log Viewer Menu”](#) (p. 2-3)). Select the logs you want.

The Log Viewer that is displayed when accessed remotely only provides real-time data, no historical data. If you need to display historical data from a remote connection use the report function.

END OF STEPS



Log Window Modes

Overview

The Log Windows allow you to view the logs in two modes — **Real Time** and **History**.

Figure 2-6, “LSMS Log Window Real Time Tab (Session Log)” (p. 2-9) and Figure 2-7, “LSMS Log Window History Tab (Session Log)” (p. 2-9) show each mode of the Session Log Window. You can change modes by clicking the appropriate tab, **Realtime** or **History**.

Figure 2-6 LSMS Log Window Real Time Tab (Session Log)

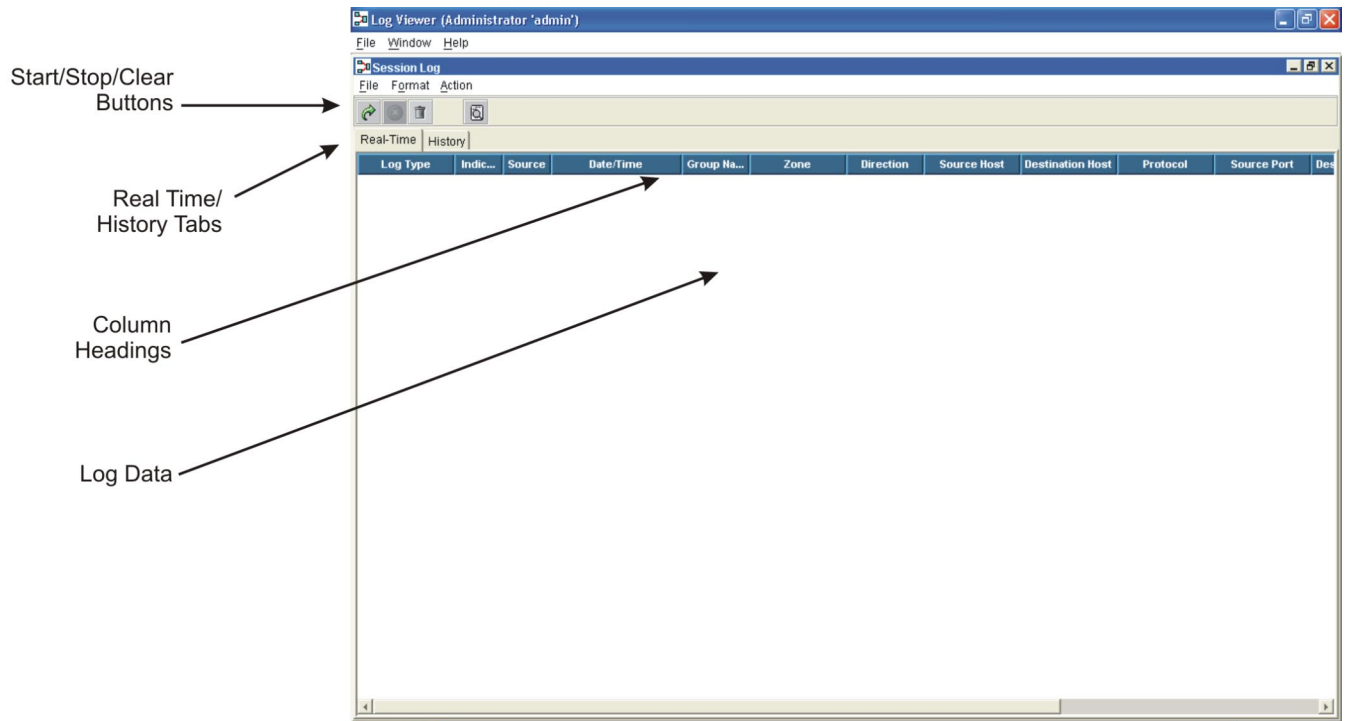
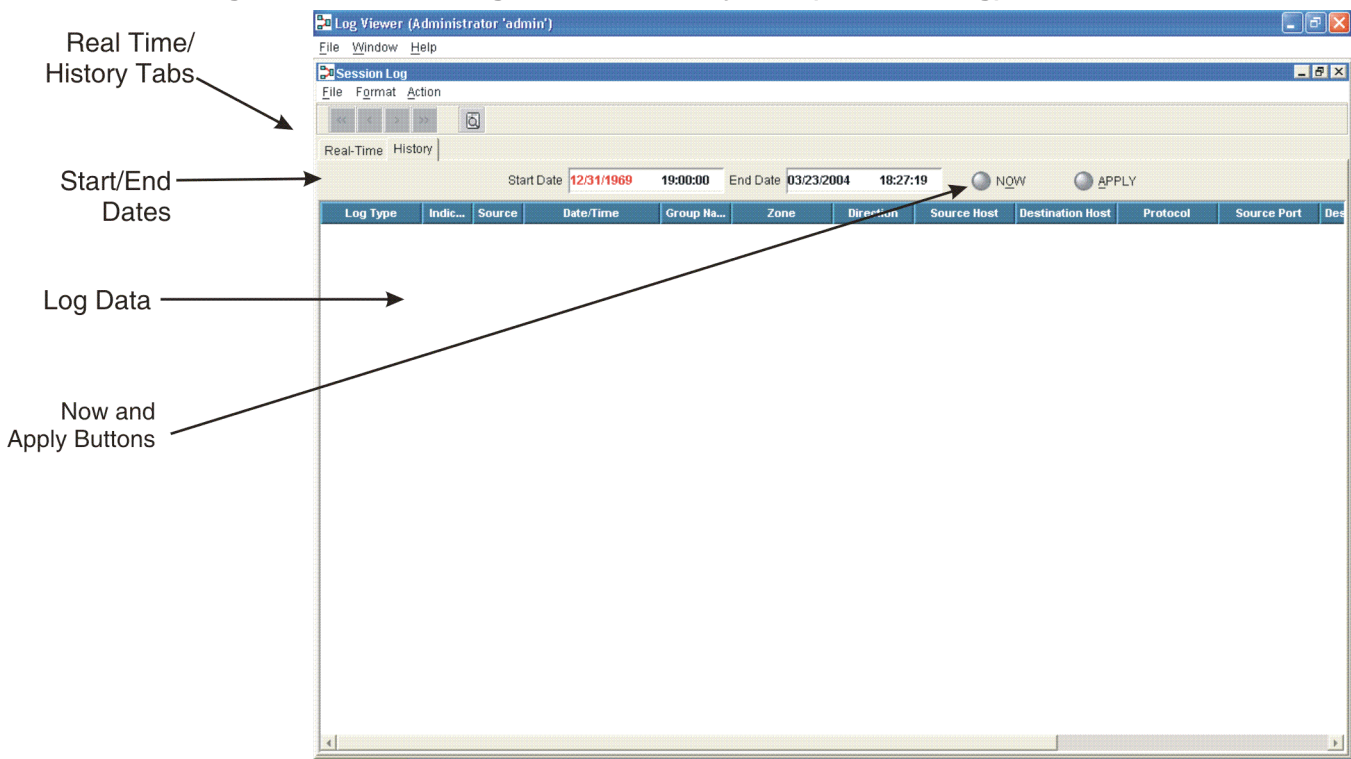


Figure 2-7 LSMS Log Window History Tab (Session Log)



To use a Log Window, you first enter the filtering criteria, as explained in the section “[Log Viewer Filters Window](#)” (p. 2-18). The filtering criteria allow you to determine which traffic or events in the log files you wish to display.

For example, when using the Session Log Window **History** tab as shown above, you can specify a particular *Brick*[®] or zone — in which case, you only see data pertaining to that Brick or zone.

If you are viewing data on the **History** tab, you also have to enter a Start Date and End Date. Then, click the **APPLY** button to apply the criteria. Once this has been done, there are other buttons you can use. These are explained in the two sections below.



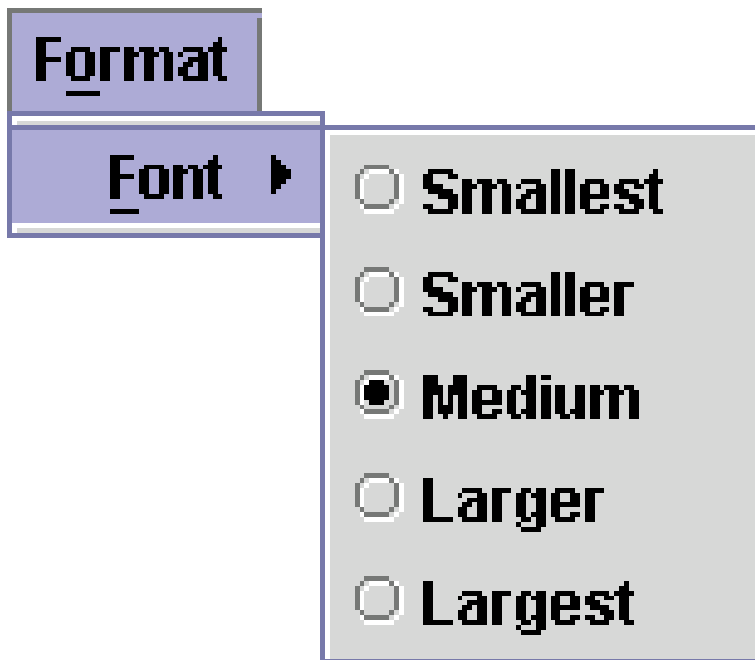
Log Window Menus

Overview

The Log Window File menu contains two selections: **Save As** and **Close**. The Save As selection allows you to save a history tab display as a comma separated text file. When you click Save As, a dialog box appears in which you can specify a name and location for the saved file.

The Log Window **Format** menu allows you to choose among five different font sizes for the log message text. The default font size is **Medium**.

Figure 2-8 LSMS Log Window Format Menu



□

Log Window Column Headings

Overview

A Log Window's output is arranged into columns. The first five columns, Log Type, Indicator, Source, Date/Time, and **Group Name** are the same regardless of which Log Window you are using. For three of the Log Windows, the heading of the fifth column has a name appropriate to the particular log window, such as **Event Log Details**, **User Auth Details**, or, as in [Figure 2-9, "Promon Log Window Column Headings"](#) (p. 2-12) below, **Promon Log Details**.

Figure 2-9 Promon Log Window Column Headings

Log Type	Indic...	Source	Date/Time	Group Name	Promon Log Details
----------	----------	--------	-----------	------------	--------------------

The **Session Log** viewer has seven additional columns, for a total of 12.

Figure 2-10 Session Log Window Column Headings

Zone	Direction	Source Host	Destination Host	Protocol	Source Port	Destination Port	Session Log Details
------	-----------	-------------	------------------	----------	-------------	------------------	---------------------

Sorting

In the History tab, you can sort columns of log data by clicking on the column heading.

Important! For performance reasons, sorting columns in logs with a size greater than 200 pages (around 40,000 records) is not recommended.



Real Time Tab

Overview

When you look at the **Real Time** tab of a Log Window, you see log information as it is being collected. It is useful to filter the log when viewing the **Real Time** tab so that you can perform real-time debugging or monitoring of a live network without impacting the performance of the system.

The Real Time tab has three buttons at the top left, below the menu bar.

Figure 2-11 Log Window Real Time Tab Buttons



These buttons are, from left to right, Start, Stop, and Clear. Clicking the **Start** button starts logging, clicking the **Stop** button stops logging. Clicking the **Clear** button clears the log list. These buttons also have exact counterparts on the **Action** menu.

Figure 2-12 Log Window Real Time Tab Action Menu



The following table explains the function of each button and menu item on a Log Window **Real Time** tab:

Button	Function
Start	Starts the display of log entries after the display has been paused using the Stop button. This button or menu item is disabled until you click Stop .
Stop	Stops displaying log entries. After Start has been selected, click Stop to pause the scrolling. This button or menu item is disabled until you click Start .
Clear	Refreshes the display.
Scroll While Capturing	When the Scroll While Capturing checkbox is checked, the log list scrolls as new entries are added. By default the checkbox is unchecked.



History Tab

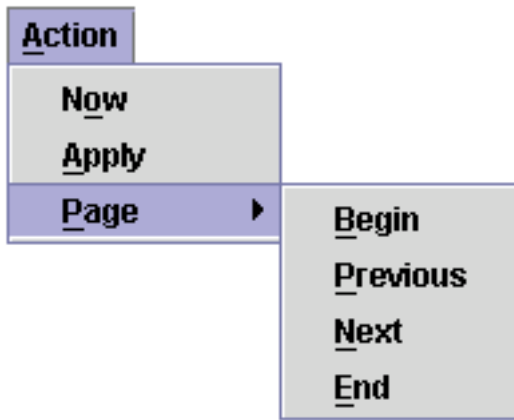
Overview

When you view the **History** tab of a Log Window, you see log information that was collected in the past. The Start Date and End Date fields allow you to specify the time frame you want displayed, down to the second. To increase performance, keep the interval between start date/time and end date/time short.

The filtering criteria allow you to specify precisely which information from that time frame you want to see.

The History tab provides the ability to step backward or forward through a log file by selecting pages. Each page is 200 lines of records. You can page through a log by using the **Begin**, **Previous**, **Next**, and **End** selections from the **Action** menu, **Page** submenu, shown in [Figure 2-13, “Log Window History Tab Action Menu”](#) (p. 2-15).

Figure 2-13 Log Window History Tab Action Menu



You can also page through a log using the paging buttons below the menu bar.

Figure 2-14 Log Window History Tab Paging Buttons



The following table explains the function of each button or menu item:

Button	Function
Now	Sets the End Date field to the current date/time.

Button	Function
Apply	Starts displaying log entries. Use after entering filtering criteria.
Begin (<<)	Displays the first page of a log file (the first 200 lines of the log). Click this menu item after you click Apply . This menu item is initially disabled.
Previous (<)	Displays the previous page of a log file (the previous 200 lines of the log). Click this menu item after you click Apply . This menu item is initially disabled.
Next (>)	Displays the next page of a log file (the next 200 lines of the log). Click this menu item after you click Apply . This menu item is initially disabled.
End (>>)	Displays the last page of a log file (the last 200 lines of the log). Click this button after you click Apply . This menu item is initially disabled.



Log Detail Window

Overview

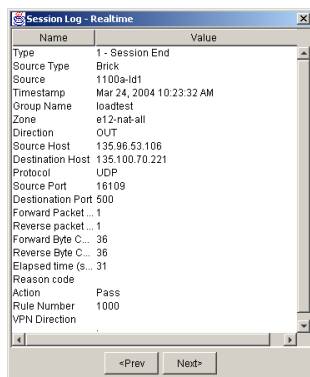
The LSMS features a Log Detail window enhancement to the log windows that allows the user to view details of individual log entries. Each log message field is labeled in the **Name** column. The Log Detail window makes interpretation of log messages much easier than in previous versions of the LSMS software. If you position the cursor over a line in any Log Window, a "Tool Tip" prompt appears to remind you of this feature.

Figure 2-15 Log Window Tool Tip Prompt

Log Type	Indicator	Source	Date/Time
] - Session Start	Brick	brick_t...	May 22, 2001 5:22:01 ..
] - Session Start	Brick	brick_t...	May 22, 2001 5:22:01 ..
] - Session Start	Brick	brick_t...	May 22, 2001 5:22:02 ..
] - Session Start	Brick	brick_t...	May 22, 2001 5:22:02 ..
] - Session Start	Br		5:35:09 ..
] - Session Start	Brick	brick_t...	May 22, 2001 6:25:57 ..
] - Session Start	Brick	brick_t...	May 22, 2001 6:33:27 ..

Double-click a row in the Log Window and the Log Detail window, shown in [Figure 2-16, "Log Window Detail Window"](#) (p. 2-17), appears.

Figure 2-16 Log Window Detail Window



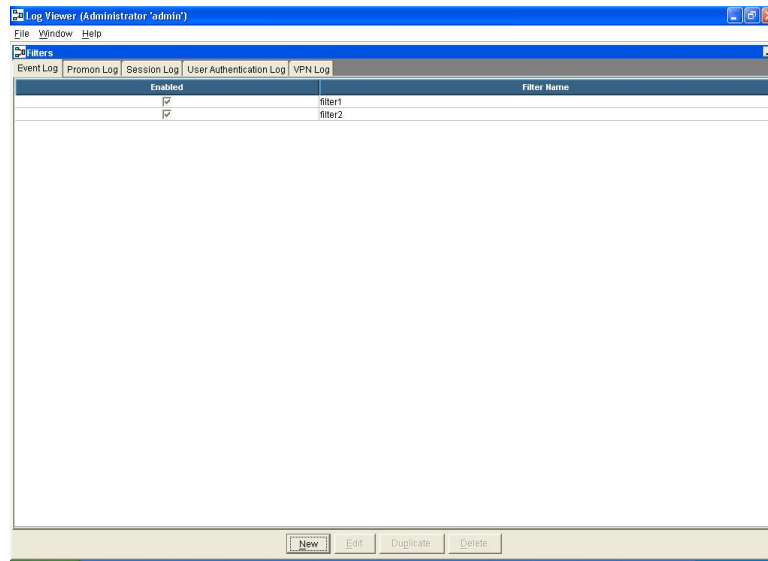
The Detail window contains two columns labeled **Name** and **Value**. You can click the **Next>** or **<Prev** buttons to view details about the next or previous events, respectively. Both the Real Time and History tabs have similar Detail windows.

Log Viewer Filters Window

Overview

When you select a log window to open from the initial Log Viewer pop-up menu, the **Log Viewer Filters** window opens at the same time.

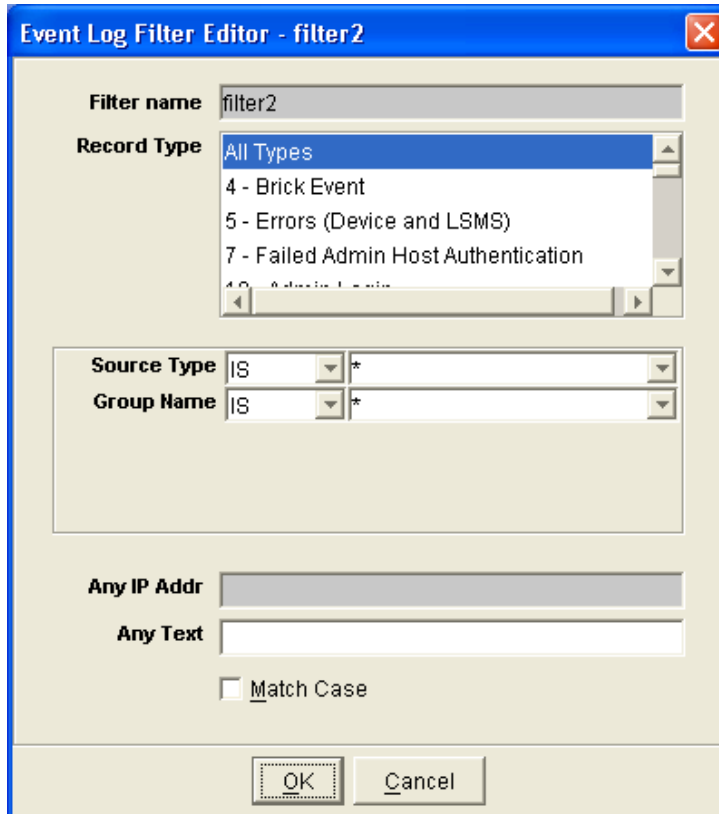
Figure 2-17 Log Viewer Filters Window



The Log Viewer Filters window has five tabs, one for each type of log. Click each tab to display filters that have already been configured for that log. A check in the **Enabled** column indicates that the filter is active.

To create a new filter, click the **New** button. The **Filter Editor** window appears.

Figure 2-18 Filter Editor Window



Assign a name to the new filter in the **Filter Name** field.

Choose **All Types** to capture all types of log records, or select one or more record types from the scrolling list. a set of log types for a given viewer

You can select more than one Filter Type by holding down the Control (CTRL) key when clicking on entries in the **Filter Type** list field. You can also select a range of Filter Types by holding down the Shift key, and clicking the first, then the last of the log types you want to include in the selected range.

The **Any IP Addr** field can be used for bi-directional IP Address filtering. This field accepts a single IP address, a range of IP addresses separated by a hyphen, or both. This field applies only to Session Log filters.

Use the **Any Text** field to define a text string for text based search. By default, the field ignores case. Check the **Match Case** checkbox to perform a case sensitive text search.

Log Filter Parameters

When you select a record type or types, the area below the Record Type list fills in with a number of fields, as shown in [Figure 2-19, “Log Filter Parameters”](#) (p. 2-20).

Figure 2-19 Log Filter Parameters

Source Type	IS	▼	*	▼
Group Name	IS	▼	*	▼

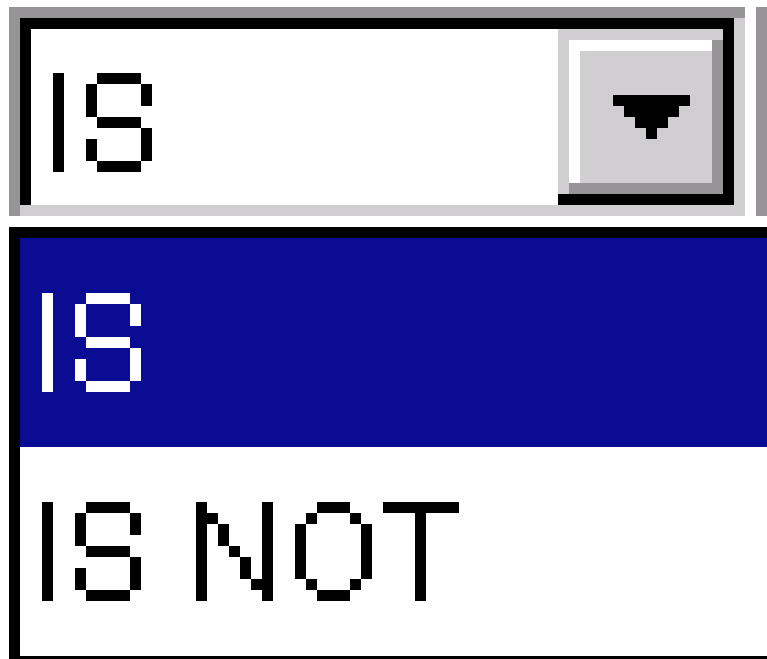
Depending on the type of log you are viewing and the record type you have selected, as few as two of these fields may appear. In most cases, however, more fields will be present.

Most of the fields provide drop-down menus that present all of the valid selections for that particular field. Some fields require the entry of an IP address or a port number.

All of the fields also include an IS/IS NOT drop-down menu that allows you to exclude certain entities. For example, in the Session log, the Protocol field entries available from the drop down list are TCP, UDP, ICMP, and * (for all protocols). By selecting IS NOT, then selecting UDP, your log would display entries for all sessions

that use any protocol except UDP. The IS/IS NOT drop-down list is shown in [Figure 2-20, “IS/IS NOT Drop-down List”](#) (p. 2-21).

Figure 2-20 IS/IS NOT Drop-down List



The following table lists all the fields present in any log window. Some fields in the table only appear in a specific log type, such as the Promon log, and are marked as appropriate.

Filter Name	Description
Source Type	This field filters the log record source. Valid values are *, Brick , LSMS Process , Proxy Server , ISS Real SecureEngine
Sub Type	Promon Log only. Sub type of Promon Log record. The valid values are Brick , Brick Interface-Generic , Brick Interface-Ethernet , LSMS Auditing , Authentication-VPN Client , Authentication Firewall and VPN Local Presence .
Brick Name	Valid Brick name. Multiple Brick names can be separated by commas.
Group Name	A valid LSMS group name. This field can accept multiple groups separated by commas.
Zone	Valid LSMS ruleset. Multiple rulesets can be separated by commas

Filter Name	Description
Source Host	Source IP Address or range. Multiple entries can be separated by commas.
Dest Host	Destination IP Address or range. Multiple entries can be separated by commas.
Protocol	Valid Protocol. Can be selected from TCP, UDP, ICMP , or enter a valid protocol number. Multiple entries can be separated by commas.
Source Port	Valid Source Port Number. Can enter valid entries between 0 and 65535. Multiple entries can be separated by commas.
Dest Port	Valid Destination Port Number. Can enter valid entries between 0 and 65535. Multiple entries can be separated by commas.
Source ID	Promon Log only. Source of Promon Log record. For Brick data, the source is Brick name.
Index Name	Promon Log only. Example: For port data, the index name is the port name.
Action	Valid Action. Can be Pass or Drop .
Direction	Valid direction. Can be IN or OUT .



Set the Help Facility

Overview

At the bottom of each Log Viewer is a **HELP** button that you can click to display Help about the Log Viewer. Depending on whether you are using Windows or Solaris, there are several actions you can perform to make the Help facility easier to use.

Windows

To make the Help facility easier to use in Solaris, do the following.

- *Solaris*

On Solaris only, in order for the Log Viewer Help files to be displayed without prompting for the absolute path of Netscape Communicator, set the *PATH* variable to the path where Netscape Communicator was installed (typically, this is */opt/netscape*).

For example, enter the following command at the command prompt or add it to a startup file (e.g., *.profile*):

```
PATH=/opt/netscape:$PATH; export PATH
```

This example assumes */opt/netscape* is the installation directory of Netscape Communicator. This may be different in your environment.



Find Text Function

Overview

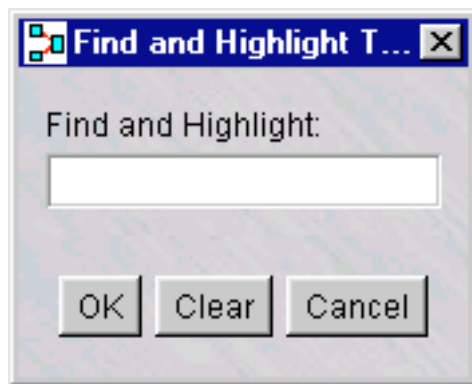
The Log Viewer provides a "find" function that enables you to search through log files and find and highlight all instances of a particular character string. You can use the find function to search for text in an existing log, or you can use it real-time, so that it highlights the text you want as the text is added to the log file.

To use the find function click this icon at the top of the window:



The find and highlight window will appear ([Figure 2-21, "Find and Highlight Window" \(p. 2-24\)](#)).

Figure 2-21 Find and Highlight Window



Enter the character string you want to find and click **OK**. To start a new search, click **Clear**, enter the new character string, and click **OK**.

□

3 Types of LSMS Logs

Administrative Events Log

Overview

The Administrative Events Log, often referred to as simply the Events Log, is the primary troubleshooting tool, providing detail on error messages as well as routing and VPN tunnel problems.

The Administrative Events Log contains log messages about administrative events (e.g., *Brick*[®] zone ruleset was loaded), Brick events (e.g., Brick was lost), error messages, and alarms that were triggered and delivered.

This log also contains informational messages, RealSecure events, and miscellaneous events not written to the other log files.

Administrative Events Logs are created and stored in `\log\adminevents` under the installation root directory.

Administrative Events Log Sample Record

The following is a sample record from an Administrative Events Log:

Figure 3-1 Administrative Events Log Sample Record

```
35:i:alarms:100941::3580:12747:Send a Console  
Message:Success:Console Message Successful in the action for  
administrator las030_admin
```

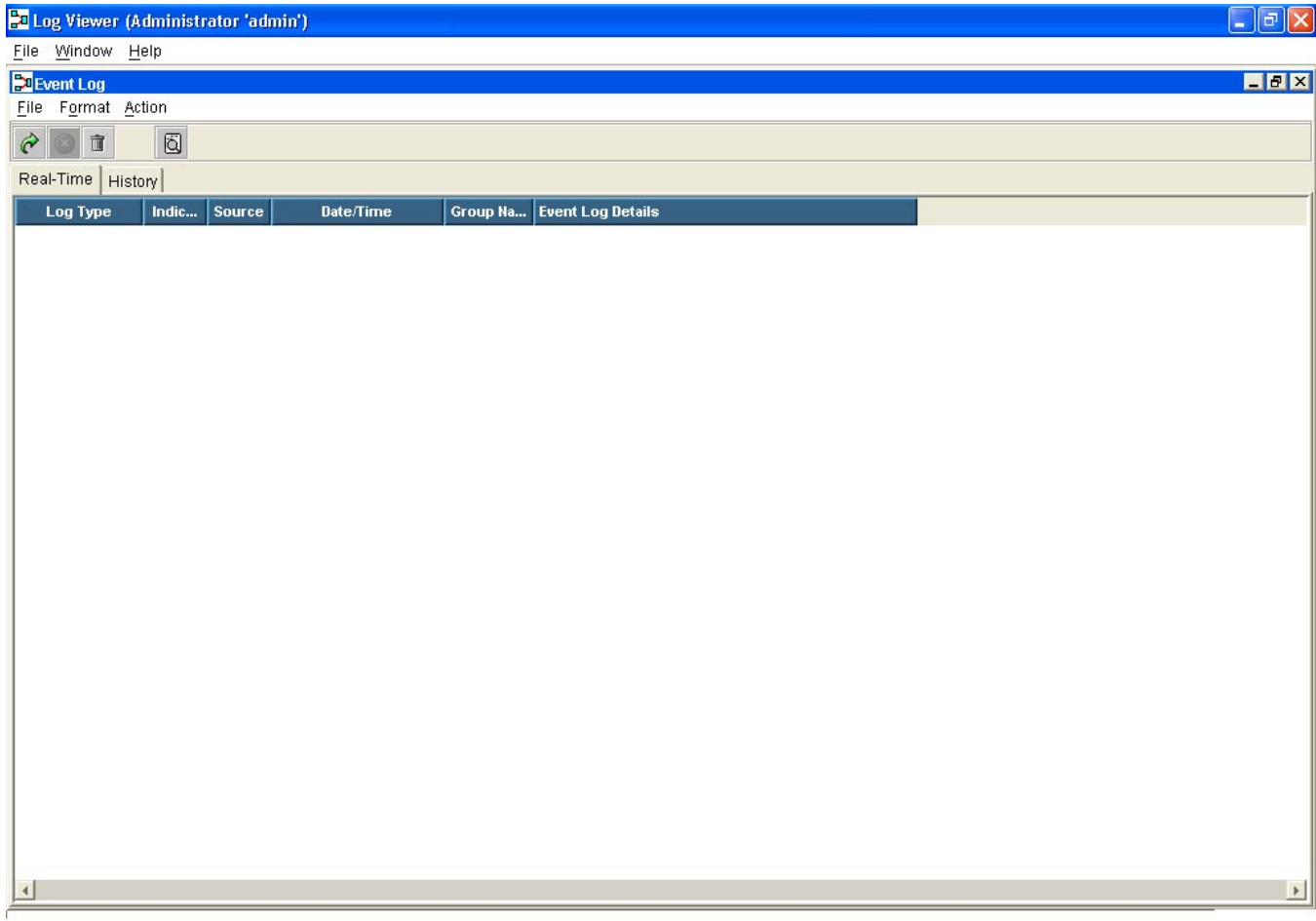
The example above shows a record that contains record type 35. Additional record types are written to this log, with each having its own format.

The record types and fields are comprehensively explained in the Help of the Administrative Events Log Viewer.

Administrative Events Log Viewer

Figure 3-2, “Administrative Events Log Viewer” (p. 3-2) shows a typical Administrative Events Log Viewer.

Figure 3-2 Administrative Events Log Viewer



Filtering Criteria

The only filtering criteria that can be applied to data in the Administrative Events Log is a text search. For example, you could enter:

- "SNMP Trap" to search for all sessions where alarms sent SNMP traps to a Network Management Station (NMS).
- "Lost" or "Contacted" for Brick connectivity.
- An error code.



Session Log

Overview

The Session Log contains Brick session records, which describe network activity through one or many Bricks. Session transactions through all Brick ports are recorded here. Session Log files are created and stored in `\log\sessions` under the installation root directory.

When a packet is passed or dropped by the Brick, the rule number that performs that action is recorded as part of the Session Log entry. This can be important information when troubleshooting.

Session Log Sample Record

The following is a sample record from a Session Log:

Figure 3-3 Session Log Sample Record

```
8:b:1b1_las030:133330-  
1:loadtest_group:las030_1b1_  
  1:OUT:125.92.10.30:125.92.21.50:6:1590:21:  
EXTERNAL:FORWARD:125.92.20.202:21ce:
```

Figure 3-3, “Session Log Sample Record” (p. 3-3) shows a record that begins with record type 8. Additional record types are written to this log, with each having its own format. The record types and fields are comprehensively explained in “Overview” (p. C-1), Appendix F, “Filterable Log Fields”, and Appendix G, “Log Field Syntax” in this manual, and in the Session Log Viewer online Help.

A field worth noting is the fourth field that contains the timestamp. The timestamp reflects both the LSMS timestamp and the source timestamp issued from a Brick.

The LSMS timestamp (e.g., 133330) adheres to a standard six-digit timestamp (hhmmss). The source timestamp is the difference between when the data was collected by the source (i.e., a Brick) and when the record was actually written to the log file (i.e., the LSMS timestamp).

For example, in Figure 3-3, “Session Log Sample Record” (p. 3-3), the fourth field is 133330-1, which means the record was written to the log at 1:33 PM and 30 seconds, and the event actually occurred at the Brick one second before.

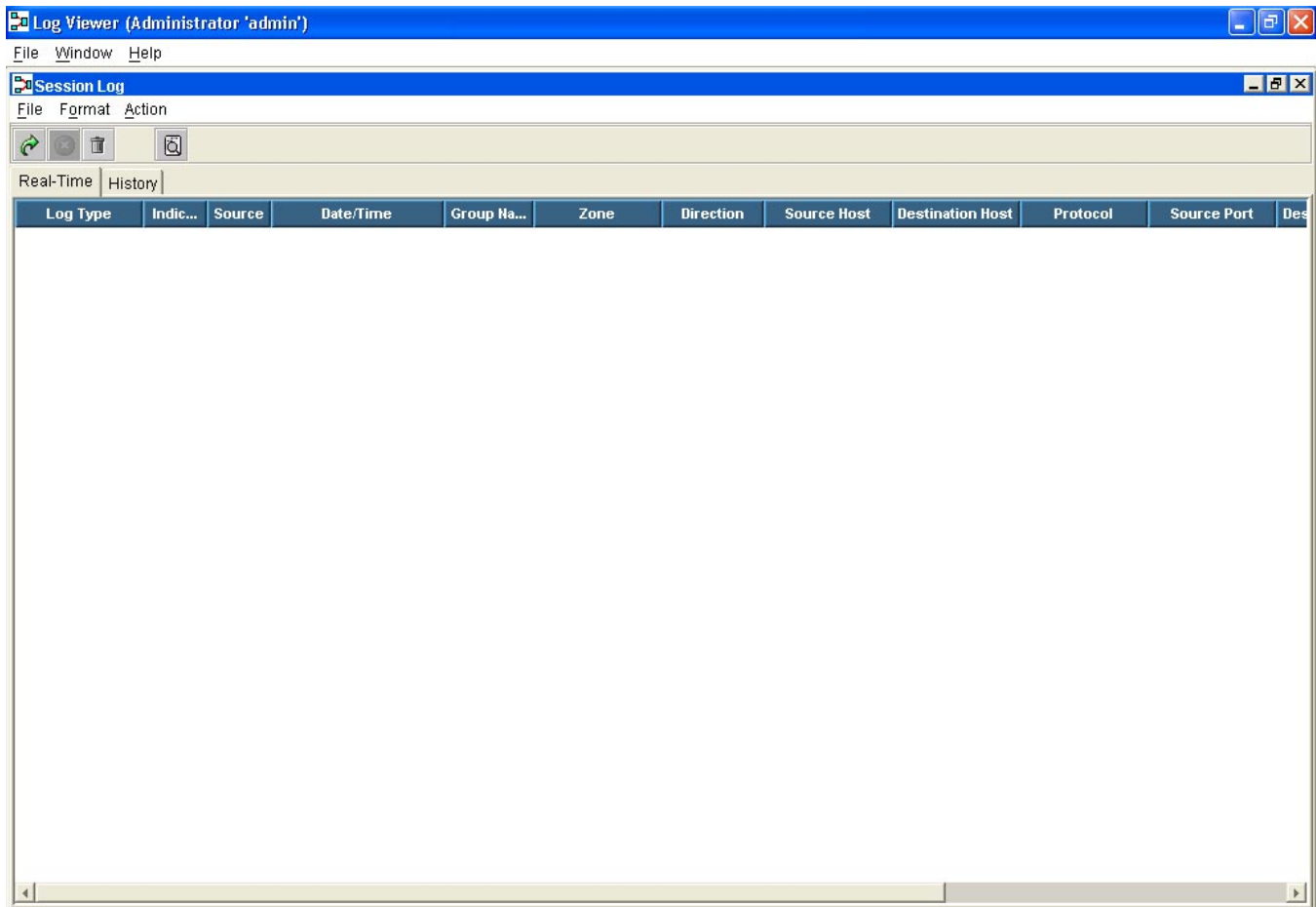
Other examples include where the LSMS timestamp is followed by a positive number, such as 133330+1 or an unusually large negative number, such as 133330-28. In these cases:

- A positive number may be indicative of a clock synchronization problem; the clock on the LSMS may not be synchronized with the clock on the Brick. Larger positive numbers (e.g., +2 or greater) may require attention (e.g., a reboot of the Brick, restart of services), where smaller numbers (e.g., +1) do not.
- A large negative number may indicate that a network interruption or failover occurred and the Brick could not communicate with the LSMS. The Brick will queue the message until communication is re-established and the message can be sent to the logger.

Session Log Viewer

Figure 3-4, “Session Log Viewer” (p. 3-4) shows a typical Session Log Viewer.

Figure 3-4 Session Log Viewer



Session Log Filtering Criteria

The table below explains the criteria you can employ to filter the Session Log before clicking **APPLY** and displaying data:

Field	Description
Source Type	Select one or more source types to include in the output. The source types are: Brick, LSMS Process, Proxy Server, and ISS Real Secure Engine.
Brick Name	Select one or more Bricks to include in the output. All Bricks that have been configured are displayed in the pulldown menu. You can manually type a Brick name as well. Commas are automatically inserted between entries. Non-selected Bricks will not be included in the output. Selecting * includes all Bricks.
Group Name	Select one or more groups to include in the output. All groups that have been configured are displayed in the pulldown menu.
Zone	Select one or more Brick zone rulesets to include in the output. All Brick zone rulesets that have been configured are displayed in the pulldown menu. You can manually type a Brick zone ruleset as well. Commas are automatically inserted between entries. Non-selected Brick zone rulesets will not be included in the output. Selecting * includes all Brick zone rulesets.
Source Host	Enter an IP address of the host that is sending the packets. If you accept the default (*), all source hosts will be included in the output.
Destination Host	Enter an IP address of the host that is receiving the packets. If you accept the default (*), all destination hosts will be included in the output.
Protocol	Select one or more protocols to include in the output. All protocols that are available are displayed in the pulldown menu. Commas are automatically inserted between entries. Non-selected protocols will not be included in the output. Selecting * includes all protocols.
Source Port	Enter a port number used by a source host. If you accept the default (*), all source ports will be included in the output.

Field	Description
Destination Port	Enter a port number used by a destination host. If you accept the default (*), all destination ports will be included in the output.
Bi-Directional IP	Enter an IP address that can be a source OR destination host. If you accept the default (*), then all IP addresses will be included in the output.
Action	Pass, Drop, or * for both actions.



Proactive Monitoring Log

Overview

The Proactive Monitoring Log (often referred to as the Promon log), contains log messages about monitored events for Bricks, the logger, VPN Gateway Controller (VGC), and the Firewall Authentication Controller (FAC).

Proactive Monitoring Logs are created and stored in `\log\promon` under the installation root directory.

Promon Log Sample Record

The following is a sample record from a Proactive Monitoring Log:

Figure 3-5 Proactive Monitoring Log Sample Record

```
53:i:logger:100114,  
0920041275::0:3:0:0957844777:30:5:ptrace:3970807:99999012:100000000
```

Log entries are recorded in the log file at 30 second intervals. The first five fields of the Proactive Monitoring Log comprise a standard header. It is as follows:

Field	Description
1	Record type The Proactive Monitoring Log only contains records of type 53.
2	Source type This is either <code>i</code> , which represents the LSMS or <code>b</code> , which represents a Brick.
3	Source identifier If source type is <code>i</code> , then this could be either the logger, FAC, or VGC. If the source type is <code>b</code> , this is the name of the Brick.

Field	Description
4	<p>LSMS timestamp</p> <p>Is in six-digit format (<i>hhmmss</i>) plus a 10-digit source timestamp. The source timestamp is the time the data was sampled, expressed as the total number of seconds that has lapsed since midnight Jan 1, 1970 GMT. The source timestamp is a unique identifier that can be used to collect all samples that occurred within a particular <i>snapshot</i> of data.</p> <p>For example, in Figure 3-5, “Proactive Monitoring Log Sample Record” (p. 3-7), the fourth field is 100114,0920041275. The first timestamp reveals that the logger received and processed the record at 10:01 AM and 14 seconds. The second timestamp is the source timestamp which reveals that the data was collected 0920041275 seconds since midnight Jan 1, 1970 GMT.</p>
5	Blank

The above standard header is followed by an additional Proactive Monitoring specific header, which is comprised of fields six through twelve. They are:

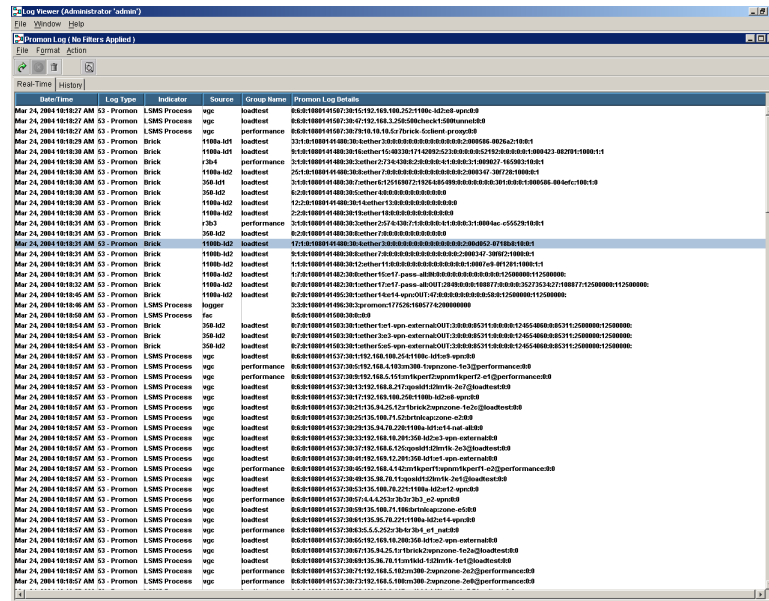
Field	Description
6	<p>Record number</p> <p>This is the record number for the source identifier.</p>
7	<p>Subtype</p> <p>This is one of the six subtypes as described in “Overview” (p. C-1). The subtype that is recorded in this field governs the type of information that is recorded in the fields that follow the Proactive Monitoring header.</p>
8	Always 0. This is the version number.
9	Time in seconds, but is offset from Field 4 by 30 seconds.
10	<p>Collection period</p> <p>This is always 30 seconds.</p>
11	<p>Index number</p> <p>Index number of the source identifier.</p>
12	<p>Index name</p> <p>If the subtype is Brick interface (generic) or (Ethernet), then the index name can be ether0 through ether10.</p> <p>If the subtype is LSMS Auditing, then the index name can be sessions, adminevents, promon, userauth, or ptrace.</p> <p>If the subtype is Brick, Authentication, or Local Map Pool, then an index name is not relevant.</p>

The record types and fields are comprehensively explained in “Overview” (p. C-1) and “Overview” (p. C-1) and in the Help of the Proactive Monitoring Log Viewer.

Proactive Monitoring Log Viewer

Figure 3-6, “Proactive Monitoring Log Viewer” (p. 3-9) shows a typical Proactive Monitoring Log Viewer.

Figure 3-6 Proactive Monitoring Log Viewer



Filtering Criteria

The table below explains the criteria you can employ to filter the Proactive Monitoring Log before clicking **APPLY** and displaying data. See “[Overview](#)” (p. C-1), and “[Overview](#)” (p. C-1) for a detailed listing of all fields.

Field	Description
Sub Type	<p>Select one of the following subtypes:</p> <p>Brick—the session traffic that transpires through all Brick ports. Use when source type=b.</p> <p>Brick interface (Generic)—data for each line coming into a Brick (e.g., packets, bytes, etc.). Source type must equal b or not be specified.</p> <p>Brick interface (Ethernet)—data on collision errors, MAC errors, framing errors, etc. Source type must equal b or not be specified.</p> <p>LSMS Auditing—status of the logger subsystem and how the log is being managed. Source must equal i or not be specified.</p> <p>Authentication (VPN Client)—VPN Gateway Controller (VGC) data, SA negotiations, IKE negotiations. Source must equal i or not be specified.</p> <p>Authentication (Firewall)—data on total authentication requests. Source must equal i or not be specified.</p> <p>Local Map Pool—a pool of free IP addresses that are used for mapping VPN end users to local addresses. Source must equal i or not be specified.</p>
Source Type	<p>Enter a letter that indicates the component that originated the record.</p> <p>i=LSMS</p> <p>b=Brick</p>
Source-ID	<p>If source type is b, then the name of a Brick can be entered.</p> <p>If source type is i, then FAC, logger, VGC, or blank can be entered.</p>
Index Name	<p>If the subtype is Brick interface (generic) or (Ethernet), then the index name can be ether0 through ether10.</p> <p>If the subtype is LSMS Auditing, then the index name can be sessions, adminevents, promon, userauth, or ptrace.</p> <p>If the subtype is Brick, Authentication, or Local Map Pool, then an index name is not relevant.</p>



User Authentication Log

Overview

The User Authentication Log contains log messages that record successful or unsuccessful authentication requests for VPN or firewall users. Login and logout messages for LSMS Administrators and Group Administrators are recorded in the Administrative Events Log.

User Authentication Logs are created and stored in `\log\userauth` under the installation root directory.

User Authentication Log Sample Record

The following is a sample record from a User Authentication Log:

Figure 3-7 User Authentication Log Sample Record

```
6:i:vgc:082730::las030_1b2_  
3:875cle82:875clecd:17:1117:500:client1::1:Eit  
her Group or User does not exist.:I:1:LVC3.0.327:NT
```

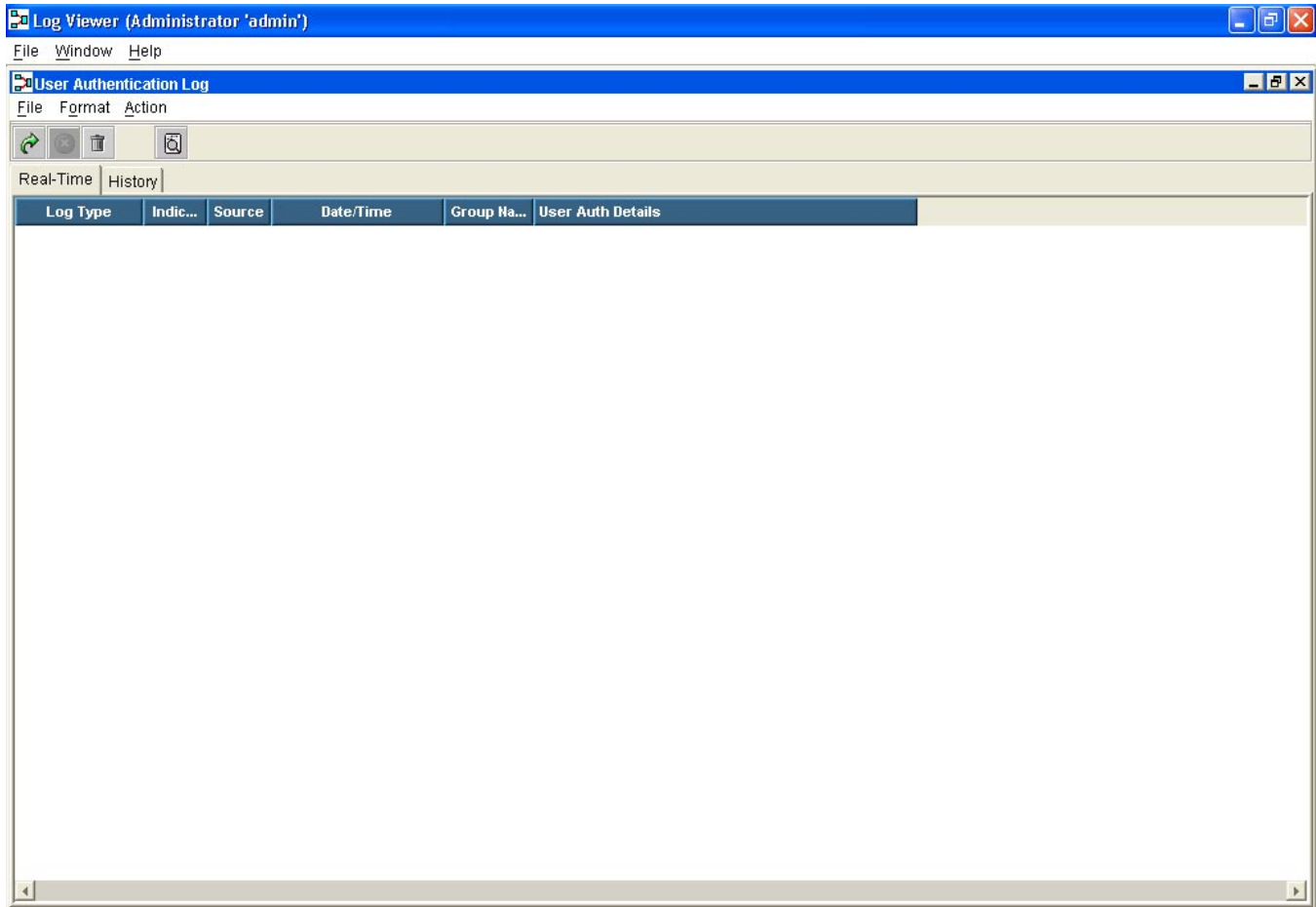
The User Authentication Log only contains records of type 6.

The record types and fields are comprehensively explained in the Help of the User Authentication Log Viewer.

User Authentication Log Viewer

Figure 3-8, “User Authentication Log Viewer” (p. 3-12) shows a typical User Authentication Log Viewer.

Figure 3-8 User Authentication Log Viewer



Filtering Criteria

The only filtering criteria that can be applied to data in the User Authentication Log is a text search. For example, you could enter a user ID. All entries are case-insensitive.



4 Introduction to Alarms

Overview

Purpose

This chapter explains how to create alarm triggers and actions to notify Administrators of events occurring in the system. Administrators configure alarm triggers and assign actions to the trigger.

The LSMS software provides preconfigured alarm triggers to notify administrators when a *Brick*[®] has been lost, when a LAN-to-LAN tunnel fails, and when unauthorized LSMS login attempts are made. You can also create your own alarm triggers and associate them with appropriate actions to facilitate monitoring system events of interest to you.

Alarm triggers and actions are configured on a per-Administrator basis and are not shared among Administrators. Therefore, when an LSMS Administrator or Group Administrator logs onto the LSMS, they can only view the alarm triggers and actions that they have configured themselves. Any alarms created by an LSMS Administrator or Group Administrator will apply to all groups that the administrator has rights to.

LSMSs and Compute Servers (LSCSs) handle alarms in an identical manner, except that the Console Message Action on Compute Servers forward the action contents up to associated LSMS in the cluster. The LSM forwards the console alarm to the appropriate destination. Other actions, like email and syslog, are directly performed by the Compute Server.

Therefore, this chapter applies to both LSMSs and Compute Servers. Any difference is identified.

Contents

What are Events, Alarm Triggers and Actions?	4-3
Console Alarms Window	4-7

Using the Wizard	4-9
------------------	-----



What are Events, Alarm Triggers and Actions?

Overview

The following explains an event, an alarm trigger, and an action:

- *Event*
An *event* refers to an incident that occurs in the system that is deemed significant or suspicious enough to warrant the attention of an Administrator. For example, an Administrator would want notification of unauthorized connection attempts, of lost Bricks, or of an excessive number of sessions attempting to connect to a particular machine. Any of these events, and others, can be associated with an alarm trigger
- *Alarm Trigger*
An *alarm trigger* is an Administrator-defined set of conditions for an event and is associated with an action. The alarm subsystem monitors the log files in real time, and when a log entry matches the conditions of an alarm trigger, an alarm is generated and the associated action is taken.
- *Alarm Action*
An *alarm action* is associated with an alarm trigger and defines how an Administrator is notified when an alarm is generated. An Administrator can be notified of an event via e-mail, a direct page, a syslog message, an SNMP trap sent to a network management system, or an alarm displayed in the Console Alarms window of the Status Monitor.

Alarm Trigger Types

Examples of alarm triggers that can be configured so that notification is sent to an Administrator include:

Alarm Trigger Type	Description
Alarm Code	A number that can be embedded in a rule so that when the rule is invoked a specified number of times within a given time frame, an Administrator is notified.
Brick Error	A trigger that scans for errors generated by a Brick. The error code entered needs to be between 1 and 299 and represents an event.
Brick Failover Event	A trigger that detects when one member of a Brick failover pair transitions from "Standby" to "Active."
Brick Port Lost	A trigger that detects connectivity problem events (e.g., a malfunctioning NIC card).

Alarm Trigger Type	Description
Brick Lost	A trigger that detects communication error events between a specified Brick and the LSMS.
Brick Proactive Monitoring	A trigger that looks for events such as high average cache memory usage, excessive number of packets dropped or passed, so that if the health of the network is deemed questionable, an Administrator is notified.
LSMS Error	A trigger that scans for errors generated by the LSMS. The error code entered needs to be between 0000 and 7999 and represents events such as socket problems, LSMS failover, logger cannot write to a file, etc.
LSMS Proactive Monitoring	A trigger that looks for events such as log rollover rate, disk space usage, so that if the health of the network is deemed questionable, an Administrator is notified.
Local Presence Map Pool	A trigger that detects if the pool of free IP addresses, which are used for mapping VPN users to local addresses, is below or equals a specified percentage.
Unauthorized LSMS Login Attempt	A trigger that detects if an unauthorized attempt has been made to log on to the LSMS.
User Authentication	A trigger that detects if an unauthorized user has attempted to log on to the LSMS.
Brick ICM Alarm	A trigger that detects <i>Brick</i> [®] ICM alarms.
LSMS Status Change	A trigger that detects a status change in an LSMS.
LAN to LAN Tunnel Lost	A trigger that detects when a LAN-to-LAN tunnel is down.
LAN to LAN Tunnel Up	A trigger that detects when a LAN-to-LAN tunnel has been brought back up.
Local Presence Map Pool	A trigger that looks for local server information.
QoS Rule Bandwidth Exceeded	A trigger that detects when a QoS bandwidth threshold setting has been exceeded.
QoS Rule Bandwidth Throttling Alarm	A trigger that detects that alarms generated by a QoS bandwidth setting have been throttled.
QoS Zone Bandwidth Guarantees Alarm	A trigger that detects that a QoS bandwidth guarantees alarm has been generated.

Alarm Trigger Type	Description
QoS Zone Bandwidth Throttling Alarm	A trigger that detects that a QoS bandwidth throttling alarm has been generated.
VPN Proactive Monitoring	A trigger that detects if a VPN Promon alarm has been generated.

Each of the alarm trigger types listed in the table is described in detail in [Chapter 6, “Configuring Alarm Triggers”](#).

Action Types

When an event has been detected and the conditions of an alarm trigger configured to look for this event are true, the actions that have been associated with the alarm trigger will be taken.

Actions that can be associated with alarm triggers include:

- Console Message (pre-configured)
- Direct Page
- E-mail Message
- SNMP Trap
- Syslog Message

An alarm trigger can be associated with one or more actions.

Preconfigured Alarm Triggers and Actions

The LSMS comes with three preconfigured alarm triggers and the Console Message action. The triggers are enabled initially but can be disabled at any time.

PreConfigured Trigger/Action	Description
Lost a Brick(Trigger)	A trigger that sends an alarm message to the Console Alarms window of the Status Monitor. Detects when the LSMS has lost contact with any Brick of any group for at least 30 seconds. Notification is also sent when connectivity is re-established.
Lost a LAN to LAN Tunnel(Trigger)	A trigger that sends an alarm message to the Console Alarms window of the Status Monitor.

PreConfigured Trigger/Action	Description
Unauthorized LSMS Login Attempts(Trigger)	A trigger that sends an alarm message to the Console Alarms window of the Status Monitor. An alarm is generated when six attempts have been made within 30 seconds to log on to the LSMS.
Send a Console Message(Action)	An action that sends an alarm message (as defined in the associated trigger) to the Console Alarms window of the Status Monitor.



Console Alarms Window

Overview

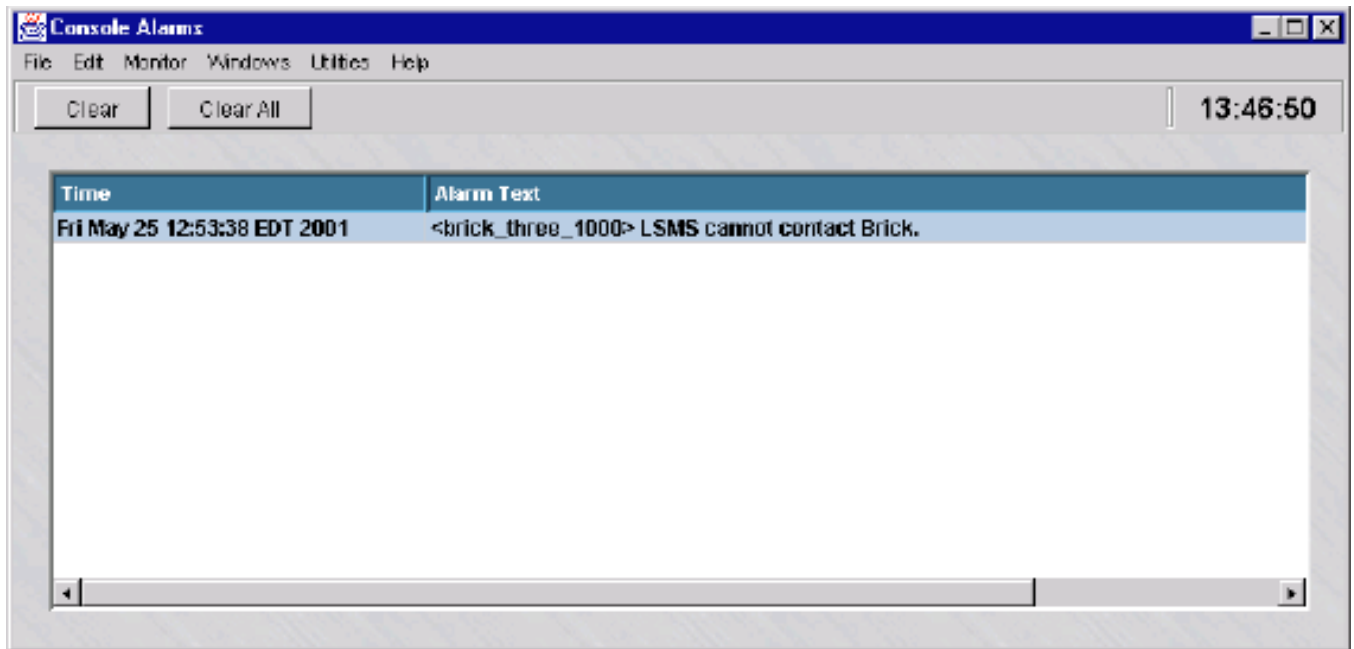
When an alarm trigger is associated with a Console Message action and the conditions of the trigger are met, an animated bell icon appears at the top of the Navigator Window, as [Figure 4-1, “Alarm Bell Icon”](#) (p. 4-7) illustrates. You must have the Navigator running to be notified of alarms by this means.

Figure 4-1 Alarm Bell Icon



To provide further details on the alarm, click the bell icon to display the Console Alarms window as shown [Figure 4-2, “Console Alarms window”](#) (p. 4-7).

Figure 4-2 Console Alarms window



The Console Alarms window can also be accessed by selecting **Console Alarms** from the **Monitor** menu on the LSMS menu bar.

The Console Alarms window can display up to 50 alarm messages. The top-most message is the most recent.

Once the problem has been rectified, you can remove the alarm message from the Console Alarms window by first highlighting the alarm and clicking the **Clear** button. To clear all messages, click the **Clear All** button.



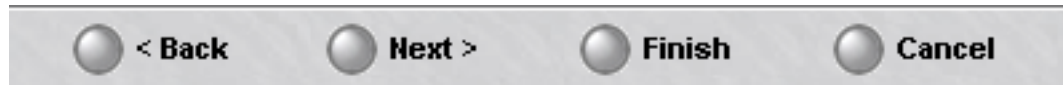
Using the Wizard

Overview

When using either the Alarm Trigger Editor or Alarm Action Wizard to define an action or alarm trigger, click the appropriate buttons at the bottom of each wizard screen after entering the information requested.

These buttons are shown in Wizard Buttons [Figure 4-3, “Wizard Buttons”](#) (p. 4-9).

Figure 4-3 Wizard Buttons



Syntax Checking

Some fields in the Alarm Trigger and Alarm Action Wizards automatically validate the parameters you enter.

When you enter invalid parameters, the characters you entered turn red. For example, if you entered an invalid IP address, in which one of the numbers was greater than 255, the address would be displayed in red.

When you correct the problem by entering a valid parameter, the color of the text returns to black.



5 Configuring Alarm Actions

Overview

Purpose

When a trigger detects an event, the action(s) that have been associated with it are taken. If a trigger needs to be associated with an action other than the preconfigured Console Message, the action needs to be configured first.

Contents

Configure a New Alarm Action	5-2
Configuring the Direct Page Action	5-5
Configuring the E-mail Action	5-9
Configuring the SNMP Trap Action	5-12
Configuring the Syslog Action	5-14
Maintaining Actions	5-18



Configure a New Alarm Action

Overview

Important! A Compute Server forwards a Console Action Message to the associated LSMS for display and processing as an administrator is not expected to log into the Compute Server.

To configure an action:

- 1 To define a new action, double-click the Alarms folder in the LSMS Navigator Folder Panel.

Figure 5-1 LSMS Navigator Folder Panel

- 2 Right-click the Actions folder and select **New Action**. The Alarm Action Wizard appears.

Figure 5-2 Alarm Action Wizard

Alarm Action Wizard-7

Please select the Action Name, Type and Description.

Lucent Technologies
Bell Labs Innovations

Select Action

Action Name

Action Type

Description

< Back Next > Finish Cancel

- 3 Enter a name for the action in the **Action Name** field. This is a required field and is displayed in the list of actions in the Contents Panel. Be as descriptive as possible. Spaces are allowed, but special characters (for example, @) are not.

-
- 4 Select an **action type** from the Action Type drop-down list. The sections that follow explain each action type.

Figure 5-3 Action Wizard Action Type Drop-down List



-
- 5 Optionally, enter a description for the action in the **Description** field. If a description is entered, it is displayed in the list of actions in the Contents Panel.
-
- 6 Select **Next** to display the next page of the wizard and enter parameters for the action type you selected. The parameters are explained below.
-
- 7 To save the action, select **Finish** in the last page of the wizard.

END OF STEPS

.....



Configuring the Direct Page Action

Overview

The Direct Page action sends a direct page to the specified recipients. The message is sent via a PSTN/modem-based connection that is made to a wireless pager service provider.

Important! Sending a direct page should be reserved for events of the utmost priority.

Pages sent via a modem could create modem bottlenecks which may take approximately 10 seconds to complete the sending of each message.

Direct pages are transmitted even in the event of a network outage. This differs from pages that are sent via an e-mail-based paging action.

In order to support sending a direct page, the alphanumeric paging service used must support TAP (Telocator Alphanumeric Protocol v1.8). The LSMS supports three paging providers that use TAP: SkyTel, *PageNet*[®], and MetroCall.

If more than one direct page message is sent, it will be placed on a queue. The Direct Page action will queue messages with all pertinent information collected at *the time the action was fired*. The messages are then sent out sequentially.

Before configuring a Direct Page action, ensure that a modem is set up correctly and operational on the LSMS. Also, use Configuration Assistant to set modem settings (for example, *Modem Port*, *Initialization String*, *Dial String*) in the Direct Paging parameter group. Refer to Chapter 10. Using the configuration Assistant in the *LSMS Administration Guide* for details.

Overview

To configure a Direct Page action:

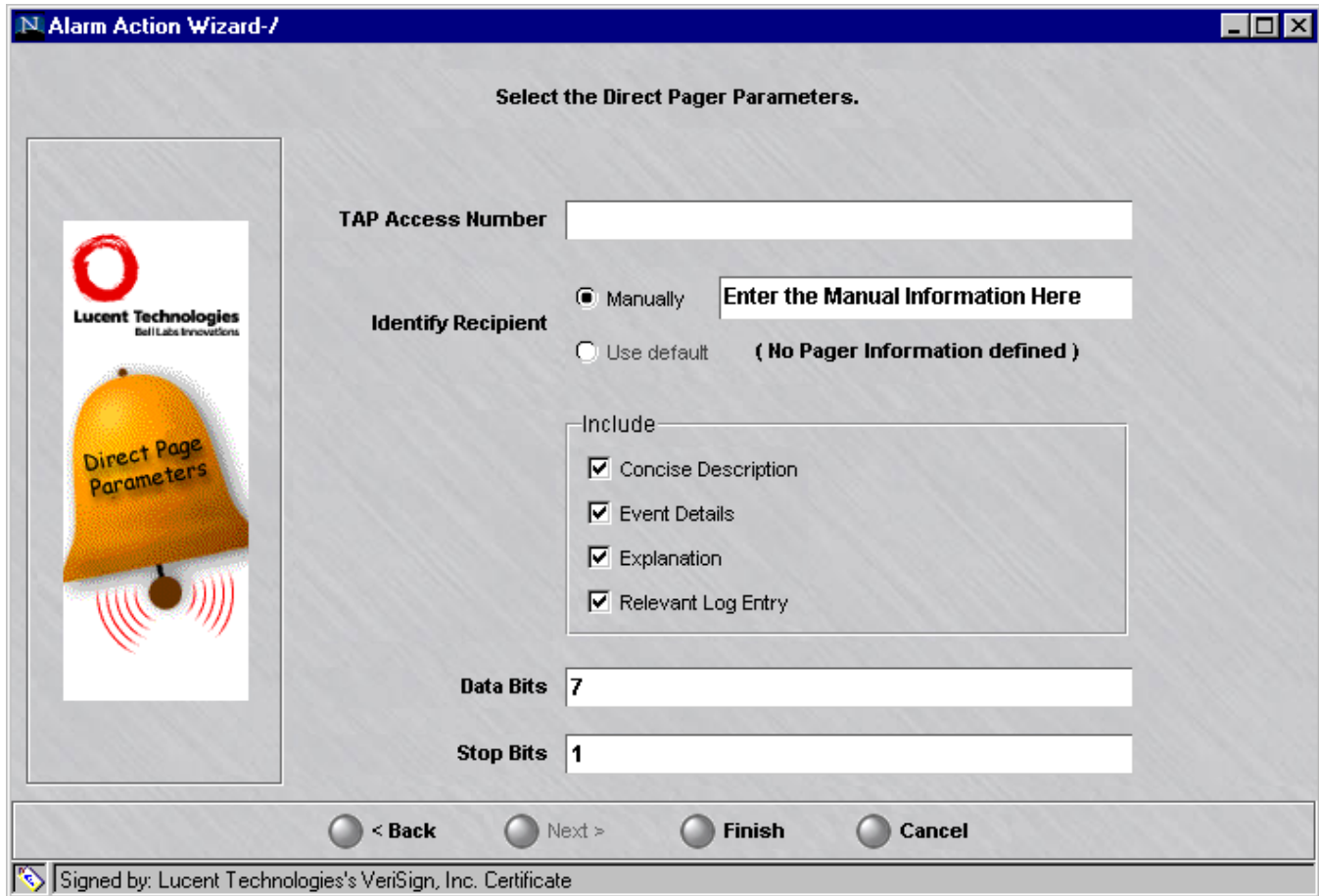
- 1 Enter an Action Name, select Direct Page from the Action Type drop-down list, then enter an optional Description.
- 2 Click **Next**.
- 3 In the next page of the wizard, shown in [Figure 5-4, “Direct Page Action”](#) (p. 5-6), enter a TAP Access Number.

The TAP Access Number is the access number that the modem dials to connect to the TAP server. Allowable characters are 0 - 9, *, #, commas, and spaces. A maximum of

20 characters can be entered. If you are using the SkyTel paging service, you can use 1.800.679.2778 as the number.

To obtain a SkyTel TAP access number for your area, you can call SkyTel at 1.800.759.8737 and choose option 5#.

Figure 5-4 Direct Page Action



-
- 4 Select one of the Identify Recipient radio buttons to specify to whom the message should be sent:
- *Manually*
Enter the PIN that is transmitted to the TAP server which uniquely identifies the recipient (e.g.,1234567).
 - *Use Default*
If your Administrator account includes a pager number in the Pager Info field, it will be displayed here.
See Chapter 8. Creating Groups and Administrators in the *LSMS Administration Guide* for details. The **Pager Info** field is dynamically linked so that when the action is fired, the most current information is used.

Important! If an account is selected but later deleted, an error message is logged when the alarm is fired and another valid account must be re-entered.

- 5 Check or uncheck one or more fields to define the contents of the page message. The following table explains.

Include Field	Description
Concise Description	The text that is entered in the Concise Description field when the trigger is configured.
Event Details	Event Details may include IP addresses, <i>Brick names</i> [®] , timestamp for the alarm.
Explanation	The text that is entered in the Explanation field when the trigger is configured.
Relevant Log Entry	The most recent log record when the alarm is generated.

It is recommended that you choose only Concise Description to accommodate pagers that accept only 240 alphanumeric characters. Otherwise, text may be truncated.

- 6 Enter the modem's data bits and stop bits. Default is 7 and 1 respectively.
- If problems are encountered with Direct Page, an Alarms Logged Report can be generated and searched for Direct Page actions with a status of "Failure". This report can be memorized and run periodically to detect transmission problems.

See [Chapter 12, “Alarms Logged Report”](#) for more information.

END OF STEPS



Configuring the E-mail Action

Overview

This action sends an e-mail message to the specified recipients. If your paging service provides the support, a page number can be linked to your e-mail address so that you also receive a page.

Before configuring the e-mail action, use the Configuration Assistant to set the SMTP Host Name and Account Name in the Alarms parameter group. Refer to Chapter 10. Using the Configuration Assistant in the *LSMS Administration Guide* for details.

Important! For some kinds of alarms, for example, **Brick Lost** due to a network outage, not all e-mail alarms may be able to reach the mail server.

Overview

To configure an e-mail action:

-
- 1 Enter an Action Name, select E-mail from the **Action Type** drop-down list, then enter an optional Description.
-
- 2 Click **Next**.

In the next page of the wizard, [Figure 5-5, “E-mail Action” \(p. 5-10\)](#), select one of the **Addresses** radio

Figure 5-5 E-mail Action

buttons:

- *Manually*
Enter one or more e-mail address (for example, john@mycompany.com) here. To specify more than one address, delimit them with commas.
- *Use Default*
If your Administrator account includes an e-mail address, it is displayed here. See Chapter 8. Creating Groups and Administrators in the *LSMS Administration Guide* for details. The **E-mail Address** field is dynamically linked so that when the action is fired, the most current information is used.

Important! If an account is selected but later deleted, an error message is logged when the alarm is fired and a valid account must be entered.

-
- 3** Define a subject header for the e-mail or page message by either:
- Leaving the checkbox unchecked so that a subject header will be generated automatically. The header will contain the Concise Description that is specified when the trigger is configured. This is the default.
 - Checking the **Subject** checkbox and manually entering your own subject header to have sent with an e-mail or page message.

Important! If your paging service supports linking your e-mail address with a page number, it is recommended to accept the default to accommodate pagers that accept only 240 alphanumeric characters. Otherwise, text may be truncated. This varies according to the paging service you are using.

END OF STEPS



Configuring the SNMP Trap Action

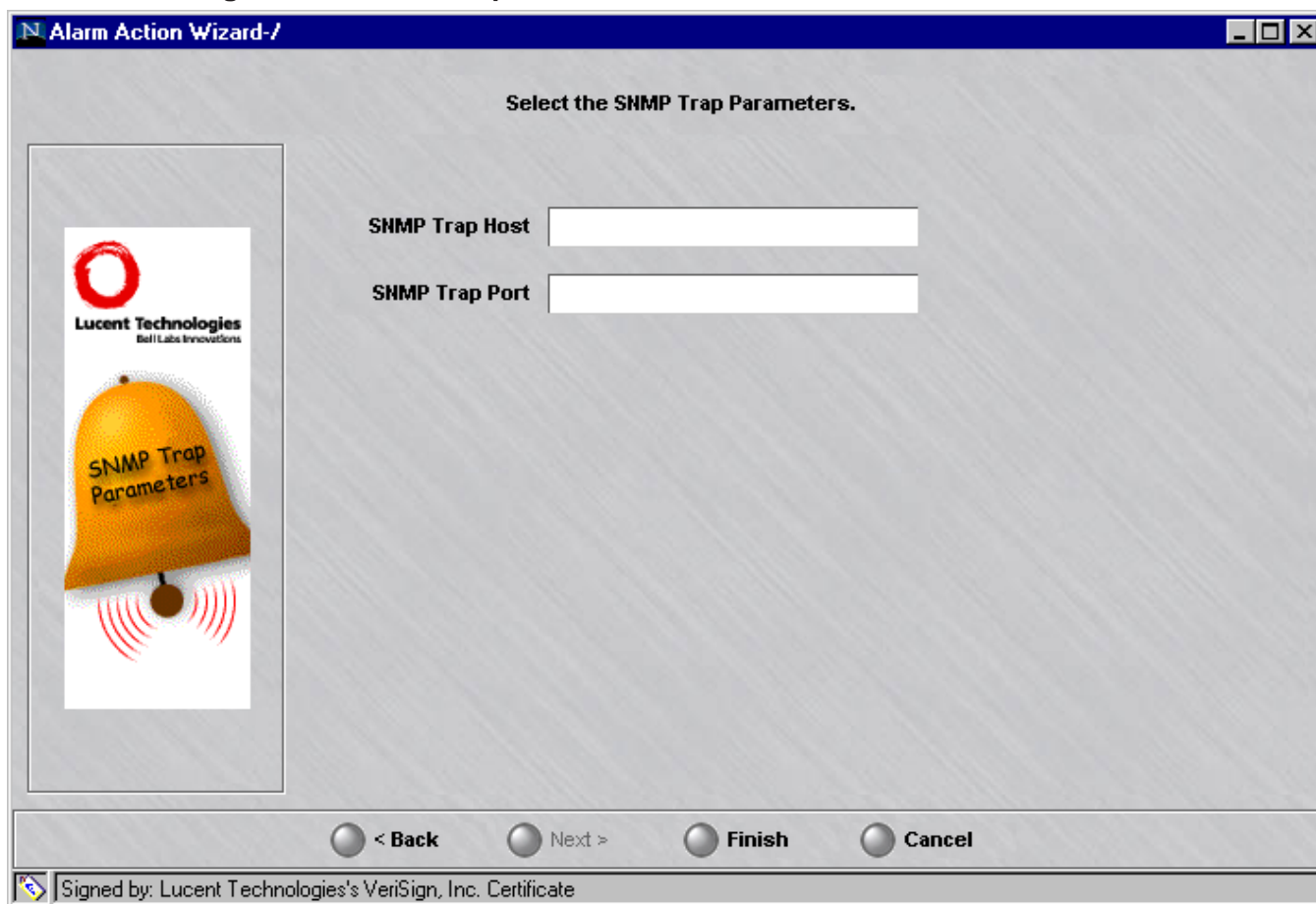
Overview

When an event is detected and an alarm is generated, the LSMS can forward Simple Network Management Protocol (SNMP) traps to a Network Management Station (NMS). SNMP traps allow an NMS Administrator to monitor Bricks, the LSMS itself, and network elements protected by a Brick.

To configure an SNMP Trap action:

- 1 Enter an Action Name, select SNMP Trap from the **Action Type** drop-down list, then enter an optional Description.
- 2 Click **Next**.

Figure 5-6 SNMP Trap Action



-
- 3** In the next page of the wizard, shown in [Figure 5-6, “SNMP Trap Action”](#) (p. 5-12), enter the IP address of the NMS in the **SNMP Trap Host** field.

In the **SNMP Trap Port** field, enter the UDP port that is used to send the SNMP trap to the NMS. Ports 1 - 65,535 can be entered. Default is 162.

Important! Defining an SNMP Trap action is only one step of the overall procedure for sending SNMP traps to an NMS.

Management Information Bases (MIBs) need to be installed and loaded on the NMS and rules may be required. Refer to [“Overview”](#) (p. A-1) for details.

END OF STEPS



Configuring the Syslog Action

Overview

This action sends a UDP packet to a UNIX syslog server. The syslog process provides a centralized reporting mechanism to consolidate error messages within a UNIX system.

Standard implementations of this mechanism provide a daemon (`syslogd`), which monitors a UDP socket to accept and log syslog entries from remote systems on port 514.

The message sent to syslog is a single line that contains the following fields:

<priValue>timestamp sms: SEVERITY = severity

^ITRIGGERTIME = triggerTime

^ICONCISE = concise

^IDetails = details

^IEXPLANATION = explanation

^ILOGENTRY = logEntry

Where:

^ represents a tab

priValue = the severity + 8 (this makes the message a "user" message)

triggerTime = time alarm was triggered

severity = numeric value based on the "Severity" field in the *syslog* alarm action:

0 - Emergency

1 - Alert

2 - Critical

3 - Error

4 - Warning

5 - Notice

6 - Informational

7 - Debug

The remaining fields are only displayed if the corresponding box is checked when configuring the syslog alarm action:

concise = concise description field from alarm trigger configuration

details = colon separated list of alarm trigger detail fields. Refer to [“Overview” \(p. C-1\)](#) for a description of these fields. They are different for each alarm time/subtype.

explanation = explanation field from alarm trigger configuration

logEntry = colon separated logEntry for the alarm (the format is described in [“Overview” \(p. C-1\)](#)).

The following is a sample *syslog* that shows a *Brick*® LOST, *Brick*® CONTACTED, and Unauthorized LSMS Login Attempt:

```
Dec 20 03:29:17 [10.1.1.24.12.80] Jan 9 13:55:00 sms: SEVERITY = 1
^ITRIGGERTIME = Fri Jan 09 13:53:58 EST 2004^ICONCISE =
<ibm_laptop> LSMS cannot contact Brick.^IDetails =
2:ibm_laptop::Brick Lost:Lost a Brick::syslog:Brick ibm_laptop^IEX-
PLANATION = The LSMS has lost communications with the Brick^ILOGEN-
TRY = 24:i:logger:135358:system:ibm_laptop:LOST:135.92.38.251
Dec 20 03:29:33 [10.1.1.24.12.81] Jan 9 13:55:21 sms: SEVERITY =
1^ITRIGGERTIME = Fri Jan 09 13:54:19 EST 2004^ICONCISE =
<ibm_laptop> LSMS has contacted Brick again.^IDetails =
3:ibm_laptop::Brick Lost:Lost a Brick::syslog:Brick ibm_laptop^IEX-
PLANATION = LSMS has re-established
communications with the Brick.^ILOENTRY = 24:i:logger:135419:sys-
tem:ibm_laptop:CONTACTED:135.92.38.251
Dec 20 03:38:54 [10.1.1.24.12.88] Jan 9 14:04:42 sms: SEVERITY =
0^ITRIGGERTIME = Fri Jan 09 14:03:40 EST 2004^ICONCISE = Unautho-
rized LSMS login Attempt - IP address 10.1.1.24^IDetails =
4:Unautho-
rized LSMS Login Attempt:Unauthorized Login
Attempts:syslog:Source 10.1.1.24, user
shsdas, reason Failed Login Attempt - Either Group or User does
not exist.^IEXPLANATION = Unauthorized user attempted to login to
LSMS and failed authentication.^ILOENTRY = 34:i:rap:140340::shsd-
das:10.1.1.24:Failed Login Attempt - Either Group or User does not
exist.
```

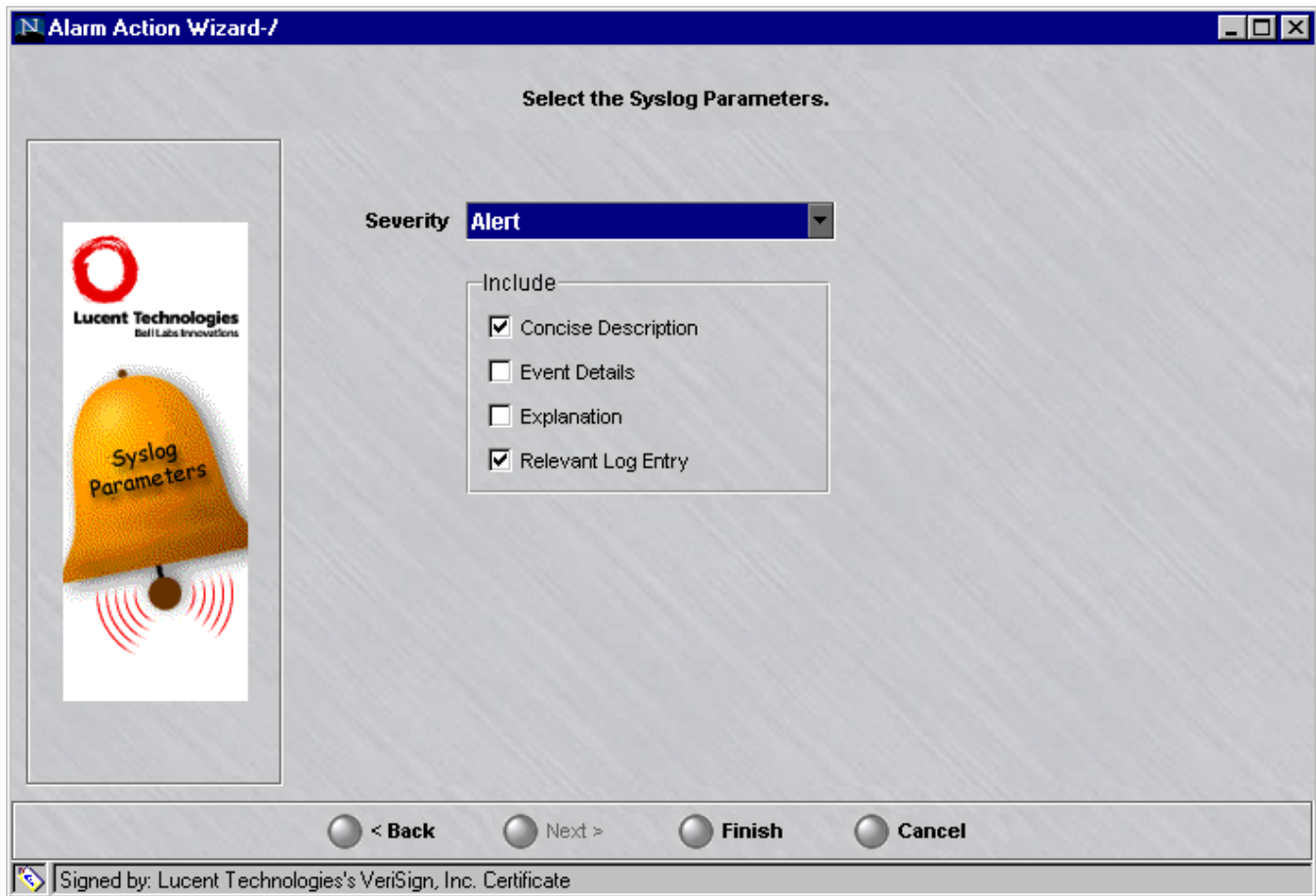
Before configuring the Syslog action, use Configuration Assistant to set the Syslog Host Name and Syslog Port in the Alarms parameter group. Refer to Chapter 10. Using the Configuration Assistant in the *LSMS Administration Guide* for details.

Overview

To configure a Syslog action:

- 1 Enter an Action Name, select Syslog from the **Action Type** drop-down list, then enter an optional Description.
- 2 Click **Next**.

Figure 5-7 Syslog Action



- 3 In the next page of the wizard, shown in [Figure 5-7, “Syslog Action” \(p. 5-16\)](#), select a Severity for the syslog message from the drop-down list. Choices are:

Severity	Description
Emergency	A panic condition that is normally broadcast to all users.

Severity	Description
Alert	Default. A condition that should be corrected immediately (e.g., a corrupted database).
Critical	Critical conditions, such as hard device errors.
Error	Messages that indicate error conditions.
Warning	Messages that indicate warning conditions.
Notice	Conditions that are not error conditions, but that may require special handling.
Informational	Purely informational in nature.
Debug	Messages that contain information normally of use only when debugging a program.

-
- 4 Check or uncheck one or more fields to define the contents of the syslog message. The following table explains.

Include Field	Description
Concise Description	The text that is entered in the Concise Description field when the trigger is configured.
Event Details	Event Details may include IP addresses, Brick names, timestamp for the alarm.
Explanation	The text that is entered in the Explanation field when the trigger is configured.
Relevant Log Entry	The most recent log record when the alarm is generated.

.....

END OF STEPS



Maintaining Actions

Duplicating Actions

To duplicate an action:

- 1 Right-click an action in the Contents Panel.

- 2 Select **Duplicate** from the pop-up menu. The Alarm Action Wizard appears.

- 3 Enter a unique name for the action and change any of the other action parameters if desired.

- 4 To save the action, select **Finish**.

END OF STEPS

Editing Actions

To edit an action:

- 1 Double-click an action in the Contents Panel. The Alarm Action Wizard appears.

- 2 Make the appropriate changes to the fields.

- 3 To save the action, select **Finish**.

END OF STEPS

Removing Actions

To remove an action:

- 1 Right-click an action in the Contents Panel.

- 2 Select **Delete** from the pop-up menu.

-
- 3 Select **Yes** in the pop-up window to confirm the deletion.

END OF STEPS



6 Configuring Alarm Triggers

Overview

Purpose

Configuring a trigger causes the LSMS to scan for the set of conditions defined in the trigger. When the event is detected, the action associated with the trigger is taken, and an alarm is generated.

If the trigger to be configured includes an action that has not yet been configured, see [“Overview” \(p. 7-1\)](#) to configure it first.

Contents

Configuring Triggers	6-3
Alarm Code Trigger	6-7
<i>Brick</i> [®] Error Trigger	6-11
Brick Failover Event Trigger	6-14
<i>Brick</i> [®] ICM Trigger	6-17
<i>Brick</i> [®] Interface Lost Trigger	6-18
<i>Brick</i> [™] Lost Trigger	6-21
Brick Proactive Monitoring Trigger	6-25
<i>Brick</i> [®] SLA Round Trip Delay Alarm Trigger	6-30
VPN proactive Monitoring Trigger	6-31
LAN-to-LAN Tunnel Lost Trigger	6-38
LAN-to-LAN Tunnel UP Trigger	6-41
Local Presence Map Pool Trigger	6-44
LSMS Error Trigger	6-47
LSMS Status Change Trigger	6-50

LSMS Proactive Monitoring Trigger	6-52
QoS Alarm Triggers	6-57
Unauthorized LSMS Login Attempt Trigger	6-59
User Authentication Trigger	6-62
Maintaining Triggers	6-65



Configuring Triggers

Overview

Configuring triggers involves three primary steps:

- Provide a name for the trigger, specify a trigger type, and enable it.
- Specify the set of conditions (parameters) that cause the associated action to take place.
- Associate one or more actions with the alarm.

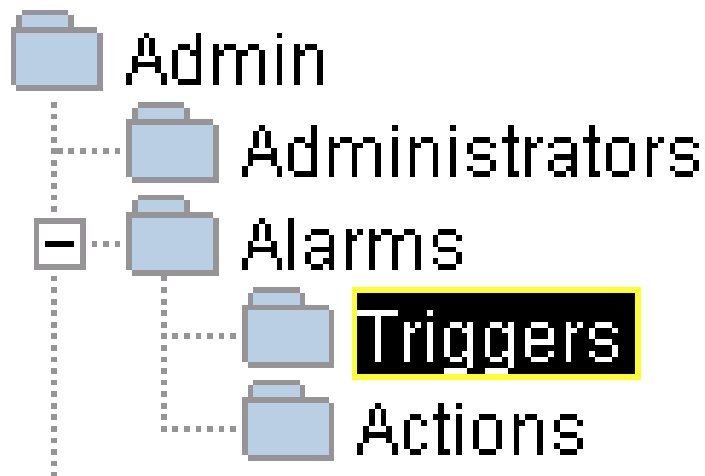
When a *Brick*[®] is related to the event, you also need to associate the *Brick*[®] group and the *Brick*[®] itself to the trigger.

Basic Steps to Configure a Trigger

To configure a trigger:

- 1 With the Navigator window displayed, open the Alarms folder.

Figure 6-1 LSMS Navigator Folder Panel



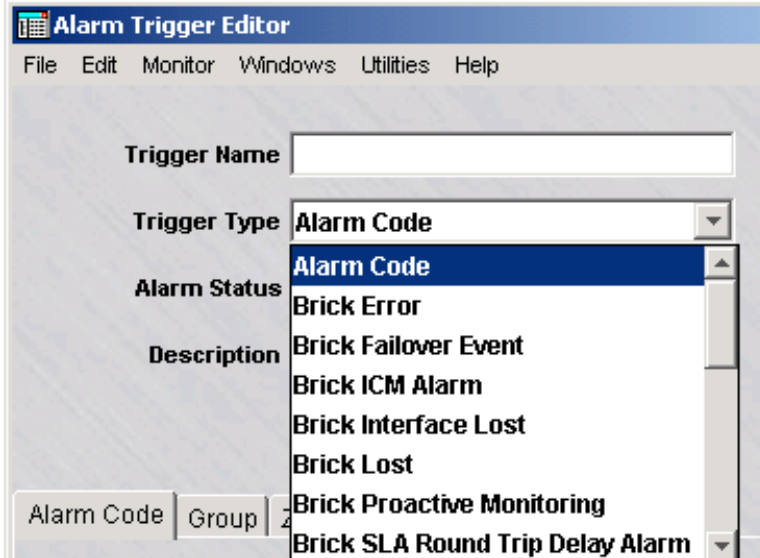
- 2 Right-click the Triggers folder and select **New Trigger**. The Alarm Trigger Editor appears.

Figure 6-2 Alarm Trigger Editor

Enter a name for the trigger in the **Trigger Name** field. This is a required field and is displayed in the list of triggers in the Contents Panel. Be as descriptive as possible. Spaces are allowed, but special characters are not (for example, @).

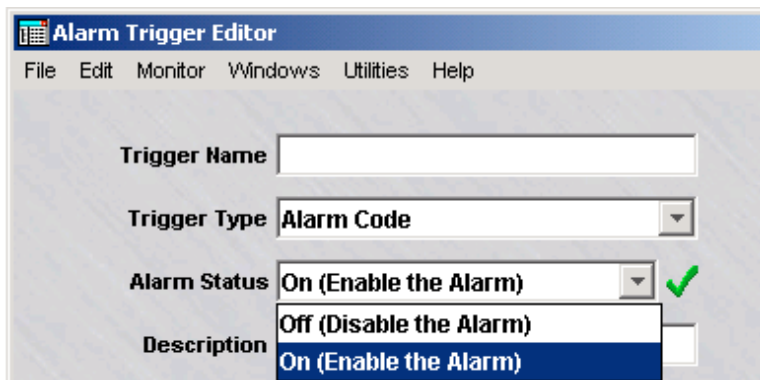
- 3 Select a trigger type from the **Trigger Type** field drop-down list. Trigger types are explained in more detail in the sections that follow.

Figure 6-3 Alarm Trigger Editor Trigger Type Drop-down List



- 4 Specify the **Alarm Status** field drop-down list. The default entry is **On (Enable the Alarm)**. Or, select **Off (Disable the Alarm)** from the drop-down list.

Figure 6-4 Alarm Trigger Editor Alarm Status Drop-down



- 5 Optionally, enter a Description for the trigger. If a description is entered, it is displayed in the list of triggers in the Contents Panel.

6 Click **Alarm Code** to display the next page of the wizard and enter parameters for the trigger type you selected. The parameters for each type of trigger are explained below.

7 To save the trigger, select **File > Save and Close** in the last page of the wizard.

Important! Include AllCheckbox When using the Alarm Trigger Editor to associate groups and actions with a trigger, you will see an **Include All** checkbox. This is to facilitate maintenance of the triggers.

If **Include All** is checked:

- All current groups will receive the alarm when it is triggered
- Any future groups or actions that are created will automatically be associated with the trigger.

END OF STEPS



Alarm Code Trigger

Overview

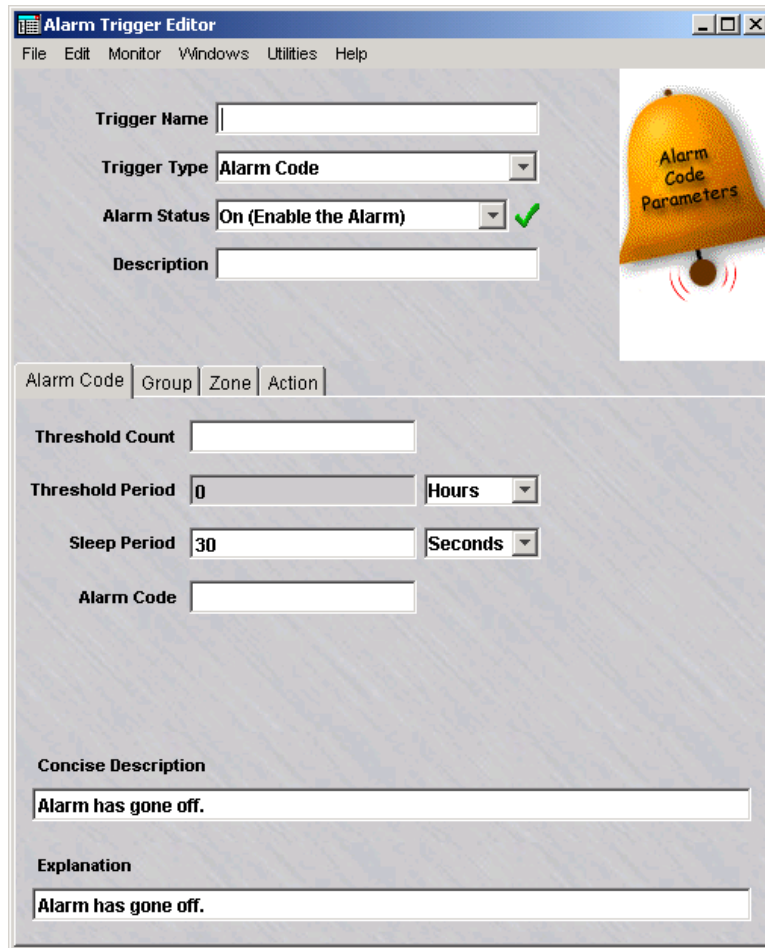
An **Alarm Code** trigger is linked with a rule of a given security policy. When an alarm code is embedded in a rule and the rule is invoked the specified number of times within a specific time frame, an alarm is generated. The mechanism for tying the trigger to a rule is the *alarm code*.

To configure an Alarm Code trigger:

- 1 Enter a Trigger Name, select **Alarm Code** from the **Trigger Type** drop-down list, select an **Alarm Status** (Off or On), then enter an optional Description as described in [“Configuring Triggers”](#) (p. 6-3).

- 2 Click **Alarm Code**.

Figure 6-5 Alarm Trigger Editor Alarm Code Trigger Parameters



- 3 In the next page of the wizard, shown in [Figure 6-5, “Alarm Trigger Editor Alarm Code Trigger Parameters”](#) (p. 6-8), enter the parameters that define the conditions of this trigger as the following table explains:

Parameter	Description
Threshold Count	The number of events that must be detected before the alarm is generated. This is a required field. If 1 is entered, then Threshold Period is not needed.

Parameter	Description
Threshold Period	The time period in which the number of events (as set in Threshold Count) must occur before the alarm is generated. This field is only active when Threshold Count is 2 or higher. Both conditions must be true in order to generate the alarm.
Sleep Period	After the initial alarm is generated, this amount of time must elapse before another alarm is generated. Enforces throttling and mitigates flooding the network (e.g., denial-of-service attacks).
Alarm Code	Enter a number that matches the Alarm Code field of the rule.
Concise Description	If the action associated with this trigger includes Concise Description, this is the message that will be forwarded in the alarm.
Explanation	If the action associated with this trigger includes Explanation, this is the message that will be forwarded in the alarm.

4 Click **Group**.

- 5** In the next page of the wizard, select at least one group to associate with this trigger from those listed in the **Available list**. Click the **Add>** button to move the groups to the **Selected** list.

Only the groups you have permission to send the alarms to are displayed in the **Available** list.

To select a range of groups, zones, Bricks, or actions from an **Available** list, hold down the **Shift** key, click the first item of the range you want to select, then click the last item. To select several non-sequential items from a list, hold down the **Control** (CTRL) key and click each item you want to select.

6 Click **Zone**.

- 7** In the next page of the wizard, select at least one zone to associate with this trigger and select **Add**. Only the zones that belong in the groups selected in the previous page are displayed.

.....

8 Click **Action**.

.....

9 In the last page of the wizard, select at least one action to associate with this trigger and select **Add**. The actions will then be moved to the **Selected** box.

Only the actions that have been already configured are displayed.

.....

10 Select **File > Save and Close**.

Important! *Alarm Code Rules* Configuring the Alarm Code trigger is only one step of generating this type of alarm. The alarm code configured here must match the alarm code of a rule. Refer to [“Overview” \(p. B-1\)](#) for details.

.....

END OF STEPS

.....



Brick[®] Error Trigger

Overview

A **Brick Error** trigger detects errors that are generated by a Brick. The error code entered needs to be between 1 and 999.

To configure a Brick Error trigger:

- 1 Enter a Trigger Name, select **Brick Error** from the **Trigger Type** drop-down list, select an **Alarm Status** (Off or On), then enter an optional **Description** as described in “Configuring Triggers” (p. 6-3).
- 2 Click **Brick Errors**.

Figure 6-6 Alarm Trigger Editor Brick Error Trigger Parameters

The screenshot shows the 'Alarm Trigger Editor' window with the following configuration:

- Trigger Name:** (Empty text field)
- Trigger Type:** Brick Error (Selected in dropdown)
- Alarm Status:** On (Enable the Alarm) (Selected in dropdown, with a green checkmark)
- Description:** (Empty text field)

On the right side of the window, there is a yellow bell icon with the text 'Device Error Parameters' written on it.

Below the main configuration area, there is a tabbed interface with the following settings:

- Brick Errors** (Selected tab) | Group | Brick | Action
- Threshold Count:** 1
- Threshold Period:** 1 Minutes
- Sleep Period:** 30 Seconds
- Brick Error Codes:** * (with a help icon)
- Severity:** (Empty text field)

At the bottom, there are two text areas for descriptions:

- Concise Description:** The Brick has detected an error.
- Explanation:** The Brick has detected an error.

- 3 In the next page of the wizard, shown in [Figure 6-6, “Alarm Trigger Editor Brick Error Trigger Parameters”](#) (p. 6-11), enter the parameters that define the conditions of this trigger. The following table explains each parameter:

Parameter	Description
Threshold Count	The number of events that must be detected before the alarm is generated. This is a required field. If 1 is entered, then Threshold Period is not needed.
Threshold Period	The time period in which the number of events (as set in Threshold Count) must occur before the alarm is generated. This field is only active when Threshold Count is 2 or higher. Both conditions must be true in order to generate the alarm.
Sleep Period	After the initial alarm is generated, this amount of time must elapse before another alarm is generated. Enforces throttling and mitigates flooding the network (e.g., denial-of-service attacks).
Brick Error Codes	A number between 1 and 999. Click View to see the list of error codes. Only the codes that are prefaced with a bell icon can be entered.
Severity	Enter 1, 2, or 3. This is an optional field. 1 indicates a serious problem; 2 indicates a system exhibiting some degradation in functionality; 3 indicates a system with no degradation in functionality.
Concise Description	If the action associated with this trigger includes Concise Description , this is the message that will be forwarded in the alarm.
Explanation	If the action associated with this trigger includes Explanation , this is the message that will be forwarded in the alarm.

- 4 Click **Group**.

- 5 In the next page of the wizard, select at least one group to associate with this trigger and select **Add**. The groups will then be moved to the **Selected** box.

Only the groups you have permission to send the alarms to will be displayed.

- 6 Click **Brick**.

.....

7 In the next page of the wizard, select at least one Brick to associate with this trigger and select **Add**. Only the Bricks that belong in the groups selected in the previous page are displayed.

.....

8 Click **Action**.

.....

9 In the last page of the wizard, select at least one action to associate with this trigger and select **Add**. The actions will then be moved to the **Selected** box.
Only the actions that have been already configured are displayed.

.....

10 Select **File > Save and Close**.

.....

END OF STEPS

.....



Brick Failover Event Trigger

Overview

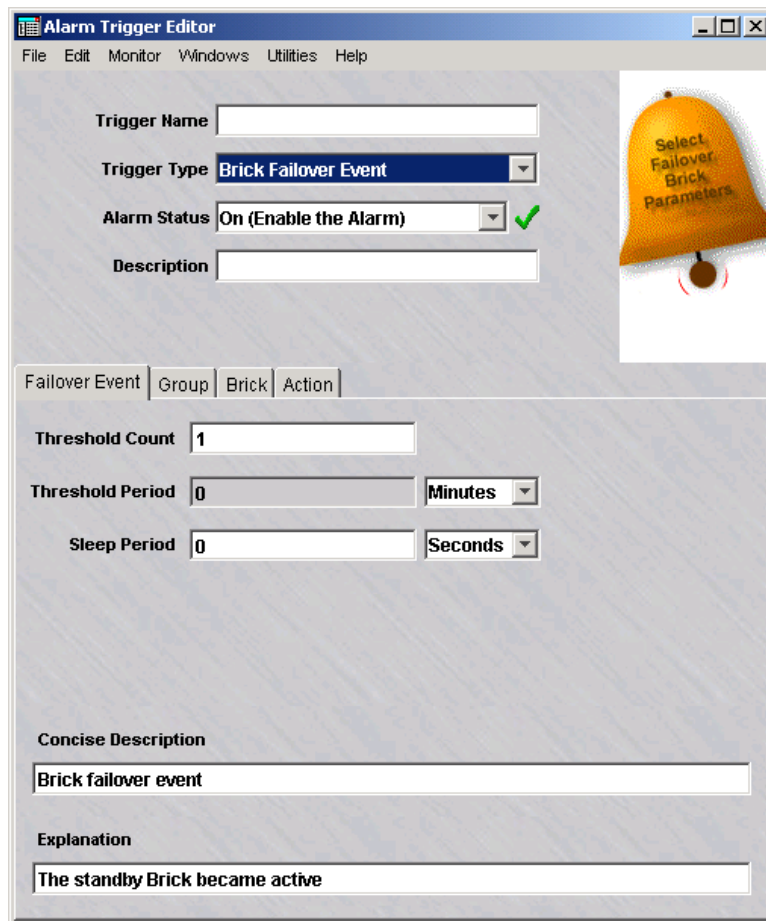
A **Brick Failover Event** trigger detects failover events, when one member of a Brick failover pair transitions from the "Standby" to the "Active" State. See *Chapter 2. Brick Failover* in the *Lucent Security Management Server LSMS and Brick Redundancy Guide*.

To configure a Brick Failover Event trigger:

- 1 Enter a Trigger Name, select **Brick Failover Event** from the **Trigger Type** drop-down list, select an **Alarm Status** (Off or On), then enter an optional **Description** as described in ["Configuring Triggers"](#) (p. 6-3).

- 2 Click **Failover Event**.

Figure 6-7 Alarm Trigger Brick Failover Event Trigger Parameters



-
- 3 In the next page of the wizard, shown in [Figure 6-7, “Alarm Trigger Brick Failover Event Trigger Parameters”](#) (p. 6-14), enter the parameters that define the conditions of this trigger, as the following table explains:

Parameter	Description
Threshold Count	The number of events that must be detected before the alarm is generated. This is a required field. If 1 is entered, then Threshold Period is not needed.
Threshold Period	The time period in which the number of events (as set in Threshold Count) must occur before the alarm is generated. This field is only active when Threshold Count is 2 or higher. Both conditions must be true in order to generate the alarm.
Sleep Period	After the initial alarm is generated, this amount of time must elapse before another alarm is generated. Enforces throttling and mitigates flooding the network (e.g., denial-of-service attacks).
Concise Description	If the action associated with this trigger includes Concise Description , this is the message that will be forwarded in the alarm.
Explanation	If the action associated with this trigger includes Explanation , this is the message that will be forwarded in the alarm.

-
- 4 Click **Group**.
-

- 5 In the next page of the wizard, select at least one group to associate with this trigger and select **Add**. The groups will then be moved to the **Selected** box.

Only the groups you have permission to send the alarms to will be displayed.

.....

- 6 Click **Brick**.
-

- 7 In the next page of the wizard, select at least one Brick to associate with this trigger and select **Add**. Only the Bricks that belong in the groups selected in the previous page are displayed.
-

- 8 Click **Action**.
-

-
- 9** In the last page of the wizard, select at least one action to associate with this trigger and select **Add**. The actions will then be moved to the **Selected** box.

Only the actions that have been already configured are displayed.

.....

- 10** Select **File > Save and Close**.

END OF STEPS

.....



Brick[®] ICM Trigger

Overview

This trigger allows the LSMS to generate an alarm when the Intelligent Cache Management (ICM) option is activated on a given Brick. In the event of a Denial of Service attack, this alarm will notify you that the Brick is purging less important sessions to preserve cache memory for new sessions.

The critical fields for this alarm trigger are:

- The actual percentage of cache full and absolute number of sessions before pruning
- The actual percentage of cache full and absolute number of sessions after pruning

As with other alarm triggers, the administrator can specify the desired alarm action as well as the applicable Bricks, sleep timer, etc.



Brick[®] Interface Lost Trigger

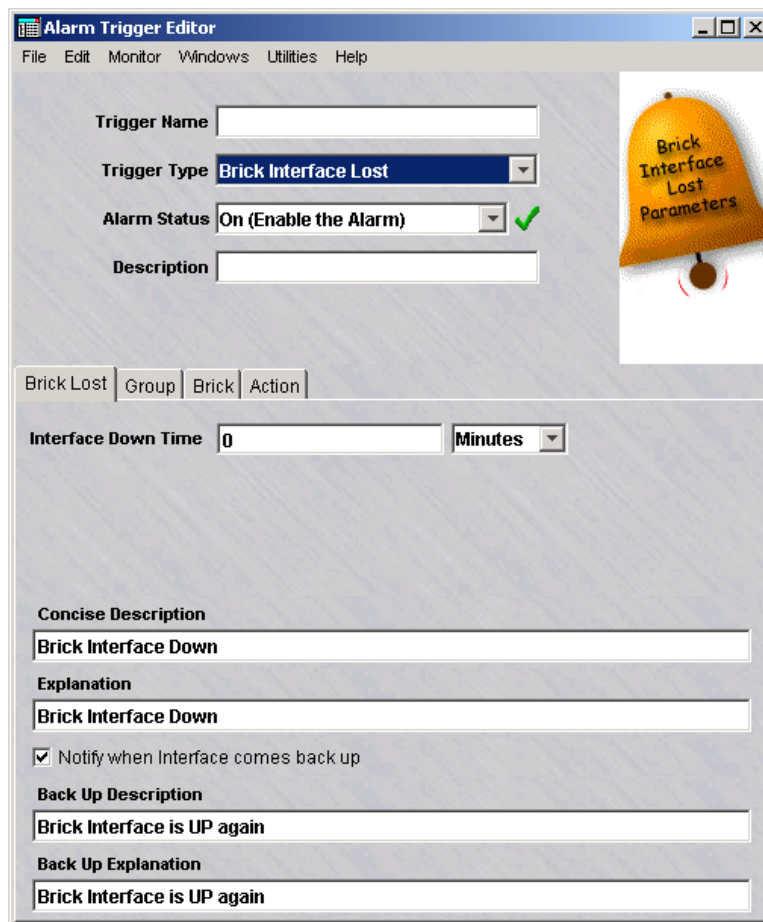
Overview

A **Brick Interface Lost trigger** detects connectivity problems (e.g., a disconnected or malfunctioning NIC card) on one of the Brick interfaces.

To configure a Brick Interface Lost trigger:

- 1 Enter a Trigger Name, select **Brick Interface Lost** from the Trigger Type drop-down list, select an **Alarm Status** (Off or On), then enter an optional Description as described in “[Configuring Triggers](#)” (p. 6-3).
 - 2 Click **Next**.
-

Figure 6-8 Alarm Trigger Editor Brick Interface Lost Parameters



- 3 In the next page of the wizard, shown in [Figure 6-8, “Alarm Trigger Editor Brick Interface Lost Parameters”](#) (p. 6-18), enter the parameters that define the conditions of the **Brick Interface Lost** trigger as the following table explains:

Parameter	Description
Interface Down Time	After the initial interface event is detected, this is the amount of time that the interface must stay down before another alarm is generated. If 0 Hours is specified, the alarm is generated when the first occurrence is detected.
Concise Description	If the action associated with this trigger includes Concise Description , this is the message that will be forwarded in the alarm.
Explanation	If the action associated with this trigger includes Explanation , this is the message that will be forwarded in the alarm.
Notify when Interface comes back up	If you want the alarm to be generated again when the event is no longer detected, leave the checkbox checked.
Concise Description	If the action associated with this trigger includes Concise Description , this is the message that will be forwarded in the Notify when Interface comes back up alarm. This message is only sent if the Notify when Interface comes back up checkbox is checked.
Explanation	If the action associated with this trigger includes Explanation , this is the message that will be forwarded in the Notify when Interface comes back up alarm. This message is only sent if the Notify when Interface comes back up checkbox is checked.

- 4 Click **Group**.

- 5 In the next page of the wizard, select at least one group to associate with this trigger and select **Add**. The groups will then be moved to the **Selected** box.

Only the groups you have permission to send the alarms to will be displayed.

- 6 Click **Brick**.

.....
7 In the next page of the wizard, select at least one Brick to associate with this trigger and select **Add**. Only the Bricks that belong in the groups selected in the previous page are displayed.

.....
8 Click **Action**.

.....
9 In the last page of the wizard, select at least one action to associate with this trigger and select **Add**. The actions will then be moved to the **Selected** box.
Only the actions that have been already configured are displayed.

.....
10 Select **File > Save and Close**.

.....
E N D O F S T E P S



Brick[™] Lost Trigger

Overview

A **Brick Lost** trigger detects communication problems between the LSMS and a Brick. A preconfigured *Brick*[®] Lost trigger already exists, so you may not need to configure another one. See "*Preconfigured Alarm Triggers and Actions*" in [Chapter 4, "Introduction to Alarms"](#).

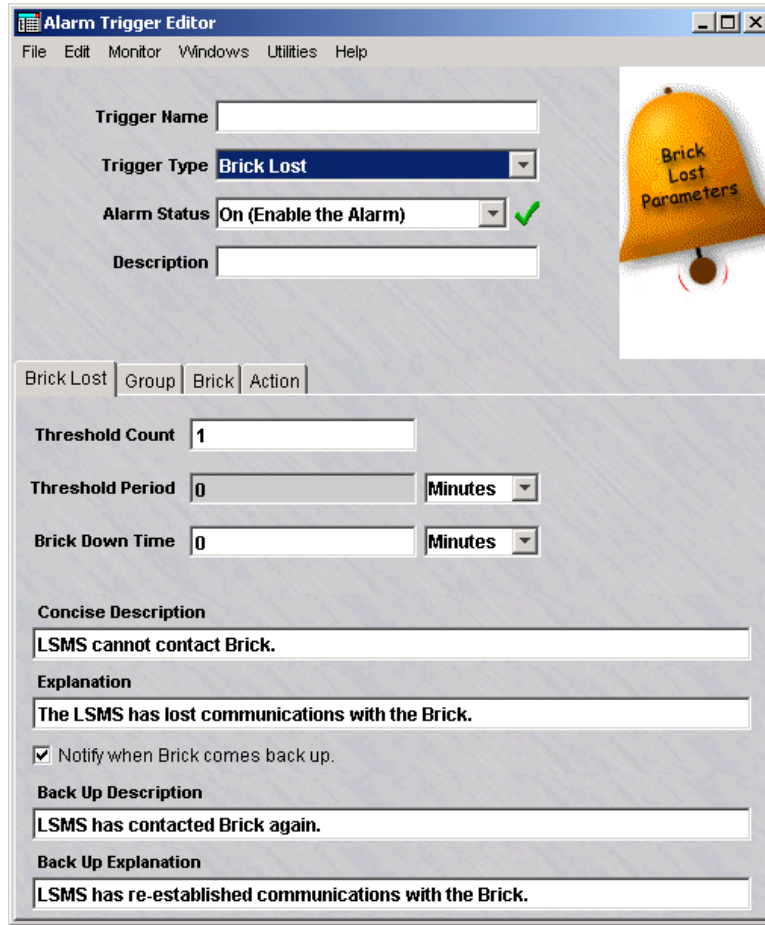
Task

To configure a *Brick*[®] Lost trigger:

- 1 Enter a Trigger Name, select **Brick Lost** from the **Trigger Type** drop-down list, select an **Alarm Status** (Off or On), then enter an optional **Description** as described in "[Configuring Triggers](#)" (p. 6-3).

2 Click **Brick Lost**.

Figure 6-9 Alarm Trigger Editor Brick Lost Parameters



3 In the next page of the wizard, shown in [Figure 6-9, “Alarm Trigger Editor Brick Lost Parameters”](#) (p. 6-22), enter the Brick Lost Parameters that define the conditions of this trigger as the following table explains:

Parameter	Description
Threshold Count	The number of events that must be detected before the alarm is generated. This is a required field. If 1 is entered, then Threshold Period is not needed.

Parameter	Description
Threshold Period	<p>The time period in which the number of events (as set in Threshold Count) must occur before the alarm is generated.</p> <p>This field is only active when Threshold Count is 2 or higher. Both conditions must be true in order to generate the alarm.</p>
Brick Down Time	<p>After the initial brick event is detected, this is amount of time that the Brick must stay down before another alarm is generated.</p> <p>If 0 Hours is specified, the alarm is generated when the first occurrence is detected.</p>
Concise Description	<p>If the action associated with this trigger includes Concise Description, this is the message that will be forwarded in the alarm.</p>
Explanation	<p>If the action associated with this trigger includes Explanation, this is the message that will be forwarded in the alarm.</p>
Notify when Brick comes back up	<p>If you want the alarm to be generated again when the event is no longer detected, leave the checkbox checked.</p>
Concise Description	<p>If the action associated with this trigger includes Concise Description, this is the message that will be forwarded in the Notify when Brick comes back up alarm.</p> <p>This message is only sent if the Notify when Brick comes back up checkbox is checked.</p>
Explanation	<p>If the action associated with this trigger includes Explanation, this is the message that will be forwarded in the Notify when Brick comes back up alarm.</p> <p>This message is only sent if the Notify when Brick comes back up checkbox is checked.</p>

.....

4 Click **Group**.

.....

5 In the next page of the wizard, select at least one group to associate with this trigger and select **Add**. The groups will then be moved to the **Selected** box.

Only the groups you have permission to send the alarms to will be displayed.

.....

6 Click **Brick**.

.....
7 In the next page of the wizard, select at least one Brick to associate with this trigger and select **Add**. Only the Bricks that belong in the groups selected in the previous page are displayed.

.....
8 Click **Action**.

.....
9 In the last page of the wizard, select at least one action to associate with this trigger and select **Add**. The actions will then be moved to the **Selected** box.
Only the actions that have been already configured are displayed.

.....
10 Select **File > Save and Close**.

.....
E N D O F S T E P S



Brick Proactive Monitoring Trigger

Overview

A **Brick Proactive Monitoring** trigger detects Brick events such as high average cache memory usage, or an excessive number of packets dropped or passed, so that if the health of the network is deemed questionable, an Administrator is notified before the problem worsens.

Before configuring this trigger, you should inspect normal traffic load and throughput of your network. Equipped with an understanding of normal traffic conditions, you are prepared to enter useful threshold criteria that reflect unusual traffic patterns.

Task

To configure a Brick Proactive Monitoring trigger:

- 1 Enter a Trigger Name, select **Brick Proactive Monitoring** from the **Trigger Type** drop-down list, select an **Alarm Status** (Off or On), then enter an optional **Description** as described in [“Configuring Triggers”](#) (p. 6-3).

2 Click Promon.

Figure 6-10 Alarm Trigger Editor Brick Proactive Monitoring Trigger Parameters



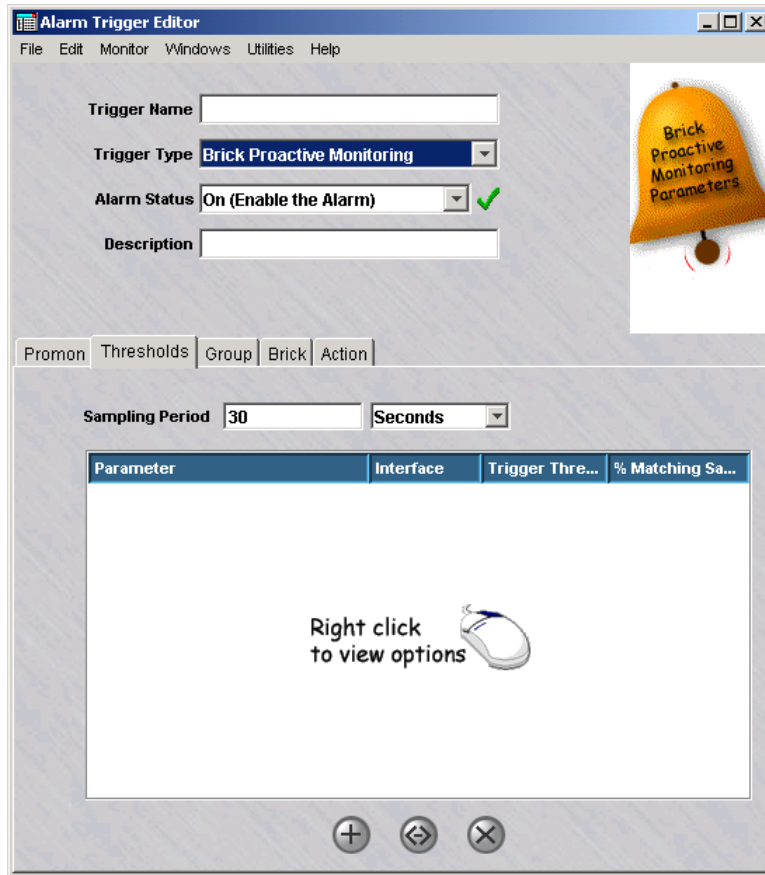
3 In the next page of the wizard, shown in [Figure 6-10](#), “[Alarm Trigger Editor Brick Proactive Monitoring Trigger Parameters](#)” (p. 6-26), enter the parameters that define the conditions of this trigger as the following table explains:

Parameter	Description
Sleep Period	After the initial alarm is generated, this amount of time must elapse before another alarm is generated. Enforces throttling and mitigates flooding the network (e.g., denial-of-service attacks).
Concise Description	If the action associated with this trigger includes Concise Description , this is the message that will be forwarded in the alarm.

Parameter	Description
Explanation	If the action associated with this trigger includes Explanation , this is the message that will be forwarded in the alarm.

4 Click **Thresholds**.

Figure 6-11 Select Threshold Values Window

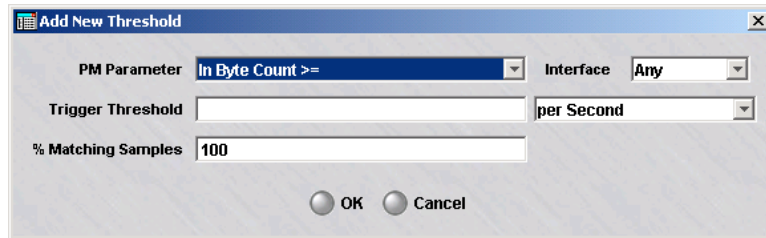


5 In the next page of the wizard, shown in enter a value for Sampling Period. This is the time period in which the event, as further defined in the next few steps, must occur before the alarm is generated.

The default of 30 seconds represents how often the data is collected by a Brick and written to the Proactive Monitoring log. The value entered for the Threshold Period determines the number of collections taken.

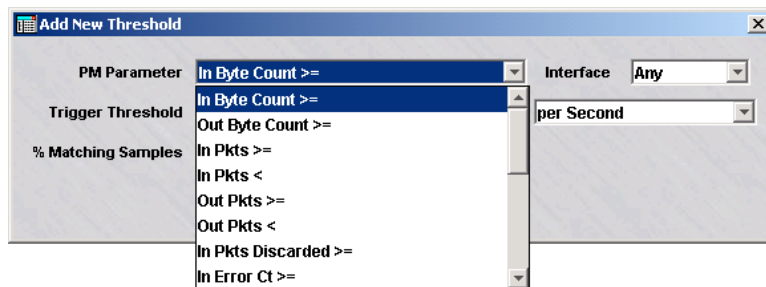
If two minutes is entered as the Threshold Period, then four data collections are taken.

- Right-click in the white box and select **New** from the pop-up menu. The **Add New Threshold** window appears:



- Select a Proactive Monitoring parameter from the **PM Parameter** drop-down list. This is the condition you want monitored.

Figure 6-12 Brick Proactive Monitoring Parameters Drop-down



These are parameters that are collected by a Brick and include processed packets, packets that are dropped, packet counts, etc. They are comprehensively described in [“Overview”](#) (p. C-1).

- For some parameters, you can specify a particular port to monitor. If an **Interface** field is present, select **Any**, or one of the ports, **ether0** through **ether19**, from the drop-down list.
- Enter a **Trigger Threshold** for the parameter to be monitored. This is the normalized threshold value per the selected unit of measure (per second, minute, hour, etc.).
- In the **% Matching Samples** field, enter a whole number between 0 and 100. This is the percentage of time that the collection interval reaches or exceeds the **Trigger Threshold**.

-
- 11** Click **OK**. The parameter now appears in the white box. To edit, delete, or create a new parameter, right-click the parameter and select an option from the pop-up menu.
-
- 12** Click **Group**.
-
- 13** In the next page of the wizard, select at least one group to associate with this trigger and select **Add**. The groups will then be moved to the Selected box.
- Only the groups you have permission to send the alarms to will be displayed.
-
- 14** Click **Brick**.
-
- 15** In the next page of the wizard, select at least one Brick to associate with this trigger and select **Add**. Only the Bricks that belong in the groups selected in the previous page are displayed.
-
- 16** Click **Action**.
-
- 17** In the last page of the wizard, select at least one action to associate with this trigger and select **Add**. The actions will then be moved to the Selected box.
- Only the actions that have been already configured are displayed.
-
- 18** Select **File > Save and Close**.

.....

END OF STEPS

.....



Brick[®] SLA Round Trip Delay Alarm Trigger

Overview

The Brick SLA Round Trip Delay Alarm Trigger may be configured and enabled if:

- You have one or more active LAN - LAN Tunnels
- You have selected the "Enable SLA Probe" checkbox under the SLA probe in the LAN-LAN Tunnel Editor. An SLA probe would be activated if a service provider wanted to monitor the availability and latency of a tunnel to ensure that a customer's Service Level Agreement requirements are met. See *Chapter 12. LAN-LAN Tunnels* in the *LSMS Policy Guide* for additional details.

As with all alarm triggers on the LSMS, you need to specify minimum criteria such as a trigger name and type, associate at least one action for the trigger and enable it.

There are two parameters of particular interest for this Alarm Trigger:

- *Percent Probes Lost* - Due to network congestion, outages, etc. some SLA probes between the tunnel endpoints may be lost. This option allows you to alarm if a defined percentage of the probes are lost during the configured sleep period.
- *Percent Probes Above Threshold* - One of the parameters in the SLA Probe tab in the LAN-LAN Tunnel Editor is "Round Trip Delay Threshold". With this option, an administrator may receive an alarm if the specified percentage of probes exceeds the threshold during the configured sleep period.

For example, let's say that you are issuing an SLA probe every 30 seconds, and your sleep period for the Alarm Trigger is set to five minutes. You've set the Percent Probes Above Threshold to 30%. So - during any five minute period, if three or more probes exceed the delay threshold, you would receive an alarm.

□

VPN proactive Monitoring Trigger

Overview

The *VPN Proactive Monitoring* trigger includes parameters for VPN client events such as:

- IKE Initiated
- IKE Failed
- User Auth (via VPN Client) Initiated
- User Auth (via VPN Client) Failed

Important! This trigger can only be used if the IKE on the *Brick*[®] feature is enabled. (Select **Help > About** to display a screen that shows whether this feature is enabled.)

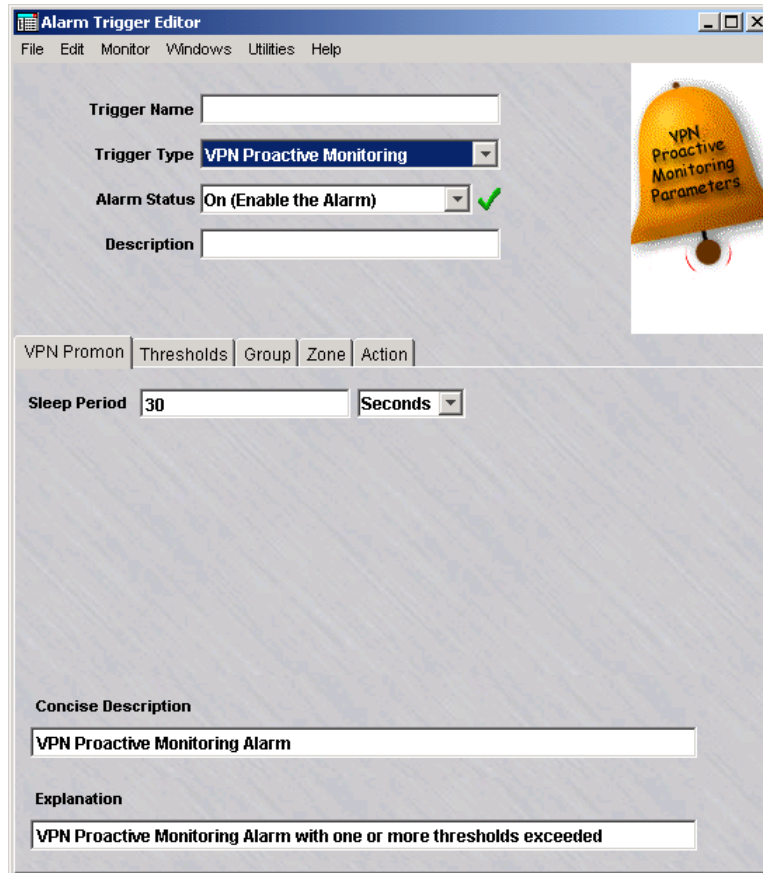
Task

To configure the VPN Proactive Monitoring Trigger:

- 1 Follow steps 1 to 3 as described in [“Configuring Triggers” \(p. 6-3\)](#).
- 2 Click the down arrow next to the **Trigger Type** field to display a drop-down list and select **VPN Proactive Monitoring**.
- 3 Specify the Alarm Status. The default entry is **On (Enable the Alarm)**. Or, select **Off (Disable the Alarm)** from the drop-down list.
- 4 Optionally, enter a **Description** for the trigger. If a description is entered, it is displayed in the list of triggers in the Contents Panel.

- Click **VPN Promon** to display the next page of the wizard and enter parameters for the trigger type you selected (shown in Figure 6-15, “Add New Threshold Window” (p. 6-34)).

Figure 6-13 Alarm Trigger Editor VPN Proactive Monitoring Trigger Parameters



- Enter the VPN Proactive Monitoring Parameters that define the conditions of this trigger as shown in the following table:

Parameter	Description
Sleep Period	After the initial alarm is generated, this amount of time must elapse before another alarm is generated. The default value is 30 (seconds). Enforces throttling and mitigates flooding of the network (as from, for example, denial-of-service attacks).

Parameter	Description
Concise Description	If the action associated with this trigger includes Concise Description, this is the message that will be forwarded in the alarm. This message is displayed on the Alarm Console on the LSMS when the alarm is triggered.
Explanation	If the action associated with this trigger includes Explanation, this is the message that will be forwarded in the alarm. This message is displayed if the email, Syslog, or Pager alarm action is configured.

- Click **Thresholds** to display the next page of the wizard (Figure 6-16, “VPN Proactive Monitoring PM Parameter Drop-Down List” (p. 6-34)).

Figure 6-14 VPN Proactive Monitoring Threshold Value Panel

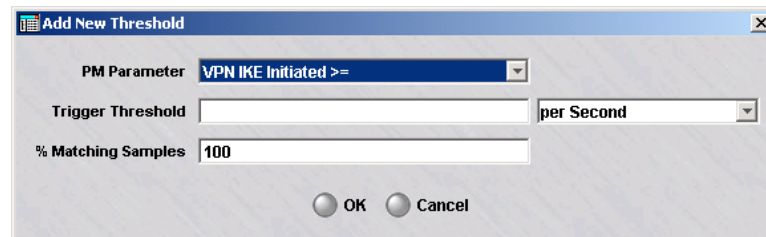


- Leave the Sampling Period as 30 Seconds.

-
- 9 Right-click and select **New**.

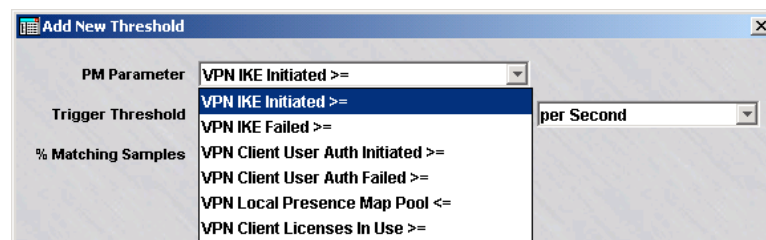
The Add New Threshold window is displayed (Figure 6-17, “VPN Proactive Monitoring Wizard (Group)” (p. 6-35)).

Figure 6-15 Add New Threshold Window



-
- 10 Click the down arrow next to the PM Parameter field to display a drop-down list (Figure 6-18, “VPN Proactive Monitoring Wizard (Zone)” (p. 6-36)).

Figure 6-16 VPN Proactive Monitoring PM Parameter Drop-Down List



-
- 11 Select **VPN Local Presence Map Pool**.
-
- 12 In the **Trigger Threshold** field, enter a percentage value for triggering an alarm when the Dynamic NAT pool of IP addresses reaches or fall belows the value entered (for example, enter 20 to trigger an alarm when the Dynamic NAT pool is only 20 percent full). The second threshold field value defaults to Percent for this trigger.
-
- 13 Leave the **% Matching Values** field value at 100.
-
- 14 Click **OK** on the Add New Threshold window.

- 15 Click **Group** to display the next wizard page (Figure 6-18, “VPN Proactive Monitoring Wizard (Zone)” (p. 6-36)).

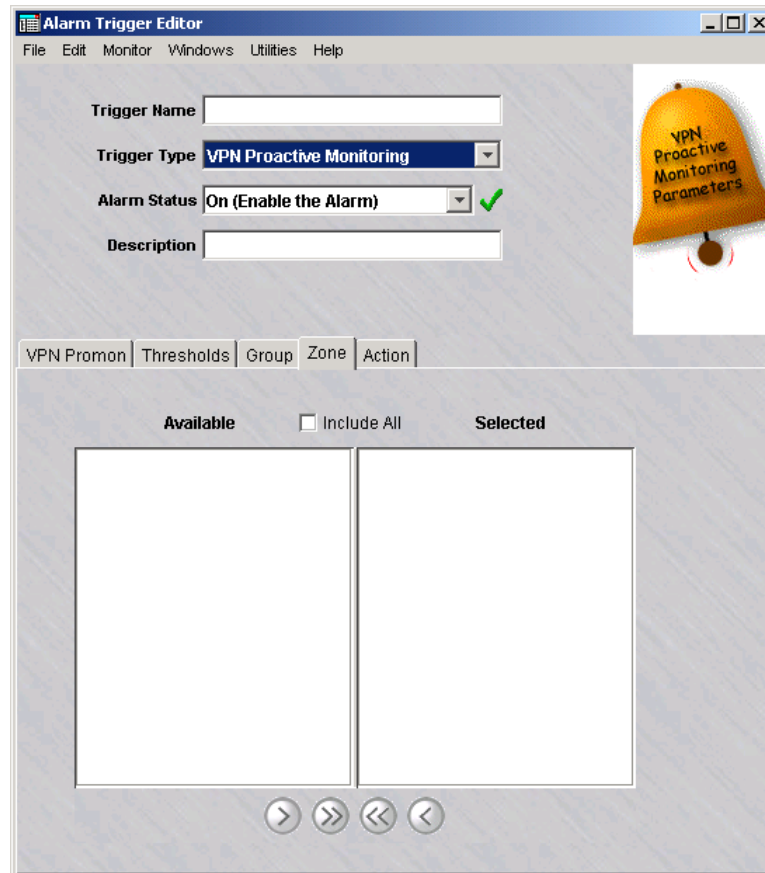
Figure 6-17 VPN Proactive Monitoring Wizard (Group)



- 16 Choose the group(s) to be associated with this trigger and click the arrow > or >> button to move the group(s) to the Selected column. You can also click the **Include All** checkbox to include all groups.

- 17 Click **Zone** to move to the next wizard page (Figure 6-19, “VPN Proactive Monitoring Wizard (Action)” (p. 6-37)).

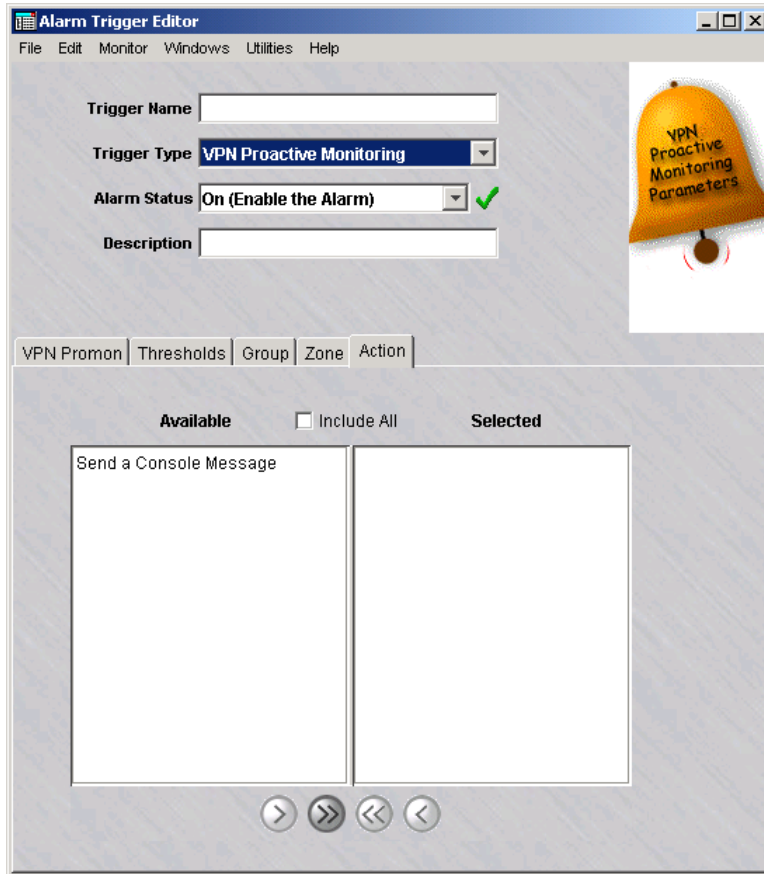
Figure 6-18 VPN Proactive Monitoring Wizard (Zone)



- 18 Select the zone(s) to be associated with this trigger and click the **Add** or **Add All** button to move the selected zone(s) to the Selected column. You can also click the **Include All** checkbox to include all zones.

- 19 Click **Action** to move to the next wizard page (Figure 6-20, “Alarm Trigger Editor LAN-to-LAN tunnel Lost Parameters” (p. 6-39)).

Figure 6-19 VPN Proactive Monitoring Wizard (Action)



- 20 Select an action to be taken when a VPN Proactive Monitoring event occurs. For this type of trigger, choose **Send a Console Message** and click the > or >> button to move it to the Selected column. You can also click the **Include All** checkbox to include all actions.

- 21 Select **File > Save and Close**.
The alarm trigger is configured.

END OF STEPS



LAN-to-LAN Tunnel Lost Trigger

Overview

A **LAN-to-LAN Tunnel Lost** trigger detects the failure of an established LAN-to-LAN tunnel. A preconfigured LAN-to-LAN Tunnel Lost trigger already exists, so you may not need to configure another one. See [“Preconfigured Alarm Triggers and Actions”](#) (p. 4-5) in [Chapter 4, “Introduction to Alarms”](#).

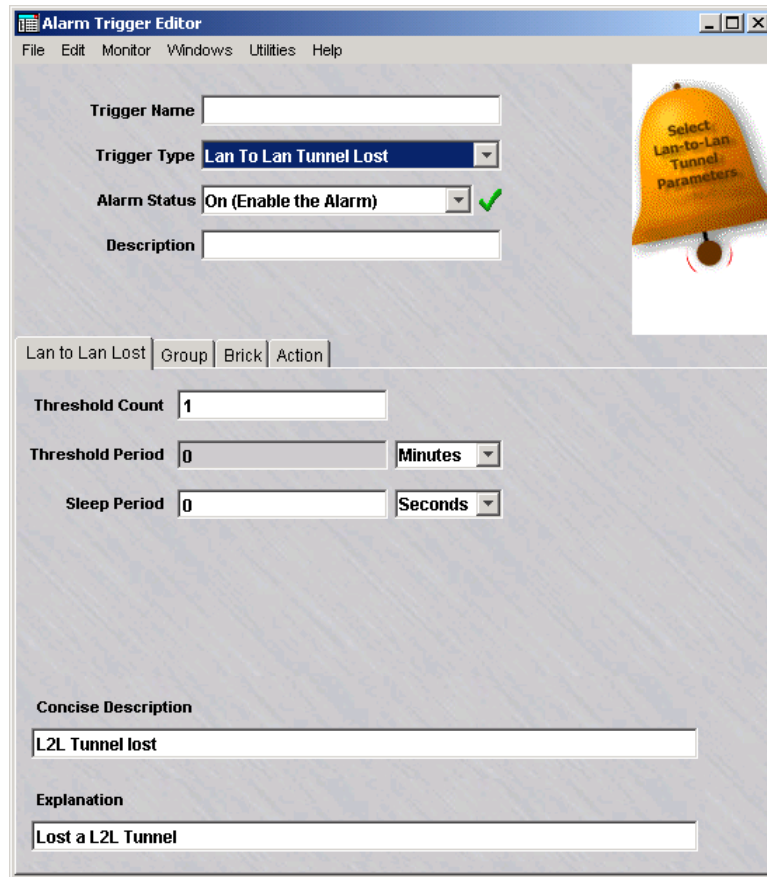
Task

To configure a LAN-to-LAN tunnel Lost trigger:

- 1 Enter a Trigger Name, select **Lan To Lan Tunnel Lost** from the **Trigger Type** drop-down list, select an **Alarm Status** (Off or On), then enter an optional **Description** as described in [“Configuring Triggers”](#) (p. 6-3).

- 2 Click Lan to Lan Lost.

Figure 6-20 Alarm Trigger Editor LAN-to-LAN tunnel Lost Parameters



- 3 In the next page of the wizard, shown in [Figure 6-20, “Alarm Trigger Editor LAN-to-LAN tunnel Lost Parameters”](#) (p. 6-39), enter the Brick Lost Parameters that define the conditions of this trigger as the following table explains:

Parameter	Description
Threshold Count	The number of events that must be detected before the alarm is generated. This is a required field. If 1 is entered, then Threshold Period is not needed.
Threshold Period	The time period in which the number of events (as set in Threshold Count) must occur before the alarm is generated. This field is only active when Threshold Count is 2 or higher. Both conditions must be true in order to generate the alarm.

Parameter	Description
Sleep Period	?? ??
Concise Description	If the action associated with this trigger includes Concise Description , this is the message that will be forwarded in the alarm.
Explanation	If the action associated with this trigger includes Explanation , this is the message that will be forwarded in the alarm.

-
- 4 Click **Group**.
.....
 - 5 In the next page of the wizard, select at least one group to associate with this trigger and select **Add**. The groups will then be moved to the **Selected** box.
Only the groups you have permission to send the alarms to will be displayed.
.....
 - 6 Click **Brick**.
.....
 - 7 In the next page of the wizard, select at least one Brick to associate with this trigger and select **Add**. Only the Bricks that belong in the groups selected in the previous page are displayed.
.....
 - 8 Click **Action**.
.....
 - 9 In the last page of the wizard, select at least one action to associate with this trigger and select **Add**. The actions will then be moved to the **Selected** box.
Only the actions that have been already configured are displayed.
.....
 - 10 Select **File > Save and Close**.

END OF STEPS



LAN-to-LAN Tunnel UP Trigger

Overview

A **LAN-to-LAN Tunnel UP** trigger is activated when a tunnel that's been previously brought down for some reason is back up. See [“Preconfigured Alarm Triggers and Actions”](#) (p. 4-5) in Chapter 4, [“Introduction to Alarms”](#).

Task

To configure a LAN-to-LAN tunnel UP trigger:

- 1 Enter a Trigger Name, select **Lan To Lan Tunnel UP** from the **Trigger Type** drop-down list, select an **Alarm Status** (Off or On), then enter an optional **Description** as described in [“Configuring Triggers”](#) (p. 6-3).
- 2 Click **Lan to Lan Lost**.

Figure 6-21 Alarm Trigger Editor LAN-to-LAN tunnel Lost Parameters



-
- 3 In the next page of the wizard, shown in [Figure 6-20, “Alarm Trigger Editor LAN-to-LAN tunnel Lost Parameters”](#) (p. 6-39), enter the Brick Lost Parameters that define the conditions of this trigger as the following table explains:

Parameter	Description
Threshold Count	The number of events that must be detected before the alarm is generated. This is a required field. If 1 is entered, then Threshold Period is not needed.
Threshold Period	The time period in which the number of events (as set in Threshold Count) must occur before the alarm is generated. This field is only active when Threshold Count is 2 or higher. Both conditions must be true in order to generate the alarm.
SleepPeriod	??? ???
Concise Description	If the action associated with this trigger includes Concise Description , this is the message that will be forwarded in the alarm.
Explanation	If the action associated with this trigger includes Explanation , this is the message that will be forwarded in the alarm.

-
- 4 Click **Group**.
-

- 5 In the next page of the wizard, select at least one group to associate with this trigger and select **Add**. The groups will then be moved to the **Selected** box.

Only the groups you have permission to send the alarms to will be displayed.

.....

- 6 Click **Brick**.
-

- 7 In the next page of the wizard, select at least one Brick to associate with this trigger and select **Add**. Only the Bricks that belong in the groups selected in the previous page are displayed.
-

- 8 Click **Action**.
-

-
- 9** In the last page of the wizard, select at least one action to associate with this trigger and select **Add**. The actions will then be moved to the **Selected** box.

Only the actions that have been already configured are displayed.

- 10** Select **File > Save and Close**.

END OF STEPS



Local Presence Map Pool Trigger

Overview

A **Local Presence Map Pool** trigger detects if the pool of free IP addresses used for mapping VPN end users to local addresses is below or equals a particular percentage. For more information on Local Presence, see *Appendix A* in the *LSMS Policy Guide*.

Important! *the Local Presence Map Pool Trigger can only be used if the IKE on the Brick[®] feature is not enabled. (Select **Help > About** to display a screen that shows if this feature is enabled.) If the IKE on the Brick[®] feature is enabled, use the Dynamic NAT Pool and VPN Proactive Monitoring trigger instead.*

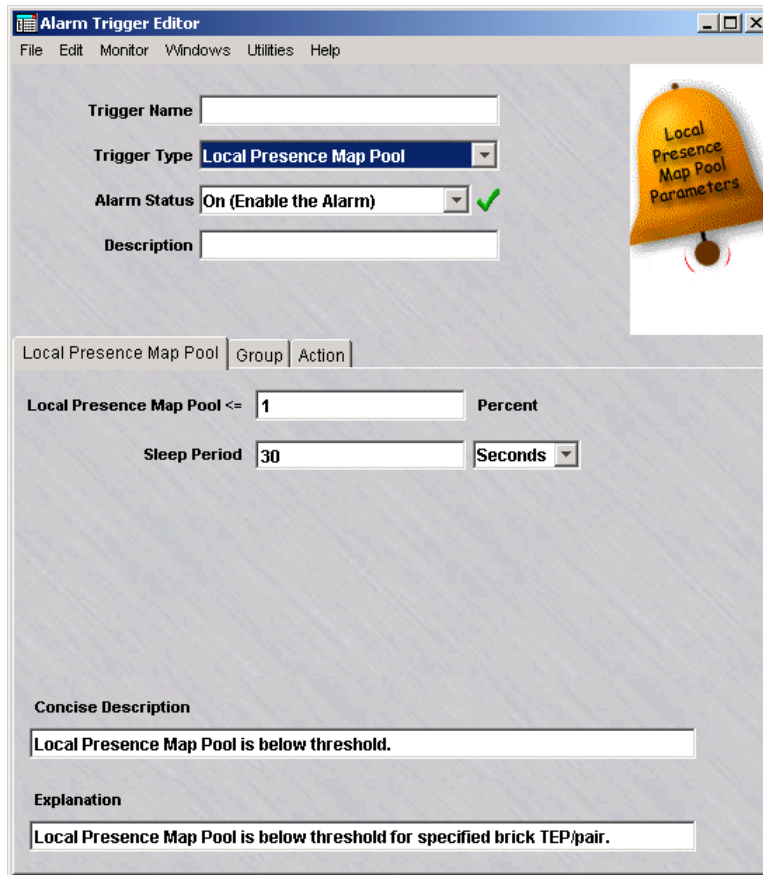
Task

To configure a Local Presence Map Pool trigger:

- 1 Enter a Trigger Name, select **Local Presence Map Pool** from the **Trigger Type** drop-down list, select an **Alarm Status** (Off or On), then enter an optional **Description** as described in [“Configuring Triggers”](#) (p. 6-3).

- 2 Click **Local Presence Map Pool**.

Figure 6-22 Alarm Trigger Editor Local Presence Map Pool Trigger Parameters



- 3 In the next page of the wizard, shown in [Figure 6-22, “Alarm Trigger Editor Local Presence Map Pool Trigger Parameters”](#) (p. 6-45), enter the parameters that define the conditions of this trigger, as the following table explains:

Parameter	Description
Local Presence Map Pool <=	A number between 1 and 100 to represent a percentage of the available pool of IP addresses. If the pool is below or equals the percentage entered, an alarm is generated.

Parameter	Description
Threshold Period	The time period in which the number of events (as set in Local Presence Map Pool <=) must occur before the alarm is generated. This field is only active when Local Presence Map Pool <= is 2 or higher. Both conditions must be true in order to generate the alarm.
Sleep Period	After the initial alarm is generated, this amount of time must elapse before another alarm is generated. Enforces throttling and mitigates flooding the network (e.g., denial-of-service attacks).
Concise Description	If the action associated with this trigger includes Concise Description , this is the message that will be forwarded in the alarm. This message is displayed on the Alarm Console on the LSMS when the alarm is triggered.
Explanation	If the action associated with this trigger includes Explanation , this is the message that will be forwarded in the alarm. This message is displayed if the email, Syslog, or Pager alarm action is configured.

.....

4 Click **Group**.

.....

5 In the next page of the wizard, select at least one group to associate with this trigger and select **Add**. The groups will then be moved to the **Selected** box.

Only the groups you have permission to send the alarms to will be displayed.

.....

6 Click **Action**.

.....

7 In the last page of the wizard, select at least one action to associate with this trigger and select **Add**. The actions will then be moved to the **Selected** box.

Only the actions that have been already configured are displayed.

.....

8 Select **File > Save and Close**.

END OF STEPS

.....



LSMS Error Trigger

Overview

An LSMS Error trigger detects errors that are generated by the LSMS. The error code is prefaced with a letter and followed by a number between 0000 and 9999 (for example, B1004). The error code represent events such as login denied due to inconsistent user certificate, unrecognized *Brick*[™], and so forth.

Task

To configure an LSMS Error trigger:

- 1 Enter a Trigger Name, select **LSMS Error** from the **Trigger Type** drop-down list, select an **Alarm Status** (Off or On), then enter an optional **Description** as described in [“Configuring Triggers”](#) (p. 6-3).

- 2 Click **LSMS Errors**.

Figure 6-23 Alarm Trigger Editor LSMS Error Trigger Parameters



- 3 In the next page of the wizard, shown in [Figure 6-23, “Alarm Trigger Editor LSMS Error Trigger Parameters”](#) (p. 6-48), enter the parameters that define the conditions of this trigger as the following table explains:

Parameter	Description
Threshold Count	The number of events that must be detected before the alarm is generated. This is a required field. If 1 is entered, then Threshold Period is not needed.
Threshold Period	The time period in which the number of events (as set in Threshold Count) must occur before the alarm is generated. This field is only active when Threshold Count is 2 or higher. Both conditions must be true in order to generate the alarm.

Parameter	Description
Sleep Period	After the initial alarm is generated, this amount of time must elapse before another alarm is generated. Enforces throttling and mitigates flooding the network (e.g., denial-of-service attacks).
Error Codes	A number prefaced with a letter and followed by a number between 0000 and 7999 (e.g., B1004). Acceptable values include a single error code (e.g., B1009); a list of error codes (e.g., B1004, B1009); wildcards (e.g., B*); question marks (e.g., ?1001). Click the View button to see the list of error codes. Error codes with a bell icon are recommended for use in alarms.
Severity	Enter 1, 2, or 3. This is an optional field. 1 indicates a serious problem; 2 indicates a system exhibiting some degradation in functionality; 3 indicates a system with no degradation in functionality.
Concise Description	If the action associated with this trigger includes Concise Description , this is the message that will be forwarded in the alarm. This message is displayed on the Alarm Console on the LSMS when the alarm is triggered.
Explanation	If the action associated with this trigger includes Explanation, this is the message that will be forwarded in the alarm. This message is displayed if the email, Syslog, or Pager alarm action is configured.

.....
4 Click **Action**.

.....
5 In the last page of the wizard, select at least one action to associate with this trigger and select **Add**. The actions will then be moved to the **Selected** box.
 Only the actions that have been already configured are displayed.

6 Select **File > Save and Close**.

.....
 END OF STEPS



LSMS Status Change Trigger

Overview

An LSMS Status Change trigger is used to define a trigger for when an LSMS that was brought down for some reason is brought back up.

Task

To configure an LSMS Status Change trigger:

- 1 Enter a Trigger Name, select **LSMS Status Change** from the **Trigger Type** drop-down list, select an **Alarm Status** (Off or On), then enter an optional **Description** as described in [“Configuring Triggers”](#) (p. 6-3).
 - 2 Click **LSMS Status Change**.
-

Figure 6-24 Alarm Trigger Editor LSMS Status Change Trigger Parameters



-
- 3 In the next page of the wizard, shown in [Figure 6-23, “Alarm Trigger Editor LSMS Error Trigger Parameters”](#) (p. 6-48), enter the parameters that define the conditions of this trigger as the following table explains:

Parameter	Description
LSMS Down Time	The ???. ???
Concise Description	If the action associated with this trigger includes Concise Description , this is the message that will be forwarded in the alarm. This message is displayed on the Alarm Console on the LSMS when the alarm is triggered.
Explanation	If the action associated with this trigger includes Explanation, this is the message that will be forwarded in the alarm. This message is displayed if the email, Syslog, or Pager alarm action is configured.
Explanation	If the action associated with this trigger includes Explanation, this is the message that will be forwarded in the alarm. This message is displayed if the email, Syslog, or Pager alarm action is configured.
Back Up Description	
Back Up Explanation	

-
- 4 Click **Action**.
-

- 5 In the last page of the wizard, select at least one action to associate with this trigger and select **Add**. The actions will then be moved to the **Selected** box.

Only the actions that have been already configured are displayed.

.....

- 6 Select **File > Save and Close**.

END OF STEPS

.....



LSMS Proactive Monitoring Trigger

Overview

An LSMS *Proactive Monitoring* trigger detects LSMS events such as platform resource utilization (such as log rollover rate and disk space usage), and number of user authentication attempts from VPN clients, so that if the health of the network is deemed questionable, an Administrator is notified before the problem worsens.

Before configuring this trigger, you should be familiar with normal conditions for log rollover rates, disk usage, and so forth. Equipped with an understanding of normal conditions, you are prepared to enter useful threshold criteria that reflect unusual resource utilization patterns.

Important! *Some parameters, such as IK initiated/failed, User Auth (via VPN Client) initiated/failed, can only be used if the IKE on the Brick® feature is not enabled. (Select **Help > About** to display a screen that shows whether this feature is enabled.) When the IKE on the Brick® feature is enabled, use the VPN Proactive Monitoring trigger instead.*

Task

To configure an LSMS Proactive Monitoring trigger:

- 1 Enter a Trigger Name, select **LSMS Proactive Monitoring** from the **Trigger Type** drop-down list, select an **Alarm Status** (Off or On), then enter an optional **Description** as described in “[Configuring Triggers](#)” (p. 6-3).

- 2 Click **LSMS Promon**.

Figure 6-25 Alarm Trigger Editor LSMS Proactive Monitoring Trigger Parameters



- 3 In the next page of the wizard, shown in [Figure 6-25, “Alarm Trigger Editor LSMS Proactive Monitoring Trigger Parameters”](#) (p. 6-53), enter the parameters that define the conditions of this trigger as the following table explains:

Parameter	Description
Sleep Period	After the initial alarm is generated, this amount of time must elapse before another alarm is generated. Enforces throttling and mitigates flooding the network (e.g., denial-of-service attacks).
Concise Description	If the action associated with this trigger includes Concise Description, this is the message that will be forwarded in the alarm.

Parameter	Description
Explanation	If the action associated with this trigger includes Explanation, this is the message that will be forwarded in the alarm.

4 Click **Thresholds**.

Figure 6-26 Select Threshold Values Window

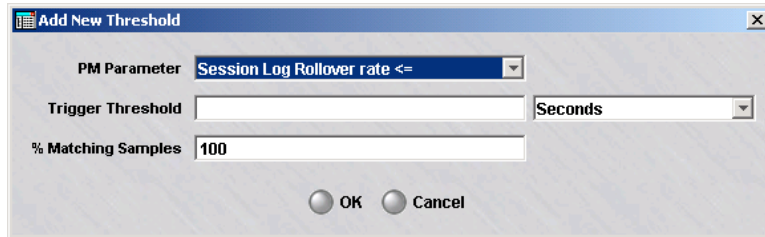


- 5 In the next page of the wizard, shown in [Figure 6-26, “Select Threshold Values Window”](#) (p. 6-54) enter a value for Sampling Period. This is the time period in which the event (as further defined in the next few steps) must occur before the alarm is generated.

The default of 30 seconds equals how often the data is collected by the LSMS and written to the Proactive Monitoring log. The value entered for the Threshold Period determines the number of collections taken.

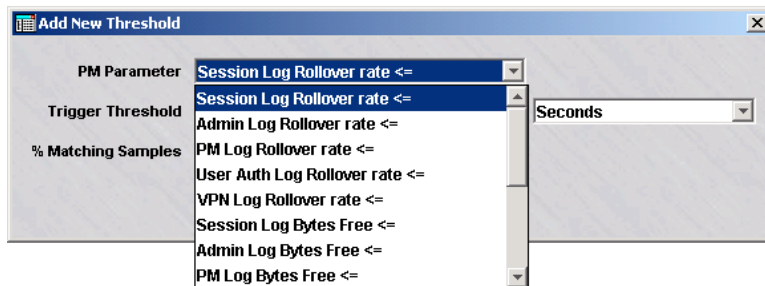
If two minutes is entered as the Sampling Period, then four data collections are taken.

- Right-click in the white box and select **New** from the pop-up menu. The **Add New Threshold** pop-up window appears:



- Select a Proactive Monitoring parameter from the **PM Parameter** drop-down list. This is the condition you want monitored.

Figure 6-27 LSMS Proactive Monitoring Parameters Drop-down List



These are parameters that are collected by the LSMS and include log rollover rates, disk space usage, etc. They are comprehensively described in [“Overview”](#) (p. C-1)

- Enter a Trigger Threshold value for the parameter to be monitored. This is the *normalized* threshold value per the selected unit of measure (per second, minute, hour, etc.).
- In the **% Matching Samples** field, enter a whole number between 0 and 100. This is the percentage of time that the collection interval reaches or exceeds the Trigger Threshold.
- Click **OK**. The parameter now appears in the box. To edit, delete, or create a new parameter, right-click the parameter and select an option from the pop-up menu.

.....
11 Click **Action**.

.....
12 In the last page of the wizard, select at least one action to associate with this trigger and select **Add**. The actions will then be moved to the **Selected** box. Only the actions that have been already configured are displayed.

.....
13 Select **File >Save and Close**.

.....
E N D O F S T E P S
.....



QoS Alarm Triggers

Overview

The following discussion assumes that the reader is familiar with the implementation of Quality of Service (QoS) / Bandwidth Management in the Lucent Security Management Server and the Brick as discussed in *Chapter 2. Brick® Zone Rulesets* in the *LSMS Policy Guide* and *Chapter 4. Configuring Brick™ Ports* in the *LSMS Administration Guide*.

When configuring QoS Alarm triggers, there are two basic aims — to ensure guarantees and limits, and to monitor rule bandwidth usage. These are explained below.

Ensuring Guarantees and Limits

When setting up QoS parameters at the individual rule level or at the zone level, a key consideration for the user community is verifying that bandwidth “guarantees” (minimum packet throughput) and “limits” (maximum packet throughput) are always met. Depending on the QoS configuration and the bandwidth needs of the users, it is possible that resource contention between multiple rules and zones may cause packet throughput to dip below one of the guarantees or exceed a configured limit.

Configuring these QoS Alarm Triggers allows the administrators to be notified for:

- QoS Rule Bandwidth Guarantees Alarm
- QoS Rule Limits Throttling Alarm
- QoS Zone Bandwidth Guarantees Alarm
- QoS Zone Limits Throttling Alarm

Monitoring Rule Bandwidth Usage

Defining QoS guarantees and limits is more of an art than a science. The administrator may need to monitor the bandwidth needs of the users over the long term to determine the most intelligent parameters. Under the TOS/Alarms tab, you may configure bandwidth restrictions and an alarm trigger point *for each rule* if desired. If the “QoS Rule Bandwidth Exceeded Alarm” trigger is active and you have bandwidth restrictions configured in one or more rules, you can receive an alarm any time that bandwidth limit is exceeded.

For example, you may have a rule with a bandwidth limit of 5 MB/sec. But you may want to monitor how frequently your throughput exceeds 3 MB/sec. Depending on the frequency that this alarm is triggered, you can adjust the rule restrictions for the most efficient use of your bandwidth.

As with all alarm triggers on the LSMS, you need to specify minimum criteria such as a trigger name and type, associate at least one action for the trigger and enable it.

While you also define the sleep period for the QOS Alarm triggers, the other

parameters that would cause the alarm to fire are actually part of the individual rules within the Brick zone rulesets or the options used when a zone ruleset is assigned to a Brick port under the Policy Assignment tab of the Brick Editor.



Unauthorized LSMS Login Attempt Trigger

Overview

An Unauthorized LSMS Login Attempt trigger detects when one or more unauthorized attempts to login to the LSMS as an LSMS or Group Administrator occur. A preconfigured Unauthorized LSMS Login Attempt trigger already exists, so you may not need to configure another one. See [“Preconfigured Alarm Triggers and Actions”](#) (p. 4-5) in Chapter 4, [“Introduction to Alarms”](#) for details.

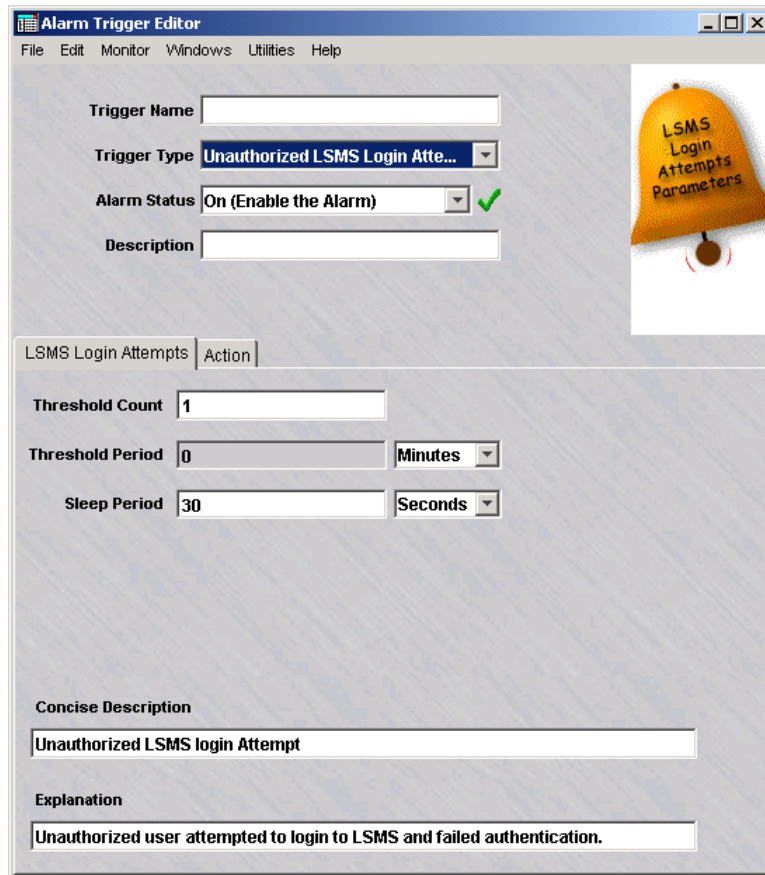
Task

To configure an Unauthorized LSMS Login Attempt trigger:

- 1 Enter a Trigger Name, select Unauthorized LSMS Login Attempt from the **Trigger Type** drop-down list, select an Alarm Status (Off or On), then enter an optional Description as described in [“Configuring Triggers”](#) (p. 6-3).

2 Click **LSMS Login Attempts**.

Figure 6-28 Alarm Trigger Editor Unauthorized Login Attempt Trigger Parameters



3 In the next page of the wizard, shown in [Figure 6-28, “Alarm Trigger Editor Unauthorized Login Attempt Trigger Parameters”](#) (p. 6-60), enter the parameters that define the conditions of this trigger as the following table explains:

Parameter	Description
Threshold Count	The number of events that must be detected before the alarm is generated. This is a required field. If 1 is entered, then Threshold Period is not needed.
Threshold Period	The time period in which the number of events (as set in Threshold Count) must occur before the alarm is generated. This field is only active when Threshold Count is 2 or higher. Both conditions must be true in order to generate the alarm.

Parameter	Description
Sleep Period	After the initial alarm is generated, this amount of time must elapse before another alarm is generated. Enforces throttling and mitigates flooding the network (e.g., denial-of-service attacks).
Concise Description	If the action associated with this trigger includes Concise Description , this is the message that will be forwarded in the alarm.
Explanation	If the action associated with this trigger includes Explanation , this is the message that will be forwarded in the alarm.

.....
4 Click **Action**.

.....
5 In the last page of the wizard, select at least one action to associate with this trigger and select **Add**. The actions will then be moved to the **Selected** box.

Only the actions that have been already configured are displayed.

6 Select **File > Save and Close**.

END OF STEPS



User Authentication Trigger

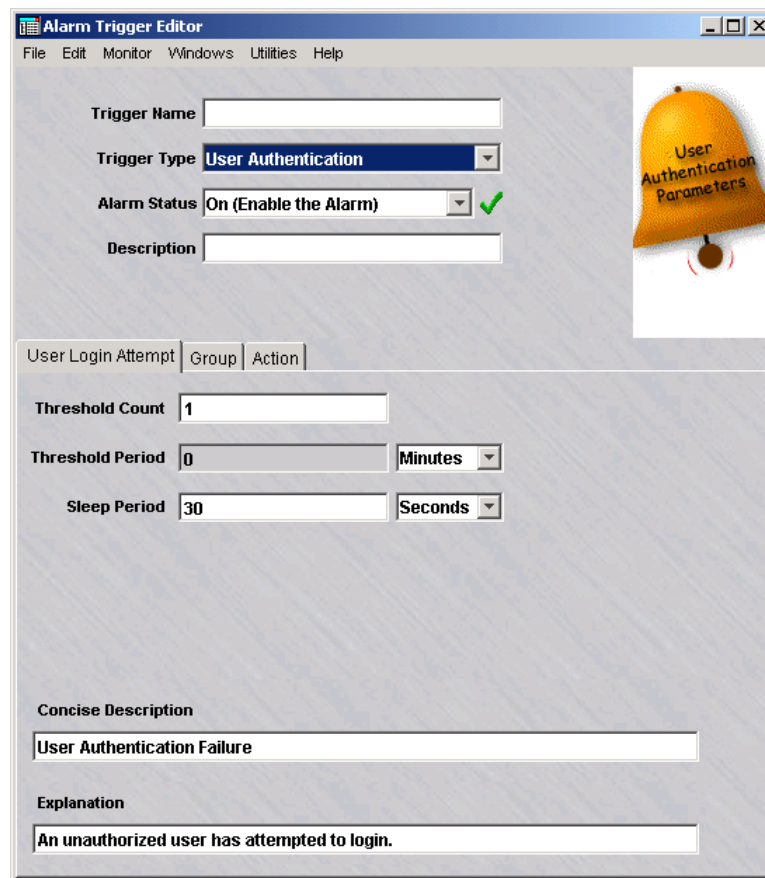
Overview

A User Authentication trigger detects when an attempt to login to the LSMS is made by authorized user fails.

To configure a User Authentication trigger:

- 1 Enter a Trigger Name, select User Authentication from the **Trigger Type** drop-down list, select an **Alarm Status** (Off or On), then enter an optional Description as described in [“Configuring Triggers”](#) (p. 6-3).
- 2 Click **User Login Attempt**.

Figure 6-29 Alarm Trigger Editor User Authentication Trigger Parameters



- 3 In the next page of the wizard, shown in [Figure 6-29, “Alarm Trigger Editor User Authentication Trigger Parameters”](#) (p. 6-62), enter the parameters that define the conditions of this trigger as the following table explains:

Parameter	Description
Threshold Count	The number of events that must be detected before the alarm is generated. This is a required field. If 1 is entered, then Threshold Period is not needed.
Threshold Period	The time period in which the number of events (as set in Threshold Count) must occur before the alarm is generated. This field is only active when Threshold Count is 2 or higher. Both conditions must be true in order to generate the alarm.
Sleep Period	After the initial alarm is generated, this amount of time must elapse before another alarm is generated. Enforces throttling and mitigates flooding the network (e.g., denial-of-service attacks).
Concise Description	If the action associated with this trigger includes Concise Description , this is the message that will be forwarded in the alarm.
Explanation	If the action associated with this trigger includes Explanation , this is the message that will be forwarded in the alarm.

- 4 Click **Group**.

- 5 In the next page of the wizard, select at least one group to associate with this trigger and select **Add**. The groups will then be moved to the **Selected** box.

- 6 Only the groups you have permission to send the alarms to will be displayed.

- 7 Click **Action**.

- 8 In the last page of the wizard, select at least one action to associate with this trigger and select **Add**. The actions will then be moved to the **Selected** box.

Only the actions that have been already configured are displayed.

9 Select **File > Save and Close**.

END OF STEPS



Maintaining Triggers

Overview

Once triggers have been initially configured, you may want to copy a trigger and its defined parameters but give it a different name and edit its parameters. Or, you may want to keep a trigger but temporarily disable it so it is no longer active.

You can also modify certain parameters of an existing trigger, or delete the trigger altogether if it is no longer needed.

Duplicating Triggers

To duplicate a trigger:

- 1 Right-click a trigger in the Contents Panel.
- 2 Select **Duplicate** from the pop-up menu.
- 3 Enter a unique name for the trigger and change any of the other trigger parameters if desired.
- 4 To save the action, click **Finish**.

END OF STEPS

Editing Triggers

To edit a trigger:

- 1 Double-click a trigger in the Contents Panel. The Alarm Trigger Editor appears.
- 2 Make the appropriate changes to the fields on each page of the wizard.
- 3 To save the trigger, click **Finish**.

END OF STEPS

Enabling/Disabling Triggers

When configuring or editing a trigger, you have the ability to dynamically turn them on (enable) or off (disable) in the **Alarm Status** field. The status of an alarm is apparent in the Contents Panel in the **Description** field. If the trigger is enabled, a ► is visible. If the trigger is disabled, an ◀ is visible.

They can also be enabled or disabled if you:

- 1 Right-click a trigger in the Contents Panel.
- 2 Select **Enable** or **Disable** from the pop-up menu.

.....
E N D O F S T E P S
.....

Removing Triggers

To remove a trigger:

- 1 Right-click a trigger in the Contents Panel.
- 2 Select **Delete** from the pop-up menu.
- 3 Select **Yes** in the pop-up window to confirm the deletion.

.....
E N D O F S T E P S
.....



7 Configuring TL1 Alarms

Overview

Purpose

The TL1 Alarms interface allows automated telecommunication maintenance systems, like NMA, to collect *Brick*[®] alarm information from the LSMS using Transaction Language 1 messages. The TL1 Alarms feature is enabled by the Configuration Assistant and certain system-wide parameters are specified there (see *Configuration Assistant in the LSMS Administration Guide*). This section shows how to specify information to allow an NMA host to connect to the LSMS. Entries for up to 12 hosts are allowed.

Contents

Configure TL1 Alarms	7-2
--------------------------------------	-----

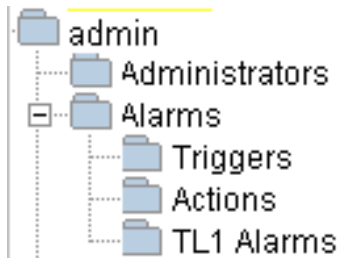
Configure TL1 Alarms

Task

Configure an NMA host interface:

- 1 To define a new TL1 Alarms interface, double-click the Alarms folder in the LSMS Navigator Folder Panel (see Figure 7-1).

Figure 7-1 LSMS Navigator Folder Panel



- 2 Right-click the TL1 Alarms folder and select **New TL1 Alarm**. The TL1 Alarm Wizard appears.

Figure 7-2 TL1 Alarm Wizard

TL1 Alarm Wizard - /

Please select the Action Name, Type and Description.

Action Name

Action Type

Description

< Back Next > Finish Cancel

- 3 Enter a name for the NMA in the **Action Name** field. This is a required field and is displayed in the list of TL1 Alarm interfaces in the Contents Panel. Be as descriptive as possible to make differentiation easy when there are multiple entries in the list.
- 4 Optionally, enter a description for the TL1 Alarm interface in the **Description** field. If a description is entered, it is displayed in the list of TL1 Alarm interfaces in the Contents Panel.

-
- 5 Select **Next** to display the next page of the wizard and enter parameters for the used to authenticate an NMA host connection.

Figure 7-3 TL11 Alarm Wizard - NMA Parameters

TL1 Alarm Wizard-1

Select the NMA Parameters.

NMA IP Address

User ID

Password

Verify Password

< Back Next > Finish Cancel

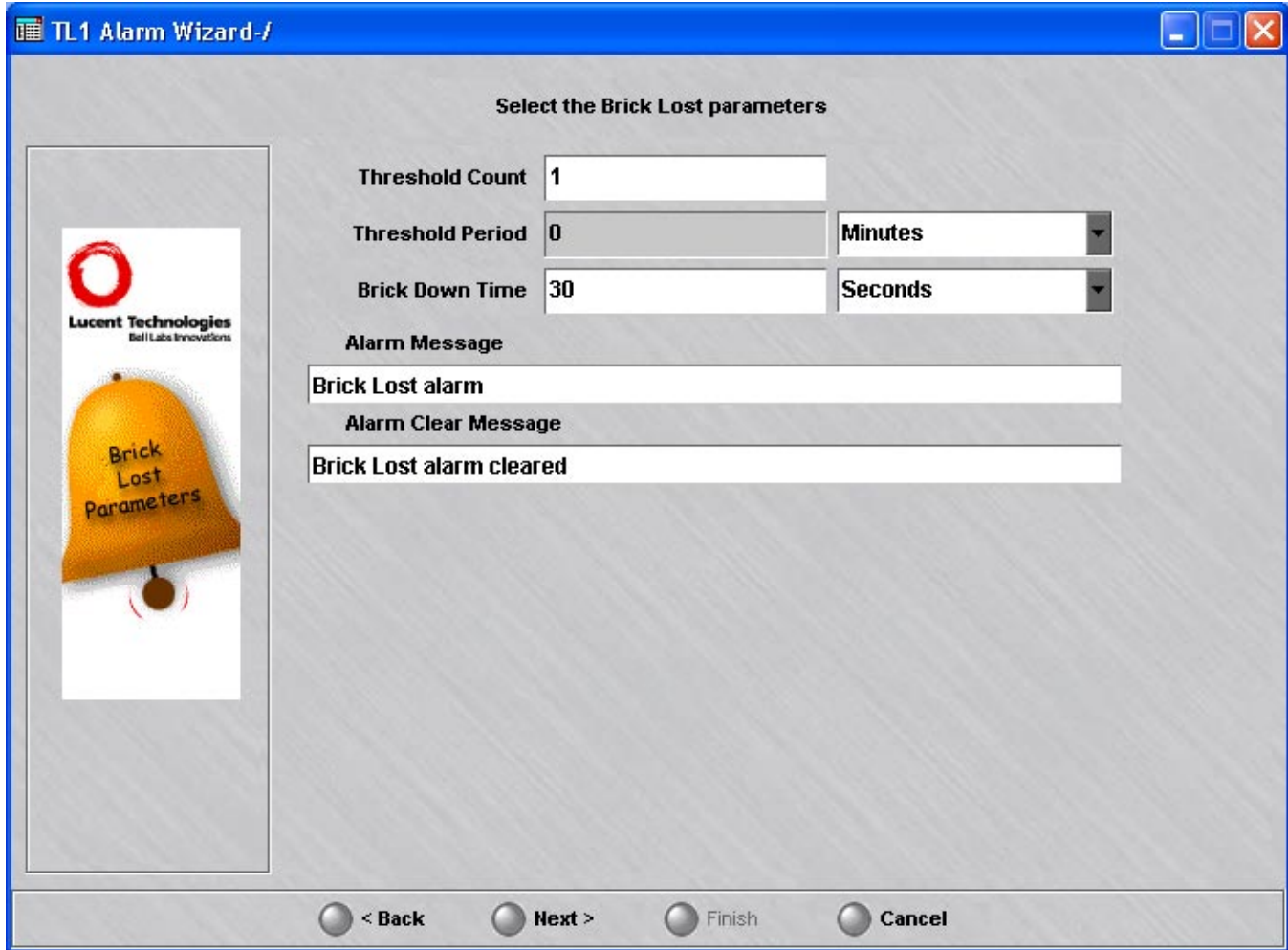
-
- 6 Enter the IP Address of the NMA in the **NMA IP Address** field. When a connection request is detected by the TL1 server, it searches all TL1 Alarm interface configurations looking for an IP address match. If none is found, the connection will be terminated.
 - 7 Enter a User ID for the NMA in the **User ID** field. This parameter is used by the NMA in the UID field of the TL1 ACT-USER authentication command.

-
- 8 Enter a Password for the NMA in the **Password** field. This parameter is used by the NMA in the PID field of the TL1 ACT-USER authentication command.
-
- 9 Re-enter the Password for the NMA in the **Verify Password** field. The actual password is not displayed and is stored in an encrypted format. Telcordia password guidelines are enforced, so at least two non-alpha characters and one special character are required.

The TL1 server expects a valid ACT-USER command to be issued by the NMA after it connects. The host's IP address, User ID, and Password must all match one of the TL1 Alarm interface configurations or the connection will be terminated. If no ACT-USER command is received, the connection is terminated after two minutes.

- 10 Select **Next** to display the next page of the wizard and enter parameters used to configure TL1 Brick Lost alarms.

Figure 7-4 TL11 Alarm Wizard - Brick Lost Parameters



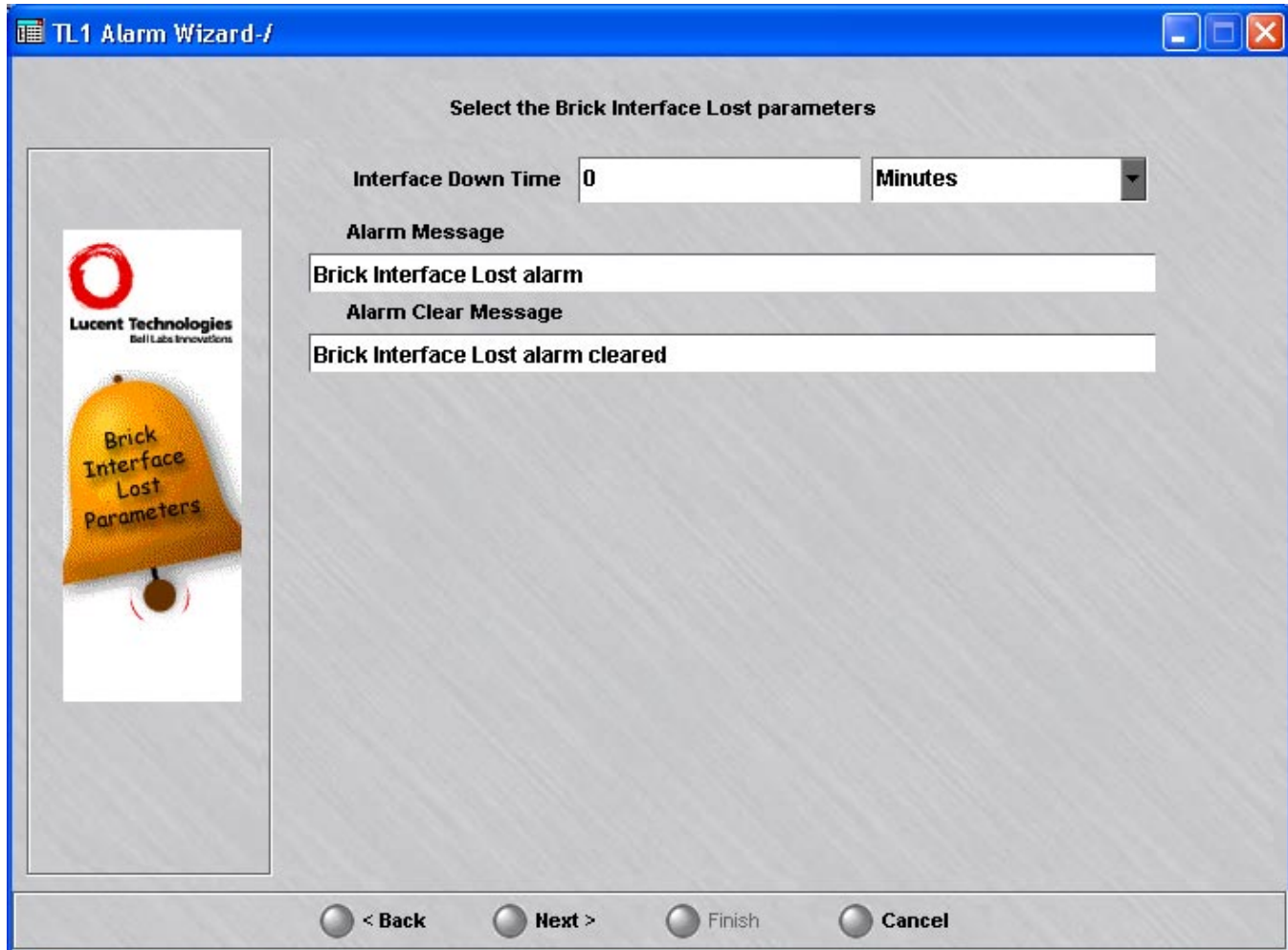
- 11 Enter the Brick Lost Parameters that define the conditions of this TL1 alarm as the following table explains:

Parameter	Description
Threshold Count	The number of events that must be detected before the alarm is generated. This is a required field. If 1 is entered, then Threshold Period is not needed.

Parameter	Description
Threshold Period	The time period in which the number of events (as set in Threshold Count) must occur before the alarm is generated. This field is only active when Threshold Count is 2 or higher. Both conditions must be true in order to generate the alarm.
Brick Down Time	After the initial Brick event is detected, this is amount of time that the Brick must stay down before another alarm is generated. If 0 Hours is specified, the alarm is generated when the first occurrence is detected.
Alarm Message	The Alarm Message field is a detailed text description of the alarm. It is sent to the NMA in the <conddescr> field of the TL1 REPT^ALM^EQPT message.
Alarm Clear Message	The Alarm Clear Message field is a detailed text description of the alarm clear. It is sent to the NMA in the <conddescr> field of the TL! REPT^ALM^EQPT clear message.

- 12 Select **Next** to display the next page of the wizard and enter parameters used to configure TL1 Brick Interface Lost alarms.

Figure 7-5 TL11 Alarm Wizard - Brick Interface Lost Parameters

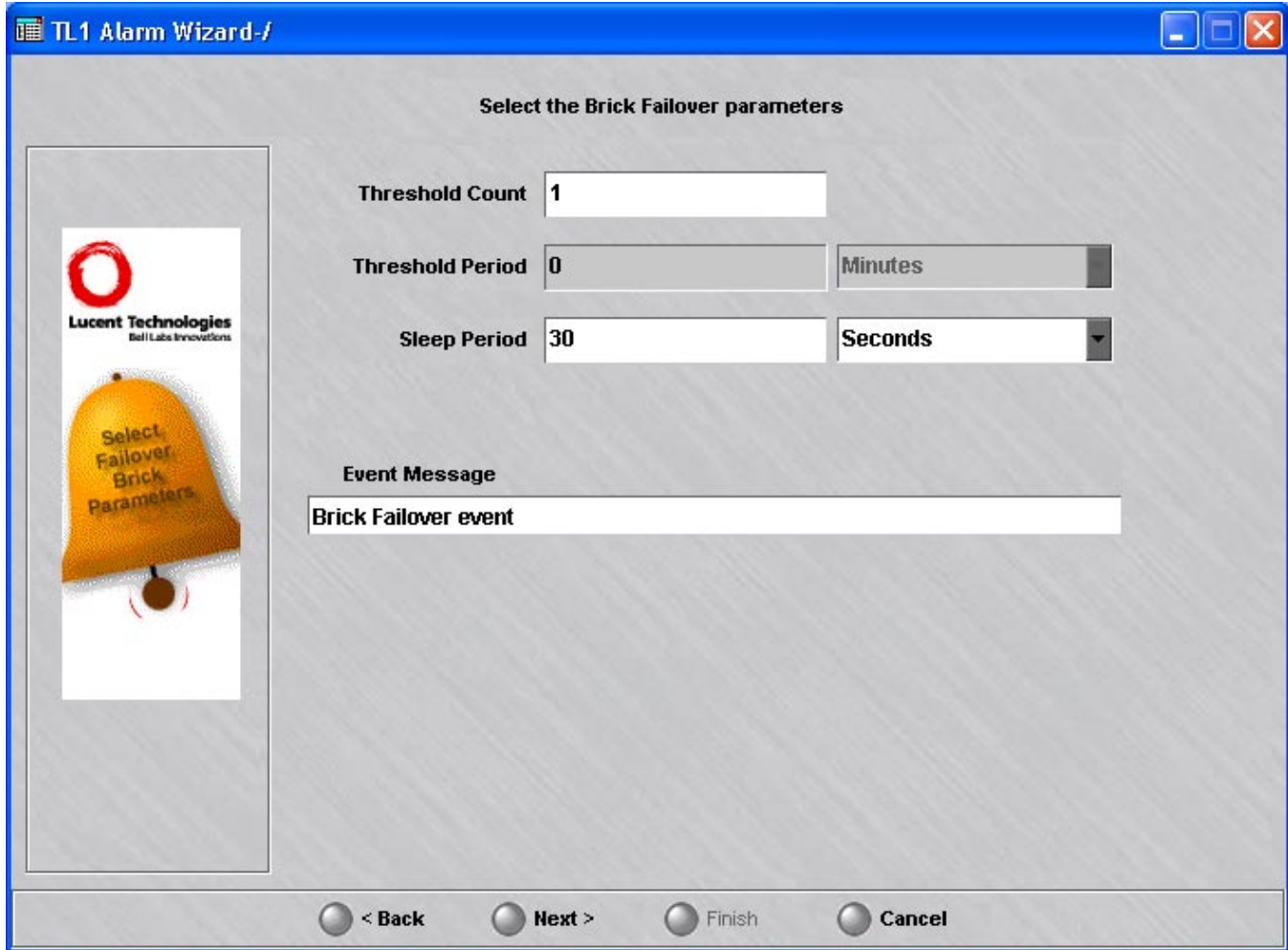


-
- 13** Enter the Brick Interface Lost Parameters that define the conditions of this TL1 alarm as the following table explains:

Parameter	Description
Interface Down Time	<p>After the initial interface event is detected, this is the amount of time that the interface must stay down before another alarm is generated.</p> <p>If 0 Hours is specified, the alarm is generated when the first occurrence is detected.</p>
Alarm Message	<p>The Alarm Message field is a detailed text description of the alarm. It is sent to the NMA in the <conddescr> field of the TL1 REPT^ALM^EQPT message.</p>
Alarm Clear Message	<p>The Alarm Clear Message field is a detailed text description of the alarm clear. It is sent to the NMA in the <conddescr> field of the TL1 REPT^ALM^EQPT clear message.</p>

- 14 Select **Next** to display the next page of the wizard and enter parameters used to configure TL1 Brick Failover events.

Figure 7-6 TL11 Alarm Wizard - Brick Failover Parameters



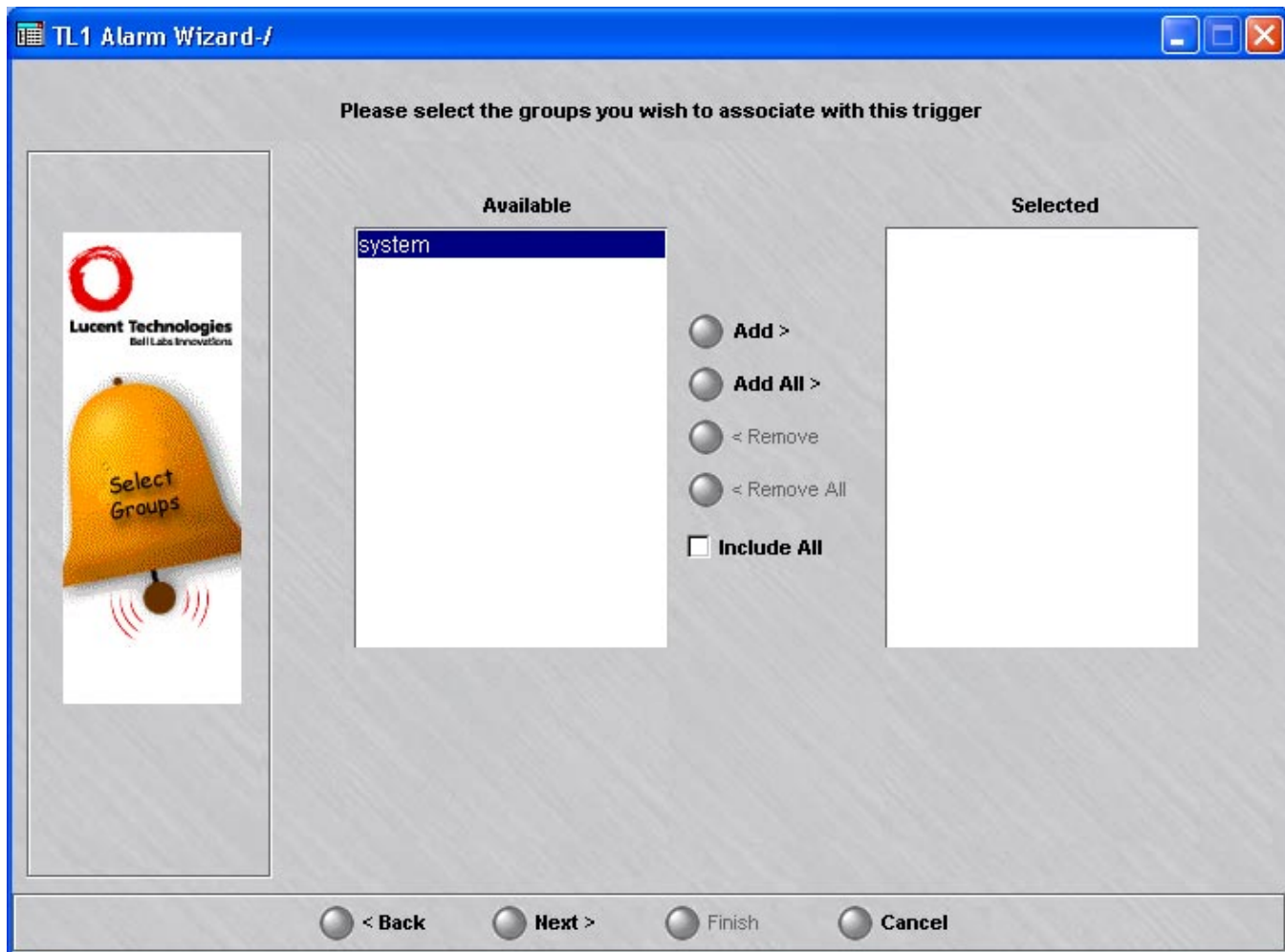
- 15 Enter Brick Failover Parameters that define the conditions of this TL1 event as the following table explains:

Parameter	Description
Threshold Count	The number of events that must be detected before the alarm is generated. This is a required field. If 1 is entered, then Threshold Period is not needed.

Parameter	Description
Threshold Period	The time period in which the number of events (as set in Threshold Count) must occur before the alarm is generated. This field is only active when Threshold Count is 2 or higher. Both conditions must be true in order to generate the alarm.
Sleep Period	After the initial alarm is generated, this amount of time must elapse before another alarm is generated. Enforces throttling and mitigates flooding the network (e.g., denial-of-service attacks).
Event Message	The Event Message field is a detailed description of the alarm clear. It is sent to the NMA in the <conddescr> field of the TL1 REPT^EVT^EQPT message.

- 16 Click **Next**.

Figure 7-7 TL11 Alarm Wizard - Select Group



- 17 On the next page of the wizard, select at least one group to associate with this TL1 Alarm NMA interface and **select** Add. The group(s) will then be moved to the **Selected** box.

- 18 Click **Next**.

Figure 7-8 TL11 Alarm Wizard - Brick Interface Lost Parameters



- 19 On the next page of the wizard, select at least one Brick to associate with this TL1 Alarm NMA interface and select **Add**. Only the Bricks that are in the groups selected on the previous page are displayed. Brick Lost and Brick Interface Lost alarms and Brick Failover events for the selected Bricks will be sent to this NMA host via the TL1 Alarm interface.

- 20 Click **Finish**.

END OF STEPS



8 Introduction to LSMS Reports

Overview

Purpose

LSMS reports provide a useful tool for identifying the nature of firewall and tunnel problems. You can use the LSMS reports Memorize function to build a library of reports to assist in diagnosis of specific kinds of transmission failures.

LSMS Administrators can run reports for any group. Group Administrators can only run reports for groups for which they have at least *View* privileges.

Reports can be run from any machine that is running the LSMS Navigator or Remote Navigator. While reports cannot display real time information, as logs can, they do allow access to the same information as contained in the Historical logs from any location.

You must have a web browser installed on your workstation to view LSMS reports.

Contents

Types of LSMS Reports	8-2
Configuration Assistant Reports Settings	8-3
Report logic	8-5



Types of LSMS Reports

Types of reports

The LSMS provides five types of reports:

- *Administrative Events Report*
The Administrative Events report can be used to monitor network events and, in particular, troubleshoot problems related to routing, LAN-LAN tunnels, and Client-LAN tunnels.
- *Session Log Report*
The Sessions Logged report can be used to monitor traffic on the network, identify potential problem areas, and troubleshoot security operations.
- *Closed Session Details Report*
The Closed Session Details report can be used to monitor traffic on the network, identify potential problem areas, and troubleshoot security operations.
- *Alarms Logged report*
The Alarms Logged report can be used to troubleshoot network problems by tracking and analyzing alarms
- *User Authentication Report*
The User Authentication Report can show all login attempts, successful and unsuccessful. It can show user authentications performed by the local LSMS database, as well as authentications performed by any RADIUS or SecurID servers referenced by the LSMS.
- *VPN Events Report*
The VPN Events Report is used to generate a report for all VPN-related events, such as setting up and taking down of VPN tunnels.

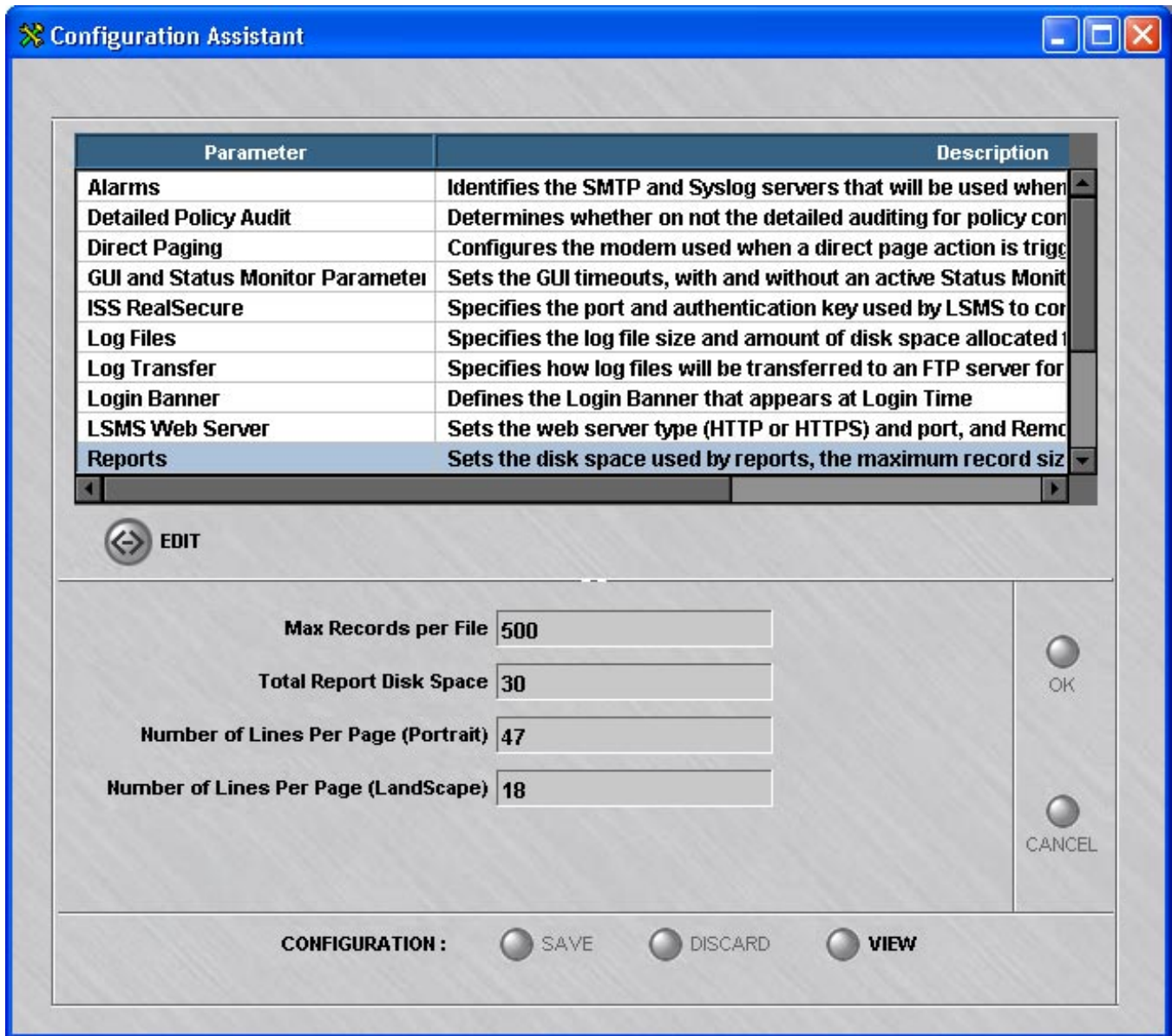
□

Configuration Assistant Reports Settings

Overview

The LSMS Configuration Assistant Reports parameters, shown in [Figure 8-1](#), “[Configuration Assistant Reports Parameters](#)” (p. 8-3), allow you to specify the maximum number of records in a report file and the total amount of disk space to be allocated for reports. They also allow you to set the number of lines per page in both portrait and landscape formats. See *Chapter 10. Using the Configuration Assistant* in the *LSMS Administration Guide* for complete details on reports settings.

Figure 8-1 Configuration Assistant Reports Parameters





Report logic

Input conventions

When using the multi-tabbed panels of each Report Editor to specify the data that is collected for report generation, certain conventions are used:

- If an asterisk (*) is left in a field, no qualifications are made for records for that criteria and is semantically equivalent to leaving it unspecified (blank).
- The ACROSS fields on the Report Editor tabs use AND logic and the WITHIN fields use OR logic. For example, if you specify on the Sessions Log Report the following fields: BrickA, direction IN, and Record Type Begin Session, then all three must be true within a given log record for it to be included in the report output. If you specify more than one Brick device, or more than one Record Type, within each of those records the system employs OR logic; for example, (Brick = = (BrickA OR BrickB) AND (Record Type = = (Begin OR End)) AND (Direction = = IN).



9 Administrative Events Report

Overview

Purpose

The Administrative Events report is an important tool that can be used to monitor network events and, in particular, troubleshoot problems related to LAN-LAN tunnels and Client-LAN tunnels.

The Administrative Events report can be configured to show all events, or just specific types of events that an Administrator is currently interested in.

A few common administrative events are pre-configured with the LSMS, as follows:

- Lucent VPN Firewall *Brick*[®] Errors
- Brick devices and LSMS Logging Connectivity
- Failed Login Attempts
- Successful Admin Logins
- Successful Admin Logouts

Contents

To Generate an Administrative Events Report	9-2
Administrative Events Report Output	9-12



To Generate an Administrative Events Report

When to use

To generate an Administrative Events report, you must display the Administrative Events Report Editor, and then enter selection criteria that will determine the scope and type of the information that is included in the report.

To display the Administrative Events Report Editor

Complete the following steps to display the Administrative Events Report Editor.

1 With the Navigator window displayed, open the **Reports** folder.

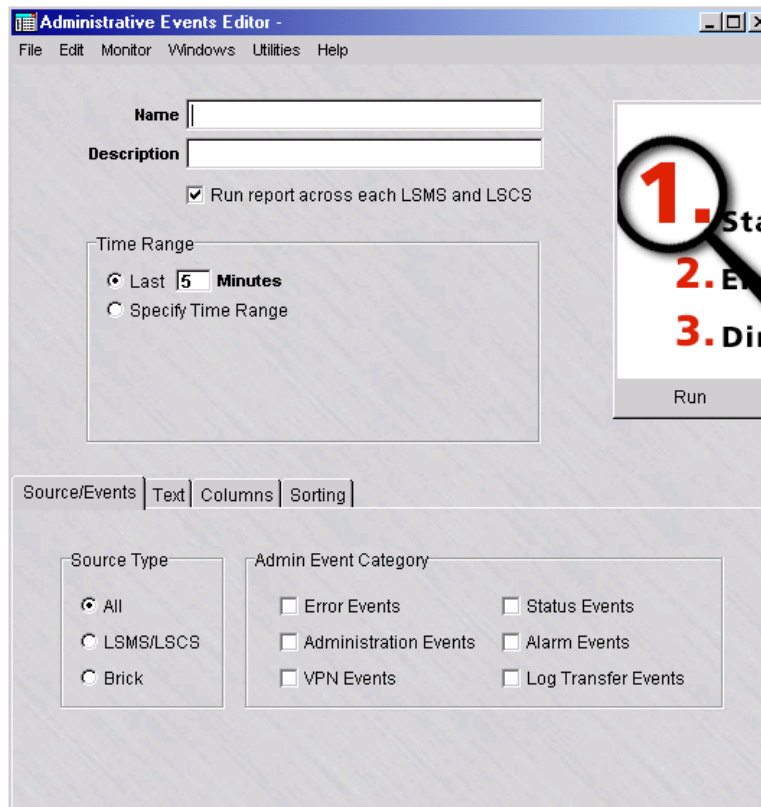
2 Right-click **Administrative Events** and select **New Administrative Events**.

To edit an existing report and its settings, right-click on the report in the list of the Contents panel and choose **Edit** from the pop-up menu.

To view an existing report, and change the Time Range for a previously run report or the checkbox that controls whether you want to run a report across all LSMs for data, right-click on the report in the list of the Contents panel and choose **View** from the pop-up menu.

Result The Administrative Events Report Editor is initially displayed with the Source/Events tab (Figure 9-1, “Administrative Events Report Editor (Source/Events tab)” (p. 9-3)).

Figure 9-1 Administrative Events Report Editor (Source/Events tab)



- 3 In the **Name** field, enter a name for the report file to be created.
- 4 In the **Description** field, enter a textual description of the report. This field is optional.
- 5 Click the **run report across each LSMS and LSCS** checkbox to collect and run a merged report of all network events for all connected LSMSs and Compute Servers. (This checkbox is checked, by default.)

6 Select the time range of the report.

To	Do This
Generate a report of the most recent network events that have occurred within the past 1 to 99 minutes.	Click the Last radio button in the Time Range portion of the window and enter a value (in minutes), up to 99.5 minutes is the default value.
Generate a report for a specific time range with beginning/end dates	Click the Specify Time Range radio button. The Start and End date fields are displayed. Click the Earliest button to select the earliest available date and time and the Now button to select the current date and time, or manually enter the month/day/year and hours/minutes/seconds values in each field.

7 Select the Source Type by selecting the source(s) of the events to be included.

The choices are:

- **All**—to report on all events from all source types
- **LSMS/LSCS**—to report on events and errors generated by the LSMS(s) and Compute Server(s)
- **Brick**—to report on events and errors for the specified Brick(s). When this option is chosen, a **Brick** field is displayed under the radio button. Right-click in this field and choose **Select a Brick**. A Browse window is displayed. Select one or more Bricks from the Bricks folder. Choose **Clear All** to clear the selection(s) made and make new selections. After making your selection(s), click **OK** to close the Browse window and activate your selection(s).

8 Select one or more Event Categories to be included in the report.

Select one or more of the following categories:

- **Error Events**—error messages that originate in the Brick device or the LSMS, such as failed login attempts
- **Administration Events**—events such as logging in or out of the LSMS, Brick zone ruleset modifications, or Brick zone ruleset assignments
- **VPN Events**—all VPN tunnel-related events
- **Status Events**—any status or informational messages generated by the Brick device or LSMS

- **Alarm Events**—information about any alarms that were activated
- **Log Transfer Events**—error messages generated when transferring log files to an FTP server

Important! If you selected **Brick** as the Source Type, only **Error Events**, **Administration Events**, and **VPN Events** are displayed in the Admin Event Category section of the window

END OF STEPS

To enter event text

- 1 Click on the **Text** tab.

Result

The Event Text Search tab is displayed (Figure 9-2, “Administrative Events Editor (Text Search tab)” (p. 9-5)

Figure 9-2 Administrative Events Editor (Text Search tab)

The screenshot shows the 'Administrative Events Editor' window with the 'Text' tab selected. The window has a menu bar with 'File', 'Edit', 'Monitor', 'Windows', 'Utilities', and 'Help'. Below the menu bar, there are input fields for 'Name' and 'Description', and a checked checkbox for 'Run report across each LSMS and LSCS'. A 'Time Range' section contains two radio buttons: 'Last 5 Minutes' (selected) and 'Specify Time Range'. To the right, there is a vertical sidebar with a magnifying glass icon and a list of steps: '1. Sta', '2. E', and '3. Di'. Below the sidebar is a 'Run' button. At the bottom of the window, there are tabs for 'Source/Events', 'Text', 'Columns', and 'Sorting'. The main area contains the text: 'Event records will be included in the report if the text typed below is found anywhere in the event record. Matches are case insensitive.' Below this text is a 'Text Contains:' input field.

-
- 2 To include event records in the report, enter a text string in the **Text Contains** field.
The report will include any event records that contain text matching the text entry. The text search ignores case.

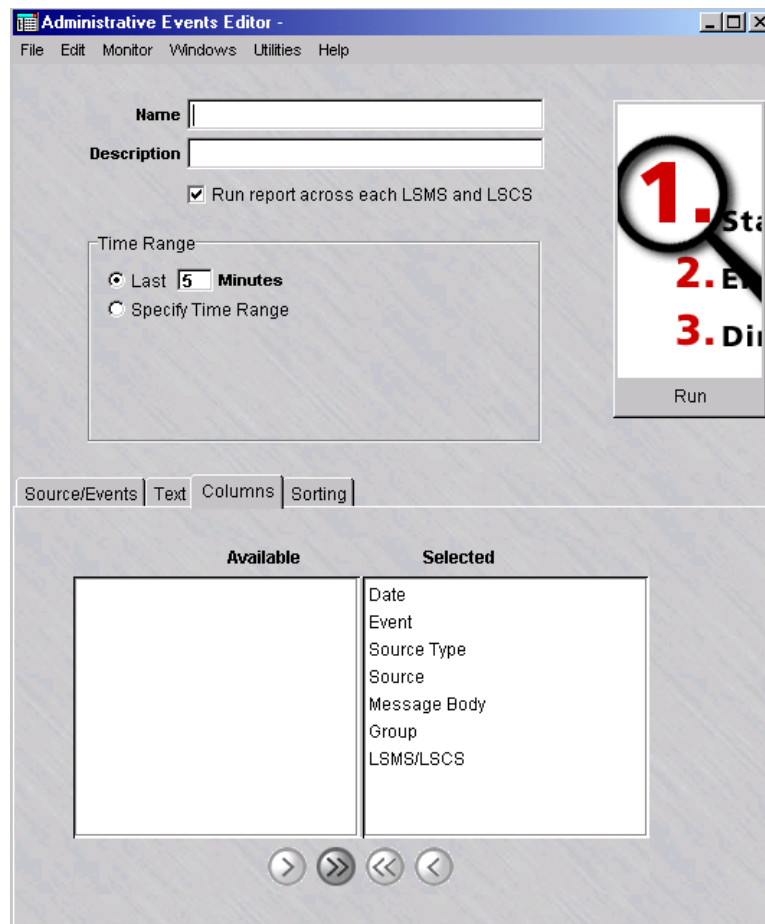
END OF STEPS

To select the columns

- 1 Click on the **Columns** tab.

Result The Columns tab is displayed ([Figure 9-3, “Administrative Events Editor \(Columns tab\)”](#) (p. 9-6)).

Figure 9-3 Administrative Events Editor (Columns tab)



2

To	Do This
Produce a report that contains all data columns	Leave all column names in the Selected portion of the tab. (This is the default.)
Produce a report with selected data column(s)	Use the arrow keys to move column names from the Selected portion to the Available portion of the tab. Only the columns in the Selected portion will be shown in the report. Use the arrow keys to move column names back and forth between the two lists as necessary.

END OF STEPS

To select the order of the report

- 1 Click the **Sorting** tab.

Result The Sorting tab is displayed (Figure 9-4, “Administrative Events Editor (Sorting tab)” (p. 9-8)).

Figure 9-4 Administrative Events Editor (Sorting tab)

The screenshot shows the 'Administrative Events Editor' window with the 'Sorting' tab selected. The interface includes a menu bar (File, Edit, Monitor, Windows, Utilities, Help), a 'Name' text field, a 'Description' text field, a checked checkbox for 'Run report across each LSMS and LSC8', and a 'Time Range' section with radio buttons for 'Last 5 Minutes' (selected) and 'Specify Time Range'. A 'Run' button is visible on the right. Below the main form, there are tabs for 'Source/Events', 'Text', 'Columns', and 'Sorting'. Under the 'Sorting' tab, there is a 'Show output' section with radio buttons for 'Ascending by time' (selected) and 'Descending by time'.

-
- 2 Select the order in which to sort the report output. The default is **Ascending by time** (in chronological order).

END OF STEPS

To save the report

Complete the following steps to save a named copy of the report and its parameter settings.

- 1 In the **Name** field, enter a name for the report.

-
- 2 In the **Description** field, enter a textual description for the report. (This step is optional.)

-
- 3 From the File menu, choose **Save**.

Result The report and its parameter settings are saved and stored in the report folder. The report is saved and can be reused as a template for similar reports when it is duplicated and renamed.

END OF STEPS

To duplicate a report

Complete the following steps to duplicate a report. You can duplicate a report, edit the parameters, and rename as necessary to generate a different report.

-
- 1 Right-click on an existing report in the Contents panel and choose **Duplicate** from the pop-up menu.

Result The initial tab of the Report Editor is displayed.

-
- 2 In the **Name** field, give the report a different name. Edit the parameter fields on the other tabs of the Report Editor, as needed.

-
- 3 From the File menu, choose **Save** to save the duplicated report under its new name.

END OF STEPS

To run the report

Complete the following steps to run the report.

-
- 1 Click the **Run** button. The Run a Report window appears.

Result A dialog window is displayed, indicating that the report is being generated. The window shows the progress of the report generation and the number of records retrieved that match the selected criteria.

If no event records are found that match the selected criteria, a warning dialog box is displayed, indicating that no records have been found and asks if you want to

view the output anyway. Choose **Yes** to view the output anyway or **No** to cancel the report output.

- 2 Close the Administrative Events Editor window and Administrative Events Log browser after viewing the output.

.....
 END OF STEPS

To run multiple reports

Complete the following steps to run multiple reports.

- 1 Right-click on existing reports in the Contents panel and choose **Run Multiple Reports** from the pop-up menu.

Result The Run Multiple Filters window is displayed.

- 2 Click the **run report across each LSMS and LSCS** checkbox to collect and run a merged report of all network events for all connected LSMSs and Compute Servers. (This checkbox is checked, by default.)

- 3 Select the time range of the report.

To	Do This
Generate a report of the most recent network events that have occurred within the past 1 to 99 minutes.	Click the Last radio button in the Time Range portion of the window and enter a value (in minutes), up to 99.5 minutes is the default value.
Generate a report for a specific time range with beginning/end dates	Click the Specify Time Range radio button. The Start and End date fields are displayed. Click the Earliest button to select the earliest available date and time and the Now button to select the current date and time, or manually enter the month/day/year and hours/minutes/seconds values in each field.

- 4 Click the **Run** button. The Run a Report window appears.

Result A dialog window is displayed, indicating that the report is being generated. The window shows the progress of the report generation and the number of records retrieved that match the selected criteria.

If no event records are found that match the selected criteria, a warning dialog box is displayed, indicating that no records have been found and asks if you want to view the output anyway. Choose **Yes** to view the output anyway or **No** to cancel the report output.

-
- 5 Close the Admin Events Editor window and Admin Events browser after viewing the output.

END OF STEPS



Administrative Events Report Output

Overview

The output from an Administrative Events report is displayed in your web browser, and consists of a header and a body in table format with up to six columns of information. [Figure 9-5, “Administrative Events Log Report” \(p. 9-13\)](#) on the next page shows a fragment of a typical Administrative Events report.

The report in [Figure 9-5, “Administrative Events Log Report” \(p. 9-13\)](#) contains all six columns. The administrator generating the report determines the number of columns that appear in the finished report.

The following sections explain the information in the header and in all six columns of the body.

Header

The header of an Administrative Events Log report contains the following information:

- Page Number and Total Number of Pages**
 In the upper right corner of the header, above the title Administrative Events Log, the report indicates the total number of pages in the report, and the number of the current page.
- Source Type**
 On the left margin, below the title Administrative Events Log, the report indicates the names of the event source that are included in the report. This information was determined by the administrator generating the report.

Figure 9-5 Administrative Events Log Report

1 of 1

Administrative Events Log

From: Sat May 27 09:45:43 EDT 2000 To: Wed May 31 09:55:43 EDT 2000

Type **Administrative Events Log**

Body

Type=All

Ascending by: Date

Records Found=8001

Date	Event	Source Type	Source	Message Body	Group
2000/05/27 18:36:42	Error	Brick	1b1_las030	:minos_monitor_sqlnet:3:87:126:Unexpected value found for "bus_type", 0. zone=las030_1b1_2 srcip=195.92.11.10 dstip=135.92.20.90 proto=6 srcpt=20 dstpt=1521-032008043001052012071012090012109001117002126004	
2000/05/27 18:36:42	Error	Brick	1b1_las030	:minos_monitor_sqlnet:3:87:127:Unexpected value found for "bus_type", 56. zone=las030_1b1_2 srcip=195.92.11.10 dstip=135.92.20.90 proto=6 srcpt=20 dstpt=1521-032008043002053012072012091012110001118002127004	
2000/05/27 18:36:42	Error	Brick	1b1_las030	:minos_monitor_sqlnet:3:87:128:Unexpected value found for "bus_type", 178. zone=las030_1b1_2 srcip=195.92.11.10 dstip=135.92.20.90 proto=6 srcpt=20 dstpt=1521-032008043003054012073012092012111001119002128004	

The fields on the Administrative Events Log report are described as follows:

- **Sort Order**

On the left margin, under the Bricks and Brick zone rulesets, the report indicates the order in which the entries in the body are listed. The choices are ascending (i.e., chronological) or descending (i.e., reverse chronological). The administrator generating the report makes the choice.

- **Time Interval**

In the center, under the sort order, the report indicates the time interval covered by the report. This is determined by the administrator when running the report.

- **Total Records**

On the left margin, under the time interval, the report indicates the number of records included in the report, including records collected from the LSMSs, and lists them. It also lists any LSMSs that could not be contacted to retrieve records. The number of entries found in the body of the report is shown. The number of records in the report depends upon how specifically you define the selection criteria when generating the report.

Date Column

The first column in the body of the report is the **Date** column. It gives the date and time the event was recorded in the administrative events log, in the format:

year/month/day

hour:minute:second

Event Column

The **Event** column indicates the type of event.

Source Type Column

The **Source Type** column indicates the source(s) of the event.

The administrator generating the report determines the source(s) that will be included in the report.

Source Column

The **Source** column pinpoints the source (e.g., logger, rap) for the selected source type.

Message Body Column

The **Message Body** column provides additional information about the event. When the Administrative Events report is displayed, a second browser window is launched

behind the report. This window provides a key that explains the contents of the report's Message Body column.

The second browser is launched as a pop-up, which may be suppressed if the browser has pop-up blocking enabled.

Group Column

The **Group** column identifies the group that the session is using.



10 Sessions Logged Report

Overview

Purpose

The Sessions Logged report enables an Administrator to view traffic through one or more Lucent VPN FirewallBricks® during a specified period of time.

The report can be configured to show all traffic through the Brick devices, or just specific types of traffic of interest to the Administrator.

The Sessions Logged report can be used to monitor traffic on the network, identify potential problem areas, and troubleshoot security operations.

Contents

To Generate a Sessions Logged Report	10-2
Sessions Logged Report Output	10-16



To Generate a Sessions Logged Report

When to use

To generate a Sessions Logged report, you must display the Sessions Logged Editor, and then enter selection criteria to determine the scope and type of the information that is included in the report.

To display the Sessions Logged Editor

Complete the following steps to display the Sessions Logged Editor.

1 With the Navigator window displayed, open the **Reports** folder.

2 Right-click the **Sessions Logged** folder and select **New Sessions Logged**.

To edit an existing report and its settings, right-click on the report in the list of the Contents panel and choose **Edit** from the pop-up menu.

To view an existing report, and change the Time Range for a previously run report or the checkbox that controls whether you want to run a report across all LSMSs for data, right-click on the report in the list of the Contents panel and choose **View** from the pop-up menu.

Result The Sessions Logged Editor is initially displayed with the Sessions Logged tab (Figure 10-1, “Sessions Logged Editor (Sessions Logged tab)” (p. 10-3)).

Figure 10-1 Sessions Logged Editor (Sessions Logged tab)

-
- 3 In the **Name** field, enter a name for the report file to be created.

 - 4 In the **Description** field, enter a textual description of the report. This field is optional.

 - 5 Click the **run report across each LSMS and LSCS** checkbox to collect and run a merged report of all network events for all connected LSMSs and Compute Servers. (This checkbox is checked, by default.)

.....

6 Select the time range of the report.

To	Do This
Generate a report of the most recent network events that have occurred within the past 15 to 6099 minutes.	Click the Last radio button in the Time Range portion of the window and enter a value (in minutes), up to 99.5 minutes is the default value.
Generate a report for a specific time range with beginning/end dates	Click the Specify Time Range radio button. The Start and End date fields are displayed. Click the Earliest button to select the earliest available date and time and the Now button to select the current date and time, or manually enter the month/day/year and hours/minutes/seconds values in each field.

.....

END OF STEPS

.....

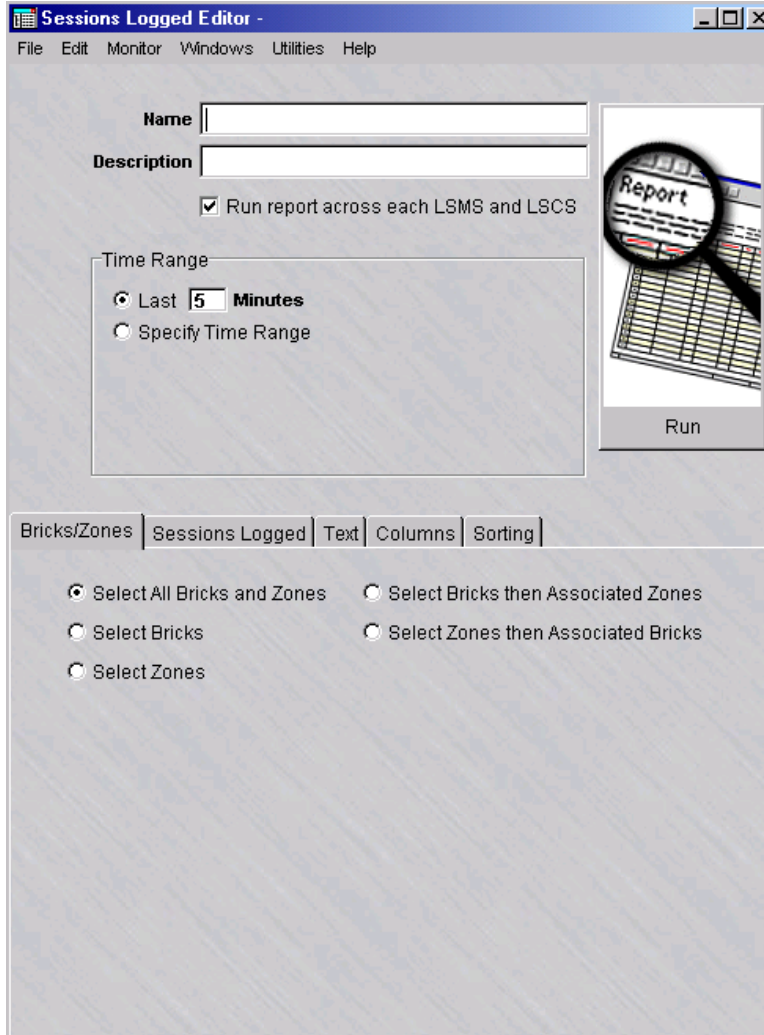
To select the Bricks and Brick zone rulesets

.....

1 Click on the **Bricks/Zones** tab.

Result The Bricks/Zones tab is displayed (Figure 10-2, “Sessions Logged Editor (Bricks/Zones tab)” (p. 10-5)).

Figure 10-2 Sessions Logged Editor (Bricks/Zones tab)



2

To	Do This
Generate a report for all Brick devices and Brick zone rule sets	Click the Select All Bricks and Zones radio button.

To	Do This
Restrict the report to the specified Brick device(s)	Click the Select Bricks radio button. Right-click in the Bricks box and choose Select a Brick from the pop-up menu. In the Browse: Select a Brick window, select the Brick device(s) from the Bricks folder and click OK . Repeat as necessary to add new Brick devices. Right-click and choose Clear Selection from the pop-up menu if you want to clear your selection(s) and make new choices.
Restrict the report to the specified Brick zone ruleset(s)	Click the Select Zones radio button. Right-click in the Zones box and choose Select a Brick Zone Ruleset from the pop-up menu. In the Browse: Select a Brick Zone Ruleset window, select the Brick zone ruleset(s) from the Brick Zone Rulesets folder and click OK . Repeat as necessary to add other Brick zone rulesets. Right-click and choose Clear Selection from the pop-up menu if you want to clear your selection(s) and make new choices.
Restrict the report to the specified Brick device(s) and associated Brick zone ruleset(s).	Click the Select Bricks then Associated Zones radio button. Right-click in the Bricks box and choose Select a Brick from the pop-up menu. In the Browse: Select a Brick window, select the Brick device(s) from the Bricks folder and click OK . Repeat as necessary to add other Brick devices. Right-click and choose Clear Selection from the pop-up menu if you want to clear your selection(s) and make new choices. The Brick zone rulesets that have been assigned to at least one port on the selected Brick device(s) are displayed in the Zones box. Select only the Brick zone ruleset(s) to be included in the report. Press the CTRL key while pressing the left mouse button to select multiple items. Press the Shift key while pressing the left mouse button to select a range of items.

To	Do This
Restrict the report to the specified Brick zone ruleset(s) and associated Brick devices	Click the Select Zones then Associated Bricks radio button. Right-click in the Zones box and choose Select a Brick Zone Ruleset from the pop-up menu. In the Browse: Select a Brick zone Ruleset window, select the Brick zone ruleset to be included in the report and click OK . Repeat as necessary to add other Brick zone rulesets. Right-click and choose Clear Selection from the pop-up menu if you want to clear your selection and choose a different zone ruleset. The Brick device(s) with at least one port assignment for the zone ruleset are displayed in the Bricks box. Select the Brick device(s) to be included in the report. Press the CTRL key while pressing the left mouse button to select multiple items. Press the Shift key while pressing the left mouse button to select a range of items.

.....
E N D O F S T E P S
.....

To select the records

.....

- 1 Click the **Sessions Logged** tab.

Result The Sessions Logged tab is displayed.

Figure 10-3 Sessions Logged Editor (Sessions Logged tab)

-
- 2 In the **Direction** field, filter the report to include only sessions in one direction. Click the down arrow next to the field and choose **IN TO ZONE** or **OUT OF ZONE** from the drop-down list. By default, the report includes sessions in both directions.
-
- 3 In the **Source Host** field, filter the report to include only sessions initiated by a specific source host. Enter either the IP address of the host or click the down arrow next to the field to display a drop-down list and select a host group. Multiple entries can be made, each separated by a comma. An alternate method is to click the **is** button next to the field to change it to **is not**, and then enter an IP address, to include all source hosts except the one entered.

-
- 4 In the **Destination Host** field, filter the report to include only sessions intended for a specific destination host. Enter either the IP address of the host or click the down arrow next to the field to display a drop-down list and select a host group. Multiple entries can be made, each separated by a comma. An alternate method is to click the **is** button next to the field to change it to **is not**, and then enter an IP address, to include all source hosts except the one entered.
-

5

To	Do This
Restrict the report to one or more protocols and ports	Click the Protocols & Ports radio button and enter the IP address of each port in the respective port field. Click the down arrow next to the Protocol field and choose a protocol from the drop-down list or enter the protocol number. If you click the is button next to the field to change it to is not , the report will include all records except for the one entered in the respective field.
Optionally restrict the report to the specified service records	Click the Service radio button. Click the down arrow next to the Service field and choose a service from the drop-down list. If you click the is button next to the field to change it to is not , the report will include all records except for the one entered in the respective field.

.....

END OF STEPS

.....

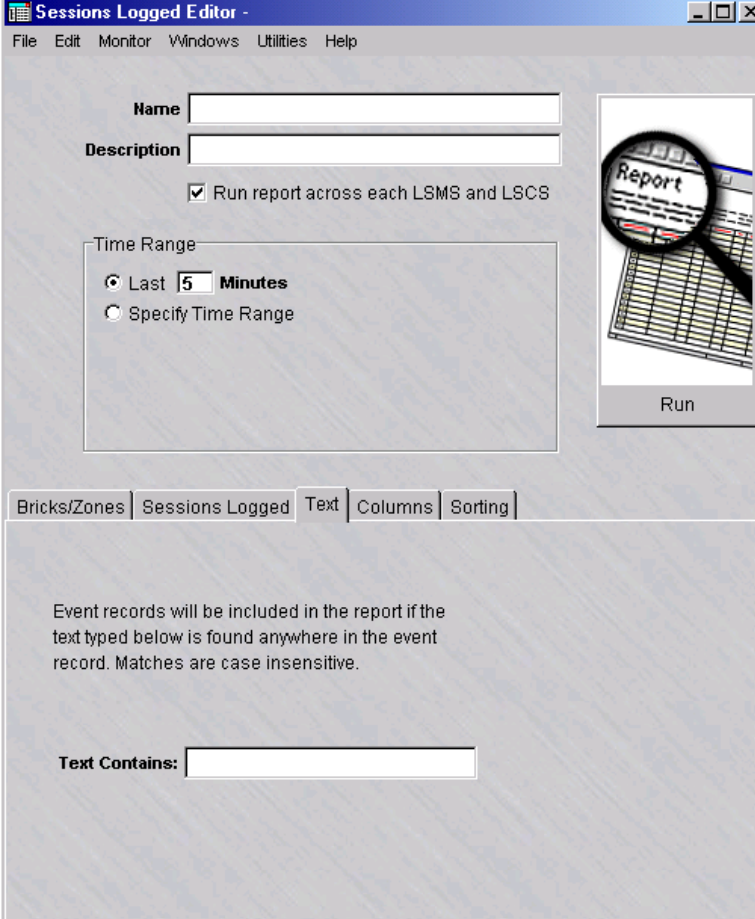
To enter event text

.....

- 1 Click on the **Text** tab.

Result The Event Text Search tab of the Sessions Logged Editor is displayed (Figure 10-4, “Sessions Logged Editor (Text Search tab)” (p. 10-10)).

Figure 10-4 Sessions Logged Editor (Text Search tab)



Sessions Logged Editor -

File Edit Monitor Windows Utilities Help

Name

Description

Run report across each LSMS and LSCS

Time Range

Last Minutes

Specify Time Range

Report

Run

Bricks/Zones Sessions Logged **Text** Columns Sorting

Event records will be included in the report if the text typed below is found anywhere in the event record. Matches are case insensitive.

Text Contains:

-
- 2 To include event records in the report, enter a text string in the **Text Contains** field. The report will include any event records that contain text matching the text entry. The text search ignores case.

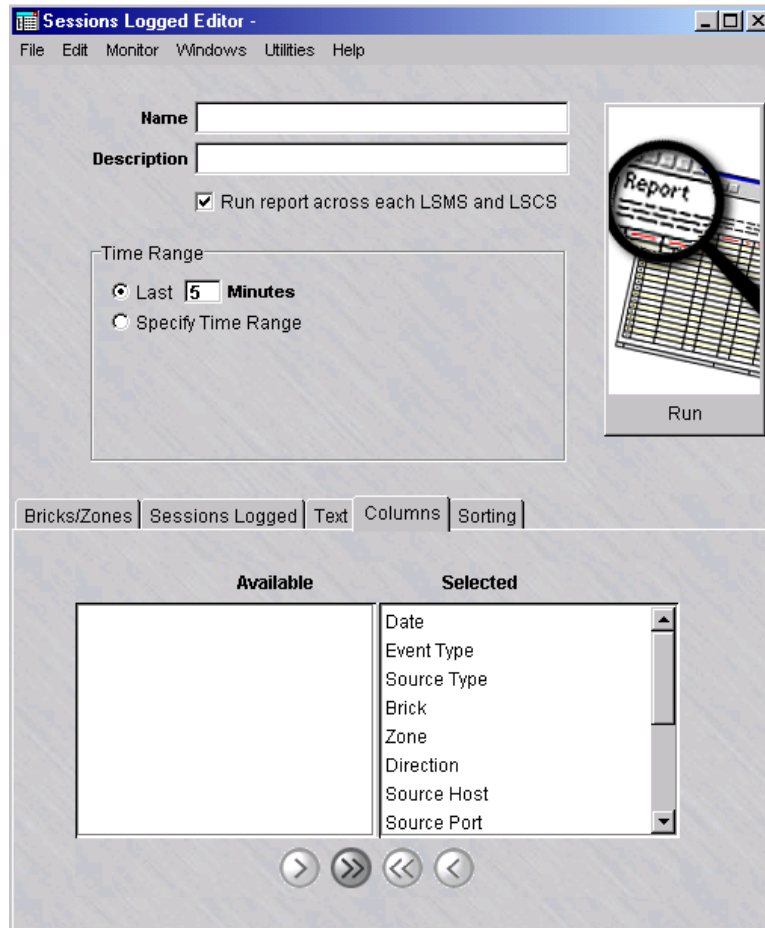
END OF STEPS

To select the columns of the report

- 1 Click on the **Columns** tab.

Result The Columns tab of the Sessions Logged Editor is displayed (Figure 10-5, “Sessions Logged Editor (Columns tab)” (p. 10-11)).

Figure 10-5 Sessions Logged Editor (Columns tab)



2

To	Do This
Produce a report that contains all data columns	Leave all column names in the Selected portion of the tab. (This is the default.)
Produce a report with selected data column(s)	Use the arrow keys to move column names from the Selected portion to the Available portion of the tab. Only the columns in the Selected portion will be shown in the report. Use the arrow keys to move column names back and forth between the two lists as necessary.

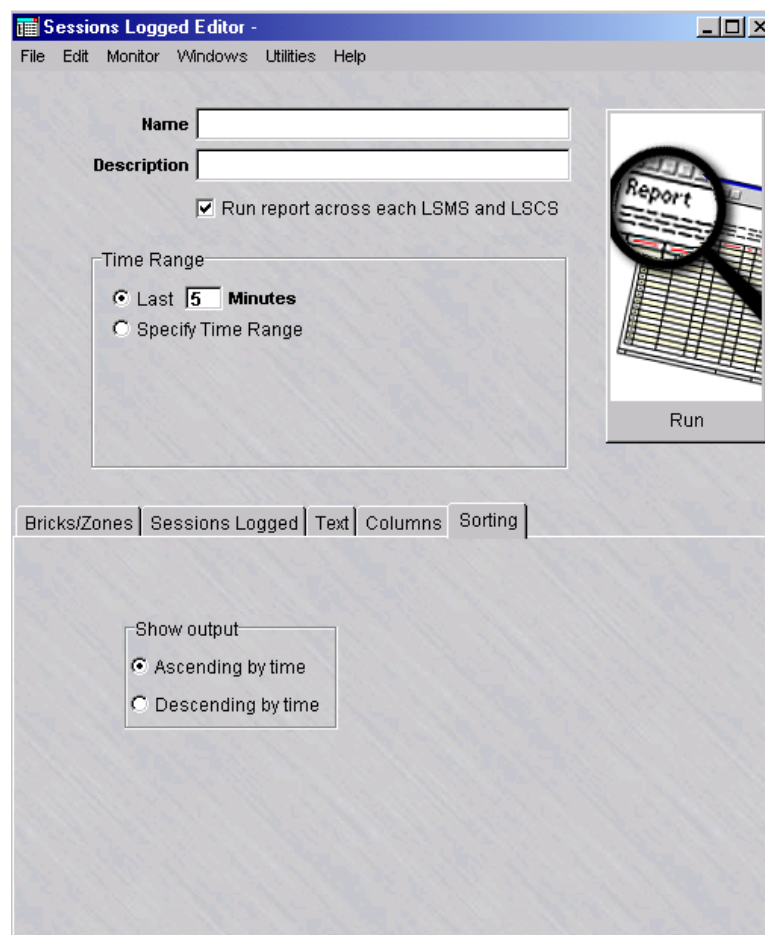
END OF STEPS

To select the order of the report

- 1 Click on the **Sorting** tab.

Result The Sorting tab of the Sessions Logged Editor is displayed (Figure 10-6, “Sessions Logged Editor (Sorting tab)” (p. 10-12)).

Figure 10-6 Sessions Logged Editor (Sorting tab)



- 2 Select the order in which to sort the report output. The default is **Ascending by time** (in chronological order).

END OF STEPS

To save the report

Complete the following steps to save a named copy of the report and its parameter settings.

- 1 In the **Name** field, enter a name for the report.
- 2 In the **Description** field, enter a textual description for the report. (This step is optional.)

- 3 From the File menu, choose **Save**.

Result The report and its parameter settings are saved and stored in the report folder. The report is saved and can be reused as a template for similar reports when it is duplicated and renamed.

END OF STEPS

To duplicate a report

Complete the following steps to duplicate a report. You can duplicate a report, edit the parameters, and rename as necessary to generate a different report.

- 1 Right-click on an existing report in the Contents panel and choose **Duplicate** from the pop-up menu.

Result The initial tab of the Report Editor is displayed.

- 2 In the **Name** field, give the report a different name. Edit the parameter fields on the other tabs of the Report Editor, as needed.

- 3 From the File menu, choose **Save** to save the duplicated report under its new name.

END OF STEPS

To run the report

Complete the following steps to run the report.

- 1 Click the **Run** button. The Run a Report window appears.

Result A dialog window is displayed, indicating that the report is being generated. The window shows the progress of the report generation and the number of records retrieved that match the selected criteria.

If no event records are found that match the selected criteria, a warning dialog box is displayed, indicating that no records have been found and asks if you want to view the output anyway. Choose **Yes** to view the output anyway or **No** to cancel the report output.

-
- 2 Close the Sessions Logged Editor window and Sessions Logged browser after viewing the output.

.....
 END OF STEPS

To run multiple reports

Complete the following steps to run multiple reports.

-
- 1 Right-click on existing reports in the Contents panel and choose **Run Multiple Reports** from the pop-up menu.

Result The Run Multiple Filters window is displayed.

-
- 2 Click the **run report across each LSMS and LSCS** checkbox to collect and run a merged report of all network events for all connected LSMSs and Compute Servers. (This checkbox is checked, by default.)

-
- 3 Select the time range of the report.

To	Do This
Generate a report of the most recent network events that have occurred within the past 1 to 99 minutes.	Click the Last radio button in the Time Range portion of the window and enter a value (in minutes), up to 99.5 minutes is the default value.

To	Do This
Generate a report for a specific time range with beginning/end dates	Click the Specify Time Range radio button. The Start and End date fields are displayed. Click the Earliest button to select the earliest available date and time and the Now button to select the current date and time, or manually enter the month/day/year and hours/minutes/seconds values in each field.

-
- 4 Click the **Run** button. The Run a Report window appears.

Result A dialog window is displayed, indicating that the report is being generated. The window shows the progress of the report generation and the number of records retrieved that match the selected criteria.

If no event records are found that match the selected criteria, a warning dialog box is displayed, indicating that no records have been found and asks if you want to view the output anyway. Choose **Yes** to view the output anyway or **No** to cancel the report output.

-
- 5 Close the Sessions Logged Editor window and Sessions Logged browser after viewing the output.

END OF STEPS



Sessions Logged Report Output

Overview

The output from a Sessions Logged report is displayed in your web browser, and consists of a header and a body in table format with up to 14 columns of information. [Figure 11-9, “Closed Session Details Report \(Part A\)” \(p. 11-24\)](#) on the next page shows a fragment of a typical Sessions Logged report.

The report in [Figure 11-9, “Closed Session Details Report \(Part A\)” \(p. 11-24\)](#) contains all 14 columns. The administrator generating the report determines the number of columns that appear in the finished report.

The following sections explain the information in the header and in all 14 columns of the body.

Important! COLORS

All Begin Session entries in the Sessions Logged report appear in green or red.

The colors are defined as follows:

- Green = a session that has been passed by the Brick device.
- Red = a session that has been dropped by the Brick device.

Header

The header of a Sessions Logged report contains the following information:

- *Page number and total number of pages*
In the upper right corner of the header, above the title Sessions Log, the report indicates the total number of pages in the report, and the number of the current page.
- *Bricks and Brick zone rulesets*
On the left margin, below the title Sessions Log, the report indicates the names of the Bricks and Brick zone rulesets that are included in the report. This information was determined by the administrator generating the report.
- *Sort order*
On the left margin, under the Bricks and Brick zone rulesets, the report indicates the order in which the entries in the body are listed. The choices are ascending (i.e., chronological) or descending (i.e., reverse chronological). The administrator generating the report makes the choice.

- *Time interval*
In the center, under the sort order, the report indicates the time interval covered by the report. This is determined by the administrator when running the report.
- *Total records*
On the left margin, under the time interval, the report indicates the number of records included in the report. This is the number of entries found in the body of the report. The number of records in the report depends upon how specifically you define the selection criteria when generating the report.

Date Column

The first column in the body of the report is the Date column. It gives the date and time the record was created in the sessions log, in the format:

year/month/day

hour:minute:second

Event Column

The **Event** column indicates the type of record. The Sessions Logged report can include the following four record types:

- Begin session records
- End session records
- Mapped session records (indicating network address translation)
- IPsec records (indicating a VPN).

The administrator generating the report determines which types of records will be included in the report.

Source Type Column

In the current release, the **Source Type** is always **Brick**. In future releases, additional source types may be supported.

Brick Column

The **Brick** column indicates the name of the Brick that passed or dropped the session and produced this record.

The administrator generating the report determines the Brick devices to be included in the report.

Zone Column

The **Zone** column indicates the name of the Brick zone ruleset whose security policy caused the Brick to pass or drop the session. The Brick zone ruleset must be assigned to a port on the Brick.

The administrator generating the report determines the Brick zone rulesets to be included in the report.

Dir Column

The **Dir** column gives the direction of the session, vis a vis the Brick zone ruleset. The alternatives are:

- IN (the session originated outside the Brick zone ruleset and is intended for a destination IP address in the Brick zone ruleset), or
- OUT (the session originated in the Brick zone ruleset and is intended for a destination IP address outside the Brick zone ruleset).

The administrator generating the report can include sessions in both directions, or choose one of the two directions.

Src Host Column

The **Src Host** column provides the IP address of the source host. This is the host that initiated the session.

The administrator generating the report determines which source hosts will be included in the report.

Src Port Column

The **Src Port** column gives the source port. This is the port used by the application on the source host that initiated the session.

The administrator generating the report determines which source ports will be included in the report.

Dst Host Column

The **Dst Host** column provides the IP address of the destination host. This is the host that is intended to receive the session.

The administrator generating the report determines which destination hosts will be included in the report.

Dst Port Column

The **Dst Port** column gives the destination port. This is the port used by the application on the destination to receive the session.

The administrator generating the report determines which destination ports will be included in the report.

Pcol Column

The **Pcol** column indicates the protocol that the session is using. The options are UDP, TCP or ICMP.

The administrator generating the report determines which protocols will be included in the report.

Service Column

The **Service** column indicates the service (Dest Port/Src Port/Protocol) that the session is using. Examples are bootps, netbios-gm, netbios-ns.

The administrator generating the report determines which services will be included in the report.

Message Body Column

The **Message Body** column provides additional information about the session.

When the Sessions Logged report is displayed, a second browser window is launched behind the report. This window provides a key that explains the contents of the report's Message Body column.

Group Column

The **Group** column identifies the group that the session is using.



11 Closed Session Details Report

Overview

Purpose

The Closed Session Details report enables an Administrator to view traffic through one or more Lucent VPN FirewallBricks® during a specified period of time. It only shows closed sessions, not active ones.

The report can be configured to show all traffic through the Bricks devices, or just specific types of traffic that the Administrator is currently interested in.

The Closed Session Details report can be used to monitor traffic on the network, identify potential problem areas, and troubleshoot security operations.

Filter criteria can be expanded to every field of the combined Begin/End record. In contrast to the Sessions Logged Report, a greater variety of columns can be chosen for the output, including the duration of the sessions. Sorting by fields other than the Start Time is supported.

The LSMS is shipped with the following pre-configured reports in this category:

- Drops by Rule 65535
- Unauthorized Brick Connection Attempts

Contents

To Generate a Closed Session Details Report	11-2
Closed Session Details Report Output	11-23



To Generate a Closed Session Details Report

When to use

To generate a Closed Session Details report, you must display the Closed Session Details Report Editor, then enter selection criteria that will determine the scope and type of the information that is included in the report.

To display the Closed Session Details Editor

Complete the following steps to display the Closed Session Details Editor.

- 1 With the Navigator window displayed, open the **Reports** folder.

- 2 Right-click the **Closed Session Details** folder and select **New Closed Session Details**.

To edit an existing report and its settings, right-click on the report in the list of the Contents panel and choose **Edit** from the pop-up menu.

To view an existing report, and change the Time Range for a previously run report or the checkbox that controls whether you want to run a report across all LSMs for data, right-click on the report in the list of the Contents panel and choose **View** from the pop-up menu.

Result The Closed Session Details Editor is initially displayed with the Hosts tab (Figure 11-1, “Closed Session Details Editor (Host tab)” (p. 11-3)).

Figure 11-1 Closed Session Details Editor (Host tab)

.....

- 3 In the **Name** field, enter a name for the report file to be created.
-
- 4 In the **Description** field, enter a textual description of the report. This field is optional.
-
- 5 Click the **run report across each LSMS and LSCS** checkbox to collect and run a merged report of all network events for all connected LSMSs and Compute Servers. (This checkbox is checked, by default.)

6 Select the time range of the report.

To	Do This
Generate a report of the most recent network events that have occurred within the past 1 to 99 minutes.	Click the Last radio button in the Time Range portion of the window and enter a value (in minutes), up to 99.5 minutes is the default value.
Generate a report for a specific time range with beginning/end dates	Click the Specify Time Range radio button. The Start and End date fields are displayed. Click the Earliest button to select the earliest available date and time and the Now button to select the current date and time, or manually enter the month/day/year and hours/minutes/seconds values in each field.

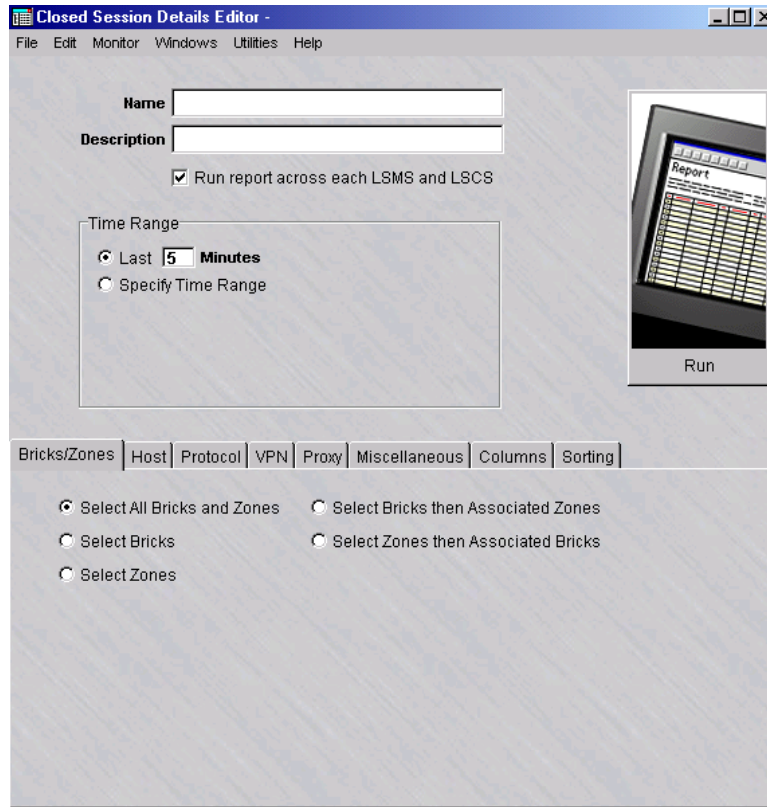
END OF STEPS

To select the Brick devices and zone rulesets

- 1 Click on the **Bricks/Zones** tab.

Result The Bricks/Zones tab of the Closed Session Details Editor is displayed (Figure 11-2, “Closed Session Details Editor (Bricks/Zones tab)” (p. 11-5)).

Figure 11-2 Closed Session Details Editor (Bricks/Zones tab)



2

To	Do This
Generate a report for all Brick devices and Brick zone rulesets	Click the Select All Bricks and Zones radio button.
Restrict the report to the specified Brick device(s)	Click the Select Bricks radio button. Right-click in the Bricks box and choose Select a Brick from the pop-up menu. In the Browse: Select a Brick window, select the Brick device(s) from the Bricks folder and click OK . Repeat as necessary to add other Bricks. Right-click and choose Clear Selection from the pop-up menu if you want to clear your selection(s) and make new choices.

To	Do This
<p>Restrict the report to the specified Brick zone ruleset(s)</p>	<p>Click the Select Zones radio button. Right-click in the Zones box and choose Select a Brick Zone Ruleset from the pop-up menu. In the Browse: Select a Brick Zone Ruleset window, select the Brick zone ruleset(s) from the Brick Zone Rulesets folder and click OK. Repeat as necessary to add other Brick zone rulesets. Right-click and choose Clear Selection from the pop-up menu if you want to clear your selection(s) and make new choices.</p>
<p>Restrict the report to the specified Brick device(s) and associated Brick zone ruleset(s).</p>	<p>Click the Select Bricks then Associated Zones radio button. Right-click in the Bricks box and choose Select a Brick from the pop-up menu. In the Browse: Select a Brick window, select the Brick device(s) from the Bricks folder and click OK. Repeat as necessary to add other Brick devices. Right-click and choose Clear Selection from the pop-up menu if you want to clear your selection(s) and make new choices. The Brick zone rulesets that have been assigned to at least one port on the selected Brick device(s) are displayed in the Zones box. Select only the Brick zone ruleset(s) to be included in the report. Press the CTRL while pressing the left mouse button to select more than one item at a time. Press the Shift key while pressing the left mouse button to select a range of items.</p>

To	Do This
Restrict the report to the specified Brick zone ruleset(s) and associated Brick devices	Click the Select Zones then Associated Bricks radio button. Right-click in the Zones box and choose Select a Brick Zone Ruleset from the pop-up menu. In the Browse: Select a Brick zone Ruleset window, select the Brick zone ruleset to be included in the report and click OK . Right-click and choose Clear Selection from the pop-up menu if you want to clear your selection and choose a different zone ruleset. The Brick device(s) with at least one port assignment for the zone ruleset are displayed in the Bricks box. Select the Brick device(s) to be included in the report. Press the CTRL while pressing the left mouse key to select more than one item at a time. Press the Shift key while pressing the left mouse button to select a range of items.

END OF STEPS

To select the hosts

Complete the following steps to choose the source and destination hosts to be included in the report.

- 1 Click on the **Host** tab.

Result The Host tab of the Closed Session Details Editor is displayed (Figure 11-3, “Closed Session Details Editor (Host tab)” (p. 11-8)).

Figure 11-3 Closed Session Details Editor (Host tab)

The screenshot shows the 'Closed Session Details Editor' window with the 'Host' tab selected. The interface includes a menu bar (File, Edit, Monitor, Windows, Utilities, Help), input fields for 'Name' and 'Description', a checked checkbox for 'Run report across each LSMS and LSCS', and a 'Time Range' section with radio buttons for 'Last 5 Minutes' (selected) and 'Specify Time Range'. Below these are tabs for 'Bricks/Zones', 'Host', 'Protocol', 'VPN', 'Proxy', 'Miscellaneous', 'Columns', and 'Sorting'. The 'Host' tab contains four filter fields: 'Source Host', 'Destination Host', 'Mapped Source Host', and 'Mapped Destination Host'. Each field has an 'is' button and a text input field with an asterisk. A 'Run' button is located at the bottom right of the window.

- 2** In the **Source Host** field, filter the report to include only sessions initiated by a specific source host. Enter either the IP address of the host or click the down arrow next to the field to display a drop-down list and select a host group. An alternate method is to click the **is** button next to the field to change it to **is not**, and then enter an IP address, to include all source hosts except the one entered.
- 3** In the **Destination Host** field, filter the report to include only sessions intended for a specific destination host. Enter either the IP address of the host or click the down arrow next to the field to display a drop-down list and select a host group. An alternate method is to click the **is** button next to the field to change it to **is not**, and then enter an IP address, to include all source hosts except the one entered.

-
- 4 In the **Mapped Source Host** field, filter the report to include only Brick zone rulesets that are using Network Address Translation (NAT) and are mapped to specific source hosts. Mapped hosts are the IP addresses that the source IPs in the incoming packet are mapped to by the Brick device. Enter either the IP address of the host or click the down arrow next to the field to display a drop-down list and select a host group. An alternate method is to click the **is** button next to the field to change it to **is not**, and then enter an IP address, to include all source hosts except the one entered.

If you do not make an entry in this field, the report includes all mapped hosts.

-
- 5 In the **Destination Source Host** field, filter the report to include only Brick zone rulesets that are using NAT and are mapped to specific destination hosts. Mapped hosts are the IP addresses that the destination IPs in the outgoing packet are mapped to by the Brick device. Enter either the IP address of the host or click the down arrow next to the field to display a drop-down list and select a host group. An alternate method is to click the **is** button next to the field to change it to **is not**, and then enter an IP address, to include all source hosts except the one entered.

If you do not make an entry in this field, the report includes all mapped hosts.

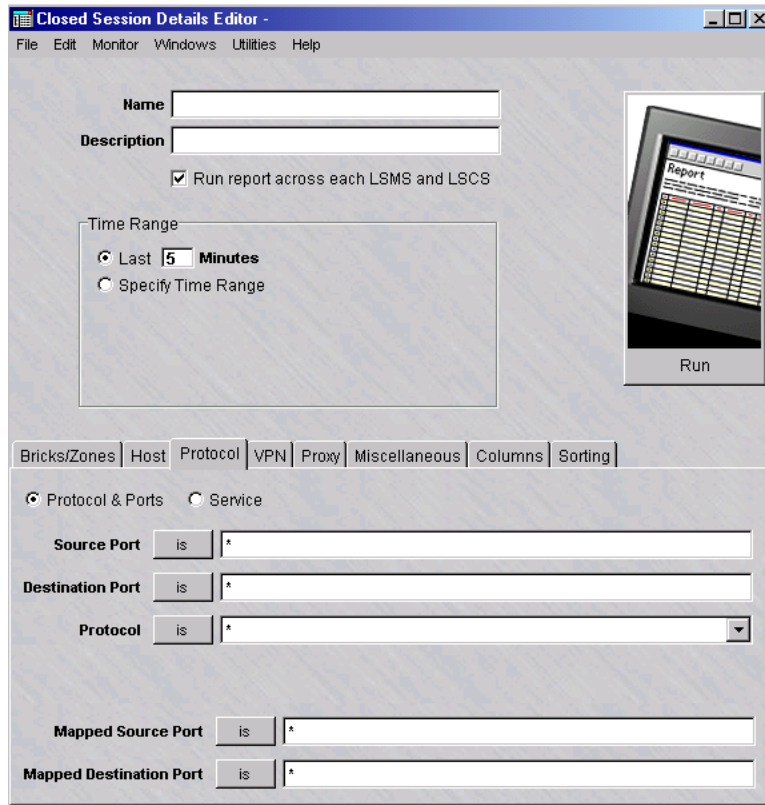
END OF STEPS

To select the ports and protocols

- 1 Click on the **Protocol** tab.

Result The Protocol tab of the Closed Session Details Editor is displayed (Figure 11-4, “Closed Session Details Editor (Protocol tab)” (p. 11-10)).

Figure 11-4 Closed Session Details Editor (Protocol tab)



2

To	Do This
Optionally restrict the report to one or more protocols and ports	Click the Protocols & Ports radio button and enter the IP address of each port in the respective port field. Click the down arrow next to the Protocol field and choose a protocol from the drop-down list, or enter the protocol number. If you click the is button next to the field to change it to is not , the report will include all records except for the one entered in the respective field.

To	Do This
Optionally restrict the report to the specified service records	Click the Service radio button. Click the down arrow next to the Service field and choose a service from the drop-down list. If you click the is button next to the field to change it to is not , the report will include all records except for the one entered in the respective field.

.....
E N D O F S T E P S

To enter VPN information

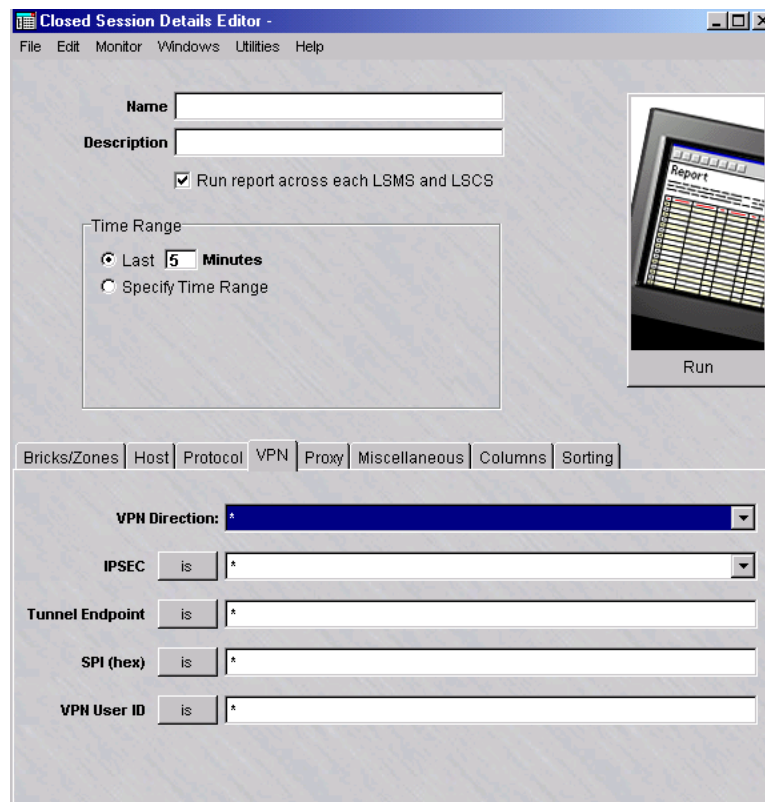
Complete the following steps to filter session details for encrypted tunnel traffic in the report.

.....

- 1 Click the **VPN** tab.

Result The VPN tab of the Closed Session Details Editor is displayed (

Figure 11-5 Closed Session Details Editor (VPN tab)



-
- 2 To include only sessions of a specific direction, click the down arrow next to the **VPN Direction** field and select the direction from the drop-down list.

The choices are:

- **Forward**—initial session from the source host to the destination host
- **Reverse**—return session from the destination host back to the source host

-
- 3 To filter the report by IPsec mode, click the down arrow next to the **IPSEC** field and select the IPsec mode to be used as filtering criteria for the report. An alternate method is to click the **is** button next to the field to change it to **is not** and select an IPsec mode from the drop-down list. The report will include sessions using all modes *except* for the one entered.

-
- 4 To filter the report by tunnel endpoint, which is the Virtual Brick Address (VBA) assigned to the Brick zone ruleset that contains the destination IP address of the

session, enter the IP address of the tunnel endpoint in the **Tunnel Endpoint** field. An alternate method is to click the **is** next to the field to change it to **is not** and enter an endpoint IP address. The report will include sessions using all tunnel endpoints *except* for the one entered. If you do not make an entry in this field, the report includes sessions from all tunnel endpoints.

- 5 To filter the report by Security Parameter Index (SPI) used in a VPN session, enter the SPI in the **SPI (hex)** field. An alternate method is to click the **is** next to the field to change it to **is not** and enter an SPI. The report will include sessions using all SPIs *except* for the one entered. If you do not make an entry in this field, the report includes sessions from all SPIs.
-

- 6 To filter the report by VPN User ID (the ID of the person who uses the IPSec Client program to set up the tunnel), enter the VPN User ID in the **VPN User ID** field. An alternate method is to click the **is** next to the field to change it to **is not** and enter a VPN User ID. The report will include sessions using all VPN User IDs *except* for the one entered. If you do not make an entry in this field, the report includes sessions for all VPN User IDs.

END OF STEPS

To enter proxy information

Complete the following steps to filter the report for sessions generated by clients running the Lucent Proxy Agent (LPA) software. This tab is only relevant and report information is only available if you are running the LPA software. If not, this tab should can be skipped.

- 1 Click on the **Proxy** tab.

Result The Proxy tab of the Closed Session Details Editor is displayed (Figure 11-6, “Closed Session Details Editor (Proxy tab)” (p. 11-14)).

Figure 11-6 Closed Session Details Editor (Proxy tab)

-
- 2 To filter the report by the reflection type for packets sent from the Brick device to the proxy server and forwarded to the client server, click the down arrow next to the **Reflection Type** field and make a choice from the drop-down list.

The choices are:

- **Single**—include packets that are sent from the Brick device to the proxy server and then directly to the requesting server
- **Dual**—include packets that are sent to the Brick device twice: once from the client to the proxy server, and then back through the Brick device where it is forwarded to the destination server

-
- 3 In the **Brick Source Host** field, you can optionally filter the report to include only reflected sessions originating from one or more Brick devices. Enter either the IP address of the Brick device or click the down arrow next to the field to display a

drop-down list, and select **BROWSE** to open a Browse window and select a host group. An alternate method to identify the source Brick host group is to click the **is** button next to the field to change it to **is not**, and then enter an IP address or host group, to include records from all originating Brick devices *except* the one(s) entered.

- 4 In the **Proxy Destination Host** field, you can optionally filter the report to include reflected sessions where the proxy server is a specific IP address. Either enter the IP address of the proxy server or click the down arrow next to the field to display a drop-down list, and select **BROWSE** to open a Browse window and select a host group. An alternate method to identify the proxy server is to click the **is** button next to the field to change it to **is not**, and then enter an IP address or host group, to include records from all proxy server(s) *except* for the one(s) entered.
-

- 5 In the **Brick Source Port** field, you can optionally filter the report to include only sessions originating from a particular Brick source port. Enter the port number of the Brick device. An alternate method to identify the Brick source port is to click the **is** button next to the field to change it to **is not**, and then enter source port, to include records from all originating Brick source port*except* the one entered.
-

- 6 In the **Proxy Destination Port** field, you can optionally filter the report to include only sessions with a particular proxy destination port. Enter the proxy destination port number. An alternate method to identify the proxy destination port is to click the **is** button next to the field to change it to **is not**, and then enter port number, to include records from all proxy destination port*except* the one entered.
-

END OF STEPS

To enter miscellaneous information

Complete the following steps to enter miscellaneous filtering criteria for sessions to be included in the report.

- 1 Click the **Miscellaneous** tab.

Result The Miscellaneous tab of the Closed Session Details Editor is displayed (Figure 11-7, “Closed Session Details Editor (Miscellaneous tab)” (p. 11-16)).

Figure 11-7 Closed Session Details Editor (Miscellaneous tab)

The screenshot shows the 'Closed Session Details Editor' window with the 'Miscellaneous' tab selected. The interface includes a menu bar (File, Edit, Monitor, Windows, Utilities, Help) and a toolbar with icons for window management. The main area contains several input fields and controls:

- Name:** A text input field.
- Description:** A text input field.
- Run report across each LSMS and LSCS
- Time Range:** A section with two radio buttons:
 - Last Minutes
 - Specify Time Range
- Run:** A button with a small inset image of a report.
- Navigation Tabs:** Bricks/Zones, Host, Protocol, VPN, Proxy, **Miscellaneous**, Columns, Sorting.
- Filter Fields:**
 - Direction:** A dropdown menu.
 - Action:** A dropdown menu with an 'is' button.
 - Alarm Code:** A text input field with an 'is' button.
 - Rule Number:** A text input field with an 'is' button.
 - Send Interface:** A dropdown menu with an 'is' button.
 - Receive Interface:** A dropdown menu with an 'is' button.
 - Send VLAN:** A text input field with an 'is' button.
 - Receive VLAN:** A text input field with an 'is' button.

- 2 In the **Direction** field, filter the report to include only sessions in one direction. Click the down arrow next to the field and choose **IN TO ZONE** or **OUT OF ZONE** from the drop-down list. By default, the report includes sessions in both directions.
- 3 In the **Action** field, filter the report to include sessions according to the action taken by the Brick device. Click the down arrow next to the field and choose **PASS**, **DROP**, or **PROXY**. An alternate means to choose the action is to click the **is** button next to the field to change it to **is not** and then enter an action, to include all sessions with all other actions *except* the one entered.
- 4 In the **Alarm Code** field, filter the report to include sessions according to alarm code. Enter one or more alarm codes, each separated by a comma. An alternate means to choose the alarm code(s) is to click the **is** button next to the field to change it to **is**

not and then enter the alarm code(s), to include all sessions with all alarm codes *except* for the one(s) entered.

- 5 In the **Rule Number** field, filter the report to include sessions that were passed, dropped, or proxied by specific rules. Enter one or more rule numbers, each separated by a comma. An alternate means to choose the rule(s) is to click the **is** button next to the field to change it to **is not** and then enter the rule(s), to include all sessions with all rules *except* the one(s) entered.

- 6 In the **Send Interface** field, filter the report to include sessions by Brick device port that is sending the first packet of the session. Click the down arrow next to the field and select the port number from the drop-down list, or leave the asterisk(*) in place to indicate all ports. An alternate means to choose the port is to click the **is** button next to the field to change it to **is not** and then select the port, to include all sessions from all ports *except* the one entered.

- 7 In the **Receive Interface** field, filter the report to include sessions by Brick device port that is receiving the first packet of the session. Click the down arrow next to the field and select the port number from the drop-down list, or leave the asterisk(*) in place to indicate all ports. An alternate means to choose the port is to click the **is** button next to the field to change it to **is not** and then select the port, to include all sessions from all ports *except* the one entered.

- 8 In the **Send VLAN** field, filter the report to include sessions by VLAN number used for the first packet send during the session. Enter the VLAN number in the field. An alternate means to choose the VLAN is to click the **is** button next to the field to change it to **is not** and then select the port, to include all sessions with all VLANs *except* the one entered.

- 9 In the **Receive VLAN** field, filter the report to include sessions by VLAN number used for the first packet received during the session. Enter the VLAN number in the field. An alternate means to choose the VLAN is to click the **is** button next to the field to change it to **is not** and then select the port, to include all sessions with all VLANs *except* the one entered.

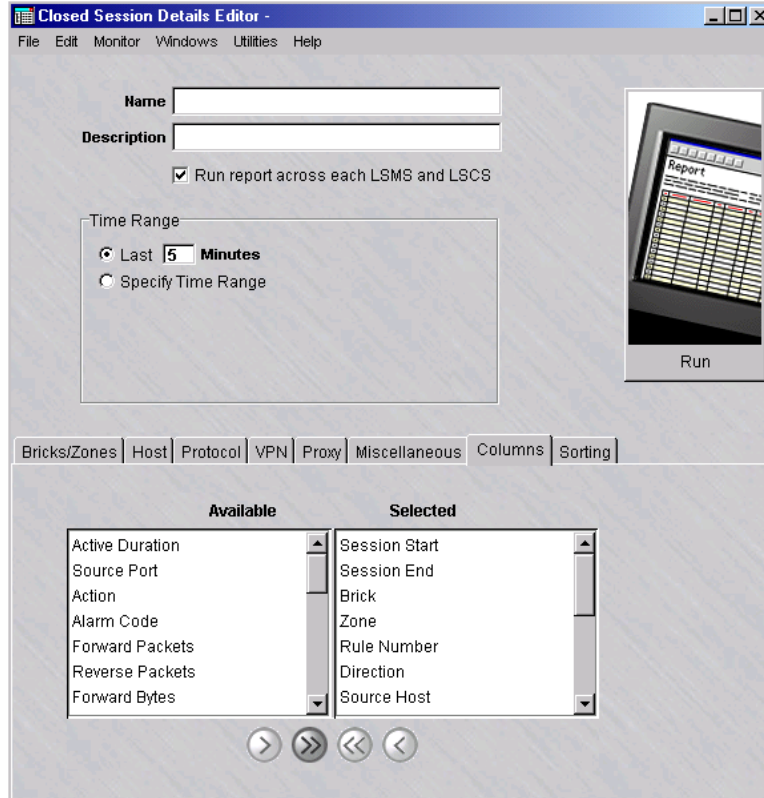
END OF STEPS

To select the columns

- 1 Click on the **Columns** tab.

Result The Columns tab of the Closed Sessions Details Editor is displayed (Figure 11-8, “Closed Session Details Editor (Columns tab)” (p. 11-18)).

Figure 11-8 Closed Session Details Editor (Columns tab)



- 2

To	Do This
Produce a report that contains all data columns	Leave all column names in the Selected portion of the tab. (This is the default.)

To	Do This
Produce a report with selected data column(s)	Use the arrow keys to move column names from the Selected portion to the Available portion of the tab. Only the columns in the Selected portion will be shown in the report. Use the arrow keys to move column names back and forth between the two lists as necessary.

.....
 END OF STEPS

To select the order of the report

-
 1 Click on the **Sorting** tab.

Result The Sorting tab of the Closed Session Details Editor is displayed.

-
 2 In the **Available** list, highlight a field to be used to determine the order of the report and click one of the arrow buttons to move it to the **Selected** list. You can select more than one field at a time from the list by clicking the left mouse button and the **CTRL** or **Shift** key.

Use the arrow keys to move the field(s) back and forth between the two lists, as necessary.

-
 3 Repeat the previous step as necessary until all fields to be used in determining the order of the report have been selected.

The order of the report output will be determined by the order of the fields shown in the **Selected** list.

.....
 END OF STEPS

To save the report

Complete the following steps to save a named copy of the report and its parameter settings.

-
 1 In the **Name** field, enter a name for the report.

-
- 2 In the **Description** field, enter a textual description for the report. (This step is optional.)

-
- 3 From the File menu, choose **Save**.

Result The report and its parameter settings are saved and stored in the report folder. The report is saved and can be reused as a template for similar reports when it is duplicated and renamed.

END OF STEPS

To duplicate a report

Complete the following steps to duplicate a report. You can duplicate a report, edit the parameters, and rename as necessary to generate a different report.

-
- 1 Right-click on an existing report in the Contents panel and choose **Duplicate** from the pop-up menu.

Result The initial tab of the Report Editor is displayed.

-
- 2 In the **Name** field, give the report a different name. Edit the parameter fields on the other tabs of the Report Editor, as needed.

-
- 3 From the File menu, choose **Save** to save the duplicated report under its new name.

END OF STEPS

To run the report

Complete the following steps to run the report.

-
- 1 Click the **Run** button. The Run a Report window appears.

Result A dialog window is displayed, indicating that the report is being generated. The window shows the progress of the report generation and the number of records retrieved that match the selected criteria.

If no event records are found that match the selected criteria, a warning dialog box is displayed, indicating that no records have been found and asks if you want to

view the output anyway. Choose **Yes** to view the output anyway or **No** to cancel the report output.

- 2 Close the Closed Sessions Details Editor window and Closed Session Details browser after viewing the output.

.....
 END OF STEPS

To run multiple reports

Complete the following steps to run multiple reports.

- 1 Right-click on existing reports in the Contents panel and choose **Run Multiple Reports** from the pop-up menu.

Result The Run Multiple Filters window is displayed.

- 2 Click the **run report across each LSMS and LSCS** checkbox to collect and run a merged report of all network events for all connected LSMSs and Compute Servers. (This checkbox is checked, by default.)

- 3 Select the time range of the report.

To	Do This
Generate a report of the most recent network events that have occurred within the past 1 to 99 minutes.	Click the Last radio button in the Time Range portion of the window and enter a value (in minutes), up to 99. 5 minutes is the default value.
Generate a report for a specific time range with beginning/end dates	Click the Specify Time Range radio button. The Start and End date fields are displayed. Click the Earliest button to select the earliest available date and time and the Now button to select the current date and time, or manually enter the month/day/year and hours/minutes/seconds values in each field.

- 4 Click the **Run** button. The Run a Report window appears.

Result A dialog window is displayed, indicating that the report is being generated. The window shows the progress of the report generation and the number of records retrieved that match the selected criteria.

If no event records are found that match the selected criteria, a warning dialog box is displayed, indicating that no records have been found and asks if you want to view the output anyway. Choose **Yes** to view the output anyway or **No** to cancel the report output.

-
- 5 Close the Closed Sessions Details Editor window and Closed Sessions Details browser after viewing the output.

END OF STEPS



Closed Session Details Report Output

When to use

The output from a Closed Session Details report is displayed in your web browser, and consists of a header and a body in table format with up to 37 columns of information. [Figure 11-9, “Closed Session Details Report \(Part A\)”](#) (p. 11-24) on the next page shows a fragment of a typical Closed Session Details report.

The administrator generating the report determines the number of columns that appear in the finished report.

The following sections explain the information in the header and 37 columns of the report output.

Header

The header of a Closed Session Details report contains the following information:

- *Page number and total number of pages*
In the upper right corner of the header, above the title Closed Session – Details, the report indicates the total number of pages in the report, and the number of the current page.
- *Time interval*
In the center, under the sort order, the report indicates the time interval covered by the report. This is determined by the administrator when running the report.
- *Total sessions found*
On the left margin, under the time interval, the report indicates the number of closed sessions included in the report. This is the number of entries found in the body of the report. The number of sessions in the report depends upon how specifically you define the selection criteria when generating the report.

Figure 11-9 Closed Session Details Report (Part A)

11-24

1 of 1

Closed Sessions - Details

From: Wed May 31 09:47:28 EDT 2000 To: Wed May 31 09:52:28 EDT 2000

260-100-019R9.1
Issue 1, July 2006

Brick	Zone	Rule No	Dir	Src Host	Dst Host	Service	Pcol	Dst Port	IPSEC	Pkts	Bytes	Send I/F	Rcv I/F
1_las030	las030_1b1_2	65535	OUT	0.0.0.0	255.255.255.255	bootps	UDP	67	none	1	328		ether2
1_las030	administrativezone@loadtest_group	65535	IN	0.0.0.0	255.255.255.255	bootps	UDP	67	none	1	328		ether0
2_las030	proxzone@loadtest_group	65535	IN	195.92.11.30	195.92.255.255	netbios-gm	UDP	138	none	2	524		ether1
1_las030	administrativezone@loadtest_group	1006	IN	195.92.11.30	195.92.255.255	netbios-ns	UDP	137	none	15	1170		ether2

Session Start

The first column in the body of the report is the **Start** column. It gives the date and time the session was started and recorded in the Sessions log, in the format of:

year/month/day

hour:minute:second

Session End

The **End** column indicates the date and time the session was ended and recorded in the Sessions log, in the format of:

year/month/day

hour:minute:second

Active Duration

The **Active Duration** column indicates the amount of time the session lasted. This is the result of subtracting the time in the **End** column from the time in the **Start** column.

Rule No.

The **Rule No.** column indicates the rule number of the security policy that caused the Brick to pass, drop, or proxy the session.

The administrator generating the report can include a particular rule number.

Brick

The **Brick** column indicates the name of the Brick that passed or dropped the session and produced this record.

The administrator generating the report determines the Brick devices to include in the report.

Zone

The **Zone** column indicates the name of the Brick zone ruleset whose security policy caused the Brick to pass or drop the session. The Brick zone ruleset must be assigned to a port on the Brick.

The administrator generating the report determines the Brick zone rulesets to include in the report.

Dir

The **Dir** column gives the direction of the session, vis a vis the Brick zone ruleset. The alternatives are:

- **IN** (the session originated outside the Brick zone ruleset and is intended for a destination IP address in the Brick zone ruleset), or
- **OUT** (the session originated in the Brick zone ruleset and is intended for a destination IP address outside the Brick zone ruleset).

The administrator generating the report can include sessions in both directions, or choose one of the two directions.

Src Host

The **Src Host** column provides the IP address of the source host. This is the host that initiated the session.

The administrator generating the report determines which source hosts to include in the report.

Src Port

The **Src Port** column gives the source port. This is the port used by the application on the source Brick that initiated the session.

The administrator generating the report determines which source ports to include in the report.

Dst Host

The **Dst Host** column provides the IP address of the destination host. This is the host that is intended to receive the session.

The administrator generating the report determines which destination hosts to include in the report.

Dst Port

The **Dst Port** column gives the destination port. This is the port used by the application on the destination host to receive the session.

The administrator generating the report determines which destination ports to include in the report.

Service

The **Service** column indicates the service (Dest Port/Src Port/Protocol) that the session is using. Examples are BOOTPS, NETBIOS-GM, NETBIOS-NS.

The administrator generating the report determines which services to include in the report.

Pcol

The **Pcol** column indicates the protocol that the session is using. The options are UDP, TCP or ICMP.

The administrator generating the report determines which protocols to include in the report.

Action

The **Action** column displays the action taken by the Brick when it encountered the session. Possibilities include:

- *Drop*
The Brick discarded the session and did not allow it through.
- *Pass*
The Brick accepted the session and allowed it through.
- *Proxy*
The Brick forwarded the session to a designated proxy server.

The administrator generating the report can include an action.

Alarm Code

The **Alarm Code** column identifies the alarm code (number between 1 and 65,535) that was configured with the rule number as displayed in the Rule No column.

If a rule is configured with an alarm code and the rule was invoked (indicating that packets processed by a Brick matched the conditions of the rule), an alarm will trigger to notify an administrator.

The administrator generating the report determines which alarm code(s) to include in the report.

Pkts

The **Pkts** column is the total number of packets that were processed in the session.

The number displayed in this column is the summation of the **For Pkts** and **Rev Pkts** columns.

For Pkts

The **For Pkts** column is the total number of packets in the session that were initiated from the source host to the destination host.

The number in this column is added to the number in the **Rev Pkts** column to display the total number of packets in the **Pkts** column.

Rev Pkts

The **Rev Pkts** column is the total number of packets in the session that were initiated from the destination host to the source host.

The number in this column is added to the number in the **For Pkts** column to display the total number of packets in the **Pkts** column.

Bytes

The **Bytes** column is the total number of bytes that were processed in the session.

The number displayed in this column is the summation of the **For Bytes** and **Rev Bytes** columns.

For Bytes

The **For Bytes** column is the total number of bytes in the session that were initiated from the source host to the destination host.

The number in this column is added to the number in the **Rev Bytes** column to display the total number of bytes in the **Bytes** column.

Rev Bytes

The **Rev Bytes** column is the total number of bytes in the session that were initiated from the destination host to the source host.

The number in this column is added to the number in the **For Bytes** column to display the total number of bytes in the **Bytes** column.

Receive I/F

The **Receive I/F** column identifies the port that is receiving the first packet of a session.

The administrator generating the report determines the receive port to include in the report.

Send I/F

The **Send I/F** column identifies the port that is sending the first packet of the session.

The administrator generating the report determines the send port to include in the report.

Mapped Src Host

If Network Address Translation was implemented, the **Mapped Src Host** column contains the IP address of the mapped source host. This is the host that initiated the session.

The administrator generating the report determines which mapped source hosts to include in the report.

Mapped Dst Host

If Network Address Translation was implemented, the **Mapped Dst Host** column contains the IP address of the mapped destination host. This is the host that is intended to receive the session.

The administrator generating the report determines which mapped destination hosts to include in the report.

Mapped Src Port

If Network Address Translation was implemented, the **Mapped Src Port** column contains the mapped source port. This is the port used by the application on the mapped source host that initiated the session.

The administrator generating the report determines which mapped source ports to include in the report.

Mapped Dst Port

If Network Address Translation was implemented, the **Mapped Dst Port** column contains the mapped destination port. This is the port used by the application on the mapped destination host that received the session.

The administrator generating the report determines which mapped destination ports to include in the report.

VPN Direction

If a Virtual Private Network was implemented, the **VPN Direction** column refers to the direction of the VPN packets. The direction is either:

- *Forward*
Refers to the initial session from the source host to the destination host.
- *Reverse*
Refers to the return session from the destination host back to the source host.

The administrator generating the report determines the direction of the VPN packets to include in the report.

IPSEC

If a Virtual Private Network was implemented, the **IPSEC** column refers to the presence of encryption or decryption in the session. The options are: None, Decrypted, Encrypted, or Decrypted and Encrypted.

The administrator generating the report determines which IPSEC mode to include in the report.

Tunnel Endpoint

If a Virtual Private Network was implemented, the **Tunnel Endpoint** column is the IP address (virtual Brick address (VBA)) assigned to the Brick zone ruleset that contains the destination IP address of the session.

The administrator generating the report determines which tunnel endpoints to include in the report.

SPI

If a Virtual Private Network was implemented, the **SPI** column contains a unique identifier that identifies the specific Security Association used in a VPN. The Security Association, in turn, provides the manual keying information that the VPN requires to perform encryption/decryption.

The administrator generating the report determines which SPIs to include in the report.

VPN User ID

If a Virtual Private Network was established between the Brick and a Lucent IPsec Client, the **VPN User ID** column contains the ID of an individual using the Lucent IPsec Client program to set up a VPN. Every user of the Client program must enter a unique ID to activate a VPN.

The administrator generating the report determines which VPN User IDs to include in the report.

Brick Src Host

If proxying to a remote host was implemented, the **Brick Src Host** column is the IP address of the Brick that is forwarding the session to a proxy host.

Proxy Dst Host

If proxying to a remote host was implemented, the **Proxy Dst Host** column is the IP address of the proxy host that is running the proxy software (e.g., Lucent Proxy Agent).

Brick Src Port

If proxying to a remote host was implemented, the **Brick Src Port** indicates the port used by the Brick to forward the session to the proxy host.

Proxy Dst Port

If proxying to a remote host was implemented, the **Proxy Dst Port** indicates the port used by the proxy host to receive the session from the Brick.

Reflection Type

If proxying to a remote host was implemented, the **Reflection Type** column indicates the type of session used for proxying. The reflection type is either:

- *Dual*
The packets are sent through the Brick twice — once from the client to the proxy host, and then back through the Brick where it appears to the server as if the session came from the original client.
- *Single*
The packets are sent from the Brick to the proxy host, and then directly to the requesting destination server. The packets are routed through the Brick only once and the destination server sees the proxy host as the originating client instead of the actual client.

□

12 Alarms Logged Report

Overview

Purpose

The Alarms Logged report enables an Administrator to produce a historical record of alarms generated by any installed Lucent VPN Firewall *Brick*®.

The report can be configured to show alarms by Brick device or Brick zone ruleset. In addition, the Administrator generating the report can enter selection criteria to determine exactly which alarms to include in the finished report.

The Alarms Logged report can be used to troubleshoot network problems by tracking and analyzing alarms.

Contents

To Generate an Alarms Logged Report	12-2
Alarms Logged Report Output	12-17



To Generate an Alarms Logged Report

When to use

To generate an Alarms Logged report, you must display the Alarms Logged Editor and then enter selection criteria that determine the scope and type of alarm information included in the report.

To display the Alarms Logged Editor

Complete the following steps to display the Alarms Logged Editor.

- 1 With the Navigator window displayed, open the **Reports** folder.

- 2 Right-click the **Alarms Logged** folder and select **New Alarms Logged**.

To edit an existing report and its settings, right-click on the report in the list of the Contents panel and choose **Edit** from the pop-up menu.

To view an existing report, and change the Time Range for a previously run report or the checkbox that controls whether you want to run a report across all LSMSs for data, right-click on the report in the list of the Contents panel and choose **View** from the pop-up menu.

Result The Alarms Logged Editor is initially displayed with the Alarms Logged tab (Figure 12-1, “Alarms Logged Editor (Alarms Logged tab)” (p. 12-3)).

Figure 12-1 Alarms Logged Editor (Alarms Logged tab)

The screenshot shows the 'Alarms Logged Editor' window with the 'Alarms Logged' tab selected. The window has a menu bar with 'File', 'Edit', 'Monitor', 'Windows', 'Utilities', and 'Help'. The main area contains several input fields and a 'Run' button. The 'Name' field is empty. The 'Description' field is empty. A checkbox labeled 'Run report across each LSMS and LSCS' is checked. The 'Time Range' section has two radio buttons: 'Last 5 Minutes' (selected) and 'Specify Time Range'. To the right, there is a magnifying glass icon over a report grid, and a 'Run' button below it. At the bottom, there are tabs for 'Bricks/Zones', 'Alarms Logged', 'Text', 'Columns', and 'Sorting'. Below these tabs, there are several filter fields: 'Serial Number: *', 'Alarm Name is *', 'Alarm Type is *', 'Alarm Code is *', 'Action is *', and 'Action Status is *'.

- 3 In the **Name** field, enter a name for the report file to be created.
- 4 In the **Description** field, enter a textual description of the report. This field is optional.
- 5 Click the **run report across each LSMS and LSCS** checkbox to collect and run a merged report of all network events for all connected LSMSs and Compute Servers. (This checkbox is checked, by default.)

6 Select the time range of the report.

To	Do This
Generate a report of the most recent network events that have occurred within the past 1 to 99 minutes	Click the Last radio button in the Time Range portion of the window and enter a value (in minutes), up to 99.5 minutes is the default value.
Generate a report for a specific time range with beginning/end dates	Click the Specify Time Range radio button. The Start and End date fields are displayed. Click the Earliest button to select the earliest available date and time and the Now button to select the current date and time, or manually enter the month/day/year and hours/minutes/seconds values in each field.

END OF STEPS

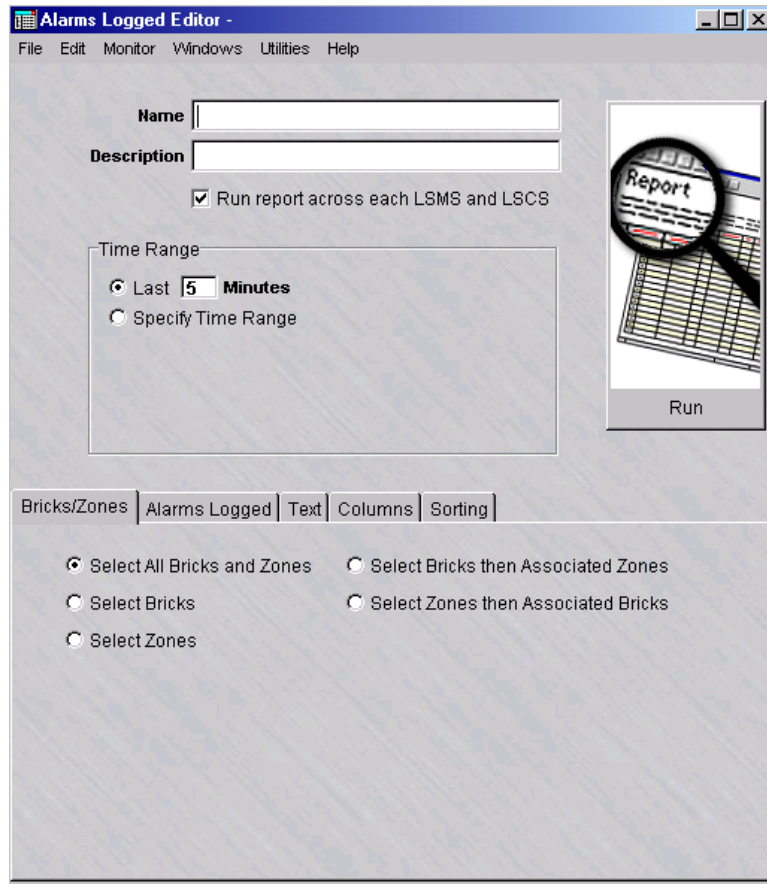
To select the source(s) of the alarms

Complete the following steps to select the source(s) of the alarms to be included in the report. You can optionally restrict the scope of the report to the specified Brick device(s) or Brick zone ruleset(s).

1 Click the **Bricks/Zones** tab.

Result The Bricks/Zones tab of the Alarms Logged Editor is displayed (Figure 12-2, “Alarms Logged Editor (Bricks/Zones tab)” (p. 12-5)).

Figure 12-2 Alarms Logged Editor (Bricks/Zones tab)



2

To	Do This
Generate a report for all Brick devices and Brick zone rulesets	Click the Select All Bricks and Zones radio button.

To	Do This
Restrict the report to the specified Brick device(s)	Click the Select Bricks radio button. Right-click in the Bricks box and choose Select a Brick from the pop-up menu. In the Browse: Select a Brick window, select the Brick device(s) from the Bricks folder and click OK . Repeat as necessary to add other Brick devices. Right-click and choose Clear Selection from the pop-up menu if you want to clear your selection(s) and make new choices.
Restrict the report to the specified Brick zone ruleset(s)	Click the Select Zones radio button. Right-click in the Zones box and choose Select a Brick Zone Ruleset from the pop-up menu. In the Browse: Select a Brick Zone Ruleset window, select the Brick zone ruleset(s) from the Brick Zone Rulesets folder and click OK . Repeat as necessary to add other Brick zone rulesets. Right-click and choose Clear Selection from the pop-up menu if you want to clear your selection(s) and make new choices.
Restrict the report to the specified Brick device(s) and associated Brick zone ruleset(s).	Click the Select Bricks then Associated Zones radio button. Right-click in the Bricks box and choose Select a Brick from the pop-up menu. In the Browse: Select a Brick window, select the Brick device(s) from the Bricks folder and click OK . Repeat as necessary to add other Brick devices. Right-click and choose Clear Selection from the pop-up menu if you want to clear your selection(s) and make new choices. The Brick zone rulesets that have been assigned to at least one port on the selected Brick device(s) are displayed in the Zones box. Select only the Brick zone ruleset(s) to be included in the report. Press the CTRL while holding the left mouse button to select more than one item. Press the Shift key while pressing the left mouse button to a range of items.

To	Do This
<p>Restrict the report to the specified Brick zone ruleset(s) and associated Brick devices</p>	<p>Click the Select Zones then Associated Bricks radio button. Right-click in the Zones box and choose Select a Brick Zone Ruleset from the pop-up menu. In the Browse: Select a Brick zone Ruleset window, select the Brick zone ruleset to be included in the report and click OK. Repeat as necessary to select other Brick zone rulesets. Right-click and choose Clear Selection from the pop-up menu if you want to clear your selection and choose a different zone ruleset. The Brick device(s) with at least one port assignment for the zone ruleset are displayed in the Bricks box. Select the Brick device(s) to be included in the report. Press the CTRL while holding the left mouse button to select more than one item. Press the Shift key while pressing the left mouse button to select a range of items.</p>

.....
 END OF STEPS

To select the alarms

Complete the following steps to select criteria for the alarm records to be included in the report.

.....

- 1 Click on the **Alarms Logged** tab.

Result The Alarms Logged tab of the Alarms Logged Editor is displayed (Figure 12-3, “Alarms Logged Editor (Alarms Logged tab)” (p. 12-8)).

Figure 12-3 Alarms Logged Editor (Alarms Logged tab)

- 2 In the **Serial Number** field, enter the serial number (1-10 digits) that uniquely identifies the alarm to be included in the report. You can enter more than one serial number, separated by commas.
- 3 Click the down arrow next to the **Alarm Name** field and select **BROWSE**. A Browse window is displayed. Select an alarm trigger and click **OK** to close the Browse window and activate your choice. Repeat as necessary to add additional alarm triggers, each separated by a comma.

An alternate means to select alarm triggers is to click the **is** button to change it to **is not** and enter one or more alarm trigger. The report will include all alarm triggers *except* the one(s) entered.

- 4 Click the down arrow next to the **Alarm Type** field to display a drop-down list and select the alarm type to include in the report. Repeat as necessary to add additional alarm types, each separated by a comma.

An alternate means to select alarm types is to click the **is** button to change it to **is not** and enter one or more alarm types. The report will include all alarm types *except* the one(s) entered.

- 5 In the **Alarm Code** field, enter one or more alarm codes, which identify the alarms when creating security rules and dependency masks, each separated by a comma.

An alternate means to select alarm codes is to click the **is** button to change it to **is not** and enter one or more alarm codes. The report will include all alarm codes *except* the one(s) entered.

- 6 Click the down arrow next to the **Action** field and choose **BROWSE**. A Browse window is displayed. Choose an alarm action and click **OK** to close the Browse window and activate your choice. Repeat as necessary to add additional alarm actions to be included in the report.

An alternate means to select alarm actions is to click the **is** button to change it to **is not** and choose one or more alarm actions. The report will include all alarm actions *except* the one(s) entered.

- 7 Click the down arrow next to the **Action Status** field to display a drop-down list and choose alarms with a specific action status to include in the report. The choices are **Success** or **Failure**.

An alternate means to select alarms with a specific action status is to click the **is** button to change it to **is not** and choose one of the actions statuses. The report will include all alarms *except* those with the action status entered.

END OF STEPS

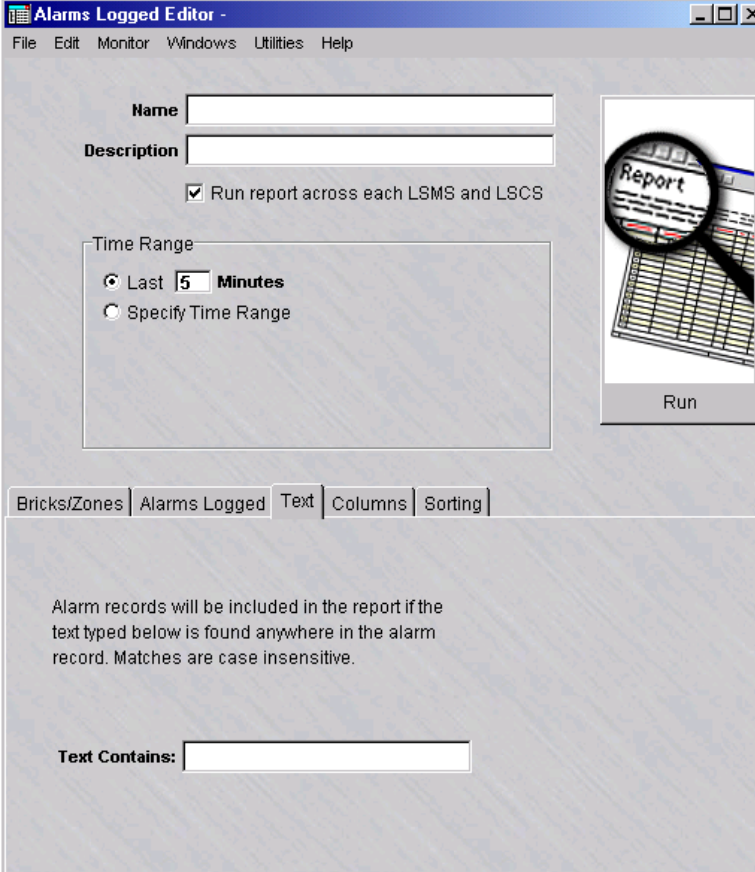
To enter alarm text

Complete the following steps to search for alarm records with the specified text to be included in the report.

- 1 Click on the **Text** tab.

Result The Text tab of the Alarms Logged Editor is displayed (Figure 12-4, “Alarms Logged Editor (Text tab)” (p. 12-10)).

Figure 12-4 Alarms Logged Editor (Text tab)



The screenshot shows the 'Alarms Logged Editor' window with the 'Text' tab selected. The interface includes a menu bar (File, Edit, Monitor, Windows, Utilities, Help), input fields for 'Name' and 'Description', a checked checkbox for 'Run report across each LSMS and LSCS', and a 'Time Range' section with radio buttons for 'Last 5 Minutes' (selected) and 'Specify Time Range'. A 'Run' button is located to the right of the 'Time Range' section. Below the input fields is a tabbed interface with 'Bricks/Zones', 'Alarms Logged', 'Text', 'Columns', and 'Sorting' tabs. The 'Text' tab is active, displaying the instruction: 'Alarm records will be included in the report if the text typed below is found anywhere in the alarm record. Matches are case insensitive.' Below this instruction is a 'Text Contains:' label and an empty text input field.

- 2 To include event records in the report, enter a text string in the **Text Contains** field.
The report will include any event records that contain text matching the text entry. The text search ignores case.

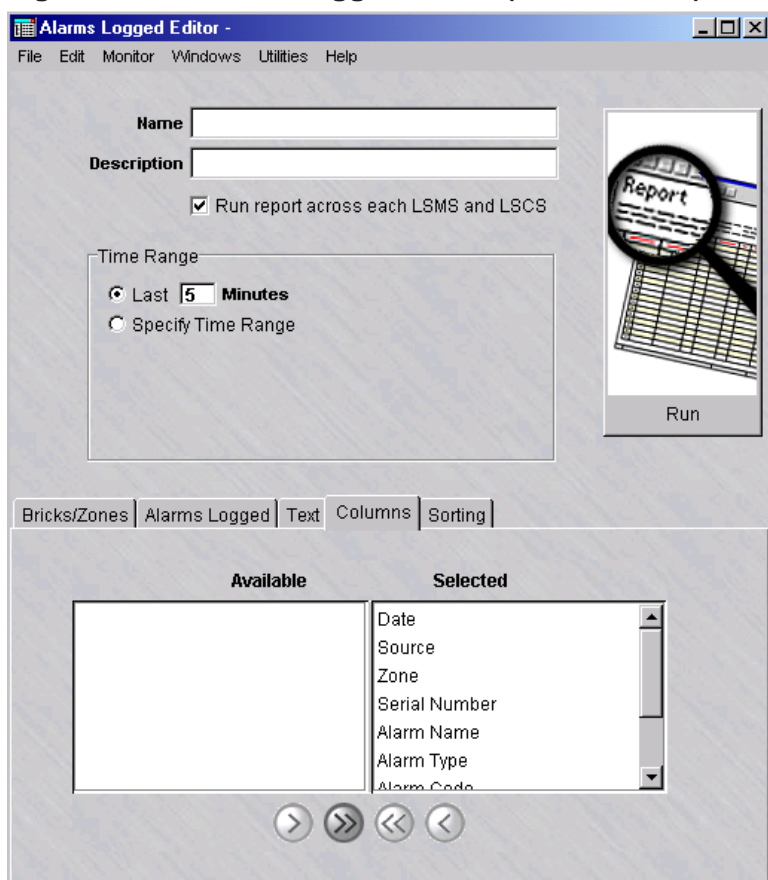
END OF STEPS

To select the columns of the report

- 1 Click on the **Columns** tab.

Result The Columns tab of the Alarms Logged Editor is displayed (Figure 12-5, “Alarms Logged Editor (Columns tab)” (p. 12-11)).

Figure 12-5 Alarms Logged Editor (Columns tab)



- 2

To	Do This
Produce a report that contains all data columns	Leave all column names in the Selected portion of the tab. (This is the default.)

To	Do This
Produce a report with selected data column(s)	Use the arrow keys to move column names from the Selected portion to the Available portion of the tab. Only the columns in the Selected portion will be shown in the report. Use the arrow keys to move column names back and forth between the two lists as necessary.

.....
E N D O F S T E P S

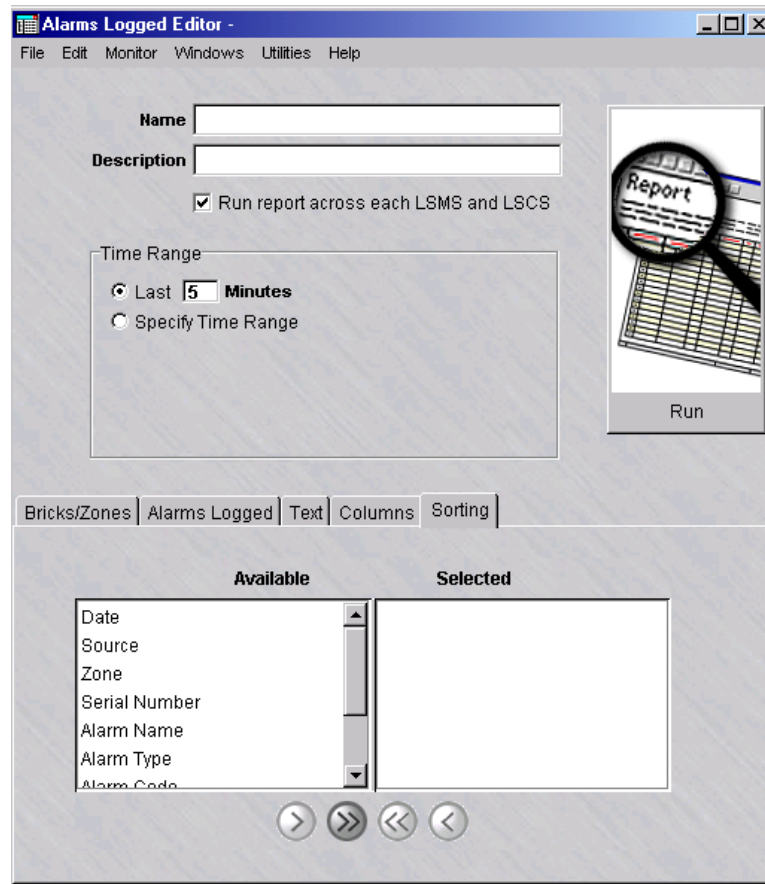
To select the order of the report

.....

- 1 Click on the **Sorting** tab.

Result The Sorting tab of the Alarms Logged Editor is displayed (Figure 12-6, “Alarms Logged Editor (Sorting tab)” (p. 12-13)).

Figure 12-6 Alarms Logged Editor (Sorting tab)



-
- 2 In the **Available** list, highlight a field to be used to determine the order of the report and click one of the arrow buttons to move it to the **Selected** list. You can select more than one field at a time from the list by clicking the left mouse button and the **CTRL** or **Shift** key.

Use the arrow keys to move the field(s) back and forth between the two lists, as necessary.

.....

- 3 Repeat the previous step as necessary until all fields to be used in determining the order of the report have been selected.

The order of the report output will be determined by the order of the fields shown in the **Selected** list.

.....
E.N.D. O.F. S.T.E.P.S.

To save the report

Complete the following steps to save a named copy of the report and its parameter settings.

.....

- 1 In the **Name** field, enter a name for the report.

.....

- 2 In the **Description** field, enter a textual description for the report. (This step is optional.)

.....

- 3 From the File menu, choose **Save**.

Result The report and its parameter settings are saved and stored in the report folder. The report is saved and can be reused as a template for similar reports when it is duplicated and renamed.

.....
E N D O F S T E P S
.....

To duplicate a report

Complete the following steps to duplicate a report. You can duplicate a report, edit the parameters, and rename as necessary to generate a different report.

.....

- 1 Right-click on an existing report in the Contents panel and choose **Duplicate** from the pop-up menu.

Result The initial tab of the Report Editor is displayed.

.....

- 2 In the **Name** field, give the report a different name. Edit the parameter fields on the other tabs of the Report Editor, as needed.

.....

- 3 From the File menu, choose **Save** to save the duplicated report under its new name.

.....
E N D O F S T E P S
.....

To run the report

Complete the following steps to run the report.

- 1 Click the **Run** button. The Run a Report window appears.

Result A dialog window is displayed, indicating that the report is being generated. The window shows the progress of the report generation and the number of records retrieved that match the selected criteria.

If no event records are found that match the selected criteria, a warning dialog box is displayed, indicating that no records have been found and asks if you want to view the output anyway. Choose **Yes** to view the output anyway or **No** to cancel the report output.
- 2 Close the Alarms Logged Editor window and Alarms Logged browser after viewing the output.

END OF STEPS

To run multiple reports

Complete the following steps to run multiple reports.

- 1 Right-click on existing reports in the Contents panel and choose **Run Multiple Reports** from the pop-up menu.

Result The Run Multiple Filters window is displayed.
- 2 Click the **run report across each LSMS and LSCS** checkbox to collect and run a merged report of all network events for all connected LSMSs and Compute Servers. (This checkbox is checked, by default.)
- 3 Select the time range of the report.

To	Do This
Generate a report of the most recent network events that have occurred within the past 1 to 99 minutes.	Click the Last radio button in the Time Range portion of the window and enter a value (in minutes), up to 99. 5 minutes is the default value.

To	Do This
Generate a report for a specific time range with beginning/end dates	Click the Specify Time Range radio button. The Start and End date fields are displayed. Click the Earliest button to select the earliest available date and time and the Now button to select the current date and time, or manually enter the month/day/year and hours/minutes/seconds values in each field.

-
- 4 Click the **Run** button. The Run a Report window appears.

Result A dialog window is displayed, indicating that the report is being generated. The window shows the progress of the report generation and the number of records retrieved that match the selected criteria.

If no event records are found that match the selected criteria, a warning dialog box is displayed, indicating that no records have been found and asks if you want to view the output anyway. Choose **Yes** to view the output anyway or **No** to cancel the report output.

-
- 5 Close the Alarms Logged Editor window and Alarms Logged browser after viewing the output.

END OF STEPS



Alarms Logged Report Output

When to use

The output from an Alarms Logged report is displayed in your web browser, and consists of a header and a body in table format with up to nine columns of information. [Figure 12-7, “Alarms Logged Report” \(p. 12-18\)](#) on the next page shows a fragment of a typical Alarms Logged Report.

The report in [Figure 12-7, “Alarms Logged Report” \(p. 12-18\)](#) contains all nine columns. The Administrator generating the report determines the number of columns that appear in the finished report.

The following sections explain the information in the header and in all nine columns of the body.

Header

The header of an Alarms Logged Report contains the following information:

- *Time interval*
In the center, under the sort order, the report indicates the time interval covered by the report. This is determined by the Administrator when running the report.
- *Total records*
On the left margin, under the time interval, the report indicates the number of records included in the report. This is the number of entries found in the body of the report. The number of records in the report depends upon how specifically you define the selection criteria when generating the report.

Figure 12-7 Alarms Logged Report

12-18

260-100-019R9.1
Issue 1, July 2006

Alarms Logged

From: Sat May 27 09:48:24 EDT 2000 To: Wed May 31 09:58:24 EDT 2000

Date	Source	Zone	Serial Number	Alarm Name	Alarm Type	Alarm Code	Actions	Alarm Info
2000/05/27 19:42:57	1b1_las030		33	Lost a Brick	Brick Lost		Send a Console Message:Success	admn_ashit, Triggered by event at 2000/05/27 19:42:27
2000/05/27 19:42:57	1b1_las030		34	Lost a Brick	Brick Lost		Send a Console Message:Success	las030_admin, Triggered by event at 2000/05/27 19:42:27
2000/05/27 19:42:57	1b1_las030		35	Lost a Brick	Brick Lost		Send a Console Message:Success	admn, Triggered by event at 2000/05/27 19:42:27
2000/05/27 19:42:57	1b1_las030		36	Lost a Brick	Brick Lost		Send a Console Message:Success	ga_admin, Triggered by event at 2000/05/27 19:42:27
2000/05/27 19:42:57	1b1_las030		37	Lost a Brick	Brick Lost		Send a Console Message:Success	null, Triggered by event at 2000/05/27 19:42:27

Date Column

The first column in the body of the report is the **Date** column. It gives the date and time the alarm was recorded in the administrative events log, in the format:

year/month/day

hour:minute:second

Source Column

The **Source** column indicates the source that originated the alarm. The source can be a Brick or a RealSecure detector.

The Administrator generating the report determines the specific sources to include in the report.

Zone Column

The **Zone** column indicates the Brick zone ruleset in which the alarm originated.

The Administrator generating the report determines the Brick zone rulesets to include in the report at the same time that the sources of the alarms are selected.

Serial Number Column

The **Serial Number** column indicates a number (1 - 10 digits) that uniquely identifies an alarm.

The number must be a positive number less than or equal to 2,147,483,647.

Alarm Name Column

The **Alarm Name** column gives the name that the Administrator assigned to this alarm when initially configuring the alarm.

The Administrator generating the report determines the names of the alarms to include in the report.

Alarm Type Column

The **Alarm Type** column indicates the type of alarm. There are twelve alarm types:

- Alarm Code
- Brick Error
- Brick Failover Event
- Brick ICM Alarm
- Brick Interface Lost

- Brick Lost
- Brick Proactive Monitoring
- Brick SLA Round Trip Delay Alarm
- LSMS Error
- LSMS Proactive Monitoring
- LSMS Status Change
- LAN To LAN Tunnel Lost
- LAN To LAN Tunnel Up
- Local Presence Map Pool
- QOS Rule Bandwidth Exceeded Alarm
- QOS Rule BandwidthGuarantees Alarm
- QOS Rule BandwidthThrottling Alarm
- QOS Zone Bandwidth Guarantees Alarm
- QOS Zone BandwidthThrottling Alarm
- RealSecure
- Unauthorized LSMS Login Attempt
- User Authentication

The Administrator generating the report determines the types of alarms to include in the report.

Alarm Code Column

The **Alarm Code** column indicates the alarm code associated with this alarm. If an Administrator associates an alarm code with a rule, the alarm will be triggered every time the rule is invoked by an incoming or outgoing session.

The Administrator generating the report determines the types of alarms to include in the report.

Actions Column

The **Actions** column indicates whether the action to notify an Administrator was a success or failure.

The Administrator generating the report determines the types of alarms to include in the report.

Alarm Info Column

The **Alarm Info** column provides text that was found in the alarm record in the log.

The Administrator generating the report identifies the text to be found.



13 User Authentication Report

Overview

Purpose

The User Authentication report enables an Administrator to view and analyze user accounts that are authorized to access hosts protected by a Lucent VPN Firewall *Brick*[®] or can connect to a Brick device via a tunnel.

The User Authentication Report can show all login attempts, successful and unsuccessful. It can show user authentications performed by the local LSMS database, as well as authentications performed by any RADIUS or SecurID servers referenced by the LSMS.

Contents

To Generate a User Authentication Report	13-2
User Authentication Report Output	13-14



To Generate a User Authentication Report

When to use

To generate a User Authentication report, you must display the User Auth Editor and then enter selection criteria that determine the scope and type of information included in the report.

To display the User Auth Editor

Complete the following steps to display the User Auth Editor.

- 1 With the Navigator window displayed, open the **Reports** folder.
-

- 2 Right-click the **User Auth** folder and select **New User Auth**.

To edit an existing report and its settings, right-click on the report in the list of the Contents panel and choose **Edit** from the pop-up menu.

To view an existing report, and change the Time Range for a previously run report or the checkbox that controls whether you want to run a report across all LSMs for data, right-click on the report in the list of the Contents panel and choose **View** from the pop-up menu.

Result The User Auth Editor is initially displayed with the User Auth tab (Figure 13-1, “User Auth Editor (User Auth tab)” (p. 13-3)).

Figure 13-1 User Auth Editor (User Auth tab)



User Auth Editor - File Edit Monitor Windows Utilities Help

Name

Description

Run report across each LSMS and LSCS

Time Range

Last 5 Minutes

Specify Time Range

Report

Run

User Auth Columns Sorting

User ID: *

Source: *

User Loc: *

Result is

Auth Action is

Auth Service is

Source Host is

Source Port is

Destination Host is

Destination Port is

Protocol is

- 3 In the **Name** field, enter a name for the report file to be created.
- 4 In the **Description** field, enter a textual description of the report. This field is optional.
- 5 Click the **run report across each LSMS and LSCS** checkbox to collect and run a merged report of all network events for all connected LSMSs and Compute Servers. (This checkbox is checked, by default.)

6 Select the time range of the report.

To	Do This
Generate a report of the most recent network events that have occurred within the past 1 to 99 minutes.	Click the Last radio button in the Time Range portion of the window and enter a value (in minutes), up to 99.5 minutes is the default value.
Generate a report for a specific time range with beginning/end dates	Click the Specify Time Range radio button. The Start and End date fields are displayed. Click the Earliest button to select the earliest available date and time and the Now button to select the current date and time, or manually enter the month/day/year and hours/minutes/seconds values in each field.

7

To	Do This
Specify one or more users for the report	Click the down arrow next to the User ID field and select BROWSE from the drop-down list. A Browse window is displayed. Select a user or administrator ID from the respective folder and click OK to close the Browse window and activate your choice. Repeat as needed. Each user ID is separated by a comma. You can also manually enter the user ID(s) in the User ID field, each separated by a comma.
Generate a report that includes all user IDs	In the User ID field, leave the asterisk (*) in place (this is the default).

8 Click the down arrow next to the **Source** field to display a drop-down list and choose the source associated with the user

The choices are:

- **Administrators**—administrators who access the managed Brick devices through the LSMS
- **Firewall**—users who attempt to establish a session through a Brick device
- **VPN**—users who attempt to set up a VPN tunnel, with a Brick device as the tunnel endpoint

An asterisk in the **Source** field indicates that the report includes users associated with all sources (the default).

- 9 Click the down arrow next to the **User Loc** field to display a drop-down list and choose the user location.

The choices are:

- **Internal**—via the LSMS
- **External**—using RADIUS, SecurID, or a VPN Certificate.

An asterisk in the **User Loc** field indicates that the report includes both internal and external user (the default).

- 10 Click the down arrow next to the **Result** field to display a drop-down list and choose one or more login results to be included in the report.

The choices are:

- **Failure**—report includes login failures
- **Password**—report indicates when additional information is processed for Local Password authentication. This typically occurs when a user password has expired and the user is prompted to select a new one.
- **Query**—report indicates when additional information is processed for RADIUS or SecurID authentication. For RADIUS users, this typically occurs when their user password has expired and they are prompted to select a new one. For SecurID users, this is typically a “challenge” page for entering a new PIN.
- **RADIUS Attributes**—report indicates when additional RADIUS attributes are processed for RADIUS users during authentication.
- **Success**—report includes successful user logins

An alternate means to select the login result is to click the **is** button next to the field to change it to **is not** and choose one or more login results; the report will include all login results *except* the one(s) entered.

- 11 Click the down arrow next to the **Auth Action** field to display a drop-down list and choose the user actions to be included in the report.
-

The choices are:

- **Lock**
- **Login**
- **Login Phase 1**
- **Logoff**
- **Password**
- **Query**
- **Query Phase 1**
- **Unlock**
- **Unlock Phase 1**

An asterisk (*) in the field indicates that the report includes all user authentication actions (the default).

An alternate means to select the user authentication action is to click the **is** button next to the field to change it to **is not** and choose one or more user authentication actions; the report will include all user authentication actions *except* the one(s) entered.

-
- 12** Click the down arrow next to the **Auth Service** field to display a drop-down list and choose **BROWSE**. A Browse window is displayed for choosing the authentication service. Choose the authentication service and click **OK** to close the Browse window and activate your choice. Repeat as necessary to select additional services, each separated by a comma in the field.

An alternate means to select the authentication service is to click the **is** button next to the field to change it to **is not** and choose one or more user authentication services from the Browse window; the report will include all user authentication services *except* the one(s) entered.

-
- 13** Click the down arrow next to the **Source Host** field to display a drop-down list and choose **BROWSE**. A Browse window is displayed for choosing the source host or host group. Choose the source host or host group and click **OK** to close the Browse window and activate your choice. Repeat as necessary to select additional source hosts or host groups, each separated by a comma in the field.

An alternate means to select the source host is to click the **is** button next to the field to change it to **is not** and choose one or more source hosts or host groups from the Browse window; the report will include all source hosts *except* the one(s) entered.

- 14** In the **Source Port** field, enter the source port number(s) to be included in the report, each separated by a comma.

An alternate means to select the source port(s) is to click the **is** button next to the field to change it to **is not** and enter one or more source port numbers; the report will include all source ports *except* the one(s) entered.

- 15** Click the down arrow next to the **Destination Host** field to display a drop-down list and choose **BROWSE**. A Browse window is displayed for choosing the destination host or host group. Choose the destination host or host group and click **OK** to close the Browse window and activate your choice. Repeat as necessary to select additional destination hosts or host groups, each separated by a comma in the field.

An alternate means to select the destination host is to click the **is** button next to the field to change it to **is not** and choose one or more destination hosts or host groups from the Browse window; the report will include all destination hosts *except* the one(s) entered.

- 16** In the **Destination Port** field, enter the destination port number(s) to be included in the report, each separated by a comma.

An alternate means to select the destination port(s) is to click the **is** button next to the field to change it to **is not** and enter one or more destination port numbers; the report will include all source ports *except* the one(s) entered.

- 17** Click the down arrow next to the **Protocol** field to display a drop-down list and choose one or more protocol types to be included in the report.

An alternate means to select the protocol(s) is to click the **is** button next to the field to change it to **is not** and choose one or more protocols; the report will include all protocols *except* the one(s) entered.

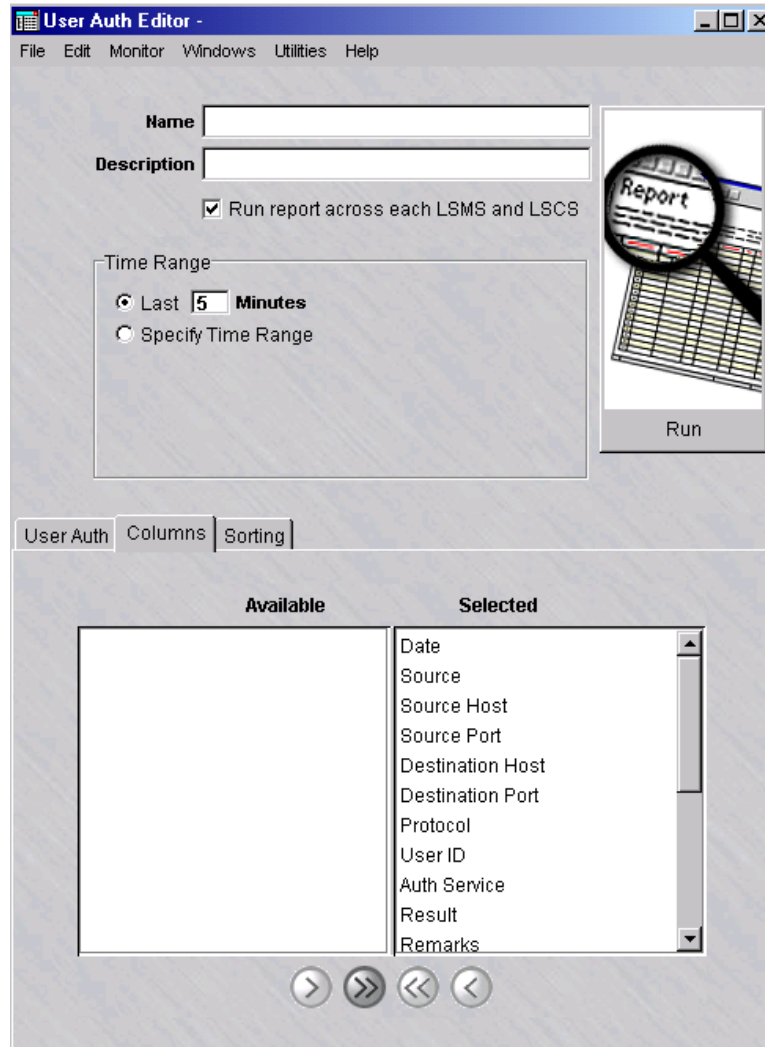
END OF STEPS

To select the columns of the report

- 1 Click on the **Columns** tab.

Result The Columns tab of the User Auth Editor is displayed (Figure 13-2, “User Auth Editor (Columns tab)” (p. 13-8)).

Figure 13-2 User Auth Editor (Columns tab)



2

To	Do This
Produce a report that contains all data columns	Leave all column names in the Selected portion of the tab. (This is the default.)
Produce a report with selected data column(s)	Use the arrow keys to move column names from the Selected portion to the Available portion of the tab. Only the columns in the Selected portion will be shown in the report. Use the arrow keys to move column names back and forth between the two lists as necessary.

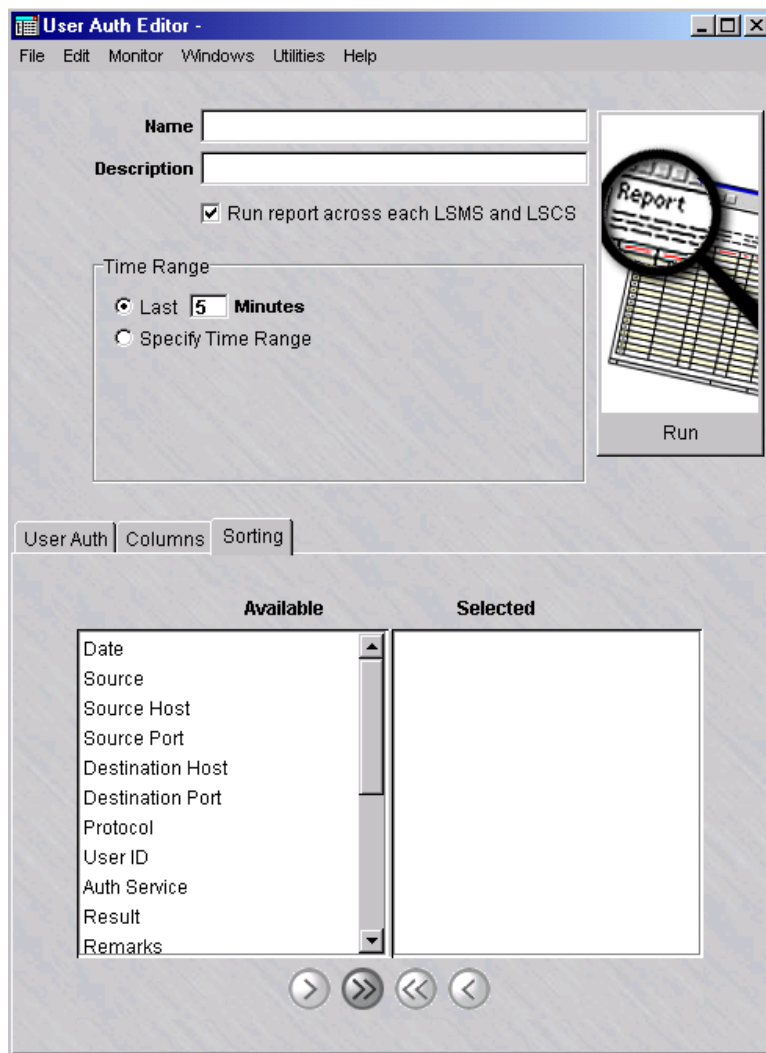
END OF STEPS

To select the order of the report

- 1 Click on the **Sorting** tab.

Result The Sorting tab of the User Auth Editor is displayed (Figure 13-3, “User Auth Editor (Sorting tab)” (p. 13-10)).

Figure 13-3 User Auth Editor (Sorting tab)



- 2 In the **Available** list, highlight a field to be used to determine the order of the report and click one of the arrow buttons to move it to the **Selected** list. You can select more than one field at a time from the list by clicking the left mouse button and the **CTRL** key. You can select a range of fields by pressing the **Shift** key and holding the left mouse button.

Use the arrow keys to move the field(s) back and forth between the two lists, as necessary.

-
- 3 Repeat the previous step as necessary until all fields to be used in determining the order of the report have been selected.

The order of the report output will be determined by the order of the fields shown in the **Selected** list.

END OF STEPS

To save the report

Complete the following steps to save a named copy of the report and its parameter settings.

-
- 1 In the **Name** field, enter a name for the report.
 - 2 In the **Description** field, enter a textual description for the report. (This step is optional.)
 - 3 From the File menu, choose **Save**.

Result The report and its parameter settings are saved and stored in the report folder. The report is saved and can be reused as a template for similar reports when it is duplicated and renamed.

END OF STEPS

To duplicate a report

Complete the following steps to duplicate a report. You can duplicate a report, edit the parameters, and rename as necessary to generate a different report.

-
- 1 Right-click on an existing report in the Contents panel and choose **Duplicate** from the pop-up menu.

Result The initial tab of the Report Editor is displayed.

-
- 2 In the **Name** field, give the report a different name. Edit the parameter fields on the other tabs of the Report Editor, as needed.

-
- 3 From the File menu, choose **Save** to save the duplicated report under its new name.

END OF STEPS

To run the report

Complete the following steps to run the report.

- 1 Click the **Run** button. The Run a Report window appears.

Result A dialog window is displayed, indicating that the report is being generated. The window shows the progress of the report generation and the number of records retrieved that match the selected criteria.

If no event records are found that match the selected criteria, a warning dialog box is displayed, indicating that no records have been found and asks if you want to view the output anyway. Choose **Yes** to view the output anyway or **No** to cancel the report output.

- 2 Close the User Auth Editor window and User Auth browser after viewing the output.

END OF STEPS

To run multiple reports

Complete the following steps to run multiple reports.

- 1 Right-click on existing reports in the Contents panel and choose **Run Multiple Reports** from the pop-up menu.

Result The Run Multiple Filters window is displayed.

- 2 Click the **run report across each LSMS and LSCS** checkbox to collect and run a merged report of all network events for all connected LSMSs and Compute Servers. (This checkbox is checked, by default.)

-
- 3 Select the time range of the report.

To	Do This
Generate a report of the most recent network events that have occurred within the past 1 to 99 minutes.	Click the Last radio button in the Time Range portion of the window and enter a value (in minutes), up to 99. 5 minutes is the default value.
Generate a report for a specific time range with beginning/end dates	Click the Specify Time Range radio button. The Start and End date fields are displayed. Click the Earliest button to select the earliest available date and time and the Now button to select the current date and time, or manually enter the month/day/year and hours/minutes/seconds values in each field.

-
- 4 Click the **Run** button. The Run a Report window appears.

Result A dialog window is displayed, indicating that the report is being generated. The window shows the progress of the report generation and the number of records retrieved that match the selected criteria.

If no event records are found that match the selected criteria, a warning dialog box is displayed, indicating that no records have been found and asks if you want to view the output anyway. Choose **Yes** to view the output anyway or **No** to cancel the report output.

-
- 5 Close the User Auth Editor window and User Auth browser after viewing the output.

.....

END OF STEPS



User Authentication Report Output

When to use

The output from a User Authentication report is displayed in your web browser, and consists of a header and a body in table format with up to eighteen columns of information. [Figure 13-4, “User Authentication Report” \(p. 13-15\)](#) on the next page shows a fragment of a typical User Authentication report.

The report in [Figure 13-4, “User Authentication Report” \(p. 13-15\)](#) contains all eighteen columns. The administrator generating the report determines the number of columns that appear in the finished report.

The following sections explain the information in the header and all eighteen columns of the body.

Header

The header of a User Authentication report contains the following information:

- Page Number and Total Number of Pages**
 In the upper right corner of the header, above the title User Authentication, the report indicates the total number of pages in the report, and the number of the current page.
- Time Interval**
 In the center, under the sort order, the report indicates the time interval covered by the report. This is determined by the administrator when running the report.
- Total Records**
 On the left margin, under the time interval, the report indicates the number of records included in the report. This is the number of entries found in the body of the report. The number of records in the report depends upon how specifically you define the selection criteria when generating the report.

Figure 13-4 User Authentication Report

Header

1 of 1

User Authentication

Body

From: Thu Apr 20 09:30:36 EDT 2000 To: Tue May 30 19:40:36 EDT 2000

Total Records Found=31

Date	Source	Src Host	Src Port	Dst Host	Dst Port	Pool	User ID	Auth Service	Result	Reason	User Loc	Auth Timeout	Auth Action	Bytes Sent	Bytes Recvd	Elapsed Time	Group
2000/04/20 16:34:42	VPN	151.198.245.40	1049	151.198.245.47	500	UDP	john	Local Password	Success	N/A	Internal	2	Login	0	0	0	system
2000/04/20 16:35:22	VPN	151.198.245.40	1049	151.198.245.47	500	UDP	john	Local Password	Success	Administrator terminated the user	Internal	0	Logout	0	0	0	system
2000/04/20 16:37:01	VPN	151.198.245.40	1031	151.198.245.47	500	UDP	john	Local Password	Failure	Invalid password	Internal	0	Login	0	0	0	system
2000/04/20 16:37:16	VPN	151.198.245.40	1033	151.198.245.47	500	UDP	john	Local Password	Success	Password expired; re-enter new password	Internal	0	Login	0	0	0	system
2000/04/20 16:37:30	VPN	151.198.245.40	1033	151.198.245.47	500	UDP	john	Local Password	Success	N/A	Internal	2	Login	0	0	0	system
2000/04/20 16:39:38	VPN	151.198.245.40	1033	151.198.245.47	500	UDP	john	Local Password	Success	User logged out due to Authentication timeout	Internal	0	Logout	0	0	0	system
2000/04/20 16:59:05	VPN	151.198.245.40	1032	151.198.245.47	500	UDP	john	Local Password	Success	N/A	Internal	2	Login	0	0	0	system
2000/04/20 17:01:08	VPN	151.198.245.40	1032	151.198.245.47	500	UDP	john	Local Password	Success	User logged out due to Authentication timeout	Internal	0	Logout	0	0	0	system
2000/05/17 09:33:42	Firewall	151.198.245.41	1635	151.198.245.47	443	TCP	MEI	Radius	Success	N/A	Internal	2	Login				system
2000/05/20 18:38:41	Firewall	151.198.245.41	3038	151.198.245.47	443	TCP	Isms	SecurID	Failure	Authentication Failure -> ACM_ACCESS_DENIED	Internal	0	Login				system

Date Column

The first column in the body of the report is the **Date** column. It gives the date and time the user was authenticated as recorded in the User Authentication log, in the format:

year/month/day

hour:minute:second

Source Column

The **Source** column indicates the source of the user authentication session. The source can be:

- *Firewall users*, who are attempting to establish a session through the Brick, and
- *VPN users*, who are attempting to set up a VPN tunnel, with the Brick as the tunnel endpoint.

The administrator generating the report determines which source will be included in the report.

Src Host Column

The **Src Host** column provides the IP address of the source host. This is the host that initiated the session.

The administrator generating the report determines which source hosts will be included in the report.

Src Port Column

The **Src Port** column gives the source port. This is the port used by the application on the source Brick that initiated the session.

The administrator generating the report determines which source ports will be included in the report.

Dst Host Column

The **Dst Host** column provides the IP address of the destination host. This is the host that is intended to receive the session.

The administrator generating the report determines which destination hosts will be included in the report.

Dst Port Column

The **Dst Port** column gives the destination port. This is the port used by the application on the destination host to receive the session.

The administrator generating the report determines which destination ports will be included in the report.

Pcol Column

The **Pcol** column indicates the protocol that the session is using. The options are UDP, TCP or ICMP.

The administrator generating the report determines which protocols will be included in the report.

User ID Column

The **User ID** column indicates the identification of the user being authenticated.

The administrator generating the report determines which IDs will be included in the report.

Result Column

The **Result** column indicates the result of any user login attempt, which can be either success, failure, query or password.

The administrator generating the report determines which the value to be included in the report.

Auth Service Column

The **Auth Service** column indicates the authentication service that is used by an authentication method (i.e., Local Password, RADIUS, SecurID, or VPN certificate).

The administrator generating the report determines the value to be included in the report.

Reason Column

The **Reason** column provides more explanation on how and if the user was authenticated.

User Loc Column

The **User Loc** column is the location of the user, which can be either internal (to the Brick zone ruleset) or external.

The administrator generating the report determines the value to be included in the report.

Auth Timeout Column

The **Auth Timeout** column is the amount of time that has elapsed before the authentication process expires.

Auth Action Column

The **Auth Action** column is the action performed by the user, which can be either login, logoff, query, or password.

The administrator generating the report determines the value to be included in the report.

Bytes Sent Column

The **Bytes Sent** column is the total number of bytes in the session that were sent during authentication when the source is a VPN user.

Bytes Rcvd Column

The **Bytes Rcvd** column is the total number of bytes in the session that were received during authentication.

Elapsed Time Column

The **Elapsed Time** column is the amount of time that has elapsed for authentication.

Group Column

The **Group** column identifies the group that the user belongs to and is used in the session during authentication.



14 WebTrends Reports

Overview

Purpose

This chapter will step the user through the process of configuring the WebTrends application to translate LSMS session log files to WELF format (using Log2WELF.jar) and then using them to generate a WebTrends report. We assume that the LSMS log files and the WebTrends application reside on the same PC.

By default, all of the LSMS log files may be found on the same machine as the LSMS application. However, in order to convert the LSMS session log files into the WELF format, the session log files must be delivered to the WebTrends PC via "ftp". See [Appendix I, "Transferring Log Files via FTP"](#) elsewhere in this manual for additional information about that process.

Contents

Preparing the Environment	14-2
Web Trends Configuration	14-5
WebTrends Reports	14-14



Preparing the Environment

Task

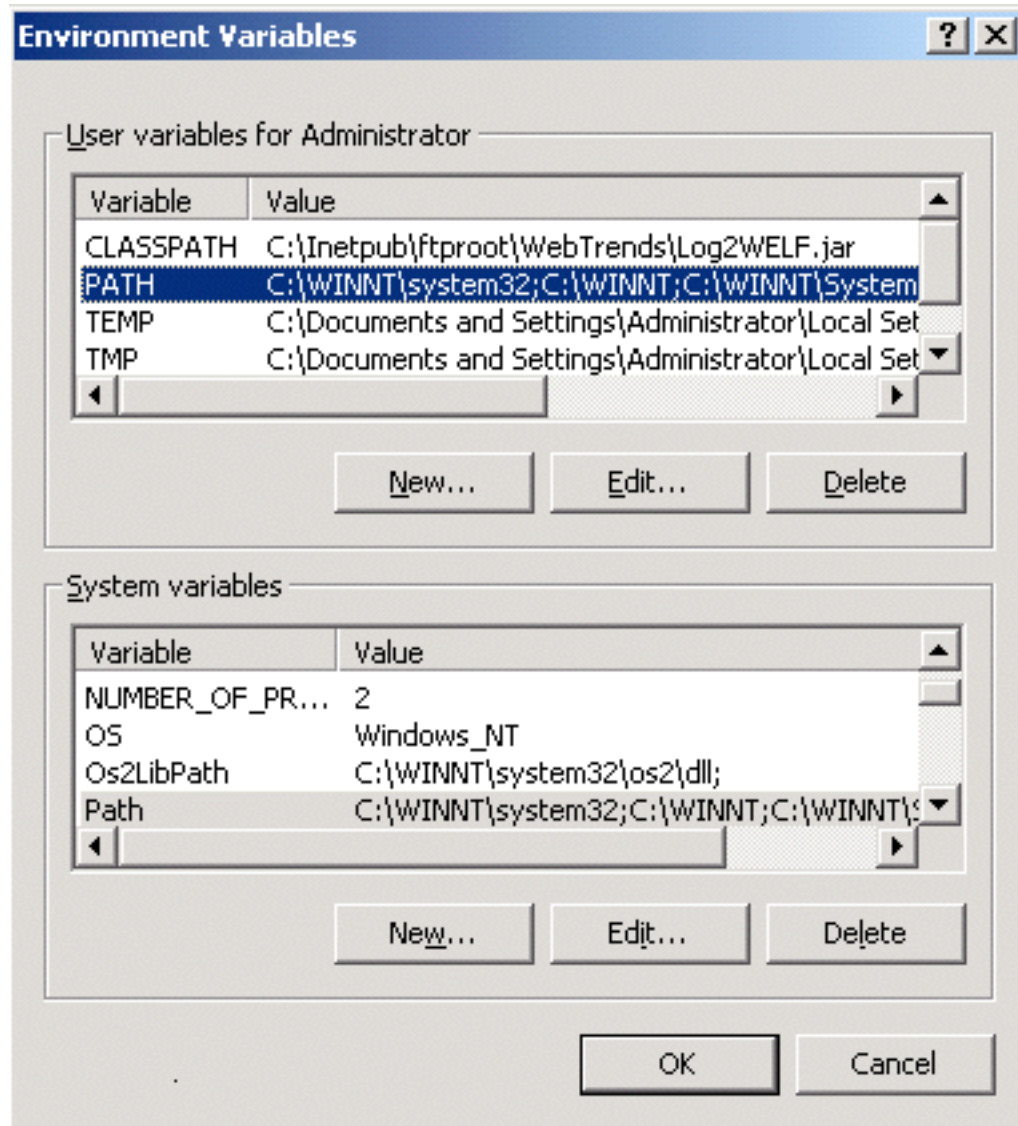
To run the Log2WELF.jar with WebTrends, the following changes must be made on the WebTrends PC:

- 1 Since Log2WELF.jar is a Java application, you must install Java version 1.3, available from www.sun.com.
- 2 The directory containing the Java executable must be added to your PATH.

To modify the PATH on Windows NT, perform the following steps:

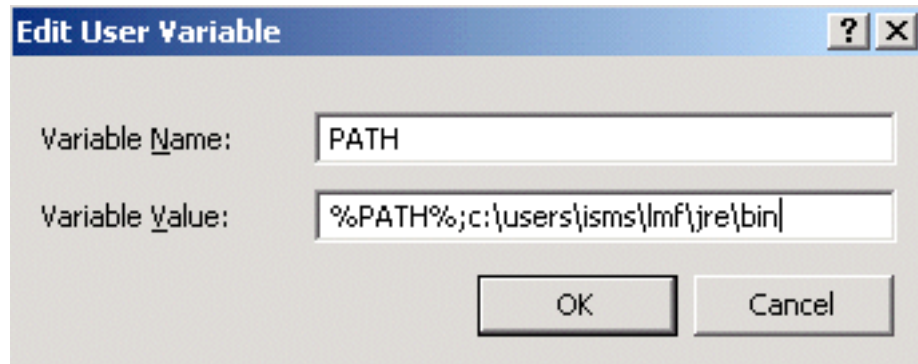
- Open the Control Panel and select the **System** icon to display the System Properties window. Then, click the **Environment** tab.
- On Windows 2000, use **System Properties** → **Advanced** → **Environment Variables**. Highlight the PATH variable as shown in [Figure 14-1, “Environmental Variables”](#) (p. 14-3).

Figure 14-1 Environmental Variables



-
- 3 Click **Edit** to append the directory for the Java executable. The Edit User Variable Window will appear (Figure 14-2, “Edit User Variable” (p. 14-4)).

Figure 14-2 Edit User Variable



-
- 4 Copy the Log2WELF.jar file from Tools\Reports folder on the LSMS CD to a directory of your choice.
 - 5 The Log2WELF.jar file must be added to your CLASSPATH. Follow the same procedure as outlined in Step 2 above.

END OF STEPS



Web Trends Configuration

Generating a WebTrends report

Now that the environmental changes have been made to the WebTrends PC, we can explore the details of the two procedures that lead to a WebTrends report:

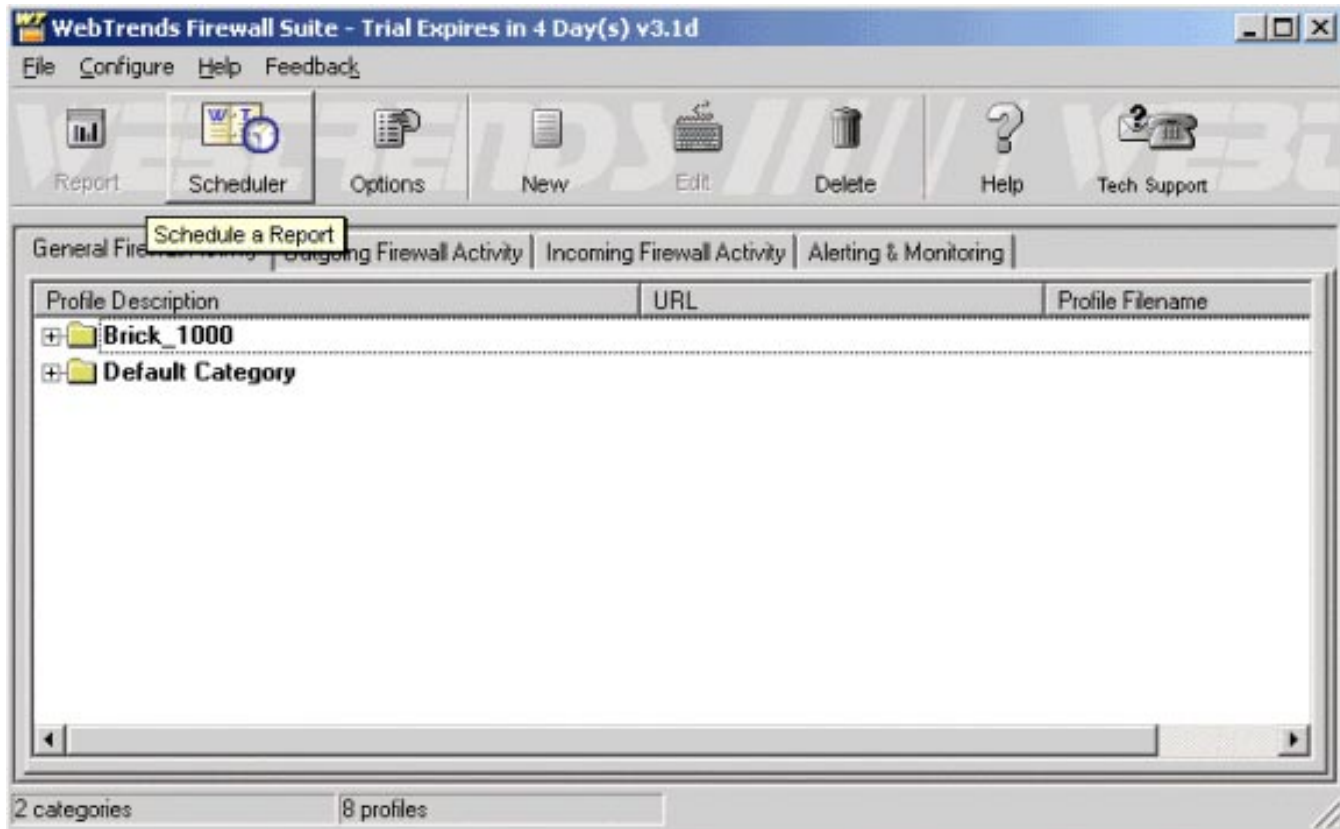
- Convert LSMS Session Logs to WELF (using Log2WELF.jar)
- Configure the WebTrends report

Convert LSMS Session Logs to WELF

The section describes how to automate the conversion of the LSMS Session Logs to WebTrends WELF format using WebTrends and Log2WELF.jar. The jar file will convert and separate session logs into a directory defined by the user. The logs will also be further divided into different directories based on *Brick*[®] Names / Group Name / Zones / Logs.

- 1 Launch WebTrends and click the **Scheduler** button. The Scheduler allows WebTrends to automatically convert LSMS logs to WELF format at specified intervals configured by users (Figure 14-3, “Webtrends Scheduler” (p. 14-6)).

Figure 14-3 Webtrends Scheduler



- 2 In the Scheduler window, click on the **Add** button. This will display a pop-up window, and you will select **Incoming Web Activity**.
- 3 In the Add Scheduled Event window, choose the duration for the **Start Time & Date** and **Repeat Every** fields and then click **Next**.
- 4 The Reporting screen defines the report style, the location where the report will be saved and the report name. The default style is HTML. Click **Next**.

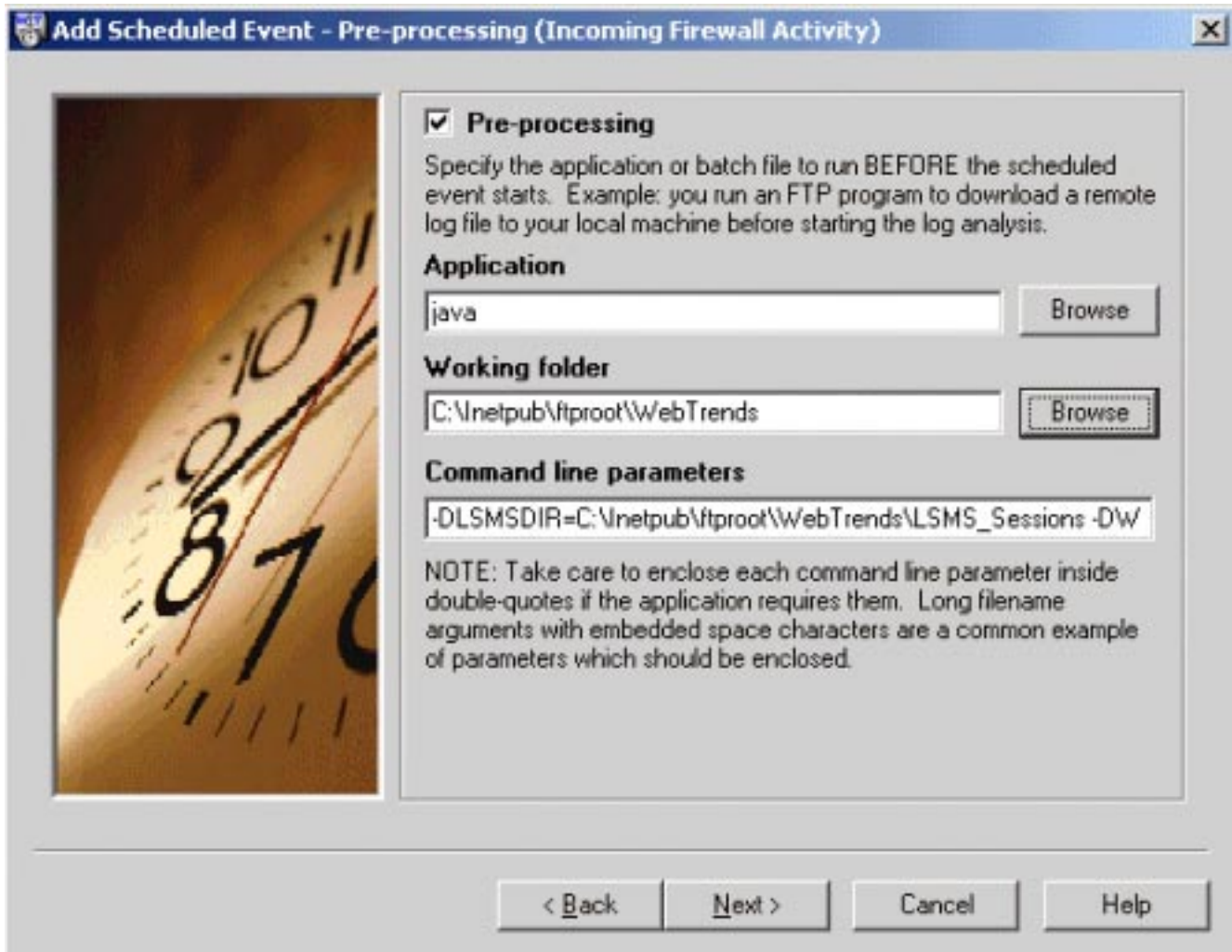
-
- 5 The Pre-processing screen specifies the application that needs to be run before creating the report. This is where the Log2WELF.jar file is used to reformat the LSMS Session Logs into WELF format, prior to generating the WebTrends reports. Fill in the following fields (Figure 14-4, “Add Scheduled Event Window” (p. 14-8)):
- **Application:** Java
 - **Working Folder:** Directory path to Log2WELF.jar
 - **Command Line Parameter:** Command used to run Log2WELF.jar. The following shows the syntax for this command. Please note that this is a one-line command that automatically wraps onto the next line when space runs out on the first line.

```
-classpath [directory path to Log2WELF.jar] -DLSMSDIR=  
[Source directory path  
where LSMS session logs reside] -DWELFDIR=  
[Target directory path where the WELF  
files will reside] LogFileMonitor
```

The following is an example of this command:

```
-classpath c:\WedTrends\Lon2WELF.jar -DLSMSDIR=C:\Inettpub\ftproot\  
WedTrends\  
LSMS_Sessions -DWEFDIR=C:\Inettpub\ftproot\WedTrends\WELF_  
Files LogFileMonitor
```

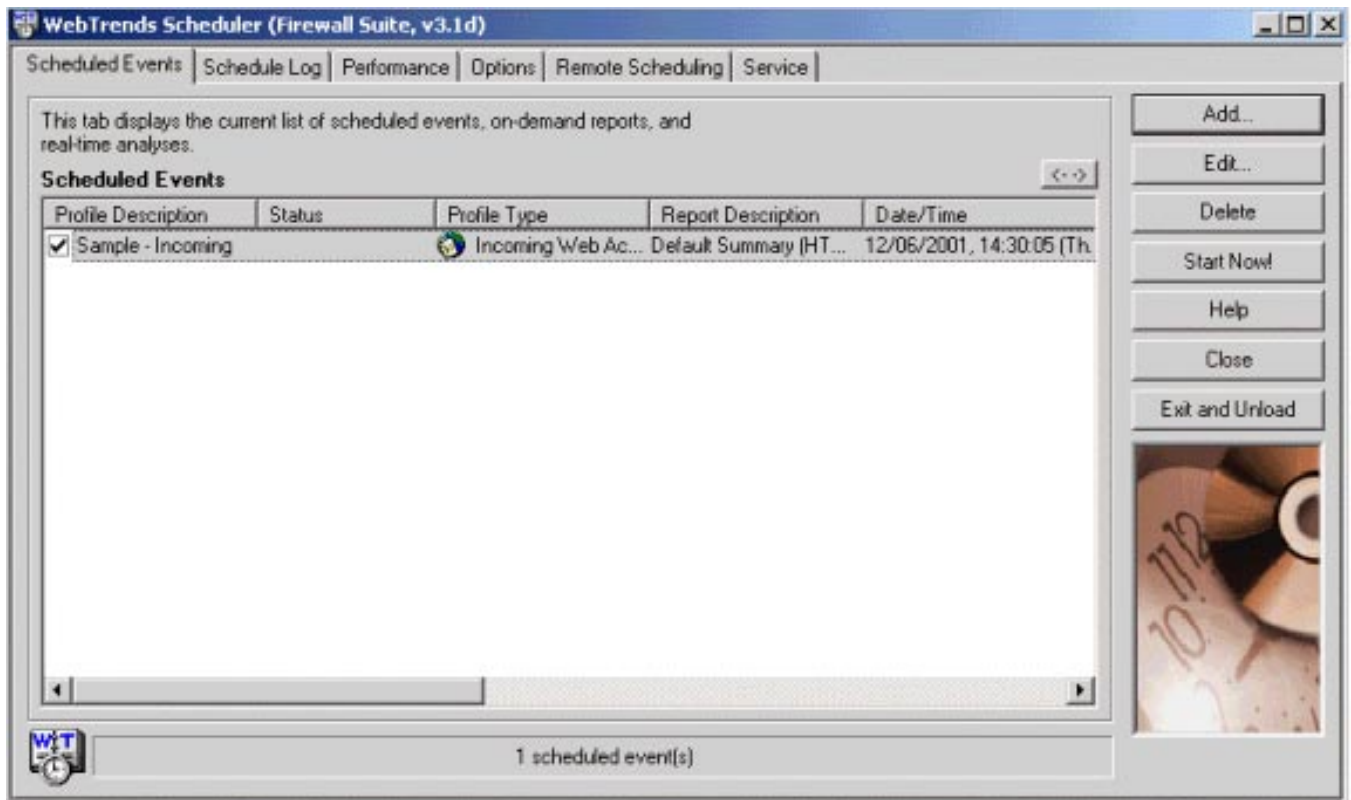
Figure 14-4 Add Scheduled Event Window



- 6 No need to configure post-processing, so click **Next**.
- 7 Select the priority for this Scheduler Event from the Priority screen. See WebTrends documentation or OnLine Help for further information.
- 8 Click **Finish**.
- 9 The Scheduled Event should now appear in the Scheduler window ([Figure 14-5, “Webtrends Scheduler”](#) (p. 14-9)). The Scheduler is now prepared to convert the

session logs into WELF format at the specified interval that you defined. The user may override this interval by clicking **Start Now**.

Figure 14-5 Webtrends Scheduler



You can also click on this button to verify that the Scheduler has been properly configured. If clicked, a DOS window should appear on the Windows desktop ([Figure 14-6, “DOS Window \(Start Now\)”](#) (p. 14-10)). In addition, the updated WELF files

should be available in the directory configured in the Pre-processing window of the Scheduler.

Figure 14-6 DOS Window (Start Now)

```

c:\users\isms\lrf\jre\bin\java.exe
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1007664689375\attappbr1\nikfailover\vpnnfo_1e
5 directory created
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1007664689375\attappbr1\nikfailover\vpnnfo_1e
5\2001-08-20-10-20-.log file created
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1007664689375\attappbr2\nikfailover\vpnfoik_2
e5 directory created
C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\1007664689375\attappbr2\nikfailover\vpnfoik_2
e5\2001-08-20-10-20-.log file created

lines read: 20000
file starts: 1
Memory - total: 1984K free: 1370K used: 615K

lines read: 30000
file starts: 1
Memory - total: 1984K free: 1663K used: 322K

lines read: 40000
file starts: 1
Memory - total: 1984K free: 1320K used: 665K

lines read: 50000
file starts: 1
Memory - total: 1984K free: 1437K used: 548K
  
```

-
- 10 You are now ready to generate WebTrends reports.

END OF STEPS

Configuring and Generating WebTrends Reports

This section will describe how to create a report for a specific zone on a Brick. In our example, it is assumed that each zone represents a different customer. More information on report configuration may be found in the WebTrends documentation.

-
- 1 Launch WebTrends and ensure that the General Firewall Activity tab is active. From the File Menu Bar, select the **New Category** option.

 - 2 Highlight the newly created Category by clicking on it, then select **New Profile** from the File menu. A profile represents a zone on a particular Brick.

-
- 3** The Add General Web Activity Profile will pop up. Select **My firewall is on one physical machine** and click **Next**.

- 4 On the "Title, Log File Format" window (Figure 14-7, "Title, Log File Format Window" (p. 14-12)), we need to:
 - Type in a description and select WebTrends Enhanced Log Format from the drop down menu.
 - Select **Yes** for the Log Path Configuration (since the WELF files reside on the same machine).
 - Enter the directory path to the WELF logs that were generated by the Log2WELF.jar tool. Use the browse option button, if there is only one specific log that you require within the Zone directory -OR - use the Extended Browse button option. Then, click the **Add** button to choose all the log files within the Zone directory. Click **Next**.

Figure 14-7 Title, Log File Format Window

Add General Web Activity Profile -- Title, Log File Format

Description:
Sim Brick
Log File Format:
WebTrends Enhanced Log Format (WELF)

Log Path Configuration:
 Yes, my firewall log files are already in a location accessible by this machine.
 No, I would like to configure WebTrends to use its built-in Syslog server to collect the logs on this machine.

Log File Path:
file:/// C:\inetpub\vtproot\WebTrend
You can use wildcards (*,?) in log file paths and log file names to process multiple files in one report. Examples...

< Back Next > Cancel Help

- 5 In the IPs Behind Firewall window, add the (optional) list of IP addresses. Click **Next**.

-
- 6 If you need to configure the DNS Lookup Window, refer to the WebTrends documentation. Once completed, click **Next**.

 - 7 In the Filters window, you can specify the type of traffic that you are looking for. The Include Everything filter is selected by default. Once completed, click **Next**.

 - 8 Enter the Cost of Bandwidth per Kilobyte and Currency, if necessary, then click **Next**.

 - 9 In the Database and Real Time window, accept the default values. If you require additional information, refer to the WebTrends documentation. Click **Next**.

 - 10 In the Advanced Fast Trends window, accept the default values. If you require additional information, refer to the WebTrends documentation. Click **Finish** to return to the main WebTrends window.

A new profile should appear under the category that you created back in step 1. To run the report, double click on the profile that you have just created. A window called Create Report will display. The default report format is HTML, so make sure that a browser is installed on your machine.

To choose a different report format, click the drop-down menu and select the format required, and click on the **Start** button.

END OF STEPS



WebTrends Reports

Types of WebTrends reports

A number of WebTrends reports can be run with the session log data provided by the LSMS:

- General Firewall Statistics
- Firewall Rules Triggered by Internal Clients and Servers
- Bandwidth Summary
- Web Summary
- E-mail Summary
- FTP Summary
- Telnet Summary
- Outgoing Traffic by Protocol
- Critical Events for Internal Clients
- Critical Events for External Clients
- Largest Outgoing E-mail Connections



Appendix A: SNMP

Overview

Purpose

This appendix explains how to send Simple Network Management Protocol (SNMP) traps from the LSMS to a Network Management Station (NMS).

The SNMP agent that comes with the LSMS software is also described. The agent responds to queries initiated by an SNMP-based Network Management System (NMS). The LSMS returns data to the NMS, which includes status of elements (such as Lucent VPN Firewall *Brick*[®], devices and the LSMS itself) in the network.

Many network administrators use an NMS (such as HP OpenView) to manage network elements within their corporate networks. Both SNMP traps and the SNMP agent allows NMS Administrators to monitor trends in the network.

Contents

What are SNMP Traps?	A-2
What is the SNMP Agent?	A-9
How to Collect Data from the LSMS	A-15



What are SNMP Traps?

Definition: SNMP traps

In the LSMS environment, SNMP traps are associated with an alarm action (see [Chapter 4, “Introduction to Alarms”](#) in this guide). The SNMP Trap action can be associated with any trigger. When the trigger fires, the SNMP trap is sent to a designated NMS host and UDP port.

Once the SNMP trap is received on the NMS and the NMS administrator is notified, the NMS administrator would log into the LSMS and analyze the situation by viewing log files or generating reports.

Important! *Unidirectional Transmission*

SNMP traps are uni-directional.

The SNMP agent supports bi-directional transmissions. The agent can be polled for statistics regarding the state and health of all Bricks in the network and the LSMS software itself (see [“What is the SNMP Agent?”](#) (p. A-9) in this appendix).

OID

Each alarm type (e.g., Unauthorized LSMS Login Attempt, Brick Lost) has a unique Object ID (OID).

This allows the NMS to uniquely associate the trap with a specific alarm type. The network administrator can then determine exactly which alarm type has occurred.

Each OID in the MIB will begin with the prefix of:

```
iso.org.dod.internet.private.enterprises.lucent.  
(1.3.6.1.4.1.1751)
```

SNMP Trap Contents

Each SNMP Trap contains data elements that are specific to the type of alarm that has occurred. These data elements are defined in the MIB. In addition to the 'alarm specific' information, each trap also includes:

- Alarm Index
- Alarm Trigger Time
- Alarm Details (unparsed)
- Alarm Log Entry
- Alarm Trigger Name

LSMS Alarms include the LSMS name while Brick alarms include the Brick name.

How to Send SNMP Traps

The LSMS can send traps in SNMPv1 or SNMPv2c format. Select the format required by your NMS as part of the SNMP Trap action configuration.

- 1 Install and load the Management Information Bases (MIBs) on the NMS. The MIBs can be found on the LSMS CD-ROM.
- 2 Optionally, if a Brick is positioned between the LSMS and the NMS, you need to create at least one rule so the SNMP trap can be passed through the Brick and onto the NMS.
- 3 Optionally, configure the NMS so that when a trap is received from the LSMS, the NMS node will change color.


END OF STEPS

Install and Load the MIBs on Windows NT

To decode the information in the trap, the NMS uses MIBs that are provided on the LSMS CD-ROM. The following steps describe how to install and load the MIBs on an HP OpenView Windows NT NMS.

- 1 Log into the NMS.
- 2 Navigate to the folder `\OpenView\tmp`.
- 3 On the LSMS CD-ROM, click the SNMP folder, then click on **SNMPv1_MIBS** or **SNMPv2c_MIBS**, depending on which version is supported by your NMS.
- 4 Copy the MIBs from the CD-ROM into `\OpenView\tmp`.
- 5 On the NMS, load the MIBs one at a time by selecting Load/Unload MIBs:SNMP from the **Options** menu.

6 To browse the trap definitions from the NMS Browser:

- Select **Tools**  **SNMP MIB Browser**.
- Double-click **Down Tree**.
- Double-click **private**.
- Double-click **enterprise**.
- Double-click **lucent**.

END OF STEPS

Install and Load the MIBs on Solaris

The following steps describe how to install and load the MIBs on a Solaris HP OpenView NMS.

1 Log into the NMS.


2 Change directory to */var/opt/OV/tmp*.

3 On the LSMS CD-ROM, click the SNMP folder, then click on **SNMPv1_MIBS** or **SNMPv2c_MIBS**, depending on which version is supported by your NMS.

4 Copy all eight MIBs from the CD-ROM into */var/opt/OV/tmp*.

5 On the NMS, load the MIBs one at a time by selecting Load/Unload MIBs:SNMP from the **Options** menu.

6 To browse the trap definitions from the NMS Browser:

- Select **Tools**  *SNMP MIB Browser*.
- Select the **Down Tree** button.
- Select **private**.
- Select the **Down Tree** button.
- Select **enterprise**.

- Select the **Down Tree** button.
- Select **lucent**.

.....
E N D O F S T E P S
.....

How to Create Rules

When SNMP traps travel between the LSMS and an NMS residing on the same LAN, creating additional security rules to pass the SNMP (UDP/162) traffic is not necessary. Typically, however, a Brick is protecting the LSMS and is positioned between the NMS and the LSMS. Therefore, creating a security rule to pass the SNMP (UDP/162) traffic between them becomes necessary. One security rule needs to be added to the Administrative Zone (or NOC Gateway Zone) to pass the SNMP trap from the LSMS to the NMS. The rule below allows SNMP traps to pass from the LSMS, from the Administrative Zone (or NOC Gateway Zone), through a Brick and onto the NMS.

To create this rule, follow the steps below:

- 1 Open the Policies folder.
.....
- 2 Open the Brick Zone Rulesets folder and double-click the administrativezone (or nocgwzone).
.....
- 3 In the Brick Zone Ruleset Editor, right-click any rule and select **New**.
The Brick Zone Rule Editor appears.
.....
- 4 In the **Direction** field, select **Out Of Zone** from the dropdown list. This rule will now apply to sessions initiated inside the Administrative Zone.
.....
- 5 In the **Source** field, click **Host** and enter the IP address of the LSMS. This ensures that only sessions initiated by this IP address are permitted to pass through the Brick.
You could also enter an asterisk, since the LSMS should be the only host in the Administrative Zone.
.....
- 6 In the **Destination** field, click **Host** and enter the IP address of the NMS.

- 7 In the **Service** or **Group** field, select BROWSE. In the Browse: Select a Service Group window, select **snmp_trap** from the dropdown list. This is a Service Group defined as UDP/162/* and provided with the LSMS specifically for this purpose.
- 8 In the Action field, select **Pass** from the dropdown list.
- 9 In the **Audit Session** field, Basic auditing is the default. You can leave this as is, or select **None** or **Detailed**, depending on your needs.
- 10 In the **Description** field, enter an optional description, if necessary.
- 11 In the **Rule Active** field, the default is **Yes**. Leave the default in place, so that the rule will become active as soon as it is applied to a Brick.
- 12 Click the Advanced tab and ensure that **Authorize Return Channel** is NOT checked.
- 13 Click the **OK** button to temporarily store the rule on the LSMS.
- 14 Display the File menu and select one of the **Save** options.

Important! *Additional Rule*

If a Brick zone ruleset does exist between the Brick and NMS, then an additional rule needs to be added for the Brick zone ruleset.


The rule would be identical to the rule above, except the Direction would be *In To Zone*.

END OF STEPS

Configure the NMS

After loading the MIBs onto the NMS, you can optionally configure the NMS so that the icon for the LSMS node on the NMS will change color when an SNMP trap is sent from the LSMS. Once a trap has been sent, double-click the LSMS node icon to change the color of the back to the normal green.

To configure the NMS so that the LSMS node changes color on a Windows NT platform:

-
- 1 Log into the NMS.
-
- 2 On the NMS, select the LSMS node.
Do the following:
 - From the taskbar, select **Map**  **Properties**.
 - Select the Applications tab.
 - Select the **IP Map** entry in the Configurable Applications pulldown and then click the **Configure For This Map** button.
 - Change the "On-Demand: To what level should submaps be persistent?" value to **Internet Level**.
 - Click **Verify** and then **OK**.
 - Click **Apply** and then **OK**.
-
- 3 Right-click the LSMS node.
Do the following:
 - Select **Symbol Properties** from the popup menu.
 - Change the Status Source to **Object**.
 - Click **OK**.
-
- 4 Restart the NMS.
- END OF STEPS
-

Task

To configure the NMS so that the LSMS node changes color on a Solaris platform:

-
- 1 Add the OV bin directory to the PATH in */etc/profile*. For example, add */opt/OV/bin*.
-
- 2 Open the NMS.
-
- 3 On the NMS Terminal, select the LSMS node.

Do the following:

- From the taskbar, select **Map ► Properties**.
 - Select the **IP Map** entry in the Configurable Applications pulldown and then click the **Configure For This Map** button.
 - Change the "On-Demand: To what level should submaps be persistent?" value to **Internet Level**.
 - Click **Verify**, then click **OK**.
 - Click **OK**.
-

4 Right-click the LSMS node.

Do the following:

- Select **Symbol** from the popup menu.
 - Change the Status Source to **Object**.
 - Click **OK**.
-

5 Restart the NMS.

END OF STEPS

Auditing and Reporting

To aid in troubleshooting, you can view the Administrative Events log file or generate an Alarms Logged report.

When an SNMP trap is sent to an NMS, the event is written with a record type of 21 or 22 to the Administrative Events log. The log message includes:

- The time/date the alarm was triggered
- A label that indicates the action was "Send an SNMP Trap"
- The IP address of the NMS host
- The UDP port used to send the SNMP trap to the NMS host
- Whether or not the trap transmission took place or not (i.e., did it experience any I/O exceptions upon transmit)

For details, refer to [Chapter 9, "Administrative Events Report"](#) and [Chapter 12, "Alarms Logged Report"](#) in this guide.



What is the SNMP Agent?

Definition: SNMP agent

The SNMP agent is a process that runs on the LSMS only. For security reasons, SNMP agents are not allowed to run on any Brick in the system. However, an agent running on the LSMS will provide data from Bricks to the NMS.

An NMS can poll the SNMP agent for statistics regarding the state and health of all Bricks in the system, and the LSMS software itself. The NMS can request configuration, status, and statistical information from many elements of the system, such as the Logger and the User Authentication Server.

The SNMP agent obtains Brick statistical information primarily from the Proactive Monitoring log. This log contains information reported by each Brick in the system and is updated every 30 seconds. Therefore, the NMS does not need to poll the LSMS for information more frequently than about every 30 seconds. For standalone LSMSs, information for all Bricks is available. For redundant LSMSs, only information on Bricks that are currently homed to a given LSMS is available on that host.

During installation of the LSMS application, you are prompted for the UDP port the agent listens on. The default port is 161. Either accept the default or enter another port number.

You should only change the default if you already have or are planning on installing a third-party agent on the LSMS host using port 161.

After installation, this port setting can be changed with Configuration Assistant. See Chapter 10. Using the Configuration Assistant in the LSMS Administration Guide for details.

Multiple SNMP Agents

The SNMP agent that comes with the LSMS software does not provide information about the LSMS host or the operating system.

If this is desired, you must install a separate third party SNMP agent (not provided with the LSMS software) on the LSMS host or configure/enable the SNMP agent that comes with the operating system (e.g., SNMP Agent Service on Windows).

If you will be running the operating system SNMP agent or a third party SNMP agent as a third party SNMP agent on the LSMS, both agents cannot be configured to use default SNMP port 161. Use the LSMS Configuration Assistant to define which port is used by the System SNMP agent and which port is used by the LSMS SNMP agent. For more information on the LSMS Configuration Assistant, see Chapter 10 Using the Configuration Assistant in the *LSMS Administration Guide*.

Configure your NMS to make GET requests to the LSMS SNMP agent port. If the request is for information in the LSMS MIB, the LSMS SNMP agent will respond. If not, the request is forwarded to the System SNMP agent.

OID 56

The Lucent Secure/VPN Solutions Group has been assigned OID 56 off Lucent Technologies' IANA-Assigned enterprises node (enterprises 1751).

Two nodes have been assigned — one for products and one for MIBs. The following is taken from the Global Registrations MIB:

```
--the root of the enterprises sub-tree for Lucent Technologies
lucentRoot OBJECT IDENTIFIER ::= { iso(1) org(3) dod(6) internet(1)
  private(4) enterprises(1) lucent(1751) }

--the Lucent Technologies TRA structure uses two arcs: products and
  MIBs
lucentProductRoot OBJECT IDENTIFIER ::= { lucentRoot products(1) }
lucentMibRoot OBJECT IDENTIFIER ::= { lucentRoot mibs(2) }

--the pair of nodes assigned to Secure/VPN Solutions
svsProductRoot OBJECT IDENTIFIER ::= { lucentProductRoot
  svsProducts(56)}
svsMibRoot OBJECT IDENTIFIER ::= {lucentMibRoot svsMibs(56)}
```

Agent and MIB Design

The SNMP agent is compliant with SNMP v2. Eight Management Information Bases (MIBs) are provided on the LSMS CD-ROM. They were written using rules outlined in SMIV2 (Structure of Management Information, v2) in RFC 1902, 1903, 1904.

The Lucent MIBs are private but based on MIB-II. Many parameters found in MIB-II are supported in the Lucent MIBs under private OIDs. All MIB modules are prefixed by "svs," which stands for Lucent "Secure/VPN Solutions."

The Lucent MIBs contain two basic types of information: configuration and statistical. Generally, the MIBs are designed such that these two pieces of information are kept separate. The MIBs are as follows:

MIB Name	MIB Description
<i>svs-global-reg.mib</i>	<p>LUCENT-SECURE-VPN-SOLUTIONS-GLOBAL-REG</p> <p>The Global Registration module contains the assigned numbers for all other modules, as well as entry points for conformance, capabilities, requirements, and experimental sections to be added.</p> <p>It also contains OIDs for current products including Bricks, the LSMS, etc. All modules depend on the Global Registration Module. This MIB includes the ipsecClient MIB.</p>
<i>svs-Brick-mib.mib</i>	<p>LUCENT-SECURE-VPN-SOLUTIONS-Brick-MIB</p> <p>The Brick module is the most complex of all the modules. Since there can be many Brick devices in the system, and each Brick device has multiple interfaces, there needs to be several layers of hierarchy to accommodate all information. However, since SMIV2 does not allow nesting of tables, the data is arranged in the following five related tables:</p> <ul style="list-style-type: none"> • Brick Configuration • Brick Statistics • Brick Interface Configuration • Brick Interface Statistics • Brick Tunnel Endpoints
<i>svs-lsms-mib.mib</i>	<p>LUCENT-SECURE-VPN-SOLUTIONS-LSMS-MIB</p> <p>The LSMS module contains basic configuration and statistical information about the LSMS, as well as all objects related to notifications (traps). The LSMSEvents object is contained in the LSMS module.</p> <p>This module also contains a table of up to six alarms, so if the NMS believes it may have missed a notification due to network packet loss, it may query the LSMS alarms table. Each entry in the table contains the same information that is sent in the notification.</p>

MIB Name	MIB Description
<i>svs-lsms-notification-mib.mib</i>	<p>LUCENT-SECURE-VPN-SOLUTIONS-LSMS-NOTIFICATIONS-MIB</p> <p>The Notifications module contains one notification-type for every LSMS alarm that exists in the LSMS. All notifications are sent with respect to objects in the LSMS module.</p> <p>Each notification contains the date/time it was triggered and a plain-text explanation as to what happened. Since each notification has its own type, no type information is included within the notification body.</p> <p>There are no tables in this module.</p>
<i>svs-auditsvr-mib.mib</i>	<p>LUCENT-SECURE-VPN-SOLUTIONS-AUDITSVR-MIB</p> <p>The Audit Server module is designed to allow the NMS to query the Audit Server process to determine the number and type of audit logs currently in service on that host, as well as current statistics regarding free space and usage rates.</p> <p>There is no ability to view log records via SNMP.</p> <p>This module contains a table with information about each audit log on the device (such as the AdminEvents log and Proactive Monitoring log).</p>
<i>svs-authsvr-mib.mib</i>	<p>LUCENT-SECURE-VPN-SOLUTIONS-AUTHSVR-MIB</p> <p>The Authentication Server module gives statistics and configuration regarding the Authentication Server process. Currently, the Auth Server must be collocated on the LSMS host.</p> <p>This module only has a very small number of parameters.</p> <p>There are no tables in this module.</p>

Issue a Query to the LSMS

The following procedure illustrates using a Windows NT HP Openview MIB Browser to query the LSMS.

To browse the MIB definitions:

-
- 1 Do the following:
 - Select **Tools** ► **SNMP MIB Browser**
 - Double-click **Down Tree**
 - Double-click **private**

- Double-click **enterprise**
 - Double-click **lucent**
-

2 To issue a query to the LSMS:

- Select any MIB Object ID (e.g., svsBrickMIBs)
 - Click the **Start Query** button
- Information for the Brick is displayed, such as the model of the Brick, the LSMS IP address, version of software running on the Brick, etc.

END OF STEPS

Create a Rule

When SNMP queries and responses travel between the LSMS and an NMS residing on the same LAN, creating additional security rules to pass the SNMP (UDP/161) traffic is not necessary. Typically, however, a Brick is protecting the LSMS and is positioned between the NMS and the LSMS. Therefore, creating a security rule to pass the SNMP (UDP/161) traffic between them becomes necessary. One security rule needs to be added to the Administrative Zone (or NOC Gateway Zone) to pass the SNMP query from the NMS to the LSMS.

To create this rule, follow the steps below:

- 1** Open the Policies folder.

- 2** Open the Brick Zone Rulesets folder and double-click the administrativezone (or nocgwzone).

- 3** In the Brick Zone Ruleset Editor, right-click any rule and select **New**.
The Brick Zone Rule Editor appears.

- 4** In the **Direction** field, select **In To Zone** from the dropdown list. This rule will now apply to sessions initiated outside of the Administrative Zone.

- 5** In the **Source** field, click **Host** and enter the IP address of the NMS. This ensures that only sessions initiated by this IP address is permitted to pass through the Brick.

-
- 6 In the **Destination** field, click **Host** and enter the IP address of the LSMS.
.....
 - 7 In the **Service or Group** field, select BROWSE. In the Browse: Select a Service Group window, select **snmp** from the dropdown list. This is a Service Group defined as UDP/161/* and provided with the LSMS specifically for this purpose.
.....
 - 8 In the **Action** field, select **Pass** from the dropdown list.
.....
 - 9 In the **Audit Session** field, **Basic** auditing is the default. You can leave this as is, or select **None** or **Detailed**, depending on your needs.
.....
 - 10 In the **Description** field, enter an optional description, if necessary.
.....
 - 11 In the **Rule Active** field, the default is **Yes**. Leave the default in place, so that the rule will become active as soon as it is applied to a Brick.
.....
 - 12 Click the Advanced tab and ensure that **Authorize Return Channel** is checked.
.....
 - 13 Click the **OK** button to temporarily store the rule on the LSMS.
.....
 - 14 Display the File menu and select one of the **Save** options.

Important! *Additional Rule*

If a Brick zone ruleset exists between the Brick and NMS, then an additional rule needs to be added for the Brick zone ruleset.

The rule would be identical to the rule above, except the *Direction* would be *Out Of Zone*.

.....
E N D O F S T E P S
.....



How to Collect Data from the LSMS

Methods of collecting information from the LSMS

There are four typical methods that an NMS or NMS Administrator could use to gather information from the LSMS.

The four methods used to obtain information from the LSMS are as follows:

- *Automatic Demand Polling*
This is generally initiated by the LSMS periodically to ensure the device is still up, available, reachable, and responding to requests. HP OpenView uses a combination of ICMP 'ping' and SNMP GETREQUEST to verify the device status. For this to work correctly, the NMS must be instructed on the exact IP address and OID to request the status for each device or subsystem.
- *Automatic Polling of Statistics*
This is almost always a manually-configured process whereby the NMS Administrator sets up certain OIDs to retrieve information periodically from specific devices. The NMS then automatically retrieves the value returned for that specific OID at the configured interval. The NMS can then be configured to alarm on threshold crossings, or archive polled values, or even display real-time graphs of these statistics. Of course, historical graphs could be generated from archived values, but this does not involve SNMP at the time when the graph is created.
- *Trap-Directed Polling*
This can be either a manual or automatically initiated process, depending on the functionality provided by the NMS. Once the NMS receives a notification (trap), the NMS would poll the source of the trap for more information. For example, if a Proactive Monitoring alarm was received with a threshold crossing event, the NMS may want to know related information. It would then perform a series of GETREQUESTS to find that additional information.
- *Administrator-Initiated Polling*
This is always a manual process, usually begun by browsing through the MIB for a particular object, and selecting an OID. The NMS then creates the GETREQUEST, sends it to the element, receives the response, and then displays it to the Administrator.

□

Appendix B: Alarm Code Rules

Overview

Purpose

This appendix explains how to embed an alarm code in a rule so that an alarm is generated. You must configure an Alarm Code trigger before you can embed an alarm code in a rule however. To configure such a trigger, see [“Alarm Code Trigger”](#) (p. 6-7) in [Chapter 6, “Configuring Alarm Triggers”](#) in this guide.

If an alarm that is associated with a trigger is generated, the way you are notified is determined by the action(s) associated with the Alarm Code trigger.

Contents

Analyze Security Events First	B-2
How to Create the Alarm Code Rules	B-3



Analyze Security Events First

When to use

Before creating the rule with the alarm code, you need to determine:

- Which security events you want to be notified of
- How you want to be notified

Certain events are potentially serious, and you will probably want to be notified immediately with a message to your pager.

Other events may not require immediate attention, and so a console or syslog message may suffice.



How to Create the Alarm Code Rules

When to use

Once you have determined the events you want to be notified of, you have to develop a security policy that define these events.

For example, suppose an Administrator wants to know when unauthorized hosts attempt to connect to a particular FTP server. Two rules would have to be written to accomplish this.

Create Rule #1

This section describes how to create the first rule that allows hosts in the host group *ftpclients* to connect to FTP servers (as defined in the *ftp_servers* host group).

To create the first rule that allows hosts in the host group *ftpclients* to connect to FTP servers, perform the following steps:

-
- 1 Open the Policies folder.

 - 2 Open the *Brick*® Zone Rulesets folder and double-click the zone protecting the FTP servers.

 - 3 In the Brick Zone Ruleset Editor, right-click any rule and select **New**.
The Brick Zone Rule Editor appears.

 - 4 In the **Direction** field, select **In To Zone** from the drop down list. This rule will now apply to sessions initiated outside of the zone.

 - 5 In the **Source** field, click **Host**, select Browse, and select the host group (*ftp_clients*) that contains the IP addresses of FTP clients that may be attempting to connect to the FTP servers.

 - 6 In the **Destination** field, click **Host**, select Browse, and select the host group that contains the IP addresses of the FTP servers (*ftp_servers*).

 - 7 In the **Service or Group** field, select Browse, and select **ftp** from the dropdown list. This is a Service Group provided with the LSMS application.

-
- 8 In the **Action** field, select **Pass** from the dropdown list.
.....
 - 9 In the **Audit Session** field, **Basic** auditing is the default. You can leave this as is, or select **None** or **Detailed**, depending on your needs.
.....
 - 10 In the **Description** field, enter an optional description, if necessary.
.....
 - 11 In the **Rule Active** field, the default is **Yes**. Leave the default in place, so that the rule will become active as soon as it is applied to a Brick.
.....
 - 12 Click the **OK** button to temporarily store the rule on the LSMS.
.....
 - 13 Display the File menu and select one of the **Save** options.

.....
E N D O F S T E P S
.....

Create Rule #2

To create the second rule that will drop all other sessions that attempt to connect to the FTP server, follow the steps below:

-
- 1 Open the Policies folder.
.....
 - 2 Open the Brick Zone Rulesets folder and double-click the zone protecting the FTP servers.
.....
 - 3 In the Brick Zone Ruleset Editor, right-click any rule and select **New**.
The Brick Zone Rule Editor appears.
.....
 - 4 In the **Direction** field, select **In To Zone** from the dropdown list. This rule will now apply to sessions initiated outside of the zone.
.....
 - 5 In the **Source** field, accept the default (*).
.....

- 6 In the **Destination** field, click **Host**, select Browse, and select the host group that contains the IP addresses of the FTP servers (*ftp_servers*).
- 7 In the **Service or Group** field, select Browse, and select **ftp** from the dropdown list. This is a Service Group provided with the LSMS application.
- 8 In the **Action** field, select **Drop** from the dropdown list.
- 9 In the **Audit Session** field, **Basic** auditing is the default. You can leave this as is, or select **None** or **Detailed**, depending on your needs.
- 10 In the **Description** field, enter an optional description, if necessary.
- 11 In the **Rule Active** field, the default is **Yes**. Leave the default in place, so that the rule will become active as soon as it is applied to a Brick.
- 12 Click the Advanced tab of the Brick Zone Rule Editor and enter the same **alarm code** in the **Alarm Code field** that was used to configure the Alarm Code trigger.
- 13 Click the **OK** button to temporarily store the rule on the LSMS.
- 14 Display the File menu and select one of the **Save** options.

END OF STEPS



Appendix C: Proactive Monitoring Trigger Parameters

Overview

Purpose

This appendix explains the parameters that can be configured in *Brick*[®] or LSMS Proactive Monitoring triggers. For procedures to configure triggers, see [Chapter 6, “Configuring Alarm Triggers”](#) in this guide.

Contents

What are the Brick Proactive Monitoring Parameters?	C-2
What are the LSMS Proactive Monitoring Parameters?	C-5



What are the Brick Proactive Monitoring Parameters?

Brick proactive monitoring statistics

The statistical data that can be monitored by configuring a Brick Proactive Monitoring trigger is described in the table that follows.

Essentially, this data is collected by a Brick and tracks traffic load and throughput.

Brick PM Parameter	Description
In Byte Count >=	Count of bytes coming into a port (e.g., ether0 through ether10). Since the ports of a Brick are in promiscuous mode, the count includes all traffic on the local LAN. This count includes Ethernet framing characters.
Out Byte Count >=	Count of bytes going out of a port (e.g., ether0 through ether10). This count includes Ethernet framing characters.
In Pkts >=In Pkts <	Count of inbound packets (unicast, multicast, and broadcast) coming into a port (e.g., ether0 through ether10). Since the ports of a Brick are in <i>promiscuous</i> mode, the count includes all traffic on the local LAN. It is acceptable to include both of these parameters in the same Proactive Monitoring alarm.
Out Pkts >=Out Pkts <	Count of outbound processed packets (unicast, multicast, and broadcast) going out of a port (e.g., ether0 through ether10).
In Pkts Discarded >=	Inbound packets that are discarded not because of error conditions, but because of resource deficiencies such as a lack of buffers.

Brick PM Parameter	Description
In Error Ct >=	<p>Total count of Ethernet inbound packets that contain receive errors (e.g., alignment errors, frame collision errors, frames exceeding maximum frame length, MAC overruns, invalid data symbols), which prevent the delivery to a higher layer protocol.</p> <p>Since the ports of a Brick are in <i>promiscuous</i> mode, the count includes all traffic on the local LAN.</p>
Out Error Ct>=	<p>Total count of Ethernet outbound packets that contain transmission errors (e.g., late collisions, excessive collisions, MAC transmissions, carrier sense errors).</p> <p>The errors prevent the delivery to a higher layer protocol.</p>
Processed Pkts >=	<p>Total count of packets that were processed by any security policy on any port of a Brick.</p> <p>The packets could have been PASSED, DROPPED, or been processed by a PROXY.</p> <p>Essentially, it is the sum of all packets that were routed, bridged, or dropped by a Brick.</p> <p>Unlike port statistics, this count excludes traffic that the Brick filters out for being localized to a particular port LAN segment.</p>
Pkts Dropped (Policy) >=	<p>Total count of packets that were dropped by a Brick's security policy.</p> <p>The count excludes traffic on the local LAN.</p>
Brick Session Ct >=	<p>The total number of concurrent sessions (including sessions using Network Address Translation (NAT)) over the collection interval.</p>
Avg % CPU Usage <=Avg % CPU Usage >=	<p>The average percentage of CPU the Brick is using during a collection interval (i.e., 30 seconds).</p> <p>If the average is a high number, it could be indicative that the Brick is overloaded.</p>

Brick PM Parameter	Description
Avg % Session Cache Memory Usage >=	<p>The average percentage of session cache memory the Brick is using during a collection interval (i.e., 30 seconds).</p> <p>A high number of failing sessions may indicate an attack, or an incorrect DNS entry being used by a lot of traffic through your network.</p> <p>To investigate the problem, check the sessions log and look for dropped sessions.</p>
Peak % Session Cache Memory Usage >=	<p>The peak usage (bursts) of session cache memory, in percent, that the Brick is using during a collection interval (i.e., 30 seconds).</p> <p>A high number may indicate that sessions are failing. To investigate the problem, check the sessions log and look for dropped sessions.</p>
Avg % Main Memory Usage >=	<p>The average percentage of main memory (i.e., packet memory plus buffers) the Brick is using during a collection interval (i.e., 30 seconds).</p> <p>A high number may indicate a Brick problem or that the Brick is under attack. To investigate the problem, check the log files.</p>
Avg % Packet Memory Usage >=	<p>The average percentage of packet memory (i.e., memory that is allocated to store packets) the Brick is using during a collection interval (i.e., 30 seconds).</p> <p>A high number may indicate that incomplete and fragmented packets are being passed or the Brick is overloaded.</p> <p>Use in conjunction with Avg % CPU Usage. If the CPU number is also high, the Brick is probably overloaded. If the CPU number is not high, then the Brick is probably passing incomplete fragmented packets.</p>
Peak % Packet Memory Usage >=	<p>The peak usage (bursts) of packet memory (i.e., memory that is allocated to store packets) that the Brick is using during a collection interval (i.e., 30 seconds).</p> <p>A high number may indicate that incomplete and fragmented packets are being passed or the Brick is overloaded.</p>



What are the LSMS Proactive Monitoring Parameters?

LSMS proactive monitoring parameters

The statistical data that can be monitored by configuring an LSMS Proactive Monitoring trigger is described in the table that follows.

The logger, the VPN Gateway Controller (VGC), and the Firewall Authentication Controller (FAC), are the sources that write the statistical data to the Proactive Monitoring log.

Essentially, this data tracks platform resource utilization (e.g., disk space usage, log rollover rate, etc.), the number of initiated IKE negotiations, and the number of initiated User Authentication attempts from VPN clients or through a firewall.

For details on platform resource utilization topics, refer to [Appendix H, “Log File Sizing Guidelines”](#) in this guide for an explanation of log sizing requirements, and Chapter 10 Using the Configuration Assistant in the *LSMS Administration Guide* for instructions on how to configure log file size and the disk space allocated to them.

LSMS PM Parameter	Description
Session Log Rollover rate <=	Rate at which the Sessions Log fills up and rolls over. The default setting allows the log to grow to 10 megabytes before creating a new log.
Admin Log Rollover rate <=	Rate at which the Administrative Events Log fills up and rolls over. The default setting allows the log to grow to 1 megabyte before creating a new log.
PM Log Rollover rate <=	Rate at which the Proactive Monitoring Log fills up and rolls over. The default setting allows the log to grow to 10 megabytes before creating a new log.
User Auth Rollover rate <=	Rate at which the User Authentication Log fills up and rolls over. The default setting allows the log to grow to 1 megabyte before creating a new log.
Session Log Bytes Free <=	The free bytes that are available to accommodate the Sessions Log. The default amount of disk space allocated to Session logs is 1000 megabytes before old logs are deleted to create new space.

LSMS PM Parameter	Description
Admin Log Bytes Free <=	The free bytes that are available to accommodate the Administrative Events Log. The default amount of disk space allocated to Administrative Event logs is 100 megabytes before old logs are deleted to create new space.
PM Log Bytes Free <=	The free bytes that are available to accommodate the Proactive Monitoring Log. The default amount of disk space allocated to Proactive Monitoring logs is 200 megabytes before old logs are deleted to create new space.
User Auth Log Bytes Free <=	The free bytes that are available to accommodate the User Authentication Log. The default amount of disk space allocated to User Authentication logs is 100 megabytes before old logs are deleted to create new space.
IKE Initiated >=	The number of IKE negotiations that were initiated. Essentially, it is the sum of all successful and failed negotiations.
IKE Failed >=	The number of IKE negotiations that failed and did not complete negotiation.
User Auth (via VPN Client) Initiated >=	The number of user authentication requests from a VPN client that were initiated. Essentially, it is the sum of all successful and failed requests.
User Auth (via VPN Client) Failed >=	The number of user authentication requests from a VPN client that failed and did not complete negotiation.
User Auth (via firewall) Initiated >=	The number of user authentication requests through a firewall that were initiated. Essentially, it is the sum of all successful and failed requests.
User Auth (via firewall) Failed >=	The number of user authentication requests through a firewall that failed and did not complete negotiation.



Appendix D: Proactive Monitoring Subtypes

Overview

Purpose

This appendix explains the fields contained in the seven subtypes of a Proactive Monitoring log record.

In the Proactive Monitoring log, each record contains a subtype. For each subtype, the fields that follow the subtype in the remainder of the log record will differ.

To view the data for a specific subtype, enter one of the seven subtypes in the Subtype field of the Proactive Monitoring Log Viewer (see [“Administrative Events Log”](#) (p. 3-1) in this guide for details). The fields explained in this appendix will assist in interpreting the data displayed in the Viewer.

Contents

Brick Data	D-2
Brick Interface Generic	D-4
Brick Interface Ethernet	D-5
LSMS Auditing	D-6
Authentication Firewall	D-7
Local Map Pool	D-8
QoS Statistics	D-9
SLA Statistics	D-10
Brick VPN Data	D-11



Brick Data

Brick data table

The following table lists the fields that are recorded when the record contains Subtype 0, Brick Data.

Field	Description
SessStarted	Number of sessions started (whether or not they were dropped due to policy).
InPkts	Number of in packets (not counting those dropped at MAC level).
DroppedPkts	Number of packets dropped because of the security policy.
IpssecPkts	Number of IPSEC packets originating or terminating at this Brick.
PeakSess	Peak number of concurrent sessions during the interval.
PeakNatSess	Peak number of sessions employing NAT during the interval.
PeakIpssecSess	Peak number of IPSEC sessions originating or terminating at this Brick during the interval.
PeakDynSa	Peak number of dynamic SAs during the interval.
PeakProxy	Peak number of sessions reflected to proxy during the interval.
AvgCPU	Average percentage CPU utilization.
AvgCacheMem	Average percentage utilization of session cache memory.
PeakCacheMem	Peak percentage utilization of session cache memory.
AvgMainMem	Average percentage utilization of main memory.
AvgPktMem	Average percentage of memory allocated to store packets.
PeakPktMem	Peak percentage of memory allocated to store packets.
PeakDropSess	Peak dropped sessions.
PassedPkts	Number of unicast packets transmitted by the Brick during the last interval.
NewTcpSess	New TCP sessions.

Field	Description
NewUdpSess	New UDP sessions.
NewIcmpSess	New ICMP sessions.
NewIpsecSess	New IPsec sessions.
TcpInvPkts	TCP invalid packets.
numberSeconds	Number of seconds since the Brick device booted.
standbyState	State of Standby Brick device in a failover pair.
activeLabel	Label for active Brick device in a failover pair.
standbyLabel	Label for standby Brick device in a failover pair.
activeHWStatus	Alarm status of fan, power supply, or alarm card for active Brick device.
standbyHWStatus	Alarm status of fan, power supply, or alarm card for standby Brick device.



Brick Interface Generic

Brick interface data

The following table lists the fields that are recorded when the record contains Subtype 1, Brick Interface — Generic.

Field	Description
InOctets	Number of inbound bytes at port.
OutOctets	Number of outbound bytes at port.
InUcastPkts	Number of inbound unicast packets.
InMcastPkts	Number of inbound multicast packets.
InBcastPkts	Number of inbound broadcast packets.
InDiscards	Number of inbound packets discarded due to resource deficiencies in the Brick (not due to packet errors).
InErrors	Number of inbound packets containing receive errors. (Because the Brick operates in promiscuous mode, this is all errors on the LAN).
InUnknowns	Number of inbound packets where the Layer-2 protocol was not recognized.
OutUcastPkts	Number of outbound unicast packets.
OutMcastPkts	Number of outbound multicast packets.
OutBcastPkts	Number of outbound broadcast packets.
OutDiscards	Number of outbound packets discarded due to resource deficiencies in the Brick (not due to packet errors).
OutErrors	Number of outbound packets discarded due to errors.
FilteredPkts	Number of packets discarded due to bridge-level operation; this is only the number of incident LAN packets not accepted for processing on this port.
OperStatus	Current operational status of port:1 = up, 2 = down
MacAddr	MAC address.
LnkSpd	Link speed.
FlowCtrl	Flow control enabled.



Brick Interface Ethernet

Ethernet interface data

The following table lists the fields that are recorded when the record contains Subtype 2, Brick Interface — Ethernet.

Field	Description
AlignErrors	Number of alignment errors during the interval.
FcsErrors	Number of frames with frame-check errors during the interval.
SingleCollFrm	Number of single-collision frames during the interval.
MultiCollFrm	Number of multi-collision frames during the interval.
DeferXmits	Number of transmitted frames during the interval that had initially been deferred, not including frames involved in collisions.
LateColl	Number of late collisions (more than 512 bit times into the transmission) during the interval.
ExcessColl	Number of packets that failed to be transmitted, because there were too many collisions. (The other "Coll" entries represent packets that eventually did get through; this is the count of those that didn't.)
MacXmitErr	Number of MAC transmission errors during the interval; transmit underruns are included here.
CarrSenseErr	Number of transmissions that experienced loss of carrier-sense during the interval.
TooLongErr	Number of frames that were too long during the interval.
MacRcvErr	Number of MAC reception errors during the interval; receive overruns are included here.
SymbolErr	Between packets we see a wrong symbol (not allowed by the protocol) on the line.



LSMS Auditing

Log data

The following table lists the fields that are recorded when the record contains Subtype 3, Log Data.

Field	Description
RolloverRate	Number of seconds of data currently stored in the log. Computed as the difference in time between the oldest record and the current time.
BytesFree	Number of bytes available in the log. Computed as the difference between the allocation and bytes used by log files. If the value is zero, the log has overflowed.
Bytes Allocated	Number of bytes allocated to the log.



Authentication Firewall

FAC data

The following table lists the fields that are recorded when the record contains Subtype 5, FAC Data.

Field	Description
Firewall Auth Initiated	Number of user authentications attempted via the firewall.
Firewall Auth Failed	Number of unsuccessful user authentications via the firewall.



Local Map Pool

VGC routing pool data

The following table lists the fields that are recorded when the record contains Subtype 6, VGC Routing Pool Data.

Field	Description
Brick	Name of the Brick device.
Zone	Name of the Brick zone ruleset.
Total IPs	Number of IPs in the pool for this Brick device and TEP.
Free IPs	Number of free (not in use) IPs in the pool for this Brick device and TEP.



QoS Statistics

QoS data

The following table lists the fields that are recorded when the record contains Subtype 7, QoS Data.

Field	Description
Interface	Interface
Zone	Name of the Brick zone ruleset.
Dir	Direction relative to zone ruleset.
NumSess	Total number of sessions.
NumClassesQ	Number of classes that queued a packet.
AvgNumQ	Average number of non-empty queues.
AvgLenQ	Average length of non-empty queues.
TotPkts	Total number of packets seen.
TotPktsQ	Total number of packets queued.
AvgWaitTime	Average wait time for packets that were queued (msec).
DropSessLimit	Number of packets dropped due to being over session limit.
DropAllowSess	Number of packets dropped within an allowed session.
BytesThru	Number of bytes allowed through.
PktsThru	Number of packets allowed through.
GuarBytesSec	Guaranteed number of bytes per second.
LimBytesSec	Limit number of bytes per second.
LimSessDir	Limit sessions in this direction.



SLA Statistics

SLA data

The following table lists the fields that are recorded when the record contains Subtype 9, SLA Data.

Field	Description
PID	Probe ID.
PSent	Number of probes sent.
PLost	Number of probes lost.
MinDelay	Minimum round trip delay.
MaxDelay	Maximum round trip delay.
AvgDelay	Average round trip delay.
POverThresh	Number of probes above threshold.
Threshold	Threshold.



Brick VPN Data

Brick VPN Data table

The following table lists the fields that are recorded when the record contains Subtype 10, Brick VPN Data.

Field	Description
Version	Version of Brick device data.
PreviousTimeStamp	Previous LSMS timestamp.
CollectionInterval	Data collection interval (seconds).
Index	Data collection index.
Name	Tunnel endpoint name (TEP IP).
Zone	Brick zone ruleset.
TotalIPsinLocalMapPool	Total IPs in Local Map Pool.
FreeIPsinLocalMapPool	Free IPs in Local Map Pool.
IKEInitiated	Number of IKE initiated sessions.
IKEFailed	Number of failed IKE initiated sessions.
UserAuthInitiated	Number of user authentication sessions initiated.
UserAuthFailed	Number of failed user authentication sessions.
ActiveIKEv1ClientSessions	Number of active client IKEv1 client sessions.
LicenseLimit	Allocated license limit.
LANLANIKEv1UpTunnels	Number of LAN-LAN IKEv1 tunnels active and up.
LANLANIKEv1DownTunnels	Number of LAN-LAN IKEv1 tunnels down.
LANLANDisabledTunnels	Number of LAN-LAN disabled tunnels.
LANLANManualTunnels	Number of LAN-LAN manual tunnels.
ClientLicensesInUse	Number of client tunnel endpoint licenses currently in use.
ActiveIKEv2ClientSessions	Number of active IKEv2 client tunnel sessions.
LANLANIKEv2UpTunnels	Number of LAN-LAN IKEv2 tunnels currently up and active.
LANLANIKEv2DownTunnels	Number of LAN-LAN IKEv2 tunnels currently down.



Appendix E: Log Field Formats

Overview

Purpose

If you are running any of the Log Viewers on the LSMS and you want more detail on an audit log entry, double-click the desired entry to view it in the Detail window.

If you are working with LSMS reports, *Appendices E, F, and G* provide explanations of the various fields in log entries. For some types, the source and srcType fields are filled in with the appropriate static values.

Contents

Record Header	E-2
Log Record Types	E-4



Record Header

Log record headers

All log messages are required to have the following header:

type:srcType:source:timestamp:[subtype]:

	Semantics	Syntax
type	The type of record, by number. For instance, a session-start record is type=0, and an error record is type=5.	ASCII decimal number
srcType	A letter designating the type of entity that originated the record.	i = LSMS process b = <i>Brick</i> [®] p = Proxy server r = ISS RealSecure engine
source	If srcType is i, the subsystem name. Subsystems include servlet, rap, rad, logger, alarm, eua, url, report and vgc. If b, the Brick name. If p, the proxy name. If r, the engine name.	String
timestamp	The time that the logger received and processed the record. Many records may also have a source timestamp, also as part of this field. The source timestamps will be on all Proactive Monitoring (promon) records, in the form of the full 10-digit timestamp. It will be on Session Log records from the Brick, in the form of the "delta" (seconds before or after) timestamp.	LSMS Timestamp Exactly six digits, of form hhmmss: hh = hours (00-23) mm = minutes (00-59) ss = seconds (00-59) [Source Timestamp] <10-digit number> Seconds since midnight Jan 1, 1970 GMT. or +<number> Seconds after, or -<number> Seconds before the LSMS timestamp.

	Semantics	Syntax
group	Name of the group whose administrators are entitled to see this record.	String
[subtype]	Some records (e.g.- type 4) have subtypes, each with its own format. For records with subtypes, the subtype lies between the fixed header and the type-dependent fields.	ASCII decimal number



Log Record Types

Log record type table

The following table documents the record types. It includes:

- The record type and the subtype in parentheses, if applicable.
- A verbal description of the purpose of the record.
- A symbol for the log in which the record is found. The symbols for the logs are as follows:
 - E = AdminEvents
 - S = Session
 - P = Proactive Monitoring
 - U = User Authentication
 - V = VPN
 - Sp = Session Log on Proxy server
(only applicable if running Lucent Proxy Agent)

- The source-type for the record, if only one source-type can create it.
- The fields in order, not including the header fields

Type & Sub-type	Description	LogSRC Type		Fields
0	Session Start	S	b	zone dir srcHost dstHost proto srcprt dstprt action recIntf sndIntf alrCode ruleNum received VLAN id send VLAN id relVpn (opt) BrickSrc (only if action is Proxy) proxyDst (only if action is Proxy) BrickPrt (only if action is Proxy) proxyPrt (only if action is Proxy) reflectType (only if action is Proxy) encapsulation type

Type & Sub-type	Description	Log	SRC	Fields
1	Session End	S	b	zone dir srcHost dstHost proto srcprt dstprt forPkt revPkt forByte revByte elapsed time reason for session termination action abbreviation rule number VPN type abbreviation TCP forward invalid segments TCP reverse invalid segments

Type & Sub-type	Description	Log	SRC	Fields
2	Packet Audit	S	b	zone dir srcHost dstHost proto srcprt dstprt action recIntf sndIntf byteCnt alrCode ruleNum VLAN ID in VLAN ID out

Type & Sub-type	Description	Log	SRC Type	Fields
3	Session Start Mapped (The optional field are present if the action is "Proxy")	S	b	zone dir srcHost dstHost proto srcprt dstprt mapSrc mapDst mapSrcprt mapDstprt action recIntf sndIntf alrCode ruleNum received VLAN id send VLAN id relVpn (opt) BrickSrc (opt) proxyDst (opt) BrickPrt (opt) proxyPrt (opt) reflectType (opt) encapsulation type
4(0)	General Brick Event	E	b	text
4(1)	Boot Brick	E	b	(no data)
4(2)	Flush Cache	E	b	zone
4(3)	Load Brick Zone Ruleset	E	b	zone
4(4)	Load Table	E	b	BrickName
4(5)	Switchover New Policy	E	b	zone
4(6)	Load Dynamic Rule	E	b	ruleFieldsTable

Type & Sub-type	Description	Log SRC Type	Fields
4(7)	Load Dynamic Host	E b	zone hostGrp hostgrpEntry
4(8)	Load Dynamic Service	E b	zone srvGrp srvgrpEntry
4(9)	Audit Ping (not a loggable event, just a keep-alive between Brick and logger)	E b	BrickName
4(10)	Abort Load	E b	zone *
4(11)	File Download (tvp, inferno.ini)	E b	filename adminID
4(12)	File Download Aborted	E b	filename adminID
4(13)	Reboot	E b	msg
4(14)	Software Version	E b	version
4(15)	Command Response	E b	msg
4(16)	Brick Disabled	E b	reason
4(17)	Brick Enabled	E b	
4(18)	Refresh MAC Table	E b	
4(19)	Load Proxy	E b	
4(20)	Feature Information	E b	featureCode statusCode
4(21)	Refresh arp table executed	E b	
4(24)	Brick has (re)homed	E b	firewall name new LSMS IP address
4(25)	Standby has changed state	E b	state my label standby's label

Type & Sub-type	Description	LogSRC Type		Fields
5	Errors (Device and LSMS) For more information on device error codes select Error Codes from the LSMS Navigator Help menu.	E	-	codeID severity errno args text
6	End User Authentication	U	i	zone srcHost dstHost proto srcprt dstprt userID authtype result euaResult reason authTimeout userDb euaAction forByte revByte elap VPN Vendor
7	Failed Admin Host Authentication	E	b	srcHost dstHost proto srcprt dstprt reason

Type & Sub-type	Description	Log	SRC	Type	Fields
8	IPSEC	S	b		zone dir srcHost dstHost proto srcprt dstprt relVpn vpnDir endpt SPI userID
9	Session Summary Stats (Not yet implemented.)			i	Brick zone httpPass httpDrop ftpPass ftpDrop telnetPass telnetDrop dnsPass dnsDrop smtpPass smtpDrop pingPass pingDrop euaPass euaDrop pktCnt byteCnt
10	Admin Login	E		i	adminID IP

Type & Sub-type	Description	LogSRC	Type	Fields
11	Admin Logout	E	i	adminID
12	Add Admin Account	E	i	adminID admRec
13	Modify Admin Account (the two records are the old and the new record, respectively)	E	i	adminID admRec admRec
14	Delete Admin Account	E	i	adminID admRec
15	Add Brick Zone Ruleset Table Entry	E	i	adminID zone zoneRec
16	Modify Brick Zone Ruleset Table Entry	E	i	adminID zone zoneRec
17	Delete Brick Zone Ruleset Table Entry	E	i	adminID zone zoneRec
18	Add Brick Table Entry	E	i	adminID BrickName BrickRec
19	Modify Brick Table Entry	E	i	adminID BrickName BrickRec
20	Delete Brick Table Entry	E	i	adminID BrickName BrickRec

Type & Sub-type	Description	Log	SRC	Fields
		Type		
21	Brick Alarm	E	i	serialno BrickName zone triggerType triggerName alarmCode actions alarmInfo
22	LSMS Alarm	E	i	serialno triggerType triggerName actions alarmInfo
23	Session Full (Brick)	S	b	zone dir srcHost dstHost proto srcprt dstprt action recIntf sndIntf alrCode ruleNum forPkt revPkt forByte revByte elap sessionStart

Type & Sub-type	Description	LogSRC	Type	Fields
24	Brick Status (LSMS message)	E	i	BrickName CONTACTED/LOST IP address (new if CONTACTED, previous if LOST)
25	LSMS Subsystem Information Message (e.g. logger process start and stop)	E	-	text
26	Add Brick Zone Ruleset to LSMS	E	i	adminID zone
27	Delete Brick Zone Ruleset from LSMS	E	i	adminID zone
28	Modify Brick Zone Ruleset in the LSMS	E	i	adminID zone
29	Add Brick	E	i	adminID BrickName
30	Delete Brick	E	i	adminID BrickName
31	Modify Brick	E	i	adminID BrickName
32	Audit GUI Request	E	i	adminID
33	Audit GUI Request for File Modification	E	i	adminID
34	Admin Login Failed	E	i	adminID IP reason
35	Alarm Alert Status (Alert passed or failed)	E	i	serialno action serialno text
36	LSMS Data Object Imported	E	i	adminID importZone objectName

Type & Sub-type	Description	Log Type	SRC Type	Fields
37	LSMS Data Object Published	E	i	adminID publishZone objectName
38	Add Brick Route	E	i	adminID BrickName
39	Delete Brick Route	E		adminID BrickName
40	Modify Brick Route	E	i	adminID BrickName
41	Start Brick Upgrade	E	i	adminID BrickName
42	End Brick Upgrade	E	i	adminID BrickName
43	ISS RealSecure Event	E	i	srcZone dstZone srcHost dstHost proto srcprt dstprt eventName priority rsTime rsActions eventInfo

Type & Sub-type	Description	LogSRC Type	Fields
44	Add Dynamic SA	V i	BrickName zone srcHost dstHost proto srcprt dstprt endpt SPI userID compression salifeKb salifeSec timeoutAction timeout tunnelID
45	Delete Dynamic SA	V i	BrickName zone srcHost dstHost proto srcprt dstprt endpt SPI userID tunnelID
46	FTP Log File	E i	fileName
47	Add RS Engine	E i	adminID engineName
48	Delete RS Engine	E i	adminID engineName

Type & Sub-type	Description	Log	SRC	Type	Fields
49	Modify RS Engine	E	i		adminID engineName
50	Duplicate Brick Zone Ruleset	E	i		adminID zone newZone
51	Start Loading Brick Config	E	i		BrickName
52	End Loading Brick Config	E	i		BrickName
53	Proactive Monitoring	P		-	See “Administrative Events Log” (p. 3-1), “Proactive Monitoring Log” (p. 3-7).

Type & Sub-type	Description	LogSRC Type		Fields
53(10)	Proactive Monitoring	P	-	source type source identifier lsms timestamp group record number subtype version number previous snapshot collection period index number index name zone total IPs IKE initiated IKE failed User Auth initiated User Auth failed Active sessions License Limit Up Tunnels Down Tunnels Disabled Tunnels Manual Tunnels
54	Start Reflected Session	Sp	p	sessionID BrickName srcHost proto srcprt dstprt

Type & Sub-type	Description	Log	SRC	Type	Fields
55	Original Session Info	Sp	p		sessionID zone dir srcHost dstHost proto srcprt dstprt reflectType mapSrc mapDst mapSrcPort mapDstPort
56	URL Filtering Result	Sp	p		sessionID result urlAction url
57	Scan URL Content Result	Sp	p		sessionID result url
58	Scan Mail Content Result	Sp	p		sessionID sender receivers result
59	Application Protocol Command Filter	Sp	p		sessionID cmd cmdResult

Type & Sub-type	Description	LogSRC Type	Fields
60	End Reflected Sessions	Sp p	sessionID BrickName srcHost proto srcprt dstprt result
61	Add Proxy Table Entry	E i	adminID proxyRec
62	Modify Proxy Table Entry	E i	adminID proxyRecNew proxyRecOld
63	Delete Proxy Table Entry	E i	adminID proxyRec
64	Add User Table Entry	E i	zone userID adminID userRec
65	Modify User Table Entry (the two records are the new and old records, respectively)	E	zone userID adminID userRec userRec
66	Delete User Table Entry	E i	zone userID adminID userRec
67	Add UserGrp Table Entry	E i	zone userGrp adminID userGrpRec

Type & Sub-type	Description	Log	SRC	Type	Fields
68	Modify UserGrp Table Entry (the two records are the new and old records, respectively)	E	i		zone userGrp adminID userGrpRec userGrpRec
69	Delete UserGrp Table Entry	E	i		zone userGrp adminID userGrpRec
70	Add AuthSvc Table Entry	E	i		zone authtype adminID authSvcRec
71	Modify AuthSvc Table Entry (the two records are the new and old records, respectively)	E	i		zone authtype adminID authSvcRec authSvcRec
72	Delete AuthSvc Table Entry	E	i		zone authtype adminID authSvcRec
73(0)	Brick SA Info: General	V	i		text
73(1)	Brick SA Info: General	V	i		text
73(2, 6)	SA replaced	V	i		zone SPI dstHost proto endpt userID tunnelEndpt tunnelID

Type & Sub-type	Description	LogSRC	Type	Fields
73(3, 7,8)	SA Deleted on Lifetime Expiry	V	i	zone SPI dstHost proto endpt userID tunnelEndpt tunnelID
73(4)	SA Deleted on Idle Timeout	V	i	zone SPI dstHost proto endpt userID tunnelEndpt tunnelID
73(5)	User-related SA info	V	i	zone userID endpt byteCnt tunnelStartTime elap SPI tunnelEndpt tunnelID
74	Kill session	E	i	adminID sessionRec
75	Kill all sessions	E	i	adminID zone

Type & Sub-type	Description	Log	SRC Type	Fields
76(0)	Add VPN routing info to pool	E	i	BrickName zone endpt clientIP localIP userID
76(1)	Remove VPN routing info from pool	E	i	BrickName zone endpt clientIP localIP userID
77	<p>Packet trace log, implemented for the "private doorbell" feature.</p> <p>Note that 'dir' is with regard to the port, not the Brick zone ruleset (there is no Brick zone ruleset in the record).</p>	T	b	recIntf dir srcHost dstHost proto srcprt dstprt length binaryData
78	<p>FTP Command</p> <p>The Brick detects FTP commands on sessions through it, and logs them.</p>	S	b	zone srcHost dstHost proto srcprt dstprt text

Type & Sub-type	Description	Log	SRC Type	Fields
79	Dynamic Rule Record the creation of a dynamic rule in the Brick	E	b	zone ruleNumber creator ruleTimeout cacheTimeout ruleFlags encryptionRequirements maxUseCount monitorType direction srcHost dstHost service mapSrcHost mapDstHost mapService ruleAction
80	Add Host Group	E	i	adminID hostGrp count=count
81	Modify Host Group	E	i	adminID hostGrp count=count
82	Delete Host Group	E	i	adminID hostGrp
83	Add Service Group	E	i	adminID svcGrp count=count
84	Modify Service Group	E	i	adminID svcGrp count=count
85	Delete Service Group	E	i	adminID svcGrp

Type & Sub-type	Description	Log SRC	Type	Fields
86	Add Dependency Mask	E	i	adminID dependencyMask
87	Modify Dependency Mask	E	i	adminID dependencyMask
88	Delete Dependency Mask	E	i	adminID dependencyMask
89	Add Group	E	i	adminID group permissions=count
90	Modify Group	E	i	adminID group permissions=count
91	Delete Group	E	i	adminID group
92	VPN Status	V	i	vpnEvent vpnEventRec
93	Add Router	E	i	adminID router
94	Modify Router	E	i	adminID router
95	Delete Router	E	i	adminID router
96	Add Router Rule Set	E	i	adminID routerRules
97	Modify Router Rule Set	E	i	adminID routerRules
98	Delete Router Rule Set	E	i	adminID routerRules
99	Add Authentication Service	E	i	adminID authSvc

Type & Sub-type	Description	LogSRC Type		Fields
100	Modify Authentication Service	E	i	adminID authSvc
101	Delete Authentication Service	E	i	adminID authSvc
102	Add User Group	E	i	adminID userGroup
103	Modify User Group	E	i	adminID userGroup
104	Delete User Group	E	i	adminID userGroup
105	Add User	E	i	adminID userID
106	Modify User	E	i	adminID userID
107	Delete User	E	i	adminID userID
111	Add LAN-to-LAN Tunnel	E	i	adminID localTepName remoteTepName
112	Modify LAN-to-LAN Tunnel	E	i	adminID localTepName remoteTepName
113	Modify LAN-to-LAN TunnelDefaults	E		adminID
115	Enable LAN-to-LAN Tunnel	E	i	adminID localTepName remoteTepName
116	Disable LAN-to-LAN Tunnel	E	i	adminID localTepName remoteTepName

Type & Sub-type	Description	Log SRC	Type	Fields
117	Delete LAN-to-LAN Tunnel	E	i	adminID localTepName remoteTepName
118	Intelligent Cache Management	E	i	msg
119	Add Client Tunnel	E	i	adminId deviceName tunnelEndpoint zone
120	Modify Client Tunnel	E	i	adminId deviceName tunnelEndpoint zone
121	Modify Client Tunnel Defaults	E	i	adminId
122	Enable Client Tunnel	E	i	adminId deviceName tunnelEndpoint zone
123	Disable Client Tunnel	E	i	adminId deviceName tunnelEndpoint zone
124	Delete Client Tunnel	E	i	adminId deviceName tunnelEndpoint zone
125	LSMS Status	E	i	lsmsName lsmsStatus lsmsVersion
126	LSMS Refresh	E	i	refreshStatus

Type & Sub-type	Description	LogSRC Type	Fields
127	Encapsulation	S b	zone srcHost dstHost proto srcprt dstprt encapReq dir
128	Tunnel Heartbeat Received	V i	zone reasonCode SPI srcHost dstHost proto TEP userId locelTepName heartBeatInterval
129	Tunnel Heartbeat Missing	V i	zone reasonCode SPI srcHost dstHost proto TEP userId locelTepName heartBeatInterval
130	List Up Tunnels	V i	zone tunnelEndpoint count tunnelID

Type & Sub-type	Description	Log	SRC	Type	Fields
131	LSMS Clock Synchronization	E	i		msg
132	Log Brick control executed	E	i		adminId BrickName cmd
133	Encapsulation entry audit	E	i		subtype 1-new, 2-changed destination port, 3-marked as deletable, 4-deleted zone target host IP or group encapsulation IP encapsulation protocol encapsulation src port encapsulation destination port encapsulation tag internal flags # of sessions currently using this entry
134	Scan FTP Content result	E	i		session id reason + action + virusname URL

Type & Sub-type	Description	Log	SRC	Type	Fields
135	Address Translation Table Action	E	i		nat type 0-direct hostgroup to hostgroup mapping subtype 1-new, 2-changed destination port, 3-marked as deletable, 4-deleted zone table name number of mappings in this table map-from host group map-to host group map-from host group (if # of mappings > 1) map-to host group (if # mappings > 1) nat tag internal flags # of sessions or rules currently using this entry
136	Archive (History) Details	E	i		adminId object type object name archive file hash archive file name
137	QOS alarm	E	i		zone name interface direction rule number (if applicable) option exception type bandwidth type units passed bandwidth after throttling

Type & Sub-type	Description	Log	SRC Type	Fields
138	Add Application Filter executed	E	i	adminId app filter name
139	Modify Application Filter executed	E	i	adminId app filter name
140	Delete Application Filter executed	E	i	adminId app filter name
141	List Application Filter executed (not currently used)	E	i	adminId app filter name
142	Application Monitor result	E	i	zone direction srcip destination ip protocol src port dest port filter name disposition (block or pass) reason (if block) pattern (if block and reason is pattern match) text of the URI that failed

Type & Sub-type	Description	LogSRC Type		Fields
143	Application Monitor exception	E	i	zone direction srcip destination ip protocol src port dest port filter name disposition (block or pass) reason (if block) pattern (if block and reason is pattern match) text of the URI that failed

Type & Sub-type	Description	Log	SRC Type	Fields
144	Strict TCP checking exception	E	i	zone direction src ip dest ip protocol src port dest port <empty> receive interface send interface alarm code rule number received VLAN id send VLAN id source TCP state source TCP next seq # source TCP right seq # source TCP window size source TCP scale source TCP time stamp source TCP time stamp echo dest TCP state dest TCP next seq # dest TCP right seq # dest TCP window size dest TCP scale dest TCP time stamp dest TCP time stamp echo TCP seqn # delta error type path direction (forward or backward) TCP sequence number TCP flags from this packet TCP segment length for this packet.....

Type & Sub-type	Description	LogSRC Type		Fields
145	VPN Error	V	i	name of the program that generated the error severity error number arguments text
146	Add Dynamic SA	V	i	device name ruleset source host destination host protocol source port destination port end point SPI user id compression life of dynamic SA in KB life of dynamic SA in seconds timeout action idle timeout replay protocol tunnel id

Type & Sub-type	Description	Log	SRC Type	Fields
147	Delete Dynamic SA	V	i	device name ruleset source host destination host protocol source port destination port end point SPI user id tunnel id
154	VPN Debug	V	i	name of the program that generated the error severity error number arguments text
155	L2L Tunnel Down	V	b	source type source identifier lsms timestamp group zone local TEP remote TEP
156	L2L Tunnel Up	V	b	source type source identifier lsms timestamp group zone local TEP remote TEP



Appendix F: Filterable Log Fields

Overview

Purpose

This section provides more information on the data listed in the `Fields` column in Appendix F.

Each field has a semantics (what it means) and a syntax (how to parse it, depending on its type). For instance:

`SourceIP` is, *semantically*, the IP address of the source. Its *syntax* is "IP".

`DestIP` is, *semantically*, the IP address of the destination. Its *syntax* is "IP".

`DestIP` is the destination, not the source. It thus has different semantics than `SourceIP`. But it is expressed in the same syntax.

`SourcePort` is, *semantically*, the port number of the source. Its *syntax* is "number".

Contents

Filterable Log Fields	F-2
---------------------------------------	---------------------



Filterable Log Fields

Log type semantics

In the following table, each log field type is defined by its semantics, and a pointer is given to its syntax. More detail on the Syntax Type column is provided in Appendix H.

Field Name	Semantics	Syntax Type
action	Action	action
actions	Which alarm actions are specified for this alarm. This can be a single action or an action group.	string
adminID	Administrator's identity	string
admRec	Administrator record. The items in the table are: adminId zone pvec fullName phone e-mail expire lockStatus comment	table
alarmInfo	Text to indicate information specific to this alarm.	string
alrCode	Alarm code that was activated, if any	number
args	A set of free-form arguments, containing any text character except newline.	args
authSvcRec	Authentication Service Record, consisting of: <ul style="list-style-type: none"> • zone • authentication service • authentication method • description • authentication service parameters 	table
authType	Authentication type, authentication service name	string
authTimeout	Authentication timeout, in minutes	number

Field Name	Semantics	Syntax Type
binaryData	Free-form byte array, which can contain any byte, including non-text information and field and record delimitation.	-
brickName	<i>Brick</i> [®] name	string
brickPrt	Source port of reflected session, Brick local port	number
brickRec	A change to an entry in the Brick table. The fields are... For a BrickData record: <ul style="list-style-type: none"> • ipAdr • defGW • intType • adminIP • auditIP • comment For a ZoneTbl record: <ul style="list-style-type: none"> • intf • fromIPAddr (opt) • toIPAddr (opt) • zone • comment 	table
brickSrc	Source IP (VBA) of reflected session	IP
byteCnt	Total byte count	number
clientIP	IP of VGC client	IP
codeID	Name of the program that generated the error	string
cmd	A command	string
cmdResult	nDisposition of a filtered protocol command	cmdres
compression	Type of compression	string
count	Count, usually the number of entries	number
creator	Who created it? (examples: "H323_Mon", "TFTP_Mon")	string
dependMask	Dependency Mask name	string
dir	Direction of travel	inOut
dstHost	Destination IP	IP
dstprt	Destination port	number

Field Name	Semantics	Syntax Type
dstZone	Destination Brick zone ruleset	string
elap	Elapsed time, in seconds	number
endpt	Endpoint of an IPSEC relation	IP
encryptReq	Encryption requirement: 0 = None 1 = Start 2 = End	number
engineName	Name of the RealSecure engine being administered	string
errno	Error number	errCode
euaAction	What caused this action to take place? 0 = Login 1 = Logoff 2 = Reauth after being queried for more info (like PIN) 3 = Reauth after entering new password	number
euaResult	0 = Success (authorized) 1 = Failure (denied) 2 = Query for more info (like PIN or SecurID token) 3 = Request for new password to replace expired one	number
eventInfo	Additional event-specific information, in the form of name-value pairs	eventArgs
eventName	Name of a RealSecure event	string
featureCode	0 = Hardware IPSEC card 1 = Compression	number
filename	Name of file being operated upon	string
flags	Arbitrary collection of bits represented by a hex string. The interpretation depends on the context.	hexString
forByte	Forward byte count	number
forPkt	Forward packet count	number
group	Group name, usually name of the group whose administrators are entitled to see this record.	string

Field Name	Semantics	Syntax Type
host	(For DynamicRule record) Can be one of: IP Host Group (with leading "@") wild card	
hostGrp	Host group name	string
hostgrpEntry	(Not yet implemented)	
importZone	The Brick zone ruleset that was imported	string
IP	IP address	IP
length	Length in bytes of the field that follows (used for fields that might contain delimiters as data.)	number
localIP		IP
mapDst	Mapped destination IP	IP
mapDstprt	Mapped destination port	number
mapSrc	Mapped source IP	IP
mapSrcprt	Mapped source port	number
maxUseCount	How many times can this be used?	number
monitorType	Monitor type, for example: "", "H.323", "H.245", "SQL*Net", "TFTP"	string
msg	The message associated with the operation	string
newZone	When Brick zone ruleset is duplicated, name of the new Brick zone ruleset	string
objectName	Name of an object	string
priority	Priority	number
privilege	(Not yet implemented)	
proto	Protocol, identified by standard number	number
proxyDst	Destination IP of reflected session, proxy server IP	IP
proxyPrt	Destination port of reflected session, proxy server port	number

Field Name	Semantics	Syntax Type
proxyRec	Proxy record, consisting of: Brick name Zone Service tuple Description Proxy host IP address Proxy listening port Encrypt (yes/no) Key Reflection type (Single/Dual)	table
publishZone	The Brick zone ruleset that was published	string
PVEC	Privilege vector	string
reason	Reason for the message	string
receivers	The argument to all "RCPT TO" commands, comma separated. (Limited to first 10, more indicated by "...")	string
recIntf	Receiving port on Brick	intf
reflectType	Reflection type, dual or single	refType
relVpn	Describes a VPN connection as internal, external, both, or neither	relVpn
result	Result of an operation	string
revByte	Reverse byte count	number
revPkt	Reverse packet count	number
router	Router name	string
routerRules	Router Ruleset name	string
rsActions	Bit vector of actions taken by RealSecure	IP
rsTime	Time that RealSecure engine reported the event	number
ruleFieldsTbl	(Not yet implemented)	
ruleNum	Rule number governing the session/packet	number
salifeKb	Life of dynamic SA in KB	number
salifeSec	Life of dynamic SA in seconds	number
sender	The argument to the "MAIL FROM" command	string
serialno	Every alarm triggered has a unique ID	string

Field Name	Semantics	Syntax Type
service	(For DynamicRule record) Can be one of: A concatenation of protocol/dstport/srcport Service Group (with leading "@" wild card	
sessionID	Unique session identifier	number.number
sessionRec	Record of an authenticated session, including: zone user ID tunnel endpoint IP	table
sessionStart	Time that the session started	timestamp
severity	Number indicating the severity of the error; lower is more severe. Current severity levels and their meanings are: 1 = critical error - Critical errors are those involving probable loss of core functionality. 2 = attention required (major error) - Major errors are those involving probable loss of data or important (but not critical) functionality. 3 = warning (minor error) - Minor errors are recoverable or not system affecting.	severity
sndIntf	Sending port on Brick	intf
SPI	Security Parameters Index, numeric ID for encryption and authentication parameters for an IPSEC relationship	number
srcHost	Source IP	IP
srcprt	Source port	number
srcZone	Source Brick zone ruleset	string
srvGrp	Service group name	string
srvgrpEntry	(Not yet implemented)	
statusCode	0 = Not available 1 = Available	number
table	Name of the table in the admin operation	string
tepName	Name of the local or remote Tunnel End Point (TEP). The format of the name depends on the device type. If Brick or fixed router: <deviceName>,<IP>,<ruleSetName> If mobile router: <deviceName>,mobile	string
text	Textual information intended for human interpretation	string

Field Name	Semantics	Syntax Type
timeout	Timeout in seconds	number
timeoutAction	What to do if we time out	string
triggerName	Name of this specific trigger	string
triggerType	Class of trigger	string
tunnelEndpoint	Local tunnel endpoint	IP
tunnelID	Unique identifier for tunnel	number
tunnelStart	Start time of tunnel	number
url	URL (Universal Resource Locator)	string
urlAction	Action due to URL filtering	urlact
userDb	Database where the user was found for authentication	userdbID
userGrp	User group name	string
userGrpRec	User group record, consisting of: zone group name description number of users in group userID list	table
userId	User identity	string

Field Name	Semantics	Syntax Type
userRec	User record, consisting of: zone userID full name account active description phone e-mail pager authSvc authTimeout disableAfter source IP range start date end date VPN pre-shared key expiration count expiration units expiration type unique history	table
version	Version of the Brick	string
vpnDir	The "in" or "out" direction of a VPN connection	inOut

Field Name	Semantics	Syntax Type
vpnEvent	<p>Type of the event, indicated by a number and a parenthetical word description. The events that can appear in the log are:</p> <ul style="list-style-type: none"> 5(Packet received that requires a client policy, but none is configured) 6(Tunnel is up) 7(Tunnel is down) 8(IKE Error) 9(Packet Received on Disabled Tunnel) 11(IKE Error) 12(Rekey complete) 13(Rekey failed) 14(Tunnel initiate failed) 21(IP Address added to user group) 22(IP Address deleted from user group) 41(Initiating Phase 1) 42(Initiating Phase 2) 43(Received an IKE Packet) 44(Sent an IKE Packet) 45(Received an IKE Packet) 47(Received a notify packet) 48(Sent a notify packet) 	

Field Name	Semantics	Syntax Type
vpnEventRec	<p>Table of parameters associated with a VPN event, which can include items from the following:</p> <ul style="list-style-type: none"> tunnelID device/TEP IP remote name remote IP user group IP address length mode type error was initiated by 	table
zone	Name of Brick zone ruleset	string
zoneRec	<p>A change to some some Brick zone ruleset. The entries in the record are:</p> <p>For a Policy record:</p> <p>ruleNumber, srcHost, dstHost, service, action, drop_notify, comment</p> <p>For a HostGroup record:</p> <p>hostGroupName, IPAdr, [toIPAdr], comment</p> <p>For a ServiceGroup record:</p> <p>serviceName, proto, [dstPort], [toDstPort] , [srcPort], [toSrcPort], comment</p> <p>For a DependencyMask:</p> <p>maskName, srcHost, dstHost, service, action, inIntf, outIntf, userAuth, alarmCode, hitCount, omment</p>	table



Appendix G: Log Field Syntax

Overview

Purpose

The syntax of any log field consists only of text (printable) characters. The field may not include a newline, because newline ends the log record. It may not contain a colon except for the "args" syntax, because colon delimits fields.

Contents

Log Field Syntax	G-2
----------------------------------	-----



Log Field Syntax

action type syntax

Syntax Type	Representation
action	"Pass", "Drop", "Proxy", "VPN", or "VpnProxy"
args	<p>A collection of free-form arguments, that may contain any characters except newline. In order for this to work, we need a different way to delimit the arguments. We do this with count fields for the number of arguments and the length of each argument. The argument list starts with a two digit decimal number which identifies the number of arguments. If there are no arguments in the message, indicate this by using a value of 00. Each argument begins with a three digit decimal number that identifies the number of characters in the argument.</p> <p>Example: the two arguments "beanie" and "not recognized" would be represented as: 02006beanie014not recognized</p>
cmdres	<p>"a" = allowed "d" = disallowed "ae" = allowed, with exception flag of "Y" "de" = disallowed, with exception flag of "N"</p>
errCode	<p>A letter to denote the subsystem that encountered the error, followed by a four-digit error number. Example: "E3001" is error 3001 from the logger, which has been assigned letter 'E'.</p> <p>For more information on device error codes select Error Codes from the LSMS Navigator Help menu.</p>

Syntax Type	Representation
eventArgs	A collection of name-value pairs, carrying event-specific information from a RealSecure event record. The representation of a pair is: <i><name>=<value></i> and the pairs are separated from each other by colons.
hexString	A sequece of hex digits (0-9,A-F) representing a bit string.
IP	Starting with LSMS v4.1, the IP is represented in the normal decimal-dot notation that people are used to seeing for IP addresses. In earlier versions, for ease of processing and compactness of staorage rather than ease of viewing, we represented the four-bytes address as 8 hex digits with no decimal point.(Note: if the lead digit is 15 or less, the representation may only be 7 digits.)In the viewer, an IP address is displayed in the normal decimal-dot notation that people are used to seeing.
inOut	"IN" or "OUT"
intf	"e0", "e1", "e2", etc. in log records from <i>Bricks</i> [®] of LSMS v4.1 vintage or later. "ether0", "ether1", "ether2", etc. in logs from <i>Bricks</i> earlier than LSMS v4.1.
number	Decimal representation of a number, in ASCII text. Example: 2345
refType	"Dual" or "Single"
relVpn	"INTERNAL", "EXTERNAL", "BOTH", or empty
severity	"1", "2", or "3"
string	Simple text string

Syntax Type	Representation
table	A string of name-value pairs giving the properties of some administered entity. The representation of a pair is <code><name>=<value></code> and the pairs are separated from each other by commas.
timestamp	Same six-digit timestamp as in the log record header
urlact	"b" = block "p" = pass "n" = passed because no filtering was done
useridbid	"I" = internal, or "E" = assumed external, because not found locally



Appendix H: Log File Sizing Guidelines

Administrative Events Log Sizing Guidelines

Notes on sizing guidelines

Default file size is 1 megabyte and the default space allocated is 100 megabytes.

Using the defaults, the log can grow to 1 megabyte before creating a new log and the amount of disk space that can be consumed by all Administrative Events Logs can be 100 megabytes before deleting old logs to create new space.

The size of the Administrative Events Log varies from site to site. Therefore, a sizing formula does not exist for this log.

Generally, you can start by making the size of the Administrative Events Log 1/10th the size of the Session Log. From then on, monitor the size and adjust it accordingly. This is especially critical as new *Bricks*[®] are added to your network and the amount of network traffic increases.



Session Log Sizing Guidelines

Notes on session log sizing guidelines

Default file size is 10 megabytes and the default space allocated is 1000 megabytes.

Fill in the formula below to help determine the amount of disk space (in bytes) needed for the Session Log:

$$\text{space(bytes)} = (86400 * M * (1000 * F)) + (86400 * 1000 * (M * V/2))$$

where:

M = Total network traffic to be audited, in megabits

F = 1 for full auditing, 1/20 (or .05) for auditing drops only

V = Fraction of traffic that goes through a VPN tunnel

The numbers in the formula (86400, 1000) are constant and are to be used literally.

Example:

If your configuration includes 10 Bricks supporting four T3's and twelve T1's and each connection operates at an average of 50% utilization (full duplex), then the total network traffic (M) is just under 200 Mbps.

Additionally, if you need to audit all traffic and keep the logs for one day and have 10% traffic traveling through VPNs (V), then you need approximately 18.1 GB of disk space, as shown below:

$$\begin{aligned} \text{space} &= (86400 * 200 * 1000) + (86400 * 1000 * (200 * 0.10/2)) = 17.3 \text{ GB} \\ &+ .8\text{GB} = 18.1 \text{ GB} \end{aligned}$$

If you need to keep the logs around for a longer period, then multiply the calculated disk space by the number of days. For example, to keep the logs for three days and using the above calculation, multiply

$$18.1 \text{ GB} \times 3 = 54.3 \text{ GB}.$$

For information on general disk space guidelines, refer to Appendix B. Sizing Guide Lines in the *LSMS Administration Guide* for details.

Important! The above formula only estimates the amount of disk space you may need — it cannot guarantee the exact amount of disk space required for your environment.



Promon Log Sizing Guidelines

Notes on promon log sizing guidelines

Default file size is 10 megabytes and the default space allocated is 200 megabytes.

Fill in the formula below to help determine the amount of disk space (in bytes) needed for the Proactive Monitoring Log:

$$\text{space(bytes)} = 86400 * (F+1) * 2KB/60$$

where:

F = Number of Bricks

The numbers in the formula (86400, 60) are constant and are to be used literally.

Example:

If you have 50 Bricks, then you need approximately .146 GB of disk space, as shown below:

$$.146 \text{ GB} = 86400 * 51 * 2000/60$$

Since you want to keep the logs for seven days, multiply the calculated disk space by the number of days (in this case, 7) to arrive at the final result of approximately 1.028 GB

$$.1.028 \text{ GB} = 7 * .146$$

For information on general disk space guidelines, refer to Appendix B. Sizing Guide Lines in the *LSMS Administration Guide* for details.

Important! The above formula only estimates the amount of disk space you may need — it cannot guarantee the exact amount of disk space required for your environment.



User Authentication Log Sizing Guidelines

Notes on user authentication sizing guidelines

Default file size is 1 megabyte and the default space allocated is 100 megabytes.

Fill in the formula below to help determine the amount of disk space (in bytes) needed for the User Authentication Log:

$$\text{space(bytes)} = 86400 * (U * 400 + V * 1200)$$

where:

U = User authentications per second

V = VPN authentications per second

The numbers in the formula are constant and are to be used literally.

Example:

If you expect an average of one authentication or negotiation per second, and an average of one VPN authentication or negotiation per second, then you need 138.24 MB per day of disk space, as shown below:

$$138.24 \text{ MB} = 86400 * (1 * 400 + 1 * 1200)$$

Since you wanted to keep the logs for seven days, multiply the calculated disk space by the number of days (in this case 7) to arrive at the final result of 967.68 MB.

$$967.68 \text{ MB} = 7 * 138.24$$

For information on general disk space guidelines, refer to Appendix B. Sizing Guide Lines in the *LSMS Administration Guide* for details.

Important! The above formula only estimates the amount of disk space you may need — it cannot guarantee the exact amount of disk space required for your environment.



VPN Log Sizing Guidelines

Notes on VPN log sizing guidelines

Default file size is 1 megabyte and the default space allocated is 100 megabytes.

Using the defaults, the log can grow to 1 megabyte before creating a new log and the amount of disk space that can be consumed by all VPN Logs can be 100 megabytes before deleting old logs to create new space.

The size of the VPN Log varies from site to site. Therefore, a sizing formula does not exist for this log.

Generally, you can start by making the size of the VPN Log 1/10th the size of the Session Log. From then on, monitor the size and adjust it accordingly. This is especially critical as new Bricks are added to your network and the amount of network traffic increases.



Appendix I: Transferring Log Files via FTP

Overview

Purpose

The LSMS allows you to transfer any of the log files to a designated FTP server and destination directory. Storing log files on a machine other than the LSMS is useful for archiving purposes or if you have third-party tools that you want to use to analyze trends using the aggregate log file data.

Configuration Assistant

Set the Log Transfer parameters in the Configuration Assistant (see [Figure I-1, “Log Transfer Parameter in Configuration Assistant”](#) (p. I-2)) to tell the LSMS where and how to transfer log files.

Figure I-1 Log Transfer Parameter in Configuration Assistant

The screenshot shows the Configuration Assistant window with the 'Log Transfer' parameter selected in a list. Below the list is a table for configuring FTP parameters for various sessions. The table has columns for Session, FTP Server, User Name, Password, Destination Dir, and Script Name. There are also checkboxes for 'Send all logs to same FTP Server with same user/password.' and 'Delete files after transfer.'.

Parameter	Description
Alarms	Identifies the SMTP and Syslog servers that will be used when an alarm triggers an e-mail or Syslog message
Detailed Policy Audit	Determines whether or not the detailed auditing for policy components is to be turned on
Direct Paging	Configures the modem used when a direct page action is triggered by an alarm
FIPS	Enable and configure LSMS to operate in FIPS 140-2 Mode
GUI and Status Monitor Parameter	Sets the GUI timeouts, with and without an active Status Monitor
ISS RealSecure	Specifies the port and authentication key used by LSMS to communicate with RealSecure detectors
Log Files	Specifies the log file size and amount of disk space allocated for log files
Log Transfer	Specifies how log files will be transferred to an FTP server for creating reports
Login Banner	Defines the Login Banner that appears at Login Time
LSMS Web Server	Sets the web server type (HTTP or HTTPS) and port, and Remote Navigator download key
Reports	Sets the disk space used by reports, the maximum record size of a report, and the number of lines in a report

	FTP Server	User Name	Password	Destination Dir	Script Name
Session					
Admin Events					
Pro Mon					
User Auth					
VPH					

Send all logs to same FTP Server with same user/password.
 Delete files after transfer.

For details on Configuration Assistant, refer to Chapter 10. Using the Configuration Assistant in the *LSMS Administration Guide*.

FTP Parameters

To transfer logs, enter:

- FTP Server (IP address or host name if DNS is accessible from the LSMS)
- Login Name for FTP Server
- Password for Login Name

- Destination directory where the logs are placed (relative path from the FTP root directory on the FTP server)
- Script name (optional)

FTP Host Requirements

The host that is receiving the log files:

- Must be configured as an FTP server
- Should be configured with any third-party tools you need to use when analyzing the log file data
- Ideally resides on a trusted network segment. If the LSMS resides on this same segment, the log files are sent in the clear and not encrypted.

The following describes how log files are treated on the LSMS with the FTP host:

- If the FTP host and the LSMS reside on different network segments, a LAN to LAN VPN could be created to encrypt the log files.
- If one or more *Bricks*[®] are positioned between the LSMS and the host, then rules must be manually entered to allow the FTP traffic. See the *LSMS Policy Guide* for more information about creating rules.

Contents

Scheduling Log Transfer	I-4
Creating FTP Scripts	I-7
Post Log Transfer	I-10
Using FTP Logs	I-11
Troubleshooting Log Transfer	I-13



Scheduling Log Transfer

Files for scheduling log transactions

In addition to designating the FTP parameter information, you also must establish a schedule that will automatically send the log files.

To establish a schedule for transferring log files, you need to edit these two files:

- `schedTables.txt`
- `schedTable`

These files determine the frequency at which the log files are sent.

You may need to periodically adjust these files according to how much traffic has been generated over the network and how large the log files have become.

Procedure

To set-up a log transfer schedule:

1 Log into the LSMS.

2 Using an ASCII editor, create a file named *schedTables.txt*.

Execute the command as follows:

- Place the file in *\$installdir/isms/scheduler*.
 - Create an entry in *schedTables.txt* as explained in the next section.
-

3 Using an ASCII editor, create a file named *schedTable*.

Do the following:

- Place the file in a directory that is readable or place it in the same directory (e.g., *\$installdir/isms/scheduler*) as the *schedTables.txt* file.
 - Create an entry in the *schedTable* file that defines the schedule as explained in the next section.
-

4 Stop and restart all LSMS services.

END OF STEPS

schedTables.txt

This file must be created in *\$installdir/isms/scheduler* and needs to contain entries conforming to this format:

user/schedTable

where:

The *user/schedTable* file is described below:

- *user* is the login that is used to transfer the files (e.g., root)
- *schedTable* includes the full path to the *schedTable* file that describes a schedule.

The format of this file differs slightly for each platform. An example of *schedTables.txt* on Windows NT is as follows:

Figure I-2 Example schedTables.txt File (Windows NT)

```
root|c:\users\isms\lmf\isms\scheduler\schedTable
```

An example of *schedTables.txt* on Solaris is as follows:

Figure I-3 Example schedTables.txt File (Solaris)

```
root|/opt/isms/lmf/isms/scheduler/schedTable
```

schedTable

This file must be created in a directory that is readable and can reside in the same directory (e.g., *\$installdir/isms/scheduler*) as the *schedTables.txt* file.

This file resembles a crontab file and needs to contain entries conforming to this format:

```
year|month|day|hour|min|day of the
week|true(false)|repeatcount|Freq(Spec)|actual action or command|
```

where:

The elements of the crontab file are described below:

- *year* = a four-digit number or wildcard (*).

and

- month = a two-digit number or wildcard (*).
- day = a two-digit number or wildcard (*).
- hour = a two-digit number (24 hour time) or wildcard (*).
- min = a two-digit number or wildcard (*).
- day of the week = a one-digit number (0-6) or wildcard (*).
- true (or false) = if true, make the repeatcount field active. If false, the repeatcount field is ignored and the logs are transferred only once.
- repeatcount = this field is active only if true is specified in the prior field. This is the number of times the scheduled event will be executed. If repeatcount is a wildcard (*), the log files will be transferred each time the schedule criteria is met.

The following entry schedules the logs to be transferred only three times. Every time the schedule criteria is satisfied, the logs are transferred. The transfer will take place 5 minutes after 3 consecutive hours (e.g., 12:05, 13:05, 14:05).

Another example illustrates repeatcount as a wildcard (*). In this example, the following entry schedules the logs to be sent every five minutes.

- Freq (or Spec) = if Freq is specified, the logs will be transferred repeatedly at the frequency specified in the time fields (e.g., year, month, day, etc). If Spec is specified, the logs will be transferred at the explicit time as specified in the time fields (e.g., year, month, day, etc.). For example, the following entry schedules the logs to be sent five minutes past midnight on the 15th of every month:
- actual action or command = any executable or script that you want to invoke. Typically, to send the logs, specify "ismsjre isms.qnr.LogSender".

Disabling the Transfer Schedule

To disable a schedule that is currently in place, you can either:

- Remove the entries from the SchedTable file and restart the LSMSSchedSvc service.
- With Configuration Assistant, remove all Log transfer parameters so they are blank. Refer to Chapter 10, Using the Configuration Assistant in the *LSMS Administration Guide* for details.

□

Creating FTP Scripts

Overview

Specifying a script in the **Script Name** field for each log is optional. For instance, if you need to compress the log before it is transferred, you can provide your own customized script. Compression is the example that is carried out through this section of the chapter.

The script you write can reside anywhere as long as you provide the entire pathname to the script (e.g., *c:\scripts\log_pkzip.bat*) or the directory is in the machine's PATH. Environment variables are also accepted as long as they have been pre-defined.

The script requires two arguments:

- The full pathname of the log file.
- The full pathname of the file to be transferred. Typically, this is the compressed file that was created by the script.

The transfer program automatically assigns the processed log to a file name with a *.lxc* extension (e.g., *2001-07-22-.lxc*).

The first argument (i.e., the actual log file) that is passed to the script is not transferred to the FTP Server.

Only the second argument (i.e., the processed file) is actually sent. See the next few sections for some script examples.

Sample PKZIP Compression Scripts

The following is a sample script that compresses a log file before it is transferred to the designated FTP Server.

The sample script is named *processlog_pkzip.bat* and runs on Windows NT. Pkzip Version 2.5 is used here because it can handle long file names (e.g., *2001-07-22-.log*).

The script accepts two arguments that were just explained:

- %1 is the original log file (e.g., *\users\isms\lmc\log\sessions\2001-07-22-.log*)
- %2 is the log file in zipped format (e.g., *\users\isms\lmc\log\sessions\2001-07-22-.lxc*) that will be transferred.

Figure I-4 Sample PKZIP Compression Script (Windows NT)

```
c:\emp\application\pkzip\pkzip25 -add -nozipextension %2 %1
```

The `-nozipextension` switch is supplied so the name of the processed log does not contain the `.zip` suffix. Otherwise, the transfer program would not recognize the file (e.g., `2001-07-22-.lxc.zip`) and the file would not be sent.

The equivalent script on Solaris would be:

Figure I-5 Sample PKZIP Compression Script (Unix)

```
/export/home/pkzip/pkzip25 -add -nozipextension $2 $1
```

Sample GZIP Compression Scripts

Another example script also compresses a log file prior to file transfer but uses a different compression utility (i.e., `gzip`).

Like `pkzip`, the `gzip` utility adds a file extension to the compressed file that must be suppressed in order for a successful transfer. However, the `gzip` utility does not have a comparable `-nozipextension` switch as does `pkzip`, so this has to be addressed in a different manner as the following sample scripts illustrate.

The sample script is named `processlog_gzip.bat` and runs on Windows NT.

Figure I-6 Sample GZIP Compression Script (Windows NT)

```
copy %1 %2
c:\emp\application\gzip\gzip %2
rename %2.gz %2
```

The first line of the script copies the contents of the original log file (e.g., `2001-07-22-.log`) to the second argument (e.g., `2001-07-22-.lxc`).

In the second line of the script, the log file is compressed and the `.gz` file extension is automatically added. So there is now a compressed file named `2001-07-22-.lxc.gz`.

The third line of the script removes the `.gz` suffix so the file is left with only the `.lxc` suffix (e.g., `2001-07-22-.lxc`). Otherwise, the transfer program would not recognize the file (e.g., `2001-07-22-.lxc.gz`) and the file would not be sent.

The equivalent script on Unix would be:

Figure I-7 Sample GZIP Compression Script (Unix)

```
cp $1 $2  
/export/home/gzip/gzip-1.2.4/gzip $2  
mv $2.gz $2
```



Post Log Transfer

Deletion of log files

After the log files have been transferred, the log files can be automatically deleted from the original machine to free up disk space.

To delete the logs automatically, check ► the **Delete files after transfer** checkbox as shown in [Figure I-1, “Log Transfer Parameter in Configuration Assistant”](#) (p. I-2). This will delete all log files that have been successfully transferred. When the **Delete files after transfer** checkbox is checked, it also ensures that logs are not transmitted twice.

Important! *Non-successful Transmission*

If the logs are not successfully transferred, the log file is not deleted and an error message is written to the Administrative Events Log.

If the FTP transfer fails, the system will attempt to transmit the file at the next scheduled transfer.



Using FTP Logs

Purpose of ftp log file

As log files are transferred via FTP, all activity is recorded to an FTP log file. This file is created in the *trace* directory under the installation root directory.

The name of the log is *ftplot.txt*. This log can be viewed to examine real-time or historical FTP activity. It is especially useful if problems were encountered with FTP.

An excerpt of *ftplot.txt* on Windows NT is as follows:

Figure I-8 ftplot.txt on Windows NT

```
July 21, 2001 1:25:00 PM GMT+02:00

Verbose mode On.
user ftptest *****
verbose
cd /nt/session
250 CWD command successful.
Local directory now C:\users\isms\lmf\log\sessions
lcd C:\users\isms\lmf\log\sessions
binary
200 Type set to I.
!c:/temp/application/gzip/processlog.bat 2001-07-21-12-.log 2001-07-
 21-12-.lxc >>C:\users\isms\lmf\trace\ftpScriptOut.txt
put 2001-07-21-12-.lxc
200 PORT command successful.
150 Opening BINARY mode data connection for 2001-07-21-12-.lxc.
```

An excerpt of *ftplot.txt* on Solaris is as follows:

Figure I-9 ftplog.txt on Solaris

```
20 july 2001 15:19:01 GMT-04:00
---> USER ftptest
---> PASS *****
Verbose mode on.
---> CWD /solaris/session
250 CWD command successful.
Local directory now /opt/isms/lmf/log/sessions
---> TYPE I
200 Type set to I.
/bin/sh -c /export/home/gzip/gzip-1.2.4/processlog.bat 2001-07-20-14-
57-.log 2001-07-20-14-57-.lxcg
---> PORT 148,70,10,4,130,123
200 PORT command successful.
---> STOR 2001-07-20-14-57-.lxcg
150 Opening BINARY mode data connection for 2001-07-20-14-57-.lxcg.
226 Transfer complete.
local: 2001-07-20-14-57-.lxcg remote: 2001-07-20-14-57-.lxcg
65376 bytes sent in 0,12 seconds (553,34 Kbytes/s)
/bin/sh -c rm 2001-07-20-14-57-.lxcg
local: 2001-07-20-14-57-.lxcg remote: 2001-07-20-14-57-.lxcg
65376 bytes sent in 0,12 seconds (553,34 Kbytes/s)
/bin/sh -c /export/home/gzip/gzip-1.2.4/processlog.bat 2001-07-20-15-
.log 1999-07-20-15-.lxcg
local: 2001-07-20-14-57-.lxcg remote: 1999-07-20-14-57-.lxcg
65376 bytes sent in 0,12 seconds (553,34 Kbytes/s)
```

The FTP logs are rolled over when the file size exceeds 5 MB. When the first *ftplog.txt* exceeds 5 MB, it is copied to *ftplog_1.txt* and a new *ftplog.txt* is created.

When *ftplog.txt* exceeds 5 MB again, *ftplog_1.txt* is copied to *ftplog_2.txt* and *ftplog.txt* is copied to *ftplog_1.txt*. Up to six FTP log files, with the oldest being *ftplog_5.txt*, are created, with each growing in size up to 5 MB.

When *ftplog_5.txt* reaches capacity, new FTP activity overwrites *ftplog_1.txt*, *ftplog_5.txt* is deleted, and the files are shifted again.

□

Troubleshooting Log Transfer

Overview

If problems occur with the transfer of any log:

- You can run an Administrative Events report and search for one or more of these record types:
 - Type 46. Indicates successful transfer.
 - Type 5. Indicates error in transfer.
 - Type 25. Informational message on the transfer.As Figure I-13 illustrates, the source of the record must be `report`. This report can be memorized and run periodically to detect transfer problems. See [Chapter 9, “Administrative Events Report”](#) for more information.
- Look in the FTP log file as described in [“Using FTP Logs” \(p. I-11\)](#) for details on recorded FTP activity.
- Look in `trace/ftplog.txt` and `trace/ftpScriptOut.txt`.
- Ensure the path for `schedTable` is correct in `schedTables.txt` file. See [“Scheduling Log Transfer” \(p. I-4\)](#).
- If using a compression script (see [“Creating FTP Scripts” \(p. I-7\)](#)), ensure the path is correct for the compression utility or if using an environment variable, ensure the variable has been defined.
- Build the script incrementally, one line at a time. Issue just the copy command first, and after it completes successfully, issue the compression commands.
- After defining the FTP parameters in Configuration Assistant and setting up the schedule, ensure that you stop and restart the services.
- Finally, try to transfer the logs manually using the same login, password, and FTP server. If a manual transfer is successful, then the problem lies elsewhere.

□

Appendix J: Pre-Configured Reports

Overview

Purpose

This appendix explains the pre-configured reports that are created when the LSMS application is installed.

An LSMS administrator can view and run all seven pre-configured reports. A Group administrator can view and run three pre-configured reports as long as they have the correct privileges.

Contents

Closed Session Details Reports	J-2
Administrative Events Reports	J-3
Run a Pre-Configured Report	J-5
Run Multiple Reports	J-6



Closed Session Details Reports

Types of Closed Session Details reports

There are two pre-configured Closed Session Details reports, as described below.

Drops by Rule 65535 Report

This report tracks all sessions that are dropped by rule 65535. This report resides in the Closed Session Details folder.

An LSMS administrator automatically can view and run this report. By default, the report includes sessions involving all *Brick*[®] zone rulesets in all groups.

A Group administrator can view and run this report if they have been assigned at least View privileges for the Policies & VPN privilege category of at least one group. See Chapter 8. Creating Groups and Administrators in the *LSMS Administration Guide* for details on privileges. Therefore, the report will contain only sessions of Brick zone rulesets in groups for which they have this privilege.

Unauthorized Brick Connection Attempts Report

This report tracks all sessions where an unauthorized connection attempt was made to one or more Bricks. This report resides in the Closed Session Details folder.

The report includes sessions that pass through the *firewall* Brick zone ruleset and when the traffic is dropped.

An LSMS administrator automatically can view and run this report. By default, the report includes sessions involving all Bricks in all groups.

A Group administrator can access and run this report if they have been assigned at least View privileges for the Devices privilege category of at least one group. See Chapter 8. Creating Groups and Administrators in the *LSMS Administration Guide* for details on privileges. Therefore, the report will contain only sessions of Bricks in groups for which they have this privilege.



Administrative Events Reports

Types of Administrative Events reports

There are five pre-configured Administrative Events reports, as described below.

Brick and LSMS Logging Connectivity Report

This report tracks all sessions that transpire between the Logger of the LSMS and all Bricks of any group. This report resides in the Administrative Events folder.

An LSMS administrator automatically can view and run this report. By default, the report includes sessions involving all Bricks in all groups.

A Group administrator will not see and cannot run this report.

Brick Errors Report

This report tracks all sessions that includes errors generated by one of more Bricks. This report resides in the Administrative Events folder.

The report includes errors with codes between 1 and 199 and represent events such as land attacks, a failed port, etc.

An LSMS administrator automatically can view and run this report. By default, the report includes sessions involving all Bricks in all groups.

A Group administrator can access and run this report if they have been assigned at least View privileges for the Devices privilege category of at least one group. See Chapter 8. Creating Groups and Administrators in the *LSMS Administration Guide* for details on privileges. Therefore, the report will contain only sessions of Bricks in groups for which they have this privilege.

Failed Login Attempts

This report tracks all sessions where an attempt to login into the LSMS failed. This report resides in the Administrative Events folder.

An LSMS administrator automatically can view and run this report. A Group administrator will not see and cannot run this report.

Successful Admin Logins

This report tracks all sessions where logins to the LSMS were successful. This report resides in the Administrative Events folder.

An LSMS administrator automatically can view and run this report. A Group administrator will not see and cannot run this report.

Successful Admin Logouts

This report tracks all sessions where logouts from the LSMS were successful. This report resides in the Administrative Events folder.

An LSMS administrator automatically can view and run this report. A Group administrator will not see and cannot run this report.



Run a Pre-Configured Report

Task

To run a pre-configured report:

- 1 With the Navigator window displayed, open the Reports folder.

- 2 Right-click the report in the Contents panel and select **Run Report** from the pop-up menu.

- 3 The default is for the report to cover the last five minutes of activity. Do any of the following:
 - Leave the default in place and click the **OK** button to run the report.
 - Change the five minutes to a different time period (it can range from one to 99 minutes) and click the **Run** button to run the report.
 - Click **Select Time Range** to display **Start Date and Time** and **End Date and Time** fields.
 - Enter the appropriate dates and times (or click the **Earliest Start Date** or **Now** buttons), and click the **Run** button to run the report.

A progress window will appear as the report is generated. Once the report is complete, it will appear in a separate browser window on your screen.

END OF STEPS



Run Multiple Reports

When to use

Multiple reports can be selected and run simultaneously to produce a single report. The output from the individual reports will be merged together.

A union of the log records is produced in the single report where the output of the report must match the filter criteria of at least one of the reports. The only restriction in running multiple reports together is that both reports must be of the same type (e.g., all Administrative Events reports).

Task

To run multiple reports together:

- 1 With the Navigator window displayed, open the Reports folder.

- 2 Open one of the reports folders and right-click a report in the Contents panel.

- 3 Select **Run Multiple Reports** from the pop-up menu.

- 4 In the window, select one or more reports. You can use the modifier keys (Ctrl or Shift) to select non-sequential reports or a range of reports.

- 5 Select **Run**.

A progress window will appear as the report is generated. Once the report is complete, it will appear in a separate browser window on your screen.

END OF STEPS



Index

Symbols

\$installdir/isms/scheduler, [I-4](#)

A Actions, [4-5](#)

Administrative Events Log, [1-2](#)

Administrative Events log, [3-1](#)

Administrative Events Report,
[8-2](#), [9-1](#)

Alarm History, [5-18](#)

Alarms Report, [12-1](#)

Alarms Wizard, [4-9](#), [4-9](#)

Audit logs, [3-3](#)

Log messages, [3-3](#)

B Brick devices

supported, [xxii](#)

C Closed Sessions Detail Report, [11-1](#)

Configuration Assistant, [I-1](#)

Configure

Alarms, [5-2](#), [6-3](#), [7-2](#)

D Direct Page, [5-5](#)

Disable alarms, [6-66](#)

E Email message, [5-9](#)

F FTP Log files, [I-1](#)

H Halt All Traffic feature, [1-7](#),
[1-7](#)

L Log file

Names, [1-4](#)

Log files

FTP, [I-1](#)

Source timestamp, [3-3](#), [3-8](#)

Log messages, [3-3](#)

Lucent Netcare Professional
Services, [xxii](#)

M MetroCall, [5-5](#)

P PageNet, [5-5](#)

Proactive Monitoring log, [3-7](#)

R Reports

Administrative Events, [8-2](#),
[9-1](#)

Alarms, [12-1](#)

Closed Sessions Detail
Report, [11-1](#)

Session Log, [10-1](#)

S schedTable, [I-4](#)

schedTables.txt, [I-4](#)

Sessions Log, [1-2](#)

Sessions log, [3-3](#)

Sizing guidelines, [H-2](#)

Sessions Log Report, [10-1](#)

SkyTel, [5-5](#)

Source timestamp

Log files, [3-3](#), [3-8](#)

syslogd, [5-14](#)

T Technical support, [xxiii](#)

Telocator Alphanumeric
Protocol v1.8, [5-5](#)

Throttling, [5-18](#)

U Unauthorized firewall

connection attempts, [4-4](#)

User Authentication log, [3-11](#)

User Authentication Report

Generate, [13-2](#), [13-14](#)
