



Security Threat Response Manager

STRM Log Management Users Guide

Release 2008.2 R2

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 530-027300-01, Revision 1

Copyright Notice

Copyright © 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense. The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: Reorient or relocate the receiving antenna. Increase the separation between the equipment and receiver. Consult the dealer or an experienced radio/TV technician for help. Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

STRM Log Management Users Guide
Release 2008.2 R2

Copyright © 2008, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Revision History

September 2008—Revision 1

The information in this document is current as of the date listed in the revision history.

CONTENTS

ABOUT THIS GUIDE

- Conventions 1
- Technical Documentation 1
- Contacting Customer Support 1

1 ABOUT STRM LOG MANAGEMENT SLIM

- Logging In to STRM Log Management 3
- Dashboard 4
- Event Viewer 5
- Reports 5
- Using STRM Log Management 6
 - Sorting Results 6
 - Refreshing the Interface 6
 - Pausing the Interface 6
 - Investigating IP Addresses 6
 - STRM Log Management Time 7
 - Accessing On-line Help 7
- STRM Log Management Administration Console 8

2 USING THE DASHBOARD

- About the Dashboard 9
 - Using the Dashboard 10
- Event Viewer 10
 - Events Over Time 10
 - Events By Severity 11
 - Top Devices 11
- Reports 12
- System Summary 12
- Adding Items 13

3 USING THE EVENT VIEWER

- Using the Event Viewer Interface 16
 - Using the Toolbar 16
 - Using the Right-Click Menu Options 16
- Viewing Events 17
 - Viewing Normalized Events 17

Viewing Raw Events	20
Viewing Aggregate Normalized Events	21
Using the Search	27
Searching Events	27
Deleting Saved Searches	30
Modifying Event Mapping	31
Exporting Events	33

4 CONFIGURING RULES

Viewing Rules	36
Enabling/Disabling Rules	37
Creating a Rule	37
Event Rule Tests	47
Copying a Rule	52
Deleting a Rule	53
Grouping Rules	53
Viewing Groups	53
Creating a Group	54
Editing a Group	55
Copying an Item to Another Group(s)	56
Deleting an Item from a Group	57
Assigning an Item to a Group	58
Editing Building Blocks	58

5 MANAGING REPORTS

Using the Reports Interface	62
Using the Navigation Menu	62
Using the Toolbar	63
Viewing Reports	63
Grouping Reports	64
Creating a Group	65
Editing a Group	66
Copying a Template to Another Group	66
Deleting a Template From a Group	67
Assigning a Report to a Group	68
Creating a Report	68
Creating a Template	69
Configuring Charts	76
Selecting a Graph Type	85
Using Default Report Templates	86
Generating a Report	87
Duplicating a Report	87
Sharing a Report	88
Branding Your Report	88

A **DEFAULT RULES AND BUILDING BLOCKS**

Default Rules 91

Default Building Blocks 101

A **GLOSSARY**

INDEX




ABOUT THIS GUIDE

The *STRM Log Management Users Guide* provides information on managing STRM Log Management including the Dashboard, Reports, and Event Viewer interfaces.

Conventions

[Table 1](#) lists conventions that are used throughout this guide.

Table 1 Icons

Icon	Type	Description
	Information note	Information that describes important features or instructions.
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, device, or network.
	Warning	Information that alerts you to potential personal injury.

Technical Documentation

You can access technical documentation, technical notes, and release notes directly from the Juniper Networks support web site at <https://juniper.net/support>. Once you access the Juniper Networks support web site, locate the product and software release for which you require documentation.

Your comments are important to us. Please send your e-mail comments about this guide or any of the Juniper Networks documentation to:

documentation@juniper.com.

Include the following information with your comments:

- Document title
- Page number

**Contacting
Customer Support**

To help you resolve any issues that you may encounter when installing or maintaining STRM Log Management, you can contact Customer Support as follows:

- Log a support request 24/7: <https://juniper.net/support>
For access to the Juniper Networks support web site, please contact Customer Support.
- Access Juniper Networks support and Self-Service support using e-mail: support@juniper.net
- Telephone assistance: 1-800-638-8296.

1

ABOUT STRM LOG MANAGEMENT

STRM Log Management is a network security management platform that provides situational awareness and compliance support through security event correlation, analysis, and reporting. This chapter provides an overview of the STRM Log Management interface including:

- [Logging In to STRM Log Management](#)
- [Dashboard](#)
- [Event Viewer](#)
- [Reports](#)
- [Using STRM Log Management](#)
- [STRM Log Management Administration Console](#)



Note: When navigating STRM Log Management, do not use the browser Back button. Use the navigation options available with STRM Log Management to navigate the interface.

Logging In to STRM Log Management

To login to STRM Log Management:

Step 1 Open your web browser.

Step 2 Log in to STRM Log Management:

https://<IP Address>

Where **<IP Address>** is the IP address of the STRM Log Management system. The default values are:

Username: **admin**

Password: **<root password>**

Where **<root password>** is the password assigned to STRM Log Management during the installation process. For more information, see the *STRM Log Management Installation Guide*.

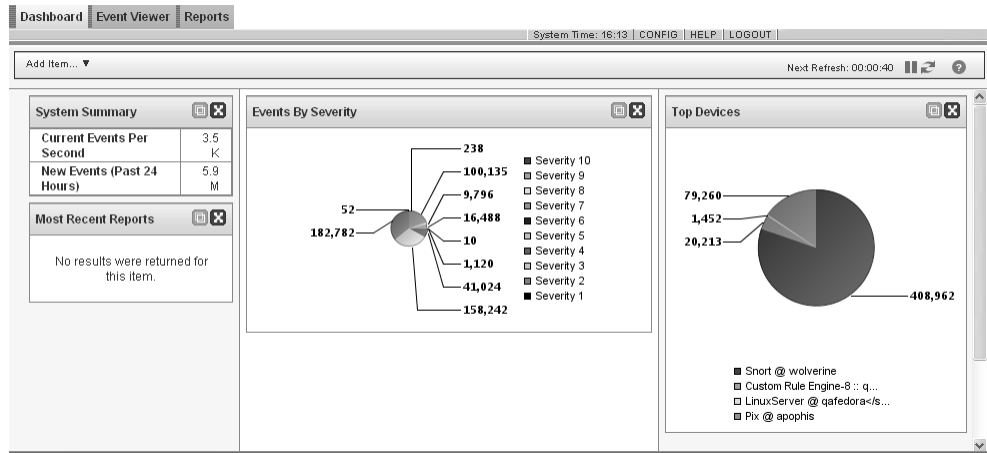
Step 3 Click **Login To STRM Log Management**.

For your STRM Log Management Console, a default license key provides you access to the interface for 5 weeks. A window appears providing the date that the

temporary license key will expire. For information on installing a permanent license key, see the *STRM Log Management Administration Guide*.

Dashboard

The Dashboard tab is the default interface that appears when you log in to STRM Log Management. The Dashboard tab provides summary and detailed information on events occurring on your network. The Dashboard is customizable on a per user basis to focus on individual user's security or network operations responsibilities.



Note: For more information on using the Dashboard, see [Chapter 2 Using the Dashboard](#).

Event Viewer

The Event Viewer allows you to view event logs being sent to STRM Log Management in real-time, or through searches. The Event Viewer is a powerful tool for performing in-depth investigations on event data.

The screenshot shows the Event Viewer interface with the following data in the event log table:

Event Name	Device	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude
Misc Exploit - Event CRE	Custom Rule Engine-8 :: radar	1	16:16	Misc Exploit	172.16.60.21	27932	172.16.210.240	635		■■■■
Misc Exploit - Event CRE	Custom Rule Engine-8 :: radar	1	16:16	Misc Exploit	172.16.60.240	30163	172.16.210.214	518		■■■■
Misc Exploit - Event CRE	Custom Rule Engine-8 :: radar	1	16:16	Misc Exploit	172.16.60.201	29270	172.16.210.145	123		■■■■
Misc Exploit - Event CRE	Custom Rule Engine-8 :: radar	1	16:16	Misc Exploit	172.16.60.193	36412	172.16.210.241	518		■■■■



Note: For more information, see [Chapter 3 Using the Event Viewer](#).

Reports

Reports is a flexible and robust reporting package that allows you to create, distribute, and manage reports for any data within STRM Log Management. Reports allows you to create customized reports for operational and executive use by combining any combination of information into a single report. You can also use the many pre-installed report templates included with STRM Log Management.

The Reports tab also allows you to brand your reports with your customized logos enabling you to support various unique logos for each report. This is beneficial for distributing reporting to different audiences.

The screenshot shows the Reports interface with the following data in the report templates table:

Template Name	Group	Schedule	Next Run Time	Last Modification	Owner	Author	Output
Weekly Virus Summary	Executive	Weekly	Inactive	2008-06-02 12:00	admin	admin	PDF
Monthly Policy Violation Summary	Executive	Monthly	Inactive	2008-06-02 12:00	admin	admin	PDF
Daily Juniper SSL VPN Authentication Activity	Security	Daily	Inactive	2008-06-02 12:00	admin	admin	PDF
Daily Web Access Summary	Executive	Daily	Inactive	2008-06-02 12:00	admin	admin	PDF
Monthly Category Distribution	Executive	Monthly	Inactive	2008-06-02 12:00	admin	admin	PDF
Daily Network Exploit Summary	Executive	Daily	Inactive	2008-06-02 12:00	admin	admin	PDF
Monthly Web Access Summary	Executive	Monthly	Inactive	2008-06-02 12:00	admin	admin	PDF
Monthly Most Active Devices	Security	Monthly	Inactive	2008-06-02 12:00	admin	admin	PDF
Daily System Admin Logins and Logouts	Security	Daily	Inactive	2008-06-02 12:00	admin	admin	PDF,XLS
Weekly User Account Activity Summary	Executive	Weekly	Inactive	2008-06-02 12:00	admin	admin	PDF



Note: For more information on Reports, see [Chapter 5 Managing Reports](#).

Using STRM Log Management

Using STRM Log Management, you can:

- Sort the results. See [Sorting Results](#).
- Refresh the interface. See [Refreshing the Interface](#).
- Pause the current display. See [Pausing the Interface](#).
- Further investigate an IP address. See [Investigating IP Addresses](#).
- View the time of the STRM Log Management Console. See [STRM Log Management Time](#).
- View the STRM Log Management on-line Help. See [Accessing On-line Help](#)

Sorting Results


In the Event Viewer tab you can sort the resulting tables by clicking on a column heading. A single click of the desired column sorts the results in descending order and a second click on the heading sorts the results in ascending order. An arrow at the top of the column indicates the direction of the sort.

For example, if you wish to sort the events by Name, click the Name heading. An arrow appears in the column heading to indicate the results are sorted in descending order.


Event Name	Device	Event Count	Time ▼	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username	Magnitude
User Login	System Audit-2 :: mustang	1	10:46	SIM User Authentication	10.100.50.71	0	10.100.100.25	0	admin	■■■■
Unknown Audit Event	System Audit-2 :: mustang	1	10:46	SIM Configuration Change	10.100.50.71	0	10.100.100.25	0	admin	■■■
User Login	System Audit-2 :: mustang	1	10:46	SIM User Authentication	10.100.50.71	0	10.100.100.25	0	admin	■■■■

Click the Name column heading again if you wish to sort the information in ascending order.

Refreshing the Interface

The Event Viewer and the Dashboard allow you to refresh the interface. This refresh option is located in the right corner of the interface. The timer indicates the amount of time since the interface was refreshed. To refresh the interface, click the refresh  icon.

Pausing the Interface

You can use the refresh timer, located on the right, to pause the current display. To pause the interface, click the pause icon . The timer flashes red to indicate the current display is paused. Click the icon again to restart the timer.

Investigating IP Addresses

You can use the right-mouse button (right-click) on any IP address to access additional menus, which allow you to further investigate that IP address. The menu options include:



Note: For information on customizing the right-click menu, see the *Customizing the Right-Click Menu Technical Note*.

Table 1-1 Additional Options

Menu	Sub-Menu	Description
Information	DNS Lookup	Searches for DNS entries based on the IP address.
	WHOIS Lookup	Searches for the registered owner of a remote IP address (Default system server: whois.crsnic.net.)
	Port Scan	Performs a NMAP scan of the selected IP address. This option is only available if NMAP is installed on your system. For more information on installing NMAP, see your vendor documentation.

STRM Log Management Time

The right corner of the STRM Log Management interface displays STRM Log Management time, which is the time of the STRM Log Management Console. The STRM Log Management Console time synchronizes all STRM Log Management appliances within the STRM Log Management deployment, and is used to determine the time events were received from other devices for proper time sync correlation.

Accessing On-line Help

You can access the STRM Log Management on-line Help through the main STRM Log Management interface. To access the on-line Help, click **Help > Help Contents**. The Help interface appears.

STRM Log Management Administration Console

The STRM Log Management Administration Console is a client-based application that provides administrative users access to administrative functionality including:

- **System Configuration** - Allows you configure system wide STRM Log Management settings including, users, thresholds, system settings, backup and recovery, license keys, network hierarchy, authentication, or automatic updates.
- **Access the deployment editor** - Allows you to manage the individual components of your STRM Log Management deployment.
- **Configure sensor devices** - Allows you to configure sensor devices, which provide events to your deployment through DSMs.

All configuration updates using the Administration Console are saved to a staging area. Once all changes are complete, you can deploy the configuration changes or all configuration settings to the remainder of your deployment.

For more information regarding the STRM Log Management Administration Console, see the *STRM Log Management Administration Guide*.

2

USING THE DASHBOARD

The Dashboard allows you to create a customized portal to monitor any data STRM Log Management collects, to which you have access. The Dashboard is the default view when you log in to STRM Log Management and allows you to monitor several areas of your network at the same time. Normal activity and suspicious behaviors can be investigated directly from the Dashboard. Also, you can detach an item and monitor the item directly from your desktop.

This chapter includes:

- [About the Dashboard](#)
- [Event Viewer](#)
- [Reports](#)
- [System Summary](#)
- [Adding Items](#)

About the Dashboard

The Dashboard allows you to monitor your security event behavior. By default, for non-administrative users, the Dashboard is empty. For administrative users, the Dashboard displays the following:

- System Summary
- Events - Average Events Per Second
- Events By Severity
- Most Recent Reports
- Top Devices



Note: *The items that appear on your Dashboard depends on the access you have been granted. For more information on user roles, see the STRM Log Management Administration Guide.*

The content that appears on the Dashboard is user-specific. You can design the Dashboard as you wish, as the changes made within a STRM Log Management session affect only your system. The next time you log in, STRM Log Management reflects your last Dashboard configuration.

You can move and position items to meet your requirements. You can stack items in one panel or distribute them evenly within the three panels. When positioning items, each item automatically resizes in proportion to the panel. The Dashboard interface refreshes regularly to display the most recent information.

Using the Dashboard You can add, remove, or detach items on the Dashboard. Once added, each item appears with a titlebar. Using the Dashboard, you can:

- **Adding Items** - Provides the list of items that you can add to your Dashboard. You can monitor the following items:
 - [Event Viewer](#)
 - [Reports](#)
 - [System Summary](#)

- **Removing an Item** - To remove an item from the Dashboard, click the red icon located in the upper right corner of the item.

A confirmation window appears before an item is removed. Removing an item does not remove the item from STRM Log Management. Removing an item clears the item from the Dashboard. You can add the item again at any time.

- **Detaching an Item** - To detach an item from the Dashboard, click the green icon located in the upper right of the item. Detaching an item does not remove the item from STRM Log Management; detaching an item duplicates the data in a new window.

Detaching an item allows you to temporarily monitor one or more particular items on your desktop. You can detach the item then remove the item from the Dashboard - the detached window remains open and refreshes during scheduled intervals. If you close the STRM Log Management application, the detached window remains open for monitoring and continues to refresh until you manually close the window or shut down your computer system.



Note: *STRM Log Management does not save the status of a detached Dashboard item when you end your STRM Log Management session.*

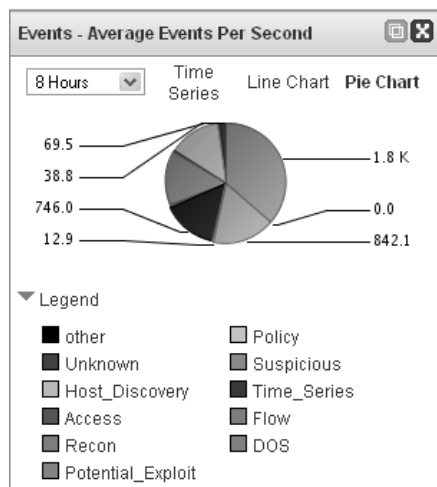
Event Viewer

You can add several Event Viewer items to your Dashboard. The Event Viewer allows you to monitor and investigate events in real-time. Event Viewer options include:

- [Events Over Time](#)
- [Events By Severity](#)
- [Top Devices](#)

Events Over Time

The Events Over Time option displays events received over the last 8 hours in 15 minute intervals, categorized by the event category.



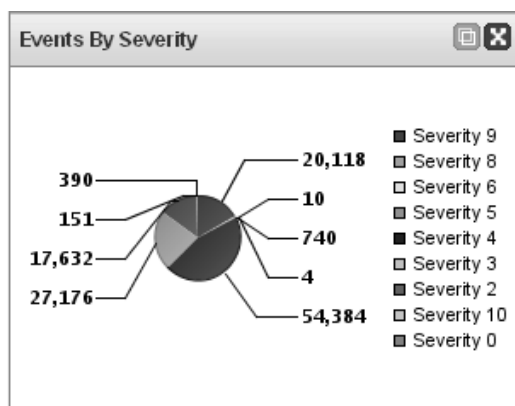
Note: You must have the required permissions to access Event Viewer items.

To customize your display:

- **Period of Time** - Using the drop-down list box, select the period of time you wish the Dashboard graph to display.
- **Chart Type** - You can display the data using a Time Series (default), Line Chart, or Pie Chart. To change the chart type, click **Time Series**, **Line Chart** or **Pie Chart** at the top of the graph.

Events By Severity

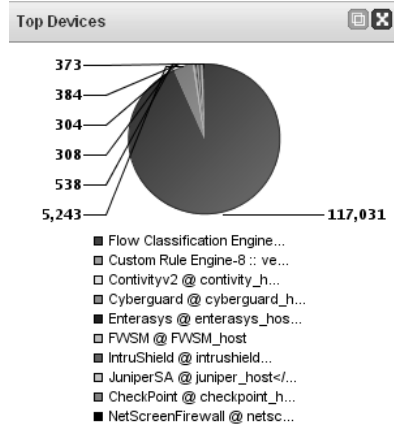
The Events By Severity item displays a pie chart that specifies the number of active events grouped by severity. This item allows you to see the number of events that are being received by the level of severity that has been assigned. Severity indicates the amount of threat an attacker poses in relation to how prepared the target is for the attack. The range of severity is 0 (low) to 10 (high).



Top Devices

The Top Devices item displays a pie chart that specifies the top 10 devices that sent events to STRM Log Management within the last 15 minutes. The number of events sent from the specified device is indicated in the pie chart. This item allows

you to view potential changes in behavior, for example, if a firewall device that is typically not in the top 10 list is now contributing to a large percentage of the overall message count, you should investigate this occurrence.



Reports

The Reports option allows you to display the top recently generated reports. The display provides the report title, the time and date the report was generated, and the format of the report.

Report Title	Generated	Format
Executive TopN Securi...	2007-08-28 01:03	
Event Distribution	2007-08-28 01:03	
Daily Top Targeted As...	2007-08-28 01:02	
Daily Top Targeted As...	2007-08-28 01:02	
Daily Top Security an...	2007-08-28 01:02	

System Summary

The Summary item provides a high-level summary of activity within the past 24 hours. Within the summary item, you can view the following information:

- **Current Events Per Second** - Specifies the number of current events per second.
- **New Events (Past 24 Hours)** - Specifies the total number of new events received within the last 24 hours.

Current Events Per Second	0
New Events (Past 24 Hours)	3

Adding Items

You can add multiple displays to the Dashboard interface. To add an item to the Dashboard:

Step 1 Click the **Dashboard** tab.

The Dashboard interface appears.

Step 2 From the toolbar, click **Add Item**.

A list of menu items appears.

Step 3 Navigate through the categories, options include:

- [Event Viewer](#)
- [Reports](#)
- [System Summary](#)

Each panel highlights as you pass an item over the panel signalling an item can be dropped into that panel. If the item titlebar is above the titlebar of an existing item, the new item assumes position above the existing item.

3

USING THE EVENT VIEWER

An event is an action that occurs on a network or a host. The Event Viewer allows you to monitor and investigate events in real-time or perform advanced searches. You must have permission to view the Event Viewer interface. For more information on assigning roles, see the *STRM Log Management Administration Guide*.

This chapter provides information on using the Event Viewer including:

- [Using the Event Viewer Interface](#)
- [Viewing Events](#)
- [Using the Search](#)
- [Modifying Event Mapping](#)
- [Exporting Events](#)



Note: When STRM Log Management normalizes events, the system normalizes names as well. Therefore, the name that appears in the Event Viewer may not match the name that appears in the event.

Using the Event Viewer Interface

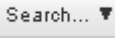




This section provides information on using the Event Viewer interface including:

- [Using the Toolbar](#)
- [Using the Right-Click Menu Options](#)

Using the Toolbar

Using the toolbar, you can access the following options:

Table 3-1 Toolbar Options

Option	Description
	<p>Allows you to perform advanced searches on events including:</p> <ul style="list-style-type: none"> • Edit Search - Allows you to perform a search. • Quick Searches - Allows you to perform previously saved searches. This option only appears when you have saved search criteria. <p>For more information, see Using the Search.</p>
	<p>Allows you to save the current search criteria.</p>
	<p>Allows you to configure custom event rules to detect a single event (within certain properties) or event sequences. For information on rules, see Chapter 4 Configuring Rules.</p>
	<p>Allows you to perform the following actions:</p> <ul style="list-style-type: none"> • Show All - Removes all filters on search criteria and presents all events. • Print - Allows you to print the events displayed in the window. • Export to XML - Allows you to export events in XML format. See Exporting Events. • Export to CSV - Allows you to export events in CSV format. See Exporting Events.
	<p>Allows you to display events grouped by criteria specified in the drop-down list box.</p>

Using the Right-Click Menu Options

Using the right mouse button (right-click), you can access the Filter menu options, which allows you to filter on the selected event, depending on the selected item in the event. For example, if you right-click on a Category of IP Protocol Anomaly, the following filter options appear:

`Filter on Category is IP Protocol Anomaly`

`Filter on Category is not IP Protocol Anomaly`

Viewing Events

By default, the Event Viewer interface displays normalized events. Initially, the Event Viewer displays events that occurred during the previous minute and the interface refreshes each minute.

You can sort the resulting tables by clicking on a column heading. A single click of the desired column sorts the results in descending order and a second click on the heading sorts the results in ascending order. An arrow at the top of the column indicates the direction of the sort.

You can also view events using the following options:

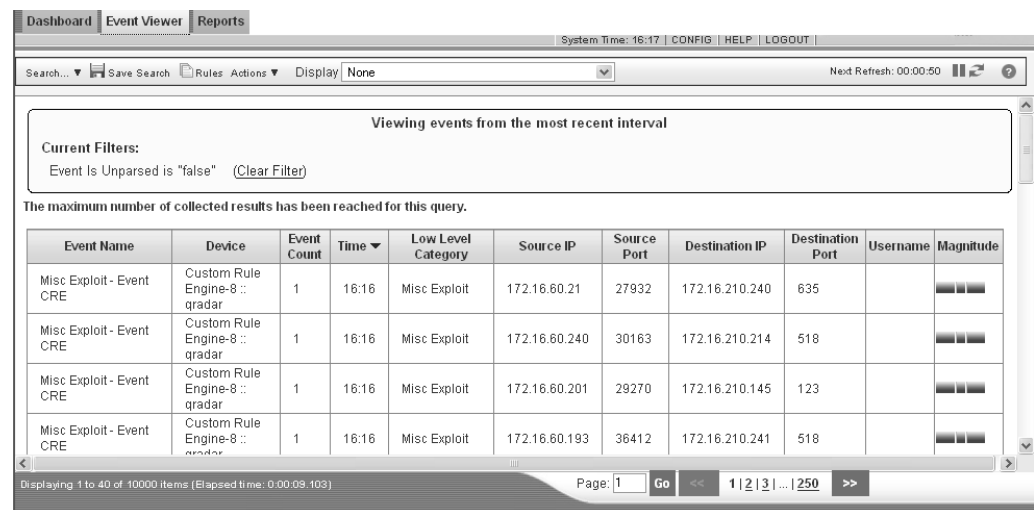
- [Viewing Normalized Events](#)
- [Viewing Raw Events](#)
- [Viewing Aggregate Normalized Events](#)

Viewing Normalized Events

To view normalized events:

Step 1 Click the **Event Viewer** tab.

The Event Viewer window appears.



Step 2 From the Display drop-down list box, select **None**.

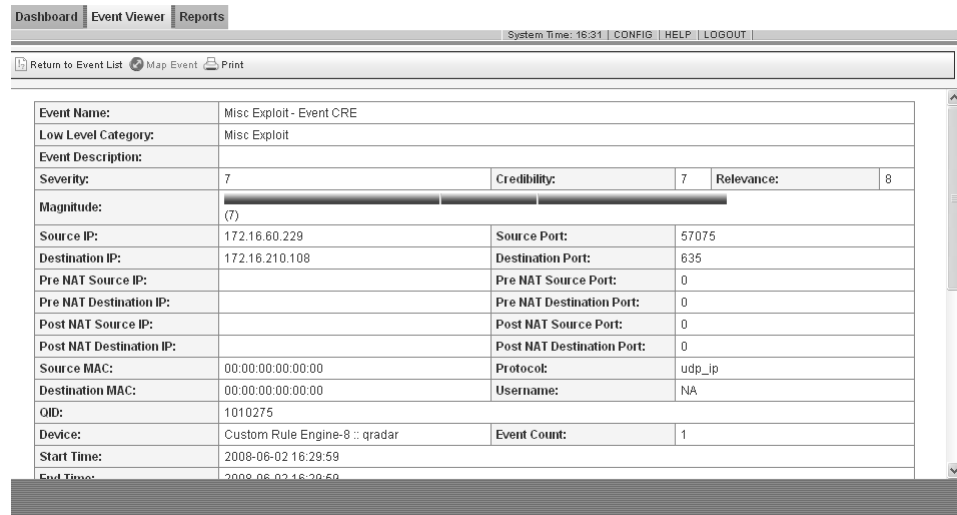
Table 3-2 Event Viewer

Parameter	Description
Current Filters	The top of the table displays the details of the filter applied to the search results. To clear these filter values, click Clear Filter .
Event Name	Specifies the normalized name of the event.
Device	Specifies the device that sent the event to STRM Log Management.

Table 3-2 Event Viewer (continued)

Parameter	Description
Event Count	Specifies the total number of bundled events that constitute this normalized event. Events are bundled when many of the same type of event for the same source and destination IP address are seen within a short period of time.
Time	Specifies the date and time that STRM Log Management received the event.
Low Level Category	Specifies the low-level category associated to this event. For more information on event categories, see the <i>Event Category Correlation Reference Guide</i> .
Source IP	Specifies the source IP address of the event.
Source Port	Specifies the source port of the event.
Destination IP	Specifies the destination IP address of the event.
Destination Port	Specifies the destination port of the event.
Username	Specifies the username associated with this event. Usernames are often available in authentication related events. For all other types of events where the username is not available, this field is empty.
Magnitude	Specifies the magnitude of this event. Variables include credibility, relevance, and severity. Point your mouse to the magnitude bar to display values and the calculated magnitude.

Step 3 Double-click the event you wish to view in greater detail.
 The event details window appears.



The details results provides the following information:

Table 3-3 Event Details




Parameter	Description
Event Name	Specifies the normalized name of the event.
Low Level Category	Specifies the low-level category of this event. For more information on categories, see the <i>Event Category Correlation Reference Guide</i> .
Event Description	Specifies a description of the event, if available.
Severity	Specifies the severity of this event.
Credibility	Specifies the credibility of this event.
Relevance	Specifies the relevance of this event.
Magnitude	Specifies the magnitude for this event.
Source IP	Specifies the source IP address of the event.
Source Port	Specifies the source port of this event.
Destination IP	Specifies the destination IP address of the event.
Destination Port	Specifies the destination port of this event.
Pre NAT Source IP	Network Address Translation (NAT) translates an IP address in one network to a different IP address in another network. For a firewall or another device capable of NAT, this parameter indicates the source IP address before the NAT values were applied.
Pre NAT Source Port	For a firewall or another device capable of NAT, this parameter indicates the source port before the NAT values were applied.
Pre NAT Destination IP	For a firewall or another device capable of NAT, this parameter indicates the destination IP address before the NAT values were applied.
Pre NAT Destination Port	For a firewall or another device capable of NAT, this parameter indicates the destination port before the NAT values were applied.
Post NAT Source IP	For a firewall or another device capable of NAT, this parameter indicates the source IP address after the NAT values were applied.
Post NAT Source Port	For a firewall or another device capable of NAT, this parameter indicates the source port after the NAT values were applied.
Post NAT Destination IP	For a firewall or another device capable of NAT, this parameter indicates the destination IP address after the NAT values were applied.
Post NAT Destination Port	For a firewall or another device capable of NAT, this parameter indicates the destination port after the NAT values were applied.
Protocol	Specifies the protocol associated with this event.
Username	Specifies the username associated with this event, if available.
QID	Specifies the STRM Log Management identifier for this event. Each event has a unique QID. For information on mapping a QID, see Modifying Event Mapping .

Table 3-3 Event Details (continued)

Parameter	Description
Device	Specifies the device that sent the event to STRM Log Management.
Event Count	Specifies the total number of bundled events that constitute this normalized event. Events are bundled when many of the same type of event for the same source and destination IP address are seen within a short period of time.
Start Time	Specifies the time of the first event, as reported to STRM Log Management by the device.
End Time	Specifies the end time of the last event, as reported to STRM Log Management by the device.
Device Time	Specifies the system time of the device.
Payload	Specifies payload content from the event. To view the payload in Hex, click Hex . To view the payload in UTF, click UTF . To view in Base64, click Base64 .
Matched Custom Rules	Specifies custom rules that have matched to this event. For more information on rules, see the <i>STRM Log Management Administration Guide</i> .
Annotations	Specifies the annotation or notes for this event.

The event details provides the following functions:

Table 3-4 Event Details Toolbar

Icon	Function
 Return to Event List	Allows you to return to the list of events.
 Map Event	Allows you to edit the event mapping. For more information, see Modifying Event Mapping .
 Print	Allows you to print the event details.

Viewing Raw Events To view raw event data:

- Step 1** Click the **Event Viewer** tab.
The Event Viewer window appears.
- Step 2** From the Display drop-down list box, select **Raw Events**.
Raw event data appears

Table 3-6 Aggregate Normalized Events (continued)

Aggregate Option	Description
High Level Category	Displays a summarized list of events grouped by the high-level category of the event. For more information on categories, see the <i>Event Category Correlation Reference Guide</i> .
Low Level Category	Displays a summarized list of events grouped by the low-level category of the event. For more information on categories, see the <i>Event Category Correlation Reference Guide</i> .
Magnitude	Displays a summarized list of events grouped by the magnitude for this event. The variables used to calculate magnitude include credibility, relevance, and severity.
Credibility	Credibility indicates the integrity of an event as determined by the credibility rating from source devices. Credibility increases as the multiple sources results grouped by the credibility of the event. This aggregate option displays a summarized list of events grouped by the credibility of the event.
Severity	Severity indicates the amount of threat an attacker poses in relation to how prepared the target is for the attack. This value is mapped to an event category that is correlated to the offense. This aggregate option displays a summarized list of events grouped by the severity of the event.
Relevance	Relevance indicates the significance of an event. This option displays a summarized list of events grouped by the relevance of the event.
Username	Displays a summarized list of events grouped by the username associated with the events.
Device	Displays a summarized list of events grouped by the devices that sent the event to STRM Log Management.
Device Type	Device Type indicates the type of device that originated the event. This aggregate option displays a summarized list of events grouped by device type.
Device Group	Displays a summarized list of events grouped by device group.
Network	Displays a summarized list of events grouped by the network associated with the event.
Src IP/ Dst IP / Dst Port/ User	Displays a summarized list of events grouped by the source IP address, destination IP address, destination port, and the user.
Src IP/ Dst IP / Dst Port/ Event Name	Displays a summarized list of events grouped by the source IP address, destination IP address, destination port, and the name of the event.
Src IP/ Event Name/ User	Displays a summarized list of events grouped by the source IP address, event name, and user.

Table 3-6 Aggregate Normalized Events (continued)

Aggregate Option	Description
Src IP/ Dst IP/ Event Name/ User	Displays a summarized list of events grouped by the source IP address, destination IP address, event name, and user.
Src IP/ Dst IP/ User	Displays a summarized list of events grouped by the source IP address, destination IP address , and the username associated with the event.
Src IP / Dst IP	Displays a summarized list of events grouped by traffic from the source IP address to destination IP address.
Dst IP/ Port	Displays a summarized list of events grouped by destination IP address and port.
Event Name/ Device	Displays a summarized list of events grouped by the event name and the device that sent the event to STRM Log Management.
Device/ High Level Cat	Displays a summarized list of events grouped by the device that sent the event to STRM Log Management and the high-level category. For more information on categories, see the <i>Event Category Correlation Reference Guide</i> .
Device/ High Level Cat./ Low Level Cat.	Displays a summarized list of events grouped by the device that sent the event to STRM Log Management and the high and low-level categories.
Matched Custom Rule	Displays a summarized list of events grouped by the associated custom rule.
Event Name/ Device Group	Displays a summarized list of events grouped by the event name and the device group.
Device Group/ High Level Cat	Displays a summarized list of events grouped by the device group and the high-level category. For more information on categories, see the <i>Event Category Correlation Reference Guide</i> .
Device Group/ High Level Cat/ Low Level Cat	Displays a summarized list of events grouped by the device group and the low-level category. For more information on categories, see the <i>Event Category Correlation Reference Guide</i> .
Src IP/ MAC	Displays a summarized list of events grouped by the source IP address and the source MAC address.
Src NAT/ Dst NAT	Network Address Translation (NAT) translates an IP address in one network to a different IP address in another network. The list of events that appears includes a summarized list of events grouped by the source and destination information (IP address and port) before and after NAT was applied.
Src IP/ High Level Cat	Displays a summarized list of events grouped by the source IP address and the high-level category. The aggregate results provides a list of source IP addresses. For more information on categories, see the <i>Event Category Correlation Reference Guide</i> .

Table 3-6 Aggregate Normalized Events (continued)

Aggregate Option	Description
Src IP/ Low Level Cat	Displays a summarized list of events grouped by the source IP address and the low-level category. For more information on categories, see the <i>Event Category Correlation Reference Guide</i> .
Dst IP/ High Level Cat	Displays a summarized list of events grouped by the destination IP address and the high-level category. For more information on categories, see the <i>Event Category Correlation Reference Guide</i> .
Dst IP/ Low Level Cat	Displays a summarized list of events grouped by the destination IP address and the low-level category. For more information on categories, see the <i>Event Category Correlation Reference Guide</i> .
Src IP / Dst IP/ High Level Cat	Displays a summarized list of events grouped by the source IP address to destination IP addresses and the high-level category. For more information on categories, see the <i>Event Category Correlation Reference Guide</i> .
Src IP / Dst IP/ Low Level Cat	Displays a summarized list of events grouped by the source IP address to destination IP addresses and the low-level category. For more information on categories, see the <i>Event Category Correlation Reference Guide</i> .

To view aggregate normalized events:

Step 1 Click the **Event Viewer** tab.

The Event Viewer window appears.

Step 2 From the Display drop-down list box, select the desired option. For more information, see [Table 3-6 Aggregate Normalized Events](#).

The event information appears.



Note: The column layout of the data depends on the chosen display option.

Dashboard | Event Viewer | Reports

System Time: 16:35 | CONFIG | HELP | LOGOUT

Search... Save Search Rules Actions Display Destination IP Next Refresh: 00:00:50

Viewing events from the most recent interval

Current Filters:
Event Is Unparsed is "false" (Clear Filter)

Destination IP	Count
205.174.165.41	815
172.16.60.18	539
172.16.60.83	538
172.16.60.14	538
172.16.60.99	536
172.16.60.115	536
172.16.10.52	534
172.16.10.39	532
10.100.100.19	483
172.16.60.249	379

(Hide Chart)

Destination IP	Source IP	Destination Port	Event Name	Device	Low Level Category	Protocol	Username	Max. Magnitude	Count
205.174.165.41	Multiple (40)	Multiple (7)	Multiple (4)	Multiple (2)	Multiple (4)	Multiple (3)		8	815
172.16.60.18	Multiple (256)	Multiple (2)	Multiple (3)	Multiple (2)	Multiple (3)	Multiple (2)		5	539
172.16.60.83	Multiple (256)	Multiple (2)	Multiple (2)	Snort @ wolverine	Multiple (2)	Multiple (2)		5	538
172.16.60.14	Multiple (256)	Multiple (2)	Multiple (2)	Snort @ wolverine	Multiple (2)	Multiple (2)		5	538

Displaying 1 to 40 of 2474 items (Elapsed time: 0:00:11.170) Page: 1 Go << 1 | 2 | 3 | ... | 62 >>

The events window results provides the following information:

Table 3-7 Event Name Parameters

Parameter	Description
Current Filters	The top of the table displays the details of the filter applied to the search results. To clear these filter values, click Clear Filter .
Graphs	Displays a bar chart representing the top 10 aggregates, depending on the chosen aggregate option. Click Hide Chart if you wish to remove the graph from your display.
Legend Reference	A colored box in this field associated this event to the graph.
Event Name	Specifies the normalized name of the event.
Source IP	Specifies the source IP address associated with this event. If there are multiple IP addresses associated with this event, this field indicates Multiple and the number.
Destination IP	Specifies the destination IP address associated with this event. If there are multiple IP addresses associated with this event, this field indicates Multiple and the number.
Destination Port	Specifies the destination ports associated with this event. If there are multiple ports associated with this event, this field indicates Multiple and the number.
Device	Specifies the device that sent the event to STRM Log Management. If there are multiple devices associated with this event, this field indicates Multiple and the number.

Table 3-7 Event Name Parameters (continued)

Parameter	Description
Category	Specifies the low-level category of this event. If there are multiple categories associated with this event, this field indicates Multiple and the number. For more information on categories, see the <i>Event Category Correlation Reference Guide</i> .
Protocol	Specifies the protocol ID associated with this event.
Username	Specifies the username associated with this event, if available.
Max Magnitude	Specifies the maximum calculated magnitude for all summarized events. Variables used to calculate magnitude include credibility, relevance, and severity.
Count	Specifies the total number of bundled events that constitute this normalized event. Events are bundled when many of the same type of event for the same source and destination IP address are seen within a short period of time.

Using the Search

The Event Viewer allows you to search for a specific event or a set of events. You can also save event search criteria for future use. This section provides information on searching events including:

- [Searching Events](#)
- [Deleting Saved Searches](#)

Searching Events

To search events:

Step 1 Click the **Event Viewer** tab.

The Event Viewer window appears.

Step 2 Choose one of the following options:

- If you have previously saved search criteria you wish to use for this search, select **Search > Quick Searches** from the drop-down list box.
- If you wish to start a new search, select **Search > Edit Search** from the drop-down list box.

The search window appears.

The screenshot displays the search configuration interface for the Event Viewer. It is organized into several sections:

- Saved Searches:** Features a dropdown menu labeled "Choose a search..." and a "Delete" button. Below are two checkboxes: "Include in my Quick Searches" and "Share with everyone".
- Time Range:** Contains three radio buttons: "Real Time (auto refresh)" (selected), "Recent" (with a "Last Minutes" dropdown), and "Specific Interval". The "Specific Interval" section includes "Start Time" and "End Time" fields, each with a date-time picker.
- Tests and Filters:** Shows a filter rule: "Any IP" (dropdown) "Equals" (dropdown) "[]" (text input). An "Add Filter" button is present. Below, the "Current Filters:" section lists "Event Is Unparsed is false". A "Remove Selected Filters" button is at the bottom.
- Search Parameters:** Includes a "Sort" dropdown, a "by" dropdown (set to "Start Time"), and "Search Order" radio buttons for "Descending" (selected) and "Ascending".

A "Filter" button is located at the bottom right of the interface.

Step 3 Enter values for the desired filter criteria:

Table 3-8 Event Search Criteria

Parameter	Description
Saved Searches	<p>Using the drop-down list box, select a previously saved search you wish to apply to this search, if desired.</p> <p>Other options include:</p> <ul style="list-style-type: none"> • Delete - Using the drop-down list box, select the search you wish to delete. Click Delete. • Include in my Quick Searches - Select the check box if you wish to include this search in your Quick Search items, which is available in the Search drop-down list box. • Share with Everyone - Select the check box if you wish to share the saved search with all other STRM Log Management users.
Time Range	<p>Choose one of the following options:</p> <ul style="list-style-type: none"> • Real Time - Select this option if you wish to filter on events while in auto-refresh mode. • Recent - Select the option and, using the drop-down list box, specify the time range you wish to filter. • Specific Interval - Select the option and, using the calendar, specify the date and time range you wish to filter.
Test and Filters	
Add Filter Options	<p>Using the options, define your specific search criteria including:</p> <ul style="list-style-type: none"> • From the first drop-down list box, select an attribute you wish to search. For example, Any IP, Source Port, or Protocol. • From the second drop-down list box, select the modifier you wish to use for the search. The list of modifiers that appear depends on the attribute selected in the first list. • In the text field, enter specific information related to your search. <p>For example, if you select Destination IP from the first drop-down list box, Equals from the second drop-down list box, and enter 10.100.10.100 for the destination IP address you wish to search, the search results returns results for this criteria.</p> <p>For each criteria you wish to add to the filter, enter the desired values and click Add Filter to add the filter to the Current Filter list. Repeat for all filters you wish to add to the search criteria.</p>
Current Filters	Lists current search criteria filters. To remove any listed filter, select the filter and click Remove Selected Filters .
Search Parameters	
Sort/Aggregate	Using the drop-down list box, specify whether you wish to sort your search results by criteria specified in the By drop-down list box or view your search results using an Aggregate value.
By	Using the drop-down list box, select additional event criteria you wish to use when searching

Table 3-8 Event Search Criteria (continued)

Parameter	Description
Search Order	Specify the order you wish to display for the search results. The options are: Descending or Ascending.

Step 4 Click **Filter**.

If you selected a **sort** criteria in your Search Parameters, the normalized events appear. For more information on your search results, see [Viewing Normalized Events](#).

If you selected an **aggregate** value in your Search Parameters, the aggregate events appear. For more information on your search results, see [Viewing Aggregate Normalized Events](#).

The results appear. If the number of returned events exceeds the value configured in the Web Max Matched Results parameter in the System Settings window (for more information, see the *STRM Log Management Administration Guide*), a message appears indicating that only the maximum search results are provided.

Step 5 To save the specified search criteria for future use:**a** Click **Save Search**.

The Save Search window appears.

b Enter values for the parameters:**Table 3-9** Save Search Parameters

Parameter	Description
Search Name	Specify a name you wish to assign to this search criteria.
Time Range	Choose one of the following options: <ul style="list-style-type: none"> Real Time - Select this option if you wish to filter on events while in auto-refresh mode. Recent - Select the option and, using the drop-down list box, specify the time range you wish to filter. Specific Interval - Select the option and, using the calendar, specify the date and time range you wish to filter.

Table 3-9 Save Search Parameters

Parameter	Description
Include in my Quick Searches	Select the check box if you wish to include this search in your Quick Search items, which is available in the Search drop-down list box.
Share with Everyone	Select the check box if you wish to share these search requirements with all other STRM Log Management users.

c Click **OK**.

Deleting Saved Searches

To delete previously saved searches:

- Step 1** Click the **Event Viewer** tab.
The Event Viewer window appears.
- Step 2** From the Search drop-down list box, select **Edit Search**.
The filter/search window appears.
- Step 3** In the Saved Searches drop-down list box, select the search you wish to delete.
- Step 4** Click **Delete**.

Modifying Event Mapping

STRM automatically maps an event of a Device Support Module (DSM), also known as a sensor device, for normalization purposes. Using the event mapping tool, you can associate or map a normalized or raw event to a high-level and low-level category (or QID). This allows STRM Log Management to map unknown device events to known STRM events so that they can be categorized and correlated appropriately.

STRM Log Management may receive events from DSMs that the system is unable to categorize. STRM Log Management categorizes these types of events as unknown. These events may occur for several reasons including:

- **User-defined Events** - Some DSMs, such as SNORT, allow you to create user-defined events.
- **New Events or Older Events** - Third party devices may update their software with maintenance releases to support new events that STRM may not support.

To modify event mapping:

Step 1 Click the **Event Viewer** tab.

The Event Viewer window appears.

Step 2 For any normalized event, double-click the event you wish to map.

For more information on viewing normalized events, see [Viewing Normalized Events](#). For information on viewing raw events, see [Viewing Raw Events](#).

Step 3 Click **Map Event**.

The Device Event window appears.

Device Event

Note: Changes to Device Event Maps may take up to 30 minutes to be reflected in the Offense Manager

Device Type Contivity
Device Event Category Session
Device Event ID Session Opened

If you know the QID to associate this event to, enter it here

Enter QID

Or browse for the desired QID below

Browse for QID

High-Level Category
Low-Level Category

QIDs

QID	Name	Severity
1114669	RDP_Login	1
1114673	SQL_Login	1
1114682	System_Successful_Login	1
1134308	Guest_user_login	1
1137898	Logon_process_registered	1
1138533	Mapped_account	1
1143544	Rlogin_Trusted_Login	1
1144664	Successful_Network_Login	1

OK Cancel

Step 4 Choose one of the following options:

- a If you know the QID that you wish to map to this event, enter the desired QID in the Enter QID field. Go to [Step 6](#).
- b If you wish to search for a particular QID, go to [Step 5](#).

Step 5 To search for a particular QID or high and low-level categories that you wish to map this event to:

- a In the High-Level Category drop-down list box, specify the high-level category you wish to apply to this event.
- b In the Low-Level Category drop-down list box, specify the low-level category you wish to apply to this event.

A list of QIDs appears.

- c From the QID list, select the QID you wish to assign to this normalized event.

Step 6 Click **Ok**.

Exporting Events

You can export events in Extensible Markup Language (XML) or Comma Separated Values (CSV).

To export events:

Step 1 Click the **Event Viewer** tab.

The Event Viewer window appears.

Step 2 Choose one of the following:

- a If you wish to export the event(s) in XML format, select **Export to XML** from the Actions drop-down list box.
- b If you wish to export the event(s) in CSV format, select **Export to CSV** from the Actions drop-down list box

The status window appears. When the export is complete, the window disappears or click **Notify When Done** to resume your activities and receive a notification when the export is complete.

4

CONFIGURING RULES

An event is an incident that is detected by your security devices in your enterprise. You can create an event rule to events by performing a series of tests. If all the conditions of a test are true, the rule generate a response. Building blocks are rules without a response. Responses to a rule include:

- Generation of an event
- Generation of a response to an external system (syslog, SNMP)
- Send an e-mail

The tests in each rule can also reference other building blocks and rules. You do not need to create rules in any specific order since the system will check for dependencies each time a new rule is added, edited, or deleted. If a rule that is referenced by another rule is deleted or disabled, a warning appears and action is not taken.

Each rule may contain the following components:

- **Functions** - With functions, you can use building blocks and other rules to create a multi-event function. You can also OR rules together, using the *when we see an event match any of the following rules* function.
- **Building blocks** - A building block is a rule without a response and is commonly used as a common variable in multiple rules or used to build complex rules or logic that you wish to use in other rules. You can save a group of tests as building blocks for use with other functions. Building blocks allow you to re-use specific rule tests in other rules. For example, you can save a building block that includes the IP addresses of all mail servers in your network and then use that building block to exclude those hosts from another rule. The building block defaults are provided as guidelines, which should be reviewed and edited based on the needs of your network.
- **Tests** - Property of an event, such as, source IP address, severity of event, or rate analysis.

A user with non-administrative access can create rules for areas of the network that they have access. You must have the appropriate role access to manage rules.

This chapter includes:

- [Viewing Rules](#)
- [Enabling/Disabling Rules](#)
- [Creating a Rule](#)
- [Copying a Rule](#)
- [Deleting a Rule](#)
- [Grouping Rules](#)
- [Editing Building Blocks](#)

Viewing Rules

To view deployed rules, rule type, and status:

Step 1 Select the **Event Viewer** tab.

The Event Viewer window appears.

Step 2 Click **Rules**.

The Rules List window appears.

Rule Name /	Group	Rule Type	Enabled	Response
Default-Rule-Anomaly: Devices with High Event Rates	Anomaly	EVENT	false	Dispatch New Event
Default-Rule-Anomaly: Excessive Database Connections	Anomaly	EVENT	true	Dispatch New Event
Default-Rule-Anomaly: Excessive Firewall Accepts Across Multiple Hosts	Anomaly	EVENT	true	Dispatch New Event
Default-Rule-Anomaly: Excessive Firewall Denies from Single Source	Anomaly	EVENT	true	Dispatch New Event
Default-Rule-Anomaly: Rate Analysis Marked Events	Anomaly	EVENT	true	Dispatch New Event
Default-Rule-Authentication: Login Failure to Disabled Account	Authenticator	EVENT	true	Dispatch New Event
Default-Rule-Authentication: Login Failure to Expired Account	Authenticator	EVENT	true	Dispatch New Event
Default-Rule-Authentication: Login Failures Across Multiple Hosts	Authenticator	EVENT	true	Dispatch New Event
Default-Rule-Authentication: Login Failures Followed By Success	Authenticator	EVENT	true	Dispatch New Event
Default-Rule-Authentication: Multiple VoIP Login Failures	Authenticator	EVENT	true	Dispatch New Event
Default-Rule-Authentication: Repeated Login Failures, Single Host	Authenticator	EVENT	true	Dispatch New Event
Default-Rule-Compliance: Excessive Failed Logins to Compliance IS	Compliance	EVENT	false	Dispatch New Event

Rule

Notes

Step 3 In the Display drop-down list box, select **Rules**.

The list of deployed rules appear. For more information on default rules and building blocks, see [Appendix A Default Rules and Building Blocks](#).

Step 4 Select the rule you wish to view.

In the Rule and Notes fields, descriptive information appears.

Enabling/Disabling Rules

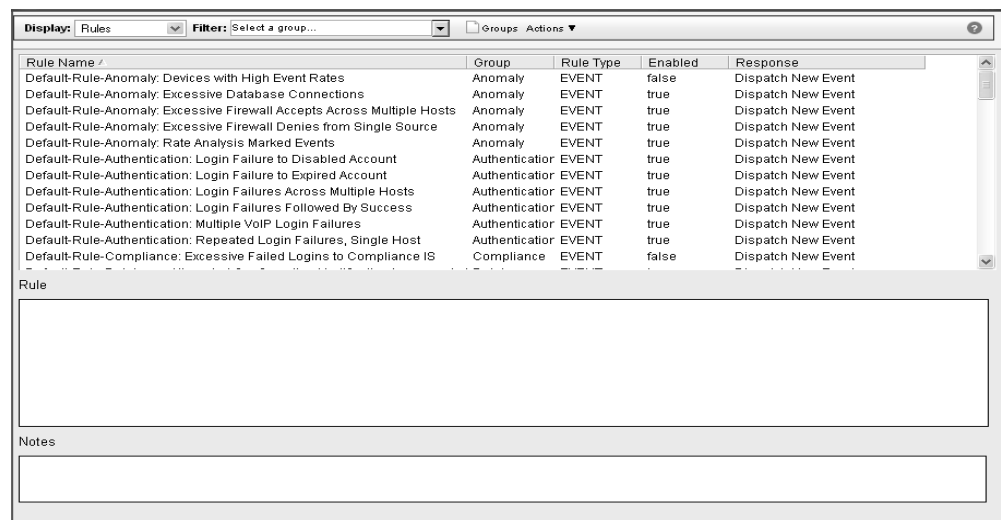
To enable or disable a rule:

- Step 1** Select the **Event Viewer** tab.
The Event Viewer window appears.
- Step 2** Click **Rules**.
The Rules List window appears.
- Step 3** In the Display drop-down list box, select **Rules**.
The list of deployed rules appear.
- Step 4** Select the rule you wish to enable or disable.
- Step 5** From the Actions drop-down list box, select **Enable/Disable**.
The Enable column indicates the status.

Creating a Rule


To create a new rule:

- Step 1** Select the **Event Viewer** tab.
The Event Viewer window appears.
- Step 2** Click **Rules**.
The Rules List window appears.

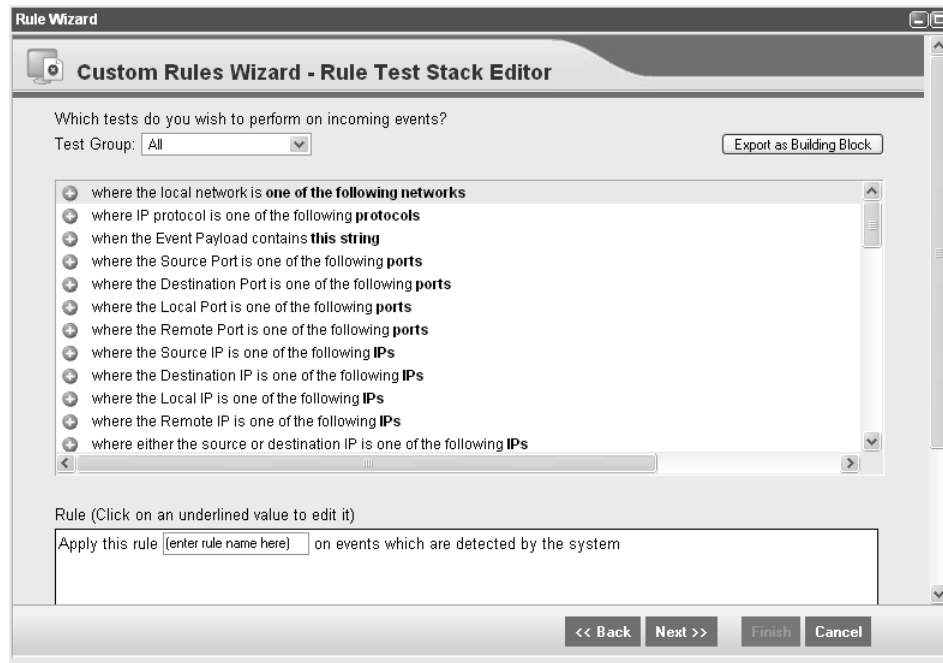


- Step 3** From the Actions drop-down list box, select **New Event Rule**.
The Custom Rule wizard appears.



 **Note:** If you do not wish to view the Welcome to the Custom Rules Wizard window again, select the Skip this page when running the rules wizard check box.

Step 4 Read the introductory text. Click **Next**.
The Rules Test Stack Editor window appears.



Step 5 To add a test to a rule:

- a In the Test Group drop-down list box, select the type of test you wish to apply to this rule.

The resulting list of tests appear. For information on tests, see [Event Rule Tests](#).

- b For each test you wish to add to the rule, select the + sign beside the test.

The selected test(s) appear in the Rule field.

- c For each test added to the Rule field that you wish to identify as an excluded test, click **and** at the beginning of the test.

The **and** appears as **and not**.

- d For each test added to the Rule field, you must customize the variables of the test. Click the underlined configurable parameter to configure. See [Event Rule Tests](#).

- e Repeat for all tests you wish to apply to this rule.

Step 6 In the **enter rule name here** field, enter a name you wish to assign to this rule.

Step 7 To export the configured tests as building blocks to use with other rules:

- a Click **Export as Building Block**.

The Save Building Block window appears.

Save Building Block

Saving your rule as a building block will allow you to re-use its logic when constructing rules in the future.

Building Block Name:
(i.e. 'My Important IPs', 'High attacker count on mail server')

Save Cancel

- b Enter the name you wish to assign to this building block.

- c Click **Save**.

Step 8 To assign multi-event functions to the rule, select **Functions** from the Test Group drop-down list box and configure the function:

The functions include:

Table 4-1 Functions Group

Test	Description	Default Test Name	Parameters
Multi-Rule Event Function	Allows you to use saved building blocks and other rules to populate this test. The event has to match either all or any of the selected rules. If you wish to create an OR statement for this rule test, specify the any parameter.	when an event matches any of the following rules	Configure the following parameters: <ul style="list-style-type: none"> • any - Specify either any or all of the configured rules apply to this test. • rules - Specify the rules you wish this test to consider.
Multi-Rule Event Function	Allows you to use saved building blocks or other rules to populate this test. This function allows you to detect a specific sequence of selected rules involving a source and destination within a configured time period.	when all of these rules, in order, from the same IP address/Port/QID/Event/Device/Category {default: source IP} to the same destination IP, over this many time intervals	Configure the following parameters: <ul style="list-style-type: none"> • these rules - Specify the rules you wish this test to consider. • in - Specify whether you wish this rule to consider in or in any order. • the same - Specify if you wish this rule to consider the same or any of the source to destination port or IP address. • IP address/Port/QID/Event/Device/Category - Specify whether you wish this rule to consider a source IP address, source port, QID, device event ID, device, or category. • the same - Specify if you wish this rule to consider the same or any of the source to destination port or IP address. • destination IP - Specify whether you wish this rule to consider a destination IP or port. • this many - Specify the number of time intervals you wish this rule to consider. • time intervals - Specify the time interval you wish this rule to consider. The options are: seconds, minutes, hours, or days.

Table 4-1 Functions Group (continued)

Test	Description	Default Test Name	Parameters
Multi-Rule Event Function	Allows you to use saved building blocks or other rules to populate this test. You can use this function to detect a number of specified rules, in sequence, involving a source and destination within a configured time interval.	when at least this number of these rules, in order, from the same IP address/Port/QID/Event/Device/Category {default: source IP} to the same destination IP, over this many time intervals	<p>Configure the following parameters:</p> <ul style="list-style-type: none"> • this number - Specify the number of rules you wish this function to consider. • these rules - Specify the rules you wish this test to consider. • in - Specify whether you wish this rule to consider in or in any order. • the same - Specify if you wish this rule to consider the same or any of the source to destination port or IP address. • IP address/Port/QID/Event/Device/Category - Specify whether you wish this rule to consider a source IP address, source port, QID, device event ID, device, or category, • the same - Specify if you wish this rule to consider the same or any of the source to destination port or IP address. • destination IP - Specify whether you wish this rule to consider a destination IP or port. • this many - Specify the number of time intervals you wish this rule to consider. • time intervals - Specify the time interval you wish this rule to consider. The options are: seconds, minutes, hours, or days.
Multi-Event Sequence Function Between Hosts	Allows you to detect a sequence of selected rules involving the same source and destination hosts within the configured time intervals. You can also use saved building blocks and other rules to populate this test.	when this sequence of rules, involving the same source and destination hosts in this many time intervals	<p>Configure the following parameters:</p> <ul style="list-style-type: none"> • of rules - Specify the rules you wish this test to consider • this many - Specify the number of time intervals you wish this test to consider. • time intervals - Specify the time measurement value, seconds, minutes, hours, or days you wish to apply to this test.

Table 4-1 Functions Group (continued)

Test	Description	Default Test Name	Parameters
Multi-Event Counter Function	Allows you to test the number of events from configured conditions, such as, source IP address. You can also use building blocks and other rules to populate this test.	when a(n) IP address/Port/QID/Event/Device/Category {default: anything} emitting/receiving more than 5 {default} of these rules across more than 5 {default} IP address /Port /QID/ Event/Device/ Category {default: destination IP} , over 10 {default} minutes	Configure the following parameters: <ul style="list-style-type: none"> • IP address/ Port/QID/Event/ Device/Category - Specify the source you wish this test to consider. The options are: anything, a source IP, a source Port, a QID, Device Event ID, or a Device. • more than - Specify if you wish this test to consider more than or exactly the number of rules. • 5 - Specify the number of rules you wish this test to consider. • these rules - Specify the rules you wish this test to consider. • more than - Specify if you wish this test to consider more than or exactly the number of destination IP address(es), destination port(s), QID(s), Device Event ID(s), or Device(s). • 5 - Specify the number of IP addresses, ports, QIDs, events, devices, or categories you wish this test to consider. • IP address /Port /QID/ Event/Device/ Category - Specify the destination you wish this test to consider. The options are: anything, destination IP(s), destination port(s), QID(s), device event ID(s), or device(s). • 10 - Specify the time value you wish to assign to this test. • minutes - Specify the time measurement value, seconds, minutes, hours, or days that you wish to apply to this test.

Table 4-1 Functions Group (continued)

Test	Description	Default Test Name	Parameters
Multi-Rule Function	You can also use building blocks or existing rules to populate this test. Allows you to detect a series of rules for a specific IP address or port followed by a series of specific rules for a specific port or IP address.	when all of these rules, in order, with the same destination IP address/port followed by all of these rules in order with the same IP address/port from the previous source , within this many time intervals	<p>Configure the following parameters:</p> <ul style="list-style-type: none"> • rules - Specify the rules you wish this test to consider. • in - Specify if you wish this test to consider rules in a specific order. • destination - Specify whether you wish this test to consider destination or source IP address or port. • IP address/Port - Specify if you wish this test to consider the IP address or port. • rules - Specify the rules you wish this test to consider. • in - Specify if you wish this test to consider rules in a specific order. • IP address/port - Specify if you wish this test to consider the IP address or port. • this many - Specify the number of time intervals you wish this rule to consider. • time intervals - Specify the time interval you wish this rule to consider. The options are: seconds, minutes, hours, or days.

Table 4-1 Functions Group (continued)

Test	Description	Default Test Name	Parameters
Multi-Rule Function	You can also use building blocks or existing rules to populate this test. Allows you to detect a number of specific rules for a specific IP address or port followed by a number of specific rules for a specific port or IP address.	when at least this number of these rules, in order, with the same destination IP address/port followed by at least this number of these rules in order with the same IP address/port from the previous source , within this many time intervals	<p>Configure the following parameters:</p> <ul style="list-style-type: none"> • this number - Specify the number of rules you wish this test to consider. • rules - Specify the rules you wish this test to consider. • in - Specify if you wish this test to consider rules in a specific order. • destination - Specify whether you wish this test to consider destination or source IP address or port. • IP address/port - Specify if you wish this test to consider the IP address or port. • this number - Specify the number of rules you wish this test to consider. • rules - Specify the rules you wish this test to consider. • in - Specify if you wish this test to consider rules in a specific order. • IP address/port - Specify if you wish this test to consider the IP address or port. • source - Specify if you wish this test to consider source or destination. • this many - Specify the number of time intervals you wish this rule to consider. • time intervals - Specify the time interval you wish this rule to consider. The options are: seconds, minutes, hours, or days.

Table 4-1 Functions Group (continued)

Test	Description	Default Test Name	Parameters
Multi-Rule Function	You can also use building blocks or existing rules to populate this test. Allows you to detect the selected rules with same source information across more than the configured number of destinations within a configured time period.	when any of these rules with the same IP address/Port/QID/Event/Device/Category more than 5 times, across more than 5 IP address/Port/QID/Event/Device/Category within 10 minutes	<p>Configure the following parameters:</p> <ul style="list-style-type: none"> • rules - Specify the rules you wish this test to consider. • IP address/Port/QID/Event/Device/Category - Specify whether you wish this rule to consider a source IP address, source port, QID, device event ID, device, or category. • 5 - Specify the number of rules you wish this test to consider. • more than - Specify if you wish this test to consider more than or exactly the number of destination IP address(es), destination port(s), QID(s), Device Event ID(s), or Device(s). • 5 - Specify the number of IP addresses, ports, QIDs, events, devices, or categories you wish this test to consider. • IP address/Port/QID/Event/Device/Category - Specify the destination you wish this test to consider. The options are: anything, destination IP(s), destination port(s), QID(s), Device Event ID(s), or Device(s). • 10 - Specify the time value you wish to assign to this test. • minutes - Specify the time measurement value, seconds, minutes, hours, or days that you wish to apply to this test.

Step 9 In the groups area, select the check box(es) of the groups to which you wish to assign this rule. For more information on grouping rules, see [Grouping Rules](#).

Step 10 In the Notes field, enter any notes you wish to include for this rule. Click **Next**.
The Rule Responses window appears, which allows you to configure the action STRM Log Management takes when the event sequence is detected.

Step 11 Configure the following parameters:

Table 4-2 Event Rule Response Parameters

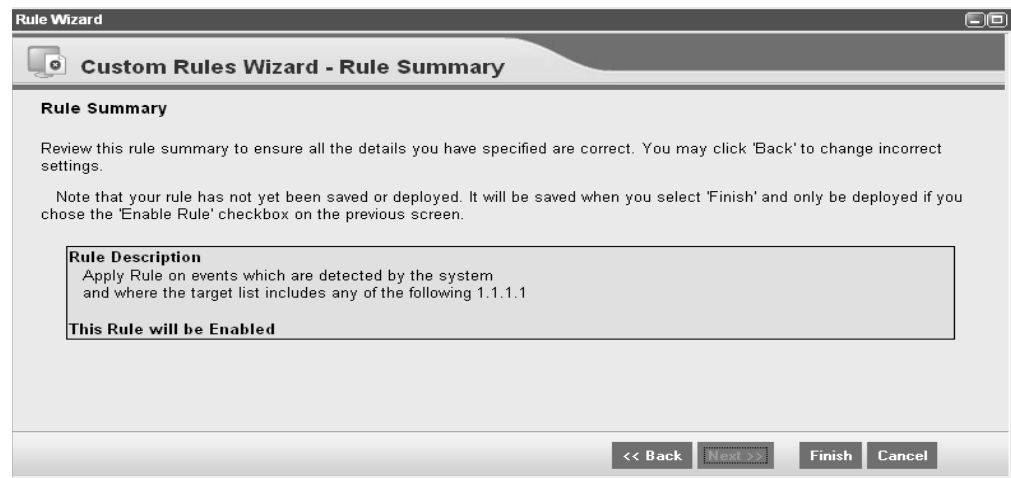
Parameter	Description
Severity	Select the check box if you wish this rule to set or adjust severity to the configured level. Once selected, you can configure the desired level.
Credibility	Select the check box if you wish this rule to set or adjust credibility to the configured level. Once selected, you can configure the desired level.
Relevance	Select the check box if you wish this rule to set or adjust relevance to the configured level. Once selected, you can configure the desired level.
Dispatch New Event	Select the check box to dispatch a new event in addition to the original event, which will be processed like all other events in the system. The Dispatch New Event parameters appear when you select the check box. By default, the check box is clear.
Event Name	Specify the name of the event you wish to display in the Event Viewer.
Event Description	Specify a description for the event. The description appears in the Annotations of the event details.
Severity	Specify the severity for the event. The range is 1 (lowest) to 10 (highest) and the default is 1. The Severity appears in the Annotation of the event details.
Credibility	Specify the credibility of the event. The range is 1 (lowest) to 10 (highest) and the default is 10. Credibility appears in the Annotation of the event details.
Relevance	Specify the relevance of the event. The range is 1 (lowest) to 10 (highest) and the default is 1. Relevance appears in the Annotation of the event details.
High-Level Category	Specify the high-level event category you wish this rule to use when processing events. For more information on event categories, see the <i>Event Category Correlation Reference Guide</i> .
Low-Level Category	Specify the low-level event category you wish this rule to use when processing events. For more information on event categories, see the <i>Event Category Correlation Reference Guide</i> .
Email	Select the check box to display the email options. By default, the check box is clear.
Enter e-mail address to notify	Specify the e-mail address(es) to send notification if the event generates. Separate multiple e-mail addresses using a comma.

Table 4-2 Event Rule Response Parameters (continued)

Parameter	Description
Send to SysLog	Select the check box if you wish to log the event. By default, the check box is clear. For example, the syslog output may resemble: <code>Sep 28 12:39:01 localhost.localdomain ECS: Rule 'Name of Rule' Fired: 172.16.60.219:12642 -> 172.16.210.126:6666 6, Event Name: SCAN SYN FIN, QID: 1000398, Category: 1011, Notes: Event description</code>
Response Limiter	Specify the frequency you wish this rule to respond.
Enable Rule	Select the check box to enable this rule. By default, the check box is selected.

Step 12 Click **Next**.

The Rule Summary window appears.

**Step 13** Review the configured rule. Click **Finish**.

Event Rule Tests This section provides information on the tests you can apply to the rules including:

- [Event Property Tests](#)
- [IP/Port Tests](#)
- [Date/Time Tests](#)
- [Device Tests](#)

Event Property Tests

The event property test group includes:

Table 4-3 Event Property Tests

Test	Description	Default Test Name	Parameters
Local Network Object	Valid when the event occurs in the specified network.	when the local network is one of the following networks	one of the following - Specify the areas of the network you wish this test to apply.
IP Protocol	Valid when the IP protocol of the event is one of the configured protocols.	when the IP protocol is one of the following protocols	protocols - Specify the protocols you wish to add to this test.
Event Payload Search	Each event contains a copy of the original unnormalized event. This test is valid when the entered search string is included anywhere in the event payload.	when the Event Payload contains this string	this string - Specify the text string you wish include for this test.
QID of Event	A QID is a unique identifier for events. This test is valid when the event identifier is a configured QID.	when the event QID is one of the following QIDs	<p>QIDs - Use of the following options to locate QIDs:</p> <ul style="list-style-type: none"> • Select the Browse By Category option and using the drop-down list boxes, select the high and low-level category QIDs you wish to locate. • Select the QID Search option and enter the QID or name you wish to locate. Click Search.
Attack Context	<p>Attack Context is the relationship between the attacker and target. For example, a local attacker to a remote target.</p> <p>Valid if the attack context is one of the following:</p> <ul style="list-style-type: none"> • Local to Local • Local to Remote • Remote to Local • Remote to Remote 	when the attack context is this context	<p>this context - Specify the context you wish this test to consider. The options are:</p> <ul style="list-style-type: none"> • Local to Local • Local to Remote • Remote to Local • Remote to Remote
Event Category	Valid when the event category is the same as the configured category, for example, Denial of Service (DoS) attack.	when the event category for the event is one of the following categories	<p>categories - Specify the event category you wish this test to consider.</p> <p>For more information on event categories, see the <i>Event Category Correlation Reference Guide</i>.</p>
Severity	Valid when the event severity is greater than, less than, or equal to the configured value. The default is 5.	when the event severity is greater than 5 {default}	<p>Configure the following parameters:</p> <ul style="list-style-type: none"> • greater than - Specify whether the severity is greater than, less than, or equal to the configured value. • this value - Specify the index, which is a value from 0 to 10.

Table 4-3 Event Property Tests (continued)

Test	Description	Default Test Name	Parameters
Credibility	Valid when the event credibility is greater than, less than, or equal to the configured value. The default is 5.	when the event credibility is greater than 5 {default}	Configure the following parameters: <ul style="list-style-type: none"> • greater than - Specify whether the credibility is greater than, less than, or equal to the configured value. • this value - Specify the index, which is a value from 0 to 10.
Relevance	Valid when the event relevance is greater than, less than, or equal to the configured value. The default is 5.	when the event relevance is greater than 5 {default}	Configure the following parameters: <ul style="list-style-type: none"> • greater than - Specify whether the relevance is greater than, less than, or equal to the configured value. • this value - Specify the index, which is a value from 0 to 10.
Source Location	Valid when the source IP address of the event is either local or remote.	when the source is local or remote {default: remote}	local or remote - Specify either local or remote traffic.
Destination Location	Valid when the destination IP address of the event is either local or remote.	when the destination is local or remote {default: remote}	local or remote - Specify either local or remote traffic.
Geographic	Valid when the source of this event is located in the configured geographic region.	when the attacker is located in this geographic location	this geographic location - Specify the geographic regions you wish this test to consider.
Rate Analysis	STRM Log Management monitors event rates of all source IP addresses/QIDs and destination IP addresses/QIDs and marks events that exhibit abnormal rate behavior. Valid when the event has been marked for rate analysis.	when the event has been marked with rate analysis	

Table 4-3 Event Property Tests (continued)

Test	Description	Default Test Name	Parameters
False Positive Tuning	When you tune false positive events in the Event Viewer, the resulting tuning values appear in this test. If you wish to remove a false positive tuning, you can edit this test to remove the necessary tuning values.	when the false positive signature matches one of the following signatures	<p>signatures - Specify the false positive signature you wish this test to consider. Enter the signature in the following format:</p> <p><CAT QID ANY>:<value>:<source IP>:<dest IP></p> <p>Where:</p> <p><CAT QID ANY> - Specify whether you wish this false positive signature to consider a category (CAT), Q1 Labs Identifier (QID), or any value.</p> <p><value> - Specify the value for the <CAT QID ANY> parameter. For example, if you specified QID, you must specify the QID value.</p> <p><source IP> - Specify the source IP address you wish this false positive signature to consider.</p> <p><dest IP> - Specify the destination IP address you wish this false positive signature to consider.</p>
Username	Valid when the configured username is associated with an event.	when the event(s) username is this string	<p>Configure the following parameters:</p> <ul style="list-style-type: none"> is - Specify the value you wish to associate with this test. Options include: is, contains, starts with, or ends with. this string - Specify a username you wish this test to consider.

IP/Port Tests

The IP/Port tests include:

Table 4-4 IP / Port Test Group

Test	Description	Default Test Name	Parameters
Source Port	Valid when the source port of the event is one of the configured source port(s).	when the source port is one of the following ports	ports - Specify the ports you wish this test to consider.
Destination Port	Valid when the destination port of the event is one of the configured destination port(s).	when the destination port is one of the following ports	ports - Specify the ports you wish this test to consider.
Local Port	Valid when the local port of the event is one of the configured local port(s).	when the local port is one of the following ports	ports - Specify the ports you wish this test to consider.

Table 4-4 IP / Port Test Group (continued)

Test	Description	Default Test Name	Parameters
Remote Port	Valid when the remote port of the event is one of the configured remote port(s).	when the remote port is one of the following ports	ports - Specify the ports you wish this test to consider.
Source IP Address	Valid when the source IP address of the event is one of the configured IP address(es).	when the source IP is one of the following IP addresses	IP addresses - Specify the IP address(es) you wish this test to consider.
Destination IP Address	Valid when the destination IP address of the event is one of the configured IP address(es).	when the destination IP is one of the following IP addresses	IP addresses - Specify the IP address(es) you wish this test to consider.
Local IP Address	Valid when the local IP address of the event is one of the configured IP address(es).	when the local IP is one of the following IP addresses	IP addresses - Specify the IP address(es) you wish this test to consider.
Remote IP Address	Valid when the remote IP address of the event is one of the configured IP address(es).	when the remote IP is one of the following IP addresses	IP addresses - Specify the IP address(es) you wish this test to consider.
IP Address	Valid when the source or destination IP address of the event is one of the configured IP address(es).	when either the source or destination IP is one of the following IP addresses	IP addresses - Specify the IP address(es) you wish this test to consider.

Date/Time Tests

The date and time tests include:

Table 4-5 Date/Time Tests

Test	Description	Default Test Name	Parameters
Event Day	Valid when the event occurs on the configured day of the month.	when the event(s) occur on the selected day of the month	Configure the following parameters: <ul style="list-style-type: none"> on - Specify if you wish this test to consider on, after, or before the configured day. selected - Specify the day of the month you wish this test to consider.
Event Week	Valid when the event occurs on the configured days of the week.	when the event(s) occur on any of these days of the week	these days of the week - Specify the days of the week you wish this test to consider.
Event Time	Valid when the event occurs on the after the configured time.	when the event(s) occur after this time	Configure the following parameters: <ul style="list-style-type: none"> after - Specify if you wish this test to consider after, before, or at the configured time. this time - Specify the time you wish this test to consider.

Device Tests

The device tests include:

Table 4-6 Device Tests

Test	Description	Default Test Name	Parameters
Source Device	Valid when one of the configured source devices is the source of the event.	when the event(s) were detected by one or more of these device	these devices - Specify the devices that you wish this test to detect.
Source Device Type	Valid when one of the configured device types is the source of the event	when the event(s) were detected by one or more of these device types	these device types - Specify the devices that you wish this test to detect.
Devices	Valid when the event(s) have not been detected by the configured devices.	when the event(s) have not been detected by one or more of these devices for 300 seconds .	Configure the following parameters: <ul style="list-style-type: none"> • these devices - Specify the devices you wish this test to consider. • 300 - Specify the time, in seconds, you wish this test to consider.
Device Groups	Valid when an event is detected by the configured device groups	when the event(s) were detected by one or more of these device groups	these device groups - Specify the groups you wish this rule to consider.

Copying a Rule

To copy a rule:

- Step 1** Select the **Event Viewer** tab.
The Event Viewer window appears.
- Step 2** Click **Rules**.
The Rules List window appears.
- Step 3** In the Display drop-down list box, select **Rules**.
- Step 4** Select the rule you wish to duplicate.
- Step 5** From the Actions drop-down list box, select **Duplicate**.
- Step 6** In the Enter name for the copied rule, enter a name for the new rule. Click **Ok**.
The duplicated rule appears.
- Step 7** Click **Edit** to edit the tests for the rule.
For more information on editing the rule, see [Creating a Rule](#).

Deleting a Rule

To delete a rule:

- Step 1** Select the **Event Viewer** tab.
The Event Viewer window appears.
- Step 2** Click **Rules**.
The Rules List window appears.
- Step 3** In the Display drop-down list box, select **Rules**.
- Step 4** Select the rule you wish to duplicate.
- Step 5** From the Actions drop-down list box, select **Delete**.

Grouping Rules

You can group and view your rules and building blocks based on functionality. Categorizing your rules or building blocks into groups allows you to efficiently view and track your rules. For example, you can view all rules related to compliance. By default, the Rules interface displays all rules and building blocks.

As you create new rules, you have a choice whether you wish to assign the rule to an existing group. For information on assigning a group to a using the rule wizard, see [Creating a Rule](#).



Note: You must have administrative access to create, edit, or delete groups. For more information on user roles, see the *STRM Log Management Administration Guide*.

This sections provides information on grouping rules and building blocks including:

- [Viewing Groups](#)
- [Creating a Group](#)
- [Editing a Group](#)
- [Copying an Item to Another Group\(s\)](#)
- [Deleting an Item from a Group](#)
- [Assigning an Item to a Group](#)

Viewing Groups

To view rules or building blocks using groups:

- Step 1** Select the **Event Viewer** tab.
The Event Viewer window appears.
- Step 2** Click **Rules**.
The Rules List window appears.
- Step 3** From the Display drop-down list box, select whether you wish to view Rules or Building blocks.
- Step 4** Form the Filter drop-down list box, select the group category you wish to view.

Step 5 The list of items assigned to that group appear.

Creating a Group To create a group:

Step 1 Select the **Event Viewer** tab.

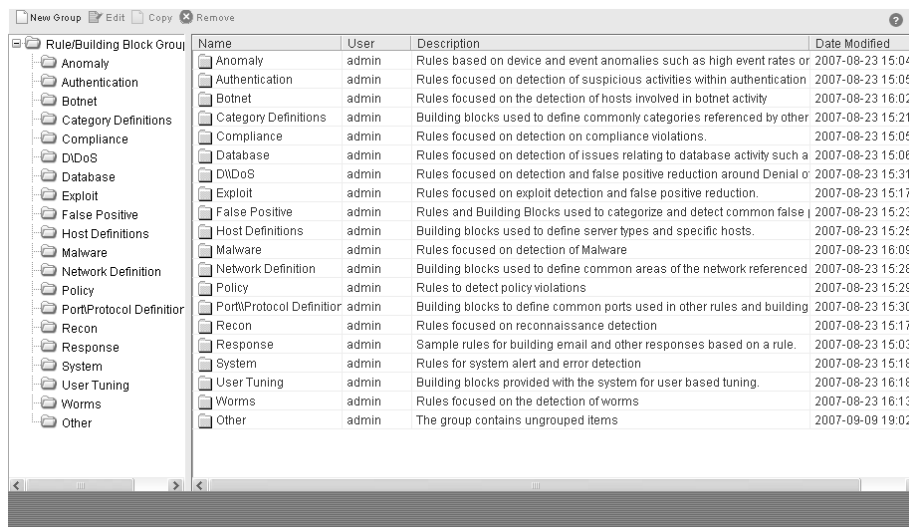
The Event Viewer window appears.

Step 2 Click **Rules**.

The Rules List window appears.

Step 3 Click **Groups**.

The Group window appears.



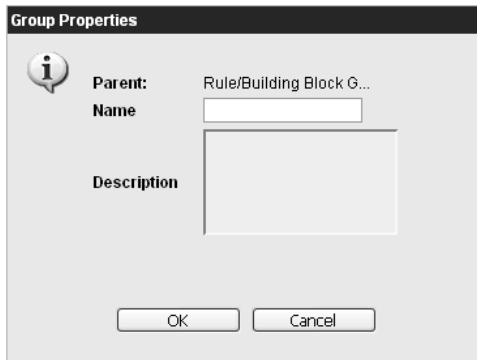
Step 4 From the menu tree, select the group under which you wish to create a new group.



Note: Once you create the group, you can drag and drop menu tree items to change the organization of the tree items.

Step 5 Click **New Group**.

The Group Properties window appears.



Step 6 Enter values for the parameters:

- **Name** - Specify the name you wish to assign to the new group. The name may be up to 255 characters in length.
- **Description** - Specify a description you wish to assign to this group. The description may be up to 255 characters in length.

Step 7 Click **Ok**.

Step 8 If you wish to change the location of the new group, click the new group and drag the folder to the desired location in your menu tree.

Step 9 Close the Groups window.

Editing a Group To edit a group:

Step 1 Select the **Event Viewer** tab.

The Event Viewer window appears.

Step 2 Click **Rules**.

The Rules List window appears.

Step 3 Click **Groups**.

The Group window appears.

Name	User	Description	Date Modified
Anomaly	admin	Rules based on device and event anomalies such as high event rates or	2007-08-23 15:04:00
Authentication	admin	Rules focused on detection of suspicious activities within authentication	2007-08-23 15:05:00
Botnet	admin	Rules focused on the detection of hosts involved in botnet activity	2007-08-23 16:02:00
Category Definitions	admin	Building blocks used to define commonly categories referenced by other	2007-08-23 15:21:00
Compliance	admin	Rules focused on detection on compliance violations.	2007-08-23 15:05:00
Database	admin	Rules focused on detection of issues relating to database activity such a	2007-08-23 15:06:00
DDoS	admin	Rules focused on detection and false positive reduction around Denial o	2007-08-23 15:31:00
Exploit	admin	Rules focused on exploit detection and false positive reduction.	2007-08-23 15:17:00
False Positive	admin	Rules and Building Blocks used to categorize and detect common false	2007-08-23 15:23:00
Host Definitions	admin	Building blocks used to define server types and specific hosts.	2007-08-23 15:25:00
Malware	admin	Rules focused on detection of Malware	2007-08-23 16:09:00
Network Definition	admin	Building blocks used to define common areas of the network referenced	2007-08-23 15:28:00
Policy	admin	Rules to detect policy violations	2007-08-23 15:29:00
Port/Protocol Definition	admin	Building blocks to define common ports used in other rules and building	2007-08-23 15:30:00
Recon	admin	Rules focused on reconnaissance detection	2007-08-23 15:17:00
Response	admin	Sample rules for building email and other responses based on a rule.	2007-08-23 15:03:00
System	admin	Rules for system alert and error detection	2007-08-23 15:18:00
User Tuning	admin	Building blocks provided with the system for user based tuning.	2007-08-23 16:18:00
Worms	admin	Rules focused on the detection of worms	2007-08-23 16:13:00
Other	admin	The group contains ungrouped items	2007-09-09 19:02:00

Step 4 From the menu tree, select the group you wish to edit.

Step 5 Click **Edit**.

The Group Properties window appears.

Step 6 Update values for the parameters, as necessary:

- **Name** - Specify the name you wish to assign to the new group. The name may be up to 255 characters in length.
- **Description** - Specify a description you wish to assign to this group. The description may be up to 255 characters in length.

Step 7 Click **Ok**.

Step 8 If you wish to change the location of the group, click the new group and drag the folder to the desired location in your menu tree.

Step 9 Close the Groups window.

Copying an Item to Another Group(s) Using the groups functionality, you can copy a rule or building block to one or many groups. To copy a rule or building block:

Step 1 Select the **Event Viewer** tab.

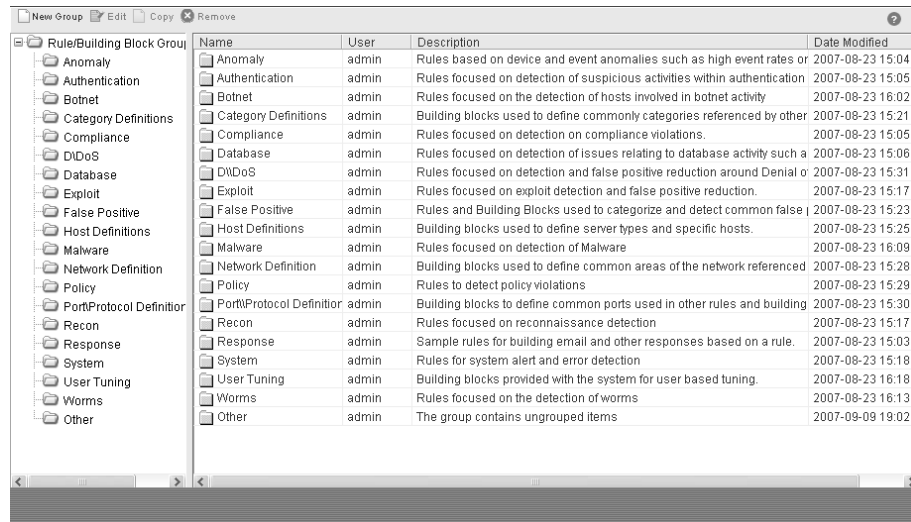
The Event Viewer window appears.

Step 2 Click **Rules**.

The Rules List window appears.

Step 3 Click **Groups**.

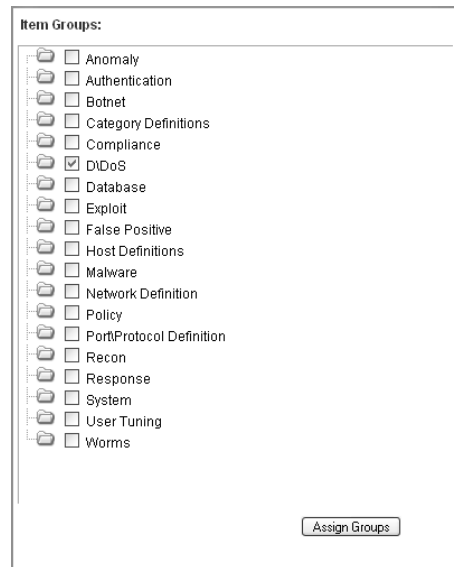
The Group window appears.



Step 4 From the menu tree, select the rule or building block you wish to copy to another group.

Step 5 Click **Copy**.

The Choose Group window appears.



Step 6 Select the check box for the group(s) to which you wish to copy the rule or building block.

Step 7 Click **Assign Groups**.

Step 8 Close the Groups window.

Deleting an Item from a Group To delete a rule or building block from a group:



Note: *Deleting a group removes this rule or building block from the Rules interface. Deleting an item from a group does not delete the rule or building block from the Rules interface.*

Step 1 Select the **Event Viewer** tab.

The Event Viewer window appears.

Step 2 Click **Rules**.

The Rules List window appears.

Step 3 Click **Groups**.

The Group window appears.

Step 4 From the menu tree, select the top level group.

Step 5 From the list of groups, select the group you wish to delete.

Step 6 Click **Remove**.

A confirmation window appears.

Step 7 Click **Ok**.

Step 8 If you wish to change the location of the new group, click the new group and drag the folder to the desired location in your menu tree.

Step 9 Close the Groups window.

Assigning an Item to a Group To assign a rule or building block to a group:

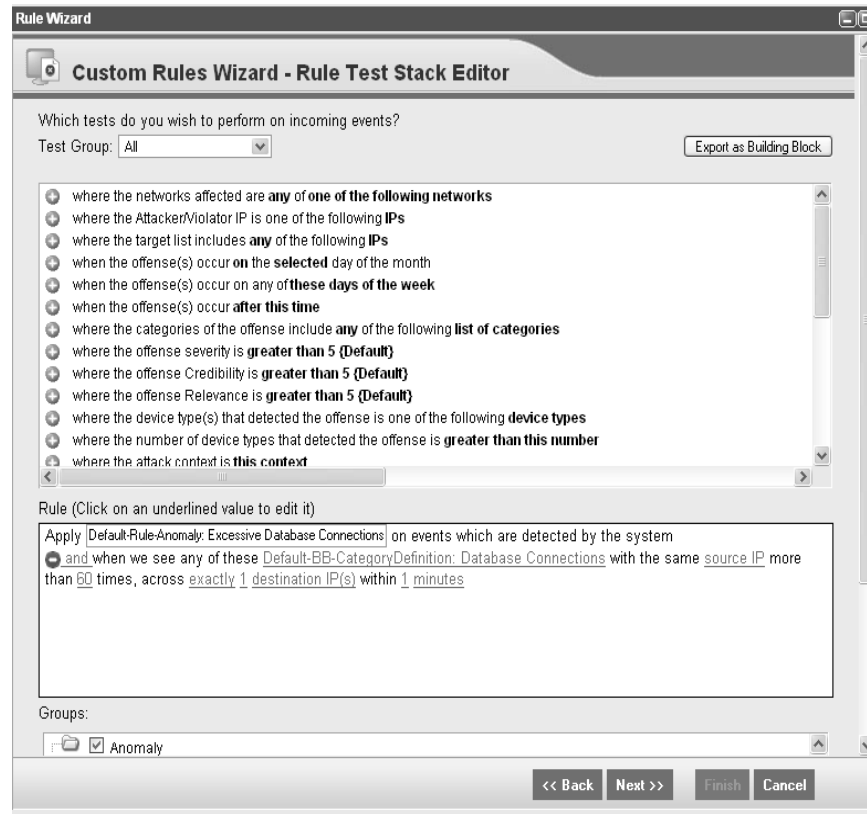
- Step 1** Select the **Event Viewer** tab.
The Event Viewer window appears.
- Step 2** Click **Rules**.
The Rules List window appears.
- Step 3** Select the rule or building block you wish to assign to a group.
- Step 4** From the Actions drop-down list box, select **Assign Groups**.
The Choose Group window appears.
- Step 5** Click **Assign Groups**.

Editing Building Blocks

Building blocks allow you to re-use specific rule tests in other rules. For example, you can save a building block that excludes the IP addresses of all mail servers in your deployment from the rule.

To edit a building block:

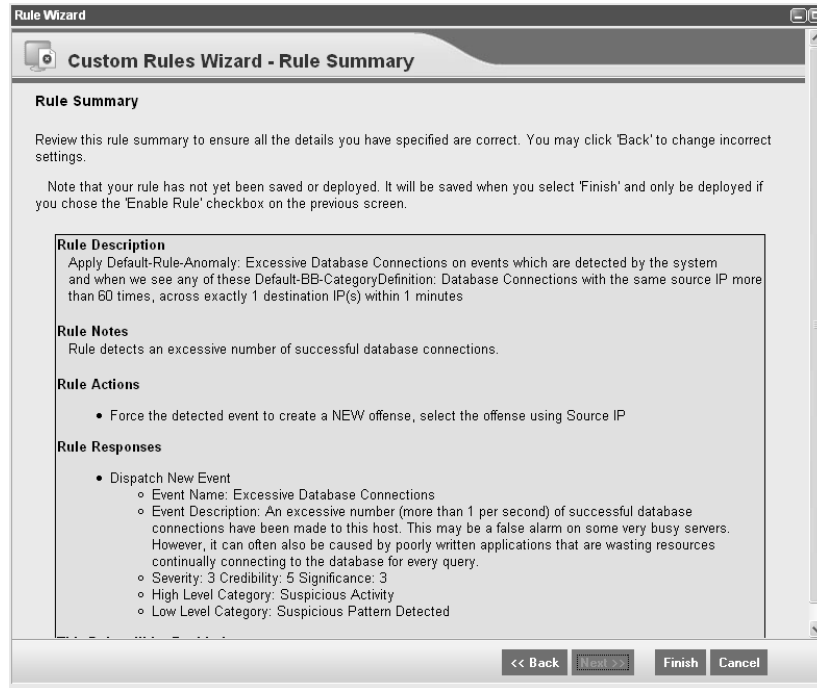
- Step 1** Select the **Event Viewer** tab.
The Event Viewer window appears.
- Step 2** Click **Rules**.
The Rules List window appears.
- Step 3** In the Display drop-down list box, select **Building Blocks**.
The Building Blocks appear.
- Step 4** Double-click the building block you wish to edit.
The Custom Rules Wizard appears.



Step 5 Update the building block, as necessary. Click **Next**.

Step 6 Continue through the wizard. For more information, see [Creating a Rule](#).

The Rule Summary appears.



Step 7 Click **Finish**.

5

MANAGING REPORTS

The Reports interface allows you to create, distribute, and manage reports. You can use the Report Wizard to create executive and operational level reports. STRM Log Management provides default templates that you can use to generate your report data, using various intervals. You can edit any template to present customized data when distributing reports to other STRM Log Management users, however, administrative users can see all reports created by STRM Log Management users.

Reports also allows you to brand your documents with customized logos, which enables you to support unique logos for each report. This is beneficial when distributing reporting to different audiences.

This chapter includes:

- [Using the Reports Interface](#)
- [Viewing Reports](#)
- [Grouping Reports](#)
- [Creating a Report](#)
- [Using Default Report Templates](#)
- [Generating a Report](#)
- [Duplicating a Report](#)
- [Branding Your Report](#)



Note: To brand reports with custom logos, you must upload and configure your logos before you begin using the Report Wizard, see [Branding Your Report](#).

Using the Reports Interface

This section provides information on using the Reports interface including:

- [Using the Navigation Menu](#)
- [Using the Toolbar](#)

Using the Navigation Menu

The default main Reports interface displays generated reports. The navigation menu provides access to reports, templates, and branding including:

Table 5-1 Navigation Menu Options



Menu	Columns	Description
Generated Reports		Displays all generated reports. Reports listed in this panel are available for immediate viewing. The Generated Reports panel lists reports with the following details
	Report Title	Displays the name of the report. By default, the report title in a default template is a duplicate of the template name.
	Group	Displays the group to which this report belongs.
	Schedule	Displays the frequency in which the report generates.
	Generated	Displays the date and time the report was generated.
	Owner	Displays the STRM Log Management user that generated the report.
	Template Author	Displays the user that created the template that generated this report.
	Format	Displays the available viewing formats.
Report Templates		Displays existing report templates. STRM Log Management provides a series of default templates that are ready for immediate access, see Using Default Report Templates . By default, templates are sorted by the report title. You can access templates in the Report Templates panel; or, click the arrow beside the Report Templates menu item and select the group (frequency) folder. The Reports Templates panel lists the configured templates with the following details:
	Template Name	Displays the template name.
	Group	Displays the group to which this report belongs.
	Schedule	Displays the frequency in which the report generates.
	Next Run Time	Displays the time in which the report is expected to generate.
	Last Modification	Displays the last modification date.
	Owner	Displays the STRM Log Management user that generated the report.

Table 5-1 Navigation Menu Options (continued)

Menu	Columns	Description
	Author	Displays the STRM Log Management user that created the template.
	Output	Displays the report format.
Branding		Navigates to the report branding option. See Branding Your Report .

Using the Toolbar You can perform the following actions:

Table 5-2 Toolbar Icon Descriptions

Option	Description
Group	Using the drop-down list box, allows you to view reports assigned to a specific group. For more information, see Grouping Reports .
	Allows you to manage report groups. For more information, see Grouping Reports .
	Allows you to perform the following actions: <ul style="list-style-type: none"> • Create - Allows you to create a new template. For more information, see Creating a Report. • Edit - Allows you to edit the selected template. You can also double-click a template to edit the content. • Duplicate - Allows you to duplicate/rename a report. For more information, see Duplicating a Report. • Assign Groups - Allows you to assign a report template to a report group. For more information, see Grouping Reports. • Share - Allows you to share report templates with other users. You must have administrative privileges to share report templates. For more information, see Sharing a Report. • Toggle Scheduling - Allows you to toggle active/inactive for the selected template. • Generate Report - Generates a report from the selected template. For more information, see Generating a Report. • Delete - Deletes the selected template. Hold the CTRL key and click on the templates you wish to delete.

Viewing Reports

You can view reports displayed in the Generated Reports interface. These reports have been previously created, generated, and optionally distributed. You can only view reports to which you have access. Reports may be formatted in one or all of the following formats:

- **PDF** - Portable Document Format

- **HTML** - Hyper Text Markup Language format
- **RTF** - Rich Text Format
- **XML** - Extensible Markup Language
- **XLS** - Microsoft Excel format.

The XML and XLS formats are only available for reports using a single chart table format (portrait or landscape).



Note: *If you are currently using the FireFox browser and you select the RTF report format, this may launch a new browser window. This does not affect STRM Log Management; this is a result of the FireFox browser configuration. Close the window and continue with your STRM Log Management session.*

To view a generated report:

Step 1 Click the **Reports** tab.

The main Reports interface appears.

Step 2 Click **Generated Reports** from the navigation menu.

Step 3 For the report you wish to view, click the icon that represents the format in which you wish to view the report.

The report opens in the selected format.

Grouping Reports

The Reports interface allows you to view your report and report templates based on functionality. Categorizing your reports into groups allows you to efficiently view and track your reports. For example, you can view all reports related to compliance. By default, the Reports interface displays all reports, however, you can view your reports the using one of the following default groups:

- Compliance
- Executive
- Network Management
- Security
- VoIP

As you create new reports, you can either assign the report to an existing group, create a new group, or do not assign the report to any group. For information on assigning a group to a using the report wizard, see [Creating a Report](#).



Note: *You must have administrative access to create, edit, or delete groups. For more information on user roles, see the STRM Log Management Administration Guide.*

This sections provides information on grouping reports including:

- [Creating a Group](#)

- [Editing a Group](#)
- [Copying a Template to Another Group](#)
- [Deleting a Template From a Group](#)
- [Assigning a Report to a Group](#)

Creating a Group To create a group:

Step 1 Click the **Reports** tab.

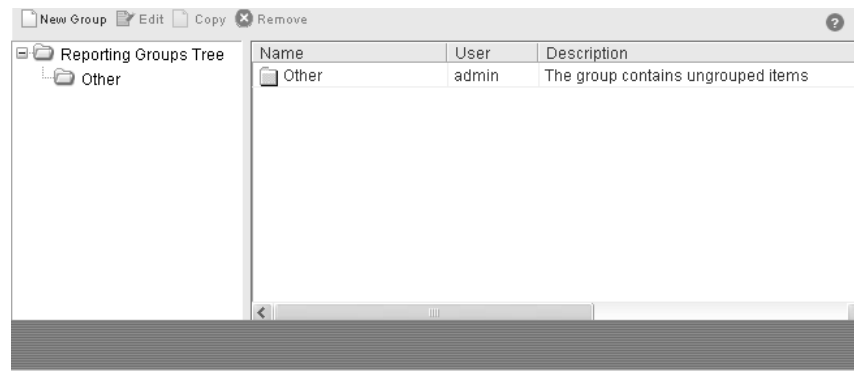
The Reports interface appears.

Step 2 Click the **Report Templates** menu option.

A list of templates appears.

Step 3 Click **Groups**.

The Reports Group window appears.



Step 4 From the menu tree, select the group under which you wish to create a new group.



Note: Once you create the group, you can drag and drop menu tree items to change the organization of the tree items.

Step 5 Click **New Group**.

The Group Properties window appears.

Group Properties

Parent: Reporting Groups Tree

Name:

Description:

OK Cancel

Step 6 Enter values for the parameters:

- **Name** - Specify the name you wish to assign to the new group. The name may be up to 255 characters in length.
- **Description** - Specify a description you wish to assign to this group. The description may be up to 255 characters in length. This field is optional.

Step 7 Click **Ok**.

Step 8 If you wish to change the location of the new group, click the new group and drag the folder to the desired location in your menu tree.

Step 9 Close the Report Groups window.

Editing a Group To edit a group:

Step 1 Click the **Reports** tab.

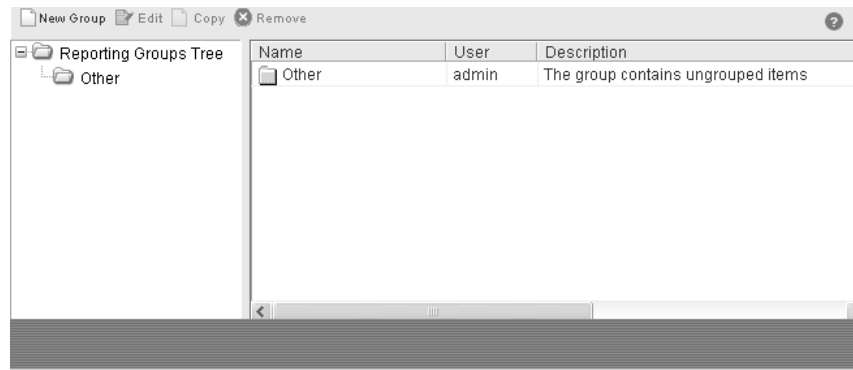
The Reports interface appears.

Step 2 Click the **Report Templates** menu option.

A list of templates appears.

Step 3 Click **Groups**.

The Reports Group window appears.



Step 4 From the menu tree, select the group you wish to edit.

Step 5 Click **Edit**.

The Group Properties window appears.

Step 6 Update values for the parameters, as necessary:

- **Name** - Specify the name you wish to assign to the new group. The name may be up to 255 characters in length.
- **Description** - Specify a description you wish to assign to this group. The description may be up to 255 characters in length. This field is optional.

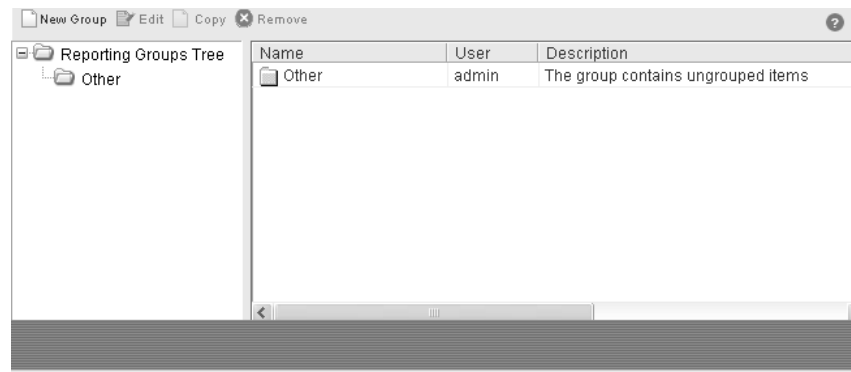
Step 7 Click **Ok**.

Step 8 If you wish to change the location of the group, click the new group and drag the folder to the desired location in your menu tree.

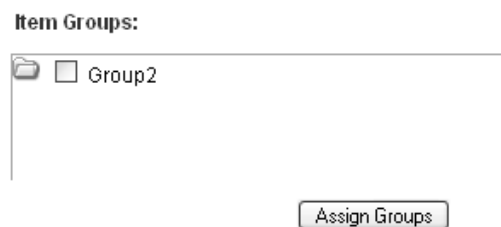
Step 9 Close the Report Groups window.

Copying a Template to Another Group Using the groups functionality, you can copy a template from one group to another. To copy a template:

- Step 1** Click the **Reports** tab.
The Reports interface appears.
- Step 2** Click the **Report Templates** menu option.
A list of templates appears.
- Step 3** Click **Groups**.
The Reports Group window appears.



- Step 4** From the menu tree, select the template you wish to copy to another group.
- Step 5** Click **Copy**.
The Choose Group window appears.



- Step 6** Select the group or groups to which you wish to copy the template.
- Step 7** Click **Assign Groups**.
- Step 8** Close the Report Groups window.

Deleting a Template From a Group To delete a template from a group:



Note: Removing a template from a group only removes this template from the group. Removing a template does not delete the template from Reports interface.

- Step 1** Click the **Reports** tab.
The Reports interface appears.

- Step 2** Click the **Report Templates** menu option.
A list of templates appears.
- Step 3** Click **Groups**.
The Reports Group window appears.
- Step 4** From the menu tree, select the top level group.
- Step 5** From the list of groups, select the group you wish to delete.
- Step 6** Click **Remove**.
A confirmation window appears.
- Step 7** Click **Ok**.
- Step 8** Close the Report Groups window.

Assigning a Report to a Group You can assign a generated report or report template to a group. To assign a report to a group:

- Step 1** Click the **Reports** tab.
The Reports interface appears.
- Step 2** Choose one of the following options:
 - a To assign a generated report to a group, click the **Generated Reports** menu option.
A list of templates appears.
 - b To assign a report template report to a group, click the **Report Templates** menu option.
A list of templates appears.
- Step 3** Select the report(s) you wish to assign to a group.
- Step 4** Click **Assign Groups**.
The Choose Group window appears.
- Step 5** From the Item Groups list, select the check box of the group you wish to assign to this report template.
- Step 6** Click **Assign Groups**.

Creating a Report

You can access the Report Wizard from the toolbar in the Reports Templates interface to create a new report. When a report is complete, you can use the template to create other reports using many of the same configurations.

The Report Wizard provides a step-by-step guide in designing, scheduling, and generating your reports. The wizard uses the following elements:

- **Layout** - Determines the positioning and size of each container.
- **Container** - Placeholder for the featured content.

- **Content** - Definition of the chart that is placed in the container.

This section includes:

- [Creating a Template](#)
- [Configuring Charts](#)
- [Selecting a Graph Type](#)

Creating a Template To create a template:

Step 1 Click the **Reports** tab.

The Reports interface appears.

Step 2 From the Actions drop-down list box, select **Create**.

The Report Wizard appears.



Note: Select the check box if you wish to disable the Welcome page.



Step 3 Select a scheduling option. Click **Next**.

Table 5-3 Report Scheduling

Parameter	Default Settings
This report should be scheduled to run	
Manually	Generates a report one time only. This is the default setting; however, you may generate this report as often as required.
Hourly	Schedules the report to generate at the end of each hour using the data from the previous hour. Using the drop-down list boxes, select a time frame to begin and end the reporting cycle. A report is generated for each hour within this time frame. Time is available in half-hour increments. The default is 1:00 a.m. for both From and To.
Daily	Schedules the report to generate each day using the data from the previous day. Each chart on a report allows you to select the previous 24 hours of the day, or select a specific time frame from the previous day. Click the check boxes beside each day you wish to generate a report. Also, using the drop-down list box, select a time to begin the reporting cycle. Time is available in half-hour increments. The default is 1:00 a.m.
Weekly	Schedules the report to generate each week using the data from the previous week. Select the day you wish to generate the report. Default is Monday. Using the drop-down list box, select a time to begin the reporting cycle. Time is available in half-hour increments. The default is 1:00 a.m.

Table 5-3 Report Scheduling (continued)

Parameter	Default Settings
Monthly	Schedules the report to generate each month using the data from the previous month. Using the drop-down list box, select the date you wish to generate the report. The default is the 1st day. Also, using the drop-down list box, select a time to begin the reporting cycle. Time is available in half-hour increments. The default is 1:00 a.m.
Allow this report to generate manually	
Yes	Enables manual generation of this report.
No	Disables manual generation of this report.

The Report Layout window appears.



A report can consist of several data. Your network and security data can be presented in a variety of styles, such as tables, pie charts, and bar charts. Styles consist of a number of options, such as delta or baseline.

When selecting the layout of a report, consider the type of report you wish to create - do not choose a small chart container for graph content that may display a large number of objects. Each graph is complete with a legend and a list of networks from which the content is derived; choose a large enough container to hold the data. To preview how each chart displays a data, see [Selecting a Graph Type](#).

Step 4 From the Orientation drop-down list box, select the page orientation and then click the desired layout. Click **Next**.

The Specify Report Contents window appears:

Step 5 Select values for the following parameters:

- **Report Title** - Specify a title for your report. The title can be up to 100 characters in length - do not use special characters.



Note: Your report is saved by the title name you enter in this field.

- **Logo** - Using the drop-down list box, select a logo. By default, the STRM Log Management logo is displayed. Other logos may be uploaded and used, see [Branding Your Report](#).
- **Chart Type** - Using the drop-down list box, select a chart for your container including:
 - [Event/Logs](#)
 - [Time Series](#)
 - [TopN Time Series](#)

The Container Details window appears.

Step 6 Configure your chart.

For detailed information on configuring your chart, see [Configuring Charts](#).

Step 7 Click **Save Container Details** for each container in a report.

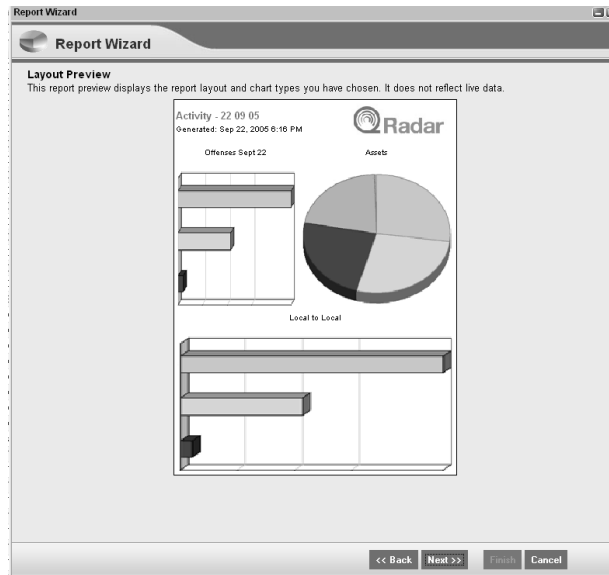
The Specify Report Contents window appears. The configured container is highlighted.

Step 8 Repeat the configuration process for each container you wish to define and click **Next**.

The Layout Preview window appears providing a preview of how your data appears.



Note: Charts that appear in the preview window do not display actual data. This is a graphical representation of the layout you have configured.



Step 9 Preview your report. Click **Next**:

The Report Format window appears. The default is PDF.



Step 10 Select the check box for any or all formats for report viewing. Click **Next**.



Note: Generated reports can be one to two megabytes in size, depending on the selected output format. We recommend the use of the PDF format; PDF format is smaller in size and does not consume a large quantity of disk space to store.

The Report Distribution Channels window appears. The default is Report Console.

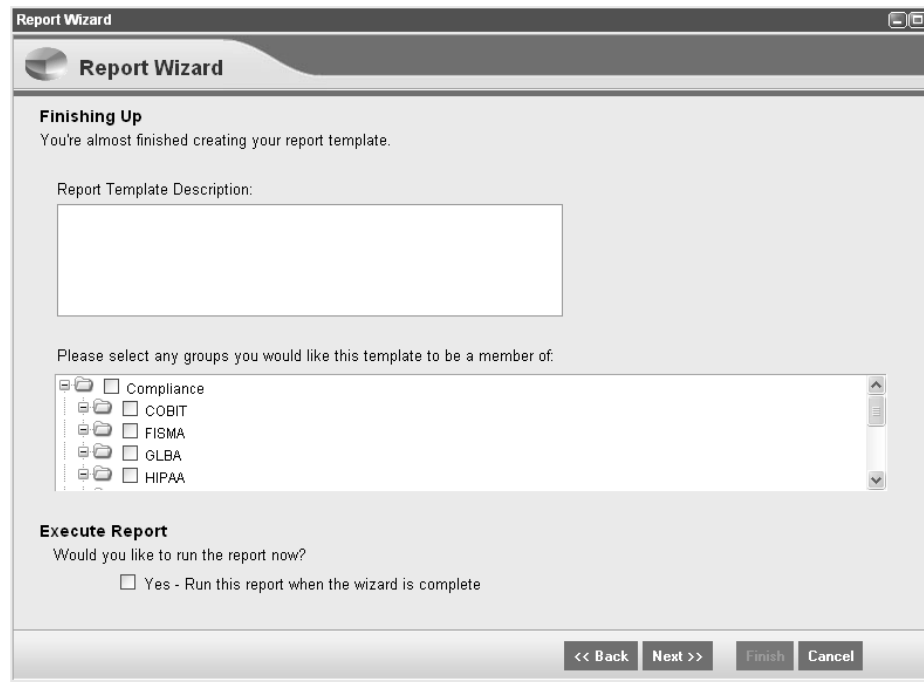


Step 11 Select the desired distribution channels. Click **Next**.

Table 5-4 Report Distribution

Parameter	Sub-Parameter	Description
Report Console		Select the check box if you wish to send the report to the Reports interface. Note: You must have appropriate network permissions to share your report with other users. For more information on permissions, see the <i>STRM Log Management Administration Guide</i> .
Email		Select the check box if you wish to distribute the report using e-mail.
	Enter the report distribution email address(es)	Specify the e-mail address(es) for each destination you wish to send the report; e-mail addresses are comma separated. Maximum characters for this parameter is 255. Note: E-mail recipients receive this e-mail from <code>no_reply_reports@STRM</code> .
	Include Report as attachment (PDF/RTF)	Select the check box to send the report as an attachment.
	Include link to Report Console	Select the check box to include a link in your e-mail.

The Finishing Up window appears.



Step 12 Enter values for the following parameters. Click **Next**.

Table 5-5 Finishing Up

Parameter	Description
Report Template Description	Specify a description for this template. This description appears on the Report Summary page and is included in the report distribution e-mail.
Groups	Specify the group(s) to which you wish to assign this report. For more information on groups, see Grouping Reports .
Would you like to run the report now?	Select the check box if you wish to generate the report when the wizard is complete. By default, the check box is clear.

The Report Summary window appears displaying details for your report. You can select the tabs available in the summary window to preview your report selections.

Step 13 Click **Finish**.

If you have selected the Execute Report option from the Finishing Up window, the report immediately generates. If you have not selected this option, the report template is saved and generates as scheduled.

Configuring Charts The chart type determines how your data and network objects are presented in your report. Data can be charted with several characteristics and created in a single report.

The following chart types are available for each template:

- [Event/Logs](#)
- [Time Series](#)
- [TopN Time Series](#)

Event/Logs

The Event/Logs Chart allows you to view event information for a specific period of time.

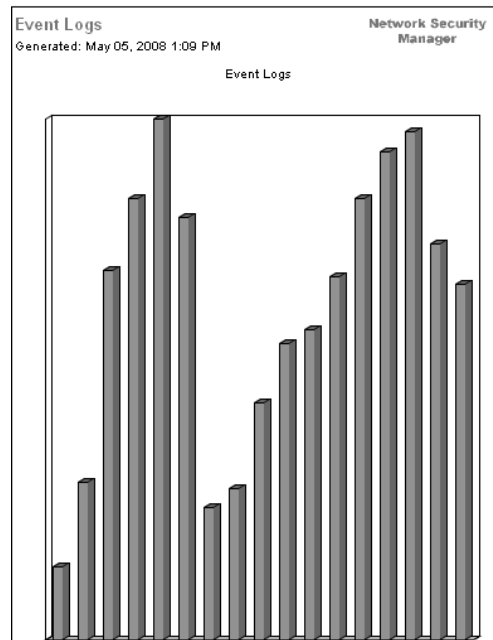


Figure 5-1 Event/Logs Report

Enter values for the following parameters:

Table 5-6 Event/Logs Chart Container Details

Parameter	Description
Container Details - Events/Logs	
Chart Title	Specify a chart title to a maximum of 100 characters.
Chart Sub-Title	Clear the check box to change the automatically created sub-title. Enter a title to a maximum of 100 characters.
Graph Type	Using the drop-down list box, select the type of graph you wish to appear on your report. Options include: <ul style="list-style-type: none"> • Bar - When selecting this option, you must also select the Timeline Interval from the Additional Details section. • Pie - When selecting this option, you must also select either total or percent. • Table - When selecting this option (full page width container only), you must also select the Timeline Interval from the Additional Details section. <p>Note: For an example of how each type of graph charts data, see Selecting a Graph Type.</p>
Graph	Using the drop-down list box, select the number of events/logs you wish to appear in the report.
Scheduling	The scheduling options depend on the template type you have selected.

Table 5-6 Event/Logs Chart Container Details (continued)

Parameter	Description
Manually	Using the calendar, select range of dates you wish this report to consider. The default is the current date. Using the drop-down list boxes, select a time to begin and end generating the report. Time is available in half-hour increments. The default is 1:00 a.m.
Hourly	Automatically graphs all data from the previous hour.
Daily	Choose one of the following options: <ul style="list-style-type: none"> All data from previous 24 hours Data of previous day from - Using the drop-down list boxes, select the period of time you wish the report to consider. Time is available in half-hour increments. The default is 1:00 a.m.
Weekly	Choose one of the following options: <ul style="list-style-type: none"> All data from previous week Data from a previous week - Using the drop-down list boxes, select the days to begin and end generating the report. Default is Sunday.
Monthly	Choose one of the following options: <ul style="list-style-type: none"> All data from previous month Data from a previous month - Using the drop-down list boxes, select the dates to begin and end generating the report. Default is 1st to 31st.
Graph Content	
Base this event report on	Using the drop-down list box, select a previously saved search. If you wish to create a new search, click Create New Event Search . For more information on creating an event search, see Chapter 3 Using the Event Viewer .

Time Series

The Time Series Chart displays options, such as pivoting and delta comparisons, that allow you to create charts that compare a data for two different periods of time.

To configure a Time Series Chart, enter values for the following parameters:

Table 5-7 Time Series Chart Container Details

Parameter	Description
Container Details - Time Series Chart	
Chart Title	Specify a chart title to a maximum of 100 characters.
Chart Sub-Title	Clear the check box to change the automatically created sub-title. Enter a title to a maximum of 100 characters.
Graph Type	Using the drop-down list box, select the type of graph you wish to appear on your report. Options include: <ul style="list-style-type: none"> • Line - When selecting this option, you must also select the Timeline Interval from the Additional Details section. • Stacked_Line -When selecting this option, you must also select the Timeline Interval from the Additional Details section. • Stacked_Base_Line - When selecting this option, you must also select the Timeline Interval and choose a Baseline from the Additional Details section. • Bar - When selecting this option, you must also select the Timeline Interval from the Additional Details section.

Table 5-7 Time Series Chart Container Details (continued)

Parameter	Description
	<ul style="list-style-type: none"> • Stacked_Bar - When selecting this option, you must also select the Timeline Interval from the Additional Details section. • Stacked_Bar_Base_Line - When selecting this option, you must also select the Timeline Interval and choose the Baseline parameters. • Delta - When selecting this option, you must also select the Timeline Interval and select an option for the Delta Span from the Additional Details. Delta chart represents the difference in traffic patterns between the current graphing interval and another equally sized interval from the past. Use the Delta chart to model how traffic patterns for networks, applications or event data are changing. <p>Note: The end date of your Delta Span must be set before the From date of the data you are graphing.</p> <ul style="list-style-type: none"> • Pie - When selecting this option, you must also select either total or percent. • Table - When selecting this option (full page width container only), you must also select the Timeline Interval from the Additional Details section. <p>Note: For an example of how each type of graph charts data, see Selecting a Graph Type.</p>
Scheduling	The scheduling options depend on the template type you have selected.
Manually	<p>Using the calendar, select the date. The default is the current date.</p> <p>Using the drop-down list boxes, select a time to begin and end generating the report. Time is available in half-hour increments. The default is 1:00 a.m.</p>
Hourly	Automatically graphs all data from the previous hour.
Daily	<p>Choose one of the following options:</p> <ul style="list-style-type: none"> • All data from previous 24 hours • Data of previous day from - Using the drop-down list boxes, select an hour to begin and end generating the report. Time is available in half-hour increments. The default is 1:00 a.m.
Weekly	<p>Choose one of the following options:</p> <ul style="list-style-type: none"> • All data from previous week • Data from a previous week - Using the drop-down list boxes, select the days to begin and end generating the report. Default is Sunday.

Table 5-7 Time Series Chart Container Details (continued)

Parameter	Description
Monthly	Choose one of the following options: <ul style="list-style-type: none"> All data from previous month Data from a previous month - Using the drop-down list boxes, select the dates to begin and end generating the report. Default is 1st to 31st.
Additional Details	
Timeline Interval	Using the drop-down list box, select the time interval. Options are based on the schedule selected. For example, a weekly report supports intervals of one hour, one day, and one week. A monthly report supports intervals of one day, one week, and one month.
Baseline	This option only appears if you select a base line type graph type. Choose one of the following options: <ul style="list-style-type: none"> Individual Baseline - Creates individual baselines for each object on the chart. <p>Note: <i>This option can create many lines on chart.</i></p> <ul style="list-style-type: none"> Aggregate Baseline - Creates a single baseline for the the aggregate of all objects on the chart. Aggregate Baseline is default.
Graph Content	
Network Location	Select the check box for each network you wish to chart data for. You must select at least one network location.
View Objects	Using the drop-down list box, select the events object.
Layers	Using the drop-down list box, select the layer you wish to appear on the graph. The layer options that appear depends on the View Objects. The layer also determines the average per second availability.
Options	
Average per second	Select the check box to graph the average of all objects that are selected.
Aggregate Selected Objects	Select the check box to graph the sum of all (view) objects or networks that are selected.
Graph	Select one of the following: <ul style="list-style-type: none"> View Objects - Displays the top view objects selected. Networks - Displays the top networks associated with the view objects you have selected.

Table 5-7 Time Series Chart Container Details (continued)

Parameter	Description
Expand To Include	<p>Using the drop-down list box, select an option to include on the graph. Options include:</p> <ul style="list-style-type: none"> • None - View Objects and Network Locations are graphed exactly as shown in the View Object tree menu. This is the default setting. • Group - Expands chart to include Groups of a Network Location or View Object, if the high level object is selected. • Leaves - Expands chart to include Network Location leaves or View Object if the high level object is selected. <p>Note: Use this option to select only the Top of the Network Location or a View Object, and display data for the groups, or leaves. This is dependent also on the Graph Top Items option.</p> <p>Note: If you select View Objects in the Graph Top Items option, and select Expand to include Group, this expands the chart to include the groups for the specific View Object selected.</p>

TopN Time Series

The TopN Time Series chart allows you to create TopN charts for any data that STRM Log Management logs over time. For example, you can create an Executive Chart to represent the Top 5 Event Categories.

Container Details - TopN Time Series Chart
Displays the activity of the top networks or view objects based on the selected dates and times.

Chart Title:

Chart Sub-Title: Automatically Specified

Graph Type: HorizontalBar

Manual Scheduling:
Graph data from the following time span
From: 2007-10-25 at 1:00 AM
To: 2007-10-25 at 1:30 AM

Graph Content

Networks:

- all
- other
- Net-10-172-192
- DMZ
- VPN_Addresses_Space
- Proxy_Servers
- NAT_Ranges
- Geographic_Location
- Server_Network
- Mail
- ...

View Objects:

- Events
- all

Layer: Select a layer...

Options:

- Average per second
- Graph top: 10
- View Objects
- Expand To Include: None

<< Back Next >> Finish Cancel

Enter values for the following parameters:

Table 5-8 TopN Time Series Container Details

Parameter	Description
Container Details - TopN Time Series Chart	
Chart Title	Specify a chart title to a maximum of 100 characters.
Chart Sub-Title	Clear the check box to change the automatically created sub-title. Enter a title to a maximum of 100 characters.
Graph Type	Using the drop-down list box, select the type of graph you wish to appear on your report. Options include: <ul style="list-style-type: none"> • HorizontalBar • Pie • Table (full page width only)
Scheduling	The scheduling options depend on the chosen chart type.
Manually	Using the calendar, select the date. The default is the current date. Using the drop-down list boxes, select a time to begin and end generating the report. Time is available in half-hour increments. The default is 1:00 a.m.
Hourly	Automatically graphs all data from the previous hour.
Daily	Choose one of the following options: <ul style="list-style-type: none"> • All data from previous 24 hours • Data of previous day from - Using the drop-down list boxes, select an hour to begin and end generating the report. Time is available in half-hour increments. The default is 1:00 a.m.
Weekly	Choose one of the following options: <ul style="list-style-type: none"> • All data from previous week • Data from a previous week - Using the drop-down list boxes, select the days to begin and end generating the report. Default is Sunday.
Monthly	Choose one of the following options: <ul style="list-style-type: none"> • All data from previous month • Data from a previous month - Using the drop-down list boxes, select the dates to begin and end generating the report. Default is 1st to 31st.
Graph Content	
Network Location	Select the check box for each network you wish to chart the data. You can select all networks or click the expand option to select network groups or leaved.
View Objects	Using the drop-down list box, select the View Object that represents the type of data you wish to display. You can graphs the number of events for the selected event categories within a specified interval. You can sort the events by the severity, credibility, and relevance layer.

Table 5-8 TopN Time Series Container Details (continued)

Parameter	Description
Layers	Using the drop-down list box, select the traffic layer you wish to appear on the graph. The layer options that appear depends on the selected View Objects.
Options	
Average per second	Select the check box to graph the average of the selected (view) objects for the chart.
Graph top items	Using the drop-down list box, select the number of items to include on graphs, then select one of the following: <ul style="list-style-type: none"> • View Objects - Displays the top view objects selected. • Networks - Displays the top networks associated with the view objects you have selected.
Expand To Include	Using the drop-down list box, select an option to include on the graph. Options include: <ul style="list-style-type: none"> • None - View Objects and Network Locations are graphed exactly as shown in the View Object tree menu. This is the default setting. • Group - Expands chart to include Groups of a Network Location or View Object, if the high level object is selected. • Leaves - Expands chart to include Network Location leaves or View Object if the high level object is selected. <p>Note: Use this option when selecting the Top of the Network Location or a View Object, and display data for the groups, or leaves. This is dependent also on the Graph Top Items option.</p> <p>Note: If you select View Objects in the Graph Top Items option, and select Expand to include Group, this expands the chart to include the groups for the specific View Object selected.</p>

Selecting a Graph Type

Each chart type has a variety of graphs to display your data. The available selection is dependent on the chart type you have selected. The colors that appear in the charts that depict network traffic are derived from the network configuration files. Colors that appear depicting IP addresses are unique.

Table 5-9 provides examples of how STRM Log Management charts your network and security data:

Table 5-9 Available Graph Types

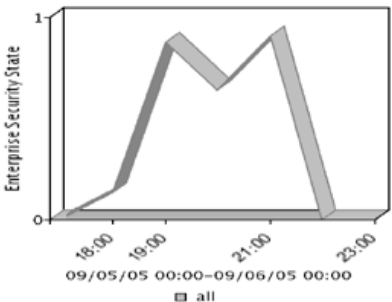
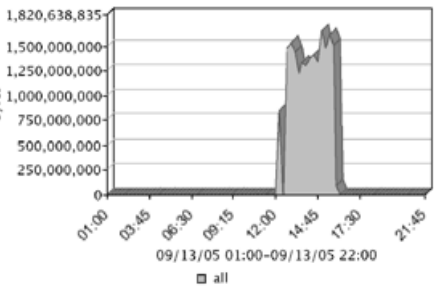
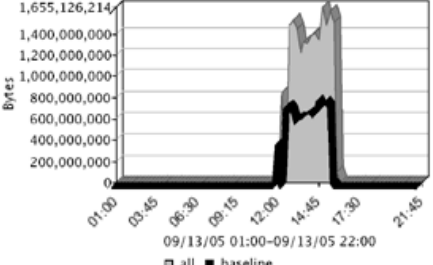
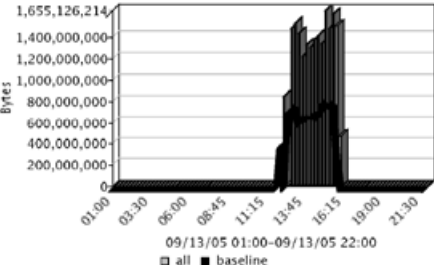
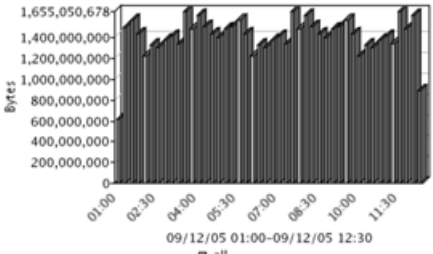
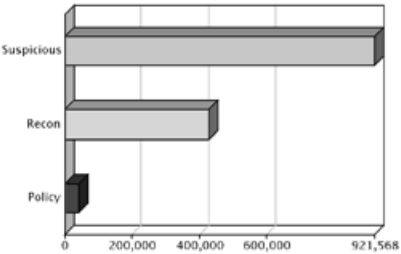
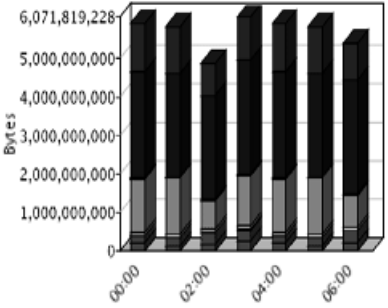
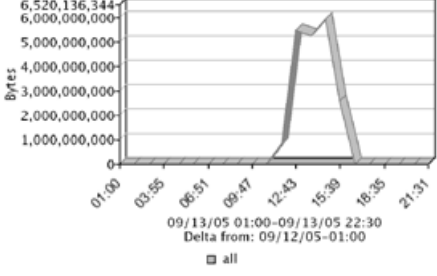
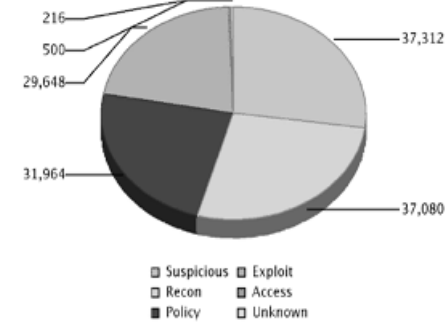
<p>Line Graph Available with the Time Series chart type.</p> 	<p>Stacked Line Graph Available with the Time Series chart type.</p> 
<p>Stacked Base Line Graph Available with the Time Series chart type.</p> 	<p>Stacked Bar Base Line Graph Available with the Time Series chart type.</p> 
<p>Bar Graph Available with the Time Series chart type.</p> 	<p>Horizontal Bar Graph Available with the TopN Time Series chart.</p> 

Table 5-9 Available Graph Types (continued)

<p>Stacked Bar Graph</p> <p>Available with the Time Series chart type.</p> 	<p>Delta Graph</p> <p>Available with the Time Series chart type.</p> 																																																																																	
<p>Pie Graph</p> <p>Available with the following chart type:</p> <ul style="list-style-type: none"> • Time Series • TopN Time Series 	<p>Table Graph</p> <p>Available with the following charts:</p> <ul style="list-style-type: none"> • Time Series • TopN Time Series <table border="1" data-bbox="953 934 1409 1102"> <thead> <tr> <th>ID</th> <th>Network</th> <th>Attacker</th> <th>Cred</th> <th>Sev</th> <th>Rel</th> <th>Mag</th> <th>Events</th> <th>Targets</th> </tr> </thead> <tbody> <tr> <td>35</td> <td>other</td> <td>10.105.57.125</td> <td>2</td> <td>5</td> <td>4</td> <td>4</td> <td>8789</td> <td>261</td> </tr> <tr> <td>360</td> <td>other</td> <td>10.101.145.100</td> <td>4</td> <td>5</td> <td>3</td> <td>4</td> <td>198</td> <td>3</td> </tr> <tr> <td>36</td> <td>other</td> <td>10.101.145.75</td> <td>4</td> <td>5</td> <td>3</td> <td>4</td> <td>99</td> <td>1</td> </tr> <tr> <td>26</td> <td>other</td> <td>10.101.242.217</td> <td>4</td> <td>5</td> <td>3</td> <td>4</td> <td>51</td> <td>1</td> </tr> <tr> <td>3</td> <td>other</td> <td>207.179.172.101</td> <td>2</td> <td>4</td> <td>3</td> <td>3</td> <td>6148</td> <td>262</td> </tr> <tr> <td>16</td> <td>Corporate_HQ HumanResources.Recrui</td> <td>10.107.96.8</td> <td>2</td> <td>4</td> <td>3</td> <td>3</td> <td>4206</td> <td>465</td> </tr> <tr> <td>7</td> <td>Corporate_HQ HumanResources.Recrui</td> <td>10.107.97.167</td> <td>2</td> <td>4</td> <td>3</td> <td>3</td> <td>4109</td> <td>465</td> </tr> <tr> <td>15</td> <td>Corporate_HQ.Legal</td> <td>10.107.96.8</td> <td>2</td> <td>4</td> <td>3</td> <td>3</td> <td>3299</td> <td>366</td> </tr> </tbody> </table>	ID	Network	Attacker	Cred	Sev	Rel	Mag	Events	Targets	35	other	10.105.57.125	2	5	4	4	8789	261	360	other	10.101.145.100	4	5	3	4	198	3	36	other	10.101.145.75	4	5	3	4	99	1	26	other	10.101.242.217	4	5	3	4	51	1	3	other	207.179.172.101	2	4	3	3	6148	262	16	Corporate_HQ HumanResources.Recrui	10.107.96.8	2	4	3	3	4206	465	7	Corporate_HQ HumanResources.Recrui	10.107.97.167	2	4	3	3	4109	465	15	Corporate_HQ.Legal	10.107.96.8	2	4	3	3	3299	366
ID	Network	Attacker	Cred	Sev	Rel	Mag	Events	Targets																																																																										
35	other	10.105.57.125	2	5	4	4	8789	261																																																																										
360	other	10.101.145.100	4	5	3	4	198	3																																																																										
36	other	10.101.145.75	4	5	3	4	99	1																																																																										
26	other	10.101.242.217	4	5	3	4	51	1																																																																										
3	other	207.179.172.101	2	4	3	3	6148	262																																																																										
16	Corporate_HQ HumanResources.Recrui	10.107.96.8	2	4	3	3	4206	465																																																																										
7	Corporate_HQ HumanResources.Recrui	10.107.97.167	2	4	3	3	4109	465																																																																										
15	Corporate_HQ.Legal	10.107.96.8	2	4	3	3	3299	366																																																																										



Note: A report designed with content displayed in a table is available only with a full page width container.

Using Default Report Templates

STRM Log Management provides a series of default templates that allows you to manipulate and customize your data. Default templates are designed for both executive level and operational level reports.

You can generate a report from any template located in the Report Templates panel. These templates are also found in the folders within the Report Templates navigation menu. Templates that do not specify an interval schedule must be manually generated; others are configured to automatically generate.



Note: By default, report titles that appears with each template has the same name in the Generated Reports panel. When you re-configure a template and enter a new report title, your template takes on the new name; however, the original template remains the same.

Each template is designed to capture and display your existing data. Point your mouse to any template to preview the summary. The summary reveals how the template is configured and the type of information the template is configured to generate.



Note: The STRM Log Management application is configured with the timezone used during the installation and setup of the application. Please check with your administrator to ensure your STRM Log Management session is synchronized with your timezone.

To customize a template:

- Step 1** Click the **Reports** tab.
The Reports interface appears.
- Step 2** Click the **Report Templates** menu option.
A list of templates appears.
- Step 3** Point your mouse over the templates and preview the summary information.
- Step 4** Double-click the desired template.
The Report Wizard appears.
- Step 5** Make the necessary changes. See [Creating a Report](#).

Generating a Report

To generate a report:

- Step 1** Click the **Reports** tab.
The main Reports interface appears.
- Step 2** Click the **Report Templates** menu option.
A list of templates appears.
- Step 3** Select the report you wish to generate.
- Step 4** Click **Generate Report**.
The report generates. See [Viewing Reports](#).

Duplicating a Report

To duplicate a report:

- Step 1** Click the **Reports** tab.
The main Reports interface appears.
- Step 2** Click the **Report Templates** menu option.
A list of templates appears.
- Step 3** Select the report you wish to duplicate.
- Step 4** Click **Duplicate**.

The enter a name window appears.

Step 5 Enter a new name, without spaces, for the template.

The new template appears.

Sharing a Report

You can share report templates with other users. This allows you to provide a copy of the selected templates for another user to edit or schedule, as necessary. Once shared, any updates that the user makes to your shared template does not affect your version of the template.



Note: You must have administrative privileges to share templates. Also, for a new user to view and access report templates, an administrative user must share all the necessary reports with the new user.

To share a template:

Step 1 Click the **Reports** tab.

The main Reports interface appears.

Step 2 Click the **Report Templates** menu option.

A list of templates appears.

Step 3 Select the report(s) you wish to share.

Step 4 Click **Share**.

The Share Templates window appears.

Step 5 From the list of users, select the user(s) you wish to share this report template with.



Note: If no users with appropriate access are available, a message appears.

Step 6 Click **Share**.

The report template is now shared.

Branding Your Report

You can import logos and specific images to brand your reports. Report branding is beneficial for your enterprise if you support more than one logo. When uploading your images to STRM Log Management, the image is automatically saved as a Portable Network Graphic (PNG). We recommend that you use graphics 144 x 50 pixels with a white background.

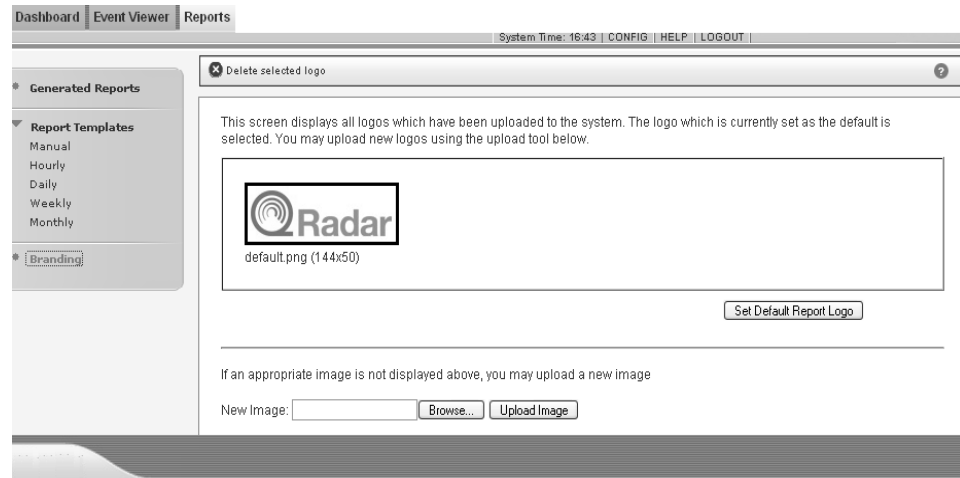
To brand your report:

Step 1 Click the **Reports** tab.

The main Reports interface appears.

Step 2 Click **Branding**.

The Branding window appears:



Step 3 Click **Browse** to browse the files located on your system.

Step 4 Select the file that contains the desired logo. Click **Open**.

The file name appears in the New Image field.

Step 5 Click **Upload Image** to upload the image to STRM Log Management.



Note: To make sure your browser displays the new logo, clear your browser cache.

Step 6 Select the logo you wish to use as the default and click **Set Default Image**. This logo appears as the first option using the drop-down menu in the Specify Content window of the Report Wizard.



Note: If you have uploaded an image that is larger in length than the report header can support, the image automatically resizes to fit the header; this is approximately 50 pixels in height.

A

DEFAULT RULES AND BUILDING BLOCKS

This appendix provides the defaults for the rules and building blocks including:

- [Default Rules](#)
- [Default Building Blocks](#)

Default Rules Default rules include:

Table B-6 Default Rules

Rule	Group	Rule Type	Enabled	Description
Default-Rule-Anomaly: Devices with High Event Rates	Anomaly	Event	False	Monitors devices for high event rates. Typically, the default threshold is low for most networks and we recommend that you adjust this value before enabling this rule. To configure which devices will be monitored, edit the Default-BB-DeviceDefinition: Devices to Monitor for High Event Rates building block.
Default-Rule-Anomaly: Excessive Database Connections	Anomaly	Event	True	Reports an excessive number of successful database connections.
Default-Rule-Anomaly: Excessive Firewall Accepts Across Multiple Hosts	Anomaly	Event	True	Reports excessive firewall accepts across multiple hosts. More than 100 events were detected across at least 100 unique destination IP addresses in 5 minutes.
Default-Rule-Anomaly: Excessive Firewall Denies from Single Source	Anomaly	Event	True	Reports excessive firewall denies from a single host. Detects more than 400 firewall deny attempts from a single source to a single destination within 5 minutes.
Default-Rule-Anomaly: Potential Honeypot Access	Anomaly	Event	False	Reports an event that was targeting or sourced from a honeypot or tarpit defined address. Before enabling this rule, you must configure the Default-BB-HostDefinition: Honeypot like addresses building block and create the appropriate sentry from the Network Surveillance interface.

Table B-6 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Default-Rule-Anomaly: Rate Analysis Marked Events	Anomaly	Event	False	Reports a host emitting events at a rate greater than normal. This may be normal, but in some cases can be an early warning sign that the host has changed behavior. We recommend that you perform an event search and/or flow search to determine if the host is exhibiting other suspicious activity.
Default-Rule-Anomaly: Remote Access from Foreign Country	Anomaly	Event	False	Reports successful logins or access from an IP address known to be in a country that does not have remote access right. Before you enable this rule, we recommend that you configure the Default-BB-CategoryDefinition: Countries with no Remote Access building block.
Default-Rule-Authentication: Login Failure to Disabled Account	Authentication	Event	True	Reports a host login message from a disabled user account. If the user is no longer a member of the organization, we recommend that you investigate any other received authentication messages from the same user.
Default-Rule-Authentication: Login Failure to Expired Account	Authentication	Event	True	Reports a host login failure message from an expired user account known. If the user is no longer a member of the organization, we recommend that you investigate any other received authentication messages.
Default-Rule - Authentication: Login Failures Across Multiple Hosts	Authentication	Event	True	Reports authentication failures on the same source IP address more than three times, across more than three destination IP addresses within 10 minutes.
Default-Rule-Authentication: Login Failures Followed By Success	Authentication	Event	True	Reports multiple log in failures to a single host, followed by a successful log in to the host.
Default-Rule-Authentication: Login Successful After Scan Attempt	Authentication	Event	True	Reports on events detected by the system when at least one of the configured rules is detected with the same source IP address followed by successful authentication with the same IP address, within 30 minutes.
Default-Rule-Authentication: Multiple VoIP Login Failures	Authentication	Event	True	Reports multiple log in failures to a VoIP PBX.
Default-Rule-Authentication: Repeated Login Failures, Single Host	Authentication	Event	True	Reports when a source IP address causes an authentication failure event at least seven times to a single destination within 5 minutes.

Table B-6 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Default-Rule-Botnet: Potential Botnet Connection (DNS)	Botnet,Exploit	Event	False	Reports a host connecting or attempting to connect to a DNS server on the Internet. This may indicate a host connecting to a Botnet. The host should be investigated for malicious code. Do not enable this rule until you have tuned the Default-BB-HostDefinition: DNS Servers building block. <i>Note: Laptops that include wireless adapters may cause this rule to generate alerts since the laptops may attempt to communicate with another IDPs DNS server. If this occurs, define the ISPs DNS server in the Default-BB-HostDefinition: DNS Servers building block.</i>
Default-Rule-Botnet: Potential Botnet Connection (IRC)	Botnet	Event	True	Reports a host connecting or attempting to connect to an IRC server on the Internet. This may indicate a host connecting to a Botnet. The host should be investigated for malicious code.
Default-Rule-Compliance: Compliance Events Become Offenses	Compliance	Event	False	Reports compliance-based events, such as, clear text passwords.
Default-Rule-Compliance: Excessive Failed Logins to Compliance IS	Compliance	Event	False	Reports excessive authentication failures to a compliance server within 10 minutes.
Default-Rule-Database: Attempted Configuration Modification by a remote host	Database	Event	True	Reports when a configuration modification is attempted to a database server from a remote network.
Default-Rule-Database: Concurrent Logins from Multiple Locations	Database	Event	True	Reports when several authentications to a database server occur across many remote IP addresses.
Default-Rule-Database: Failures Followed by User Changes	Database	Event	True	Reports when there are failures followed by the addition or change of a user account.
Default-Rule-Database: Groups changed from Remote Host	Database	Event	True	Monitors changes to groups on a database when the change is initiated from a remote network.
Default-Rule-Database: Multiple Database Failures Followed by Success	Database	Event	True	Reports when there are multiple database failures followed by a success within a short period of time.
Default-Rule-Database: Remote Login Failure	Database	Event	True	Increases the severity of a failed login attempt to a database from a remote network.

Table B-6 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Default-Rule-Database: Remote Login Success	Database	Event	True	Reports when a successful authentication occurs to a database server from a remote network.
Default-Rule-Database: User Rights Changed from Remote Host	Database	Event	True	Reports when changes to user privileges occurs to a database from a remote network.
Default-Rule-DDoS Attack Detected	D\DoS	Event	False	Reports network Distributed Denial of Service (DDoS) attacks on a system.
Default-Rule-DoS: Network DoS Attack Detected	D\DoS	Event	True	Reports network Denial of Service (DoS) attacks on a system.
Default-Rule-DoS: Service DoS Attack Detected	D\DoS	Event	True	Reports a DoS attack against a local target that is known to exist and the target port is open.
Default-Rule-Exploit: Exploit Followed by Suspicious Host Activity	Exploit	Event	False	Reports an exploit or attack type activity from a source IP address followed by suspicious account activity on the destination host within 15 minutes.
Default-Rule-Exploit: Exploit/Malware Events Across Multiple Targets	Exploit	Event	True	Reports a source IP address generating multiple (at least 5) exploits or malicious software (malware) events in the last 5 minutes. These events are not targeting hosts that are vulnerable and may indicate false positives generating from a device.
Default-Rule-Exploit: Multiple Exploit Types Against Single target	Exploit	Event	True	Reports a target attempting to be exploited using multiple types of attacks from one or more attackers.
Default-Rule-Exploit: Potential VoIP Toll Fraud	Exploit	Event	False	Reports multiple failed logins to your VoIP hardware followed by sessions being opened. At least 3 events were detected within 30 seconds. This action could indicate that illegal users are executing VoIP sessions on your network.
Default-Rule-Exploit: Recon followed by Exploit	Exploit	Event	True	Reports reconnaissance followed by an exploit from the same source IP address to the same destination port within 1 hour.
Default-Rule-False Positive: False Positive Rules and Building Blocks	False Positive	Event	True	Reports events that include false positive rules and building blocks, such as, Default-BB-FalsePositive: Windows Server False Positive Events. Events that match the above conditions are stored but also dropped. If you add any new building blocks or rules to remove events from becoming offenses, you must add these new rules or building blocks to this rule.

Table B-6 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Default-Rule-Policy: Local P2P Server Detected	Policy	Event	True	Reports local Peer-to-Peer (P2P) traffic or any event categorized as P2P. More than 10 hosts were detected connecting to a local host that appears to be operating as a P2P server.
Default-Rule-Policy: Upload to Local WebServer	Policy	Event	False	Reports potential file uploads to a local web server. To edit the details of this rule, edit the Default-BB-CategoryDefinition: Upload to Local WebServer building block.
Default-Rule-Recon: Aggressive Local Scanner Detected	Recon	Event	True	Reports an aggressive scan from a local source IP address, scanning other local or remote IP addresses. More than 400 targets received reconnaissance or suspicious events in less than 2 minutes. This may indicate a manually driven scan, an exploited host searching for other targets, or a worm is present on the system.
Default-Rule-Recon: Aggressive Remote Scanner Detected	Recon	Event	True	Reports an aggressive scan from a remote source IP address, scanning other local or remote IP addresses. More than 50 targets received reconnaissance or suspicious events in less than 3 minutes. This may indicate a manually driven scan, an exploited host searching for other targets, or a worm on a system.
Default-Rule-Recon: Excessive Firewall Denies Across Local Host	Recon	Event	True	Reports excessive attempts, across local hosts, to access the firewall and access is denied. More than 40 attempts are detected across at least 40 destination IP addresses in 5 minutes.
Default-Rule-Recon: Excessive Firewall Denies Across Remote Host	Recon	Event	True	Reports excessive attempts, across remote hosts, to access the firewall and access is denied. More than 40 attempts are detected across at least 40 destination IP addresses in 5 minutes.
Default-Rule-Recon: Host Port Scan Detected by Local Host	Recon	Event	True	Reports a single source IP address scanning more than 50 ports in under 3 minutes.
Default-Rule-Recon: Host Port Scan Detected by Remote Host	Recon	Event	True	Reports when more than 400 ports were scanned from a single source IP address in under 2 minutes.
Default-Rule-Recon: Increase Magnitude of High Rate Scans	Recon	Event	True	If a high rate flow-based scanning attack is detected, this rule increases the magnitude of the current event.
Default-Rule-Recon: Increase Magnitude of Medium Rate Scans	Recon	Event	True	If a medium rate flow-based scanning attack is detected, this rule increases the magnitude of the current event.

Table B-6 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Default-Rule-Recon: Local LDAP Server Scanner	Recon	Event	True	Reports a source IP address attempting reconnaissance or suspicious connections on common LDAP ports to more than 60 hosts in 10 minutes.
Default-Rule-Recon: Local Database Scanner	Recon	Event	True	Reports a scan from a local host against other local or remote targets. At least 30 host were scanned in 10 minutes.
Default-Rule-Recon: Local DHCP Scanner	Recon	Event	True	Reports a source IP address attempting reconnaissance or suspicious connections on common DHCP ports to more than 60 hosts in 10 minutes.
Default-Rule-Recon: Local DNS Scanner	Recon	Event	True	Reports a source IP address attempting reconnaissance or suspicious connections on common DNS ports to more than 60 hosts in 10 minutes.
Default-Rule-Recon: Local FTP Scanner	Recon	Event	True	Reports a source IP address attempting reconnaissance or suspicious connections on common FTP ports to more than 30 hosts in 10 minutes.
Default-Rule-Recon: Local Game Server Scanner	Recon	Event	True	Reports a source IP address attempting reconnaissance or suspicious connections on common game server ports to more than 60 hosts in 10 minutes.
Default-Rule-Recon: Local ICMP Scanner	Recon	Event	True	Reports a source IP address attempting reconnaissance or suspicious connections on common ICMP ports to more than 60 hosts in 10 minutes.
Default-Rule-Recon: Local IM Server Scanner	Recon	Event	True	Reports a source IP address attempting reconnaissance or suspicious connections on common IM server ports to more than 60 hosts in 10 minutes.
Default-Rule-Recon: Local IRC Server Scanner	Recon	Event	True	Reports a source IP address attempting reconnaissance or suspicious connections on common IRC server ports to more than 10 hosts in 10 minutes.
Default-Rule-Recon: Local Mail Server Scanner	Recon	Event	True	Reports a source IP address attempting reconnaissance or suspicious connections on common mail server ports to more than 60 hosts in 10 minutes.
Default-Rule-Recon: Local P2P Server Scanner	Recon	Event	True	Reports a source IP address attempting reconnaissance or suspicious connections on common Peer-to-Peer (P2P) server ports to more than 60 hosts in 10 minutes.

Table B-6 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Default-Rule-Recon: Local Proxy Server Scanner	Recon	Event	True	Reports a source IP address attempting reconnaissance or suspicious connections on common proxy server ports to more than 60 hosts in 10 minutes.
Default-Rule-Recon: Local RPC Server Scanner	Recon	Event	True	Reports a source IP address attempting reconnaissance or suspicious connections on common RPC server ports to more than 60 hosts in 10 minutes.
Default-Rule-Recon: Local Scanner Detected	Recon	Event	True	Reports a scan from a local host against other hosts or remote targets. At least 60 hosts were scanned within 20 minutes. This activity was using a protocol other than TCP, UDP, or ICMP.
Default-Rule-Recon: Local SNMP Scanner	Recon	Event	True	Reports a source IP address attempting reconnaissance or suspicious connections on common SNMP ports to more than 60 hosts in 10 minutes.
Default-Rule-Recon: Local SSH Server Scanner	Recon	Event	True	Reports a source IP address attempting reconnaissance or suspicious connections on common SSH ports to more than 30 hosts in 10 minutes.
Default-Rule-Recon: Local Suspicious Probe Events Detected	Recon	Event	False	Reports when various suspicious or reconnaissance events have been detected from the same local source IP address to more than 5 destination IP address in 4 minutes. This can indicate various forms of host probing, such as Nmap reconnaissance, which attempts to identify the services and operation systems of the target.
Default-Rule-Recon: Local TCP Scanner	Recon	Event	True	Reports a source IP address attempting reconnaissance or suspicious connections on common TCP ports to more than 60 hosts in 10 minutes.
Default-Rule-Recon: Local UDP Scanner	Recon	Event	True	Reports a source IP address attempting reconnaissance or suspicious connections on common UDP ports to more than 60 hosts in 10 minutes.
Default-Rule-Recon: Local Web Server Scanner	Recon	Event	True	Reports a source IP address attempting reconnaissance or suspicious connections on common local web server ports to more than 60 hosts in 10 minutes.
Default-Rule-Recon: Local Windows Server Scanner	Recon	Event	True	Reports a source IP address attempting reconnaissance or suspicious connections on common Windows server ports to more than 60 hosts in 10 minutes.

Table B-6 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Default-Rule-Recon: Recon Followed by Accept	Recon	Event	False	Adds an additional event into the event stream when a host that has been performing reconnaissance also has a firewall accept following the reconnaissance activity.
Default-Rule-Recon: Remote Database Scanner	Recon	Event	True	Reports a scan from a remote host against other local or remote targets. At least 30 hosts were scanned in 10 minutes.
Default-Rule-Recon: Remote DHCP Scanner	Recon	Event	True	Reports a remote host attempting reconnaissance or suspicious connections on common DHCP ports to more than 30 hosts in 10 minutes.
Default-Rule-Recon: Remote DNS Scanner	Recon	Event	True	Reports a source IP address attempting reconnaissance or suspicious connections on common DNS ports to more than 60 hosts in 10 minutes.
Default-Rule-Recon: Remote FTP Scanner	Recon	Event	True	Reports a remote host attempting reconnaissance or suspicious connections on common FTP ports to more than 30 hosts in 10 minutes.
Default-Rule-Recon: Remote Game Server Scanner	Recon	Event	True	Reports a remote host attempting reconnaissance or suspicious connections on common game server ports to more than 30 hosts in 10 minutes.
Default-Rule-Recon: Remote ICMP Scanner	Recon	Event	True	Reports a remote host attempting reconnaissance or suspicious connections on common ICMP ports to more than 60 hosts in 10 minutes.
Default-Rule-Recon: Local IM Server Scanner	Recon	Event	True	Reports a remote host attempting reconnaissance or suspicious connections on common IM server ports to more than 60 hosts in 10 minutes.
Default-Rule-Recon: Local IRC Server Scanner	Recon	Event	True	Reports a remote host attempting reconnaissance or suspicious connections on common IRC server ports to more than 10 hosts in 10 minutes.
Default-Rule-Recon: Remote LDAP Server Scanner	Recon	Event	True	Reports a scan from a remote host against other local or remote targets. At least 30 hosts were scanned in 10 minutes.
Default-Rule-Recon: Remote Mail Server Scanner	Recon	Event	True	Reports a remote host attempting reconnaissance or suspicious connections on common mail server ports to more than 30 hosts in 10 minutes.
Default-Rule-Recon: Remote P2P Server Scanner	Recon	Event	True	Reports a remote host attempting reconnaissance or suspicious connections on common Peer-to-Peer (P2P) server ports to more than 60 hosts in 10 minutes.

Table B-6 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Default-Rule-Recon: Remote Proxy Server Scanner	Recon	Event	True	Reports a remote host attempting reconnaissance or suspicious connections on common proxy server ports to more than 30 hosts in 10 minutes.
Default-Rule-Recon: Remote RPC Server Scanner	Recon	Event	True	Reports a remote host attempting reconnaissance or suspicious connections on common RPC server ports to more than 30 hosts in 10 minutes.
Default-Rule-Recon: Remote Scanner Detected	Recon	Event	True	Reports a scan from a remote host against other hosts or remote targets. At least 60 hosts were scanned within 20 minutes. This activity was using a protocol other than TCP, UDP, or ICMP.
Default-Rule-Recon: Remote SNMP Scanner	Recon	Event	True	Reports scans from a remote host against local or remote targets. At least 30 hosts were scanned in 10 minutes.
Default-Rule-Recon: Remote SSH Server Scanner	Recon	Event	True	Reports a remote host attempting reconnaissance or suspicious connections on common SSH ports to more than 30 hosts in 10 minutes.
Default-Rule-Recon: Remote Suspicious Probe Events Detected	Recon	Event	False	Reports various suspicious or reconnaissance events from the same remote source IP address to more than 5 destination IP addresses in 4 minutes. This may indicate various forms of host probing, such as Nmap reconnaissance that attempts to identify the services and operating system of the targets.
Default-Rule-Recon: Remote TCP Scanner	Recon	Event	True	Reports a remote host attempting reconnaissance or suspicious connections on common TCP ports to more than 60 hosts in 10 minutes.
Default-Rule-Recon: Remote UDP Scanner	Recon	Event	True	Reports a remote host attempting reconnaissance or suspicious connections on common UDP ports to more than 60 hosts in 10 minutes.
Default-Rule-Recon: Remote Web Server Scanner	Recon	Event	True	Reports a remote host attempting reconnaissance or suspicious connections on common local web server ports to more than 60 hosts in 10 minutes.
Default-Rule-Recon: Remote Windows Server Scanner	Recon	Event	True	Reports a remote host attempting reconnaissance or suspicious connections on common Windows server ports to more than 60 hosts in 10 minutes.

Table B-6 Default Rules (continued)

Rule	Group	Rule Type	Enabled	Description
Default-Rule-Recon: Single Merged Recon Events	Recon	Event	True	Reports merged reconnaissance events generated by some devices. This rule causes all these events to create an offense. All devices of this type and their categories should be added to the Default-BB-ReconDetected: Devices which Merge Recon into Single Events building block.
Default-Rule-System: Device Stopped Sending Events	System	Event	False	Reports when an event source has not sent an event to the system in over 1 hour. Edit this rule to add devices you wish to monitor.
Default-Rule-Recon: Multiple System Errors	System	Event	False	Reports when as source has 10 system errors within 3 minutes.
Default-Rule-Worms Detection: Local Mass Mailing Host Detected	Worm	Event	True	Reports a local host sending more than 20 SMTP flows in 1 minute. This may indicate a host being used as a spam relay or infected with a form of mass mailing worm.
Default-Rule-Worms Detection: Possible Local Worm Detected	Worm	Event	True	Reports a local host generating reconnaissance or suspicious events across a large number of hosts (greater than 300) in 20 minutes. This may indicate the presence of a worm on the network or a wide spread scan.
Default-Rule-Worms Detection: Worm Detected (Events)	Worm	Event	True	Reports exploits or worm activity on a system for local-to-local or local-to-remote traffic.

Default Building Blocks

Default building blocks include:

Table B-7 Default Building Blocks

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
Default-BB-Category Definition: Authentication Failures	Category Definitions	Event	Edit this BB to include all events that indicate an unsuccessful attempt to access the network.	
Default-BB-Category Definition: Authentication Success	Category Definitions	Event	Edit this BB to include all events that indicate successful attempts to access the network.	
Default-BB-Category Definition: Authentication to Disabled Account	Category Definitions	Event	Edit this BB to include all events that indicate failed attempts to access the network using a disabled account.	
Default-BB-Category Definition: Authentication to Expired Account	Category Definitions	Event	Edit this BB to include all events that indicate failed attempts to access the network using an expired account.	
Default-BB-Category Definition: Authentication User or group added or changed	Category Definitions	Event	Edit this building block to include all events that indicate modification to accounts or groups.	
Default-BB-Category Definition: Countries with no Remote Access	Category Definitions	Event	Edit this BB to include any geographic location that typically would not be allowed remote access to the enterprise. Once configured, you can enable the Default-Rule-Anomaly: Remote Access from Foreign Country rule.	
Default-BB-Category Definition: Database Connections	Category Definitions	Event	Edit this BB to define successful logins to databases. You may need to add additional device types for this BB.	
Default-BB-Category Definition: DDoS Attack	Category Definitions	Event	Edit this BB to include all event categories that you wish to categorize as a DDoS attack.	
Default-BB-Category Definition: Exploits, Backdoors, and Trojans	Category Definitions	Event	Edit this BB to include all events that are typically exploits, backdoor, or trojans.	
Default-BB-Category Definition: Firewall or ACL Accept	Category Definitions	Event	Edit this BB to include all events that indicate access to the firewall.	
Default-BB-Category Definition: Firewall or ACL Denies	Category Definitions	Event	Edit this BB to include all events that indicate unsuccessful attempts to access the firewall.	

Table B-7 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
Default-BB-Category Definition: Firewall System Errors	Category Definitions	Event	Edit this BB to include all events that may indicate a firewall system error. By default, this BB applies when an event is detected by one or more of the following devices: <ul style="list-style-type: none"> • CheckPoint • Generic Firewall • Iptables • NetScreen Firewall • Cisco Pix 	
Default-BB-Category Definition: High Magnitude Events	Category Definitions	Event	Edit this BB to the severity, credibility, and relevance levels you wish to generate an event. The defaults are: <ul style="list-style-type: none"> • Severity = 6 • Credibility = 7 • Relevance = 7 	
Default-BB-Category Definitions: KeyLoggers	Category Definitions	Event	Edit this BB to include all events that are typically exploits, backdoor, or trojans.	
Default-BB-Category Definition: Mail Policy Violation	Category Definitions	Event	Edit this BB to define mail policy violations.	
Default-BB-Category Definition: Malware Annoyances	Category Definitions	Event	Edit this BB to include event categories that are typically associated with spyware infections.	
Default-BB-Category Definition: Network DoS Attack	Category Definitions	Event	Edit this BB to include all event categories that you wish to categorize as a network DoS attack.	
Default-BB-Category Definition: Policy Events	Category Definitions	Event	Edit this BB to include all event categories that may indicate a violation to network policy.	
Default-BB-Category Definition: Post Exploit Account Activity	Category Definitions	Event	Edit this BB to include all event categories that may indicate exploits to accounts.	
Default-BB-Category Definition: Rate Analysis Marked Events	Category Definitions	Event	STRM monitors event rates of all source IP addresses/QIDs and destination IP addresses/QIDs and marks events that exhibit abnormal rate behavior. Edit this BB to include events that are marked with rate analysis.	

Table B-7 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
Default-BB-Category Definition: Recon Events	Category Definitions	Event	Edit this BB to include all events that indicate reconnaissance activity.	
Default-BB-Category Definition: Service DoS	Category Definitions	Event	Edit this BB to define Denial of Service (DoS) attack events.	
Default-BB-Category Definition: Suspicious Events	Category Definitions	Event	Edit this BB to include all events that indicate suspicious activity.	
Default-BB-Category Definition: System Errors and Failures	Category Definitions	Event	Edit this BB to include all events that may indicate a system error or failure. By default, this BB applies when the event category for the event is one of the following System categories: <ul style="list-style-type: none"> • Service Failure • System Error • System Failure 	
Default-BB-Category Definition: Upload to Local WebServer	Category Definitions	Event	Typically, most networks are configured to restrict applications that use the PUT method running on their web application servers. This BB detects if a remote host has used this method on a local server. The BB could be duplicated to also detect other unwanted methods or for local hosts using the method connecting to remote servers. This building block is referenced by the Default-Rule-Policy: Upload to Local WebServer rule.	
Default-BB-Category Definition: VoIP Authentication Failure Events	Category Definitions	Event	Edit this BB to include all events that indicate a VoIP login failure.	
Default-BB-Category Definition: VoIP Session Opened	Category Definitions	Event	Edit this BB to include all events that indicate the start of a VoIP session.	
Default-BB-Category Definition: Windows Compliance Events	Category Definitions	Event	Edit this BB to include all event categories that indicate compliance events.	
Default-BB-Category Definition: Worm Events	Category Definitions	Event	Edit this BB to define worm events. This BB only applies to events not detected by a custom rule.	

Table B-7 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
Default-BB-Compliance Definition: GLBA Servers	Compliance, Host Definitions	Event	Edit this BB to include your GLBA IP systems. You must then apply this BB to rules related to failed logins, remote access, etc.	
Default-BB-Compliance Definition: HIPAA Servers	Compliance, Host Definitions	Event	Edit this BB to include your HIPAA Servers by IP address. You must then apply this BB to rules related to failed logins, remote access, etc.	
Default-BB-Compliance Definition: SOX Servers	Compliance, Host Definitions	Event	Edit this BB to include your SOX IP Servers. You must then apply this BB to rules related to failed logins, remote access, etc.	
Default-BB-Compliance Definition: PCI DSS Servers	Compliance, Host Definitions, Response	Event	Edit this BB to include your PCI DSS servers by IP address. You must apply this BB to rules related to failed logins, remote access, etc.	
Default-BB-Database: System Action Allow	Category Definitions, Database	Event	Edit this BB to include any events that indicates successful actions within a database.	
Default-BB-Database: System Action Deny	Category Definitions, Database	Event	Edit this BB to include any events that indicate unsuccessful actions within a database.	
Default-BB-Database: User Addition or Change	Category Definitions, Database	Event	Edit this BB to include events that indicate the successful addition or change of user privileges	
Default-BB-Device Definition: Devices to Monitor for High Event Rates	Category Definitions	Event	Edit this BB to include devices you wish to monitor for high event rates. The event rate threshold is controlled by the Default-Rule-Anomaly: Devices with High Event Rates.	
Default-BB-FalsePositive: All Default False Positive BBs	False Positive	Event	Edit this BB to include all false positive building blocks.	All Default-BB-False Positive building blocks
Default-BB-FalsePositive: Broadcast Address False Positive Categories	False Positive	Event	Edit this BB to define all the false positive categories that occur to or from the broadcast address space.	
Default-BB-FalsePositive: Database Server False Positive Categories	False Positive	Event	Edit this BB to define all the false positive categories that occur to or from database servers that are defined in the Default-BB-HostDefinition: Database Servers building block.	Default-BB-HostDefinition: Database Servers

Table B-7 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
Default-BB-FalsePositive: Database Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from database servers that are defined in the Default-BB-HostDefinition: Database Servers building block.	Default-BB-HostDefinition: Database Servers
Default-BB-FalsePositive: Device and Specific Event	False Positive	Event	Edit this BB to include the devices and QID of devices that continually generate false positives.	
Default-BB-FalsePositive: DHCP Server False Positive Categories	False Positive	Event	Edit this BB to define all the false positive categories that occur to or from DHCP servers that are defined in the Default-BB-HostDefinition: DHCP Servers building block.	Default-BB-HostDefinition: DHCP Servers
Default-BB-FalsePositive: DHCP Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from DHCP servers that are defined in the Default-BB-HostDefinition: DHCP Servers building block.	Default-BB-HostDefinition: DHCP Servers
Default-BB-FalsePositive: DNS Server False Positive Categories	False Positive	Event	Edit this BB to define all the false positive categories that occur to or from DNS based servers that are defined in the Default-BB-HostDefinition: DNS Servers building block.	Default-BB-HostDefinition: DNS Servers
Default-BB-FalsePositive: DNS Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from DNS-based servers that are defined in the Default-BB-HostDefinition: DNS Servers building block.	Default-BB-HostDefinition: DNS Servers
Default-BB-FalsePositive: FTP Server False Positive Categories	False Positive	Event	Edit this BB to define all the false positive categories that occur to or from FTP based servers that are defined in the Default-BB-HostDefinition: FTP Servers building block.	Default-BB-HostDefinition: FTP Servers
Default-BB-FalsePositive: FTP False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from FTP-based servers that are defined in the Default-BB-HostDefinition: FTP Servers building block.	Default-BB-HostDefinition: FTP Servers
Default-BB-FalsePositive: Global False Positive Events	False Positive	Event	Edit this BB to include any event QIDs that you wish to ignore.	

Table B-7 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
Default-BB-FalsePositive: Internal Attacker to Internal Target False Positives	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from Local-to-Local (L2L) based servers.	
Default-BB-FalsePositive: Internal Attacker to Remote Target False Positives	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from Local-to-Remote (L2R) based servers.	
Default-BB-FalsePositive: LDAP Server False Positive Categories	False Positive	Event	Edit this BB to define all the false positive categories that occur to or from LDAP servers that are defined in the Default-BB-HostDefinition: LDAP Servers building block.	Default-BB-HostDefinition: LDAP Servers
Default-BB-FalsePositive: LDAP Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from LDAP servers that are defined in the Default-BB-HostDefinition: LDAP Servers building block.	Default-BB-HostDefinition: LDAP Servers
Default-BB-FalsePositive: Mail Server False Positive Categories	False Positive	Event	Edit this BB to define all the false positive categories that occur to or from mail servers that are defined in the Default-BB-HostDefinition: Mail Servers building block.	Default-BB-HostDefinition: Mail Servers
Default-BB-FalsePositive: Mail Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from mail servers that are defined in the Default-BB-HostDefinition: Mail Servers building block.	Default-BB-HostDefinition: Mail Servers
Default-BB-FalsePositive: Network Management Servers Recon	False Positive	Event	Edit this BB to define all the false positive categories that occur to or from network management servers that are defined in the Default-BB-HostDefinition: Network Management Servers building block.	Default-BB-HostDefinition: Network Management Servers
Default-BB-FalsePositive: Proxy Server False Positive Categories	False Positive	Event	Edit this BB to define all the false positive categories that occur to or from proxy servers that are defined in the Default-BB-HostDefinition: Proxy Servers building block.	Default-BB-HostDefinition: Proxy Servers
Default-BB-FalsePositive: Proxy Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from proxy servers that are defined in the Default-BB-HostDefinition: Proxy Servers building block.	Default-BB-HostDefinition: Proxy Servers

Table B-7 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
Default-BB-FalsePositive: Remote Attacker to Internal Target False Positives	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from Remote-to-Local (R2L) based servers.	
Default-BB-FalsePositive: RPC Server False Positive Categories	False Positive	Event	Edit this BB to define all the false positive categories that occur to or from RPC servers that are defined in the Default-BB-HostDefinition: RPC Servers building block.	Default-BB-HostDefinition: RPC Servers
Default-BB-FalsePositive: RPC Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from RPC servers that are defined in the Default-BB-HostDefinition: RPC Servers building block.	Default-BB-HostDefinition: RPC Servers
Default-BB-FalsePositive: SNMP Sender or Receiver False Positive Categories	False Positive	Event	Edit this BB to define all the false positive categories that occur to or from SNMP servers that are defined in the Default-BB-HostDefinition: SNMP Servers building block.	Default-BB-HostDefinition: SNMP Servers
Default-BB-FalsePositive: SNMP Sender or Receiver False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from SNMP servers that are defined in the Default-BB-HostDefinition: SNMP Servers building block.	Default-BB-HostDefinition: SNMP Servers
Default-BB-FalsePositive: Source IP and Specific Event	False Positive	Event	Edit this BB to include source IP addresses or specific events that you wish to remove.	
Default-BB-FalsePositive: SSH Server False Positive Categories	False Positive	Event	Edit this BB to define all the false positive categories that occur to or from SSH servers that are defined in the Default-BB-HostDefinition: SSH Servers building block.	Default-BB-HostDefinition: SSH Servers
Default-BB-FalsePositive: SSH Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from SSH servers that are defined in the Default-BB-HostDefinition: SSH Servers building block.	Default-BB-HostDefinition: SSH Servers
Default-BB-FalsePositive: Syslog Sender False Positive Categories	False Positive	Event	Edit this BB to define all false positive categories that occur to or from syslog sources.	Default-BB-HostDefinition: Syslog Servers and Senders
Default-BB-FalsePositive: Syslog Sender False Positive Events	False Positive	Event	Edit this BB to define all false positive events that occur to or from syslog sources or destinations.	Default-BB-HostDefinition: Syslog Servers and Senders

Table B-7 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
Default-BB-FalsePositive: Virus Definition Update Categories	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from virus definition or other automatic update hosts that are defined in the Default-BB-HostDefinition: Virus Definition and Other Update Servers building block.	Default-BB-HostDefinition: Virus Definition
Default-BB-FalsePositive: Web Server False Positive Categories	False Positive	Event	Edit this BB to define all the false positive categories that occur to or from web servers that are defined in the Default-BB-HostDefinition: Web Servers building block.	Default-BB-HostDefinition: Web Servers
Default-BB-FalsePositive: Web Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from Web servers that are defined in the Default-BB-HostDefinition: Web Servers building block.	Default-BB-HostDefinition: Web Servers
Default-BB-FalsePositive: Windows Server False Positive Categories Local	False Positive	Event	Edit this BB to define all the false positive categories that occur to or from Windows servers that are defined in the Default-BB-HostDefinition: Windows Servers building block.	Default-BB-HostDefinition: Windows Servers
Default-BB-FalsePositive: Windows Server False Positive Events	False Positive	Event	Edit this BB to define all the false positive QIDs that occur to or from Windows servers that are defined in the Default-BB-HostDefinition: Windows Servers building block.	Default-BB-HostDefinition: Windows Servers
Default-BB-Host Definition: Database Servers	Host Definitions	Event	Edit this BB to define typical database servers.	Default-BB-FalsePositive: Database Server False Positive Categories Default-BB-FalsePositive: Database Server False Positive Events
Default-BB-Host Definition: DHCP Servers	Host Definitions	Event	Edit this BB to define typical DHCP servers.	Default-BB-False Positive: DHCP Server False Positives Categories Default-BB-FalsePositive: DHCP Server False Positive Events
Default-BB-Host Definition: DNS Servers	Host Definitions	Event	Edit this BB to define typical DNS servers.	Default-BB-False Positive: DNS Server False Positives Categories Default-BB-FalsePositive: DNS Server False Positive Events

Table B-7 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
Default-BB-Host Definition: FTP Servers	Host Definitions	Event	Edit this BB to define typical FTP servers.	Default-BB-False Positive: FTP Server False Positives Categories Default-BB-FalsePositive: FTP Server False Positive Events
Default-BB-Host Definition: Host with Port Open	Host Definitions	Event	Edit this BB to include a host and port that is actively or passively seen.	
Default-BB-Host Definition: LDAP Servers	Host Definitions	Event	Edit this BB to define typical LDAP servers.	Default-BB-False Positive: LDAP Server False Positives Categories Default-BB-FalsePositive: LDAP Server False Positive Events
Default-BB-Host Definition: Mail Servers	Host Definitions	Event	Edit this BB to define typical mail servers.	Default-BB-False Positive: Mail Server False Positives Categories Default-BB-FalsePositive: Mail Server False Positive Events
Default-BB-Host Definition: Network Management Servers	Host Definitions	Event	Edit this BB to define typical network management servers.	
Default-BB-Host Definition: Proxy Servers	Host Definitions	Event	Edit this BB to define typical proxy servers.	Default-BB-False Positive: Proxy Server False Positives Categories Default-BB-FalsePositive: Proxy Server False Positive Events
Default-BB-Host Definition: RPC Servers	Host Definitions	Event	Edit this BB to define typical RPC servers.	Default-BB-False Positive: RPC Server False Positives Categories Default-BB-FalsePositive: RPC Server False Positive Events
Default-BB-Host Definition: Servers	Host Definitions	Event	Edit this BB to define generic servers.	
Default-BB-Host Definition: SNMP Sender or Receiver	Host Definitions	Event	Edit this BB to define SNMP senders or receivers.	Default-BB-PortDefinition: SNMP Ports

Table B-7 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
Default-BB-Host Definition: SSH Servers	Host Definitions	Event	Edit this BB to define typical SSH servers.	Default-BB-False Positive: SSH Server False Positives Categories Default-BB-FalsePositive: SSH Server False Positive Events
Default-BB-Host Definition: Syslog Servers and Senders	Host Definitions	Event	Edit this BB to define typical host that send or receive syslog traffic.	Default-BB-FalsePositive: Syslog Server False Positive Categories Default-BB-FalsePositive: Syslog Server False Positive Events
Default-BB-Host Definition: VA Scanner Source IP	Host Definitions	Event	Edit this BB to include the source IP address of your VA scanner. By default, this BB applies when the source IP address is 127.0.0.2.	
Default-BB-Host Definition: Virus Definition and Other Update Servers	Host Definitions	Event	Edit this BB to include all servers that include virus protection and update functions.	
Default-BB-Host Definition: VoIP IP PBX Server	Host Definitions	Event	Edit this BB to define typical VoIP IP PBX servers.	
Default-BB-Host Definition: Web Servers	Host Definitions	Event	Edit this BB to define typical web servers.	Default-BB-False Positive: Web Server False Positives Categories Default-BB-FalsePositive: Web Server False Positive Events
Default-BB-Host Definition: Windows Servers	Host Definitions	Event	Edit this BB to define typical Windows servers, such as domain controllers or exchange servers.	Default-BB-False Positive: Windows Server False Positives Categories Default-BB-FalsePositive: Windows Server False Positive Events
Default-BB-Network Definition: Broadcast Address Space	Network Definition	Event	Edit this BB to include the broadcast address space of your network. This is used to remove false positive events that may be caused by the use of broadcast messages.	
Default-BB-Network Definition: Client Networks	Network Definition	Event	Edit this BB to include all networks that include client hosts.	

Table B-7 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
Default-BB-Network Definition: Honeypot like Addresses	Network Definition	Event	Edit this BB by replacing the <i>other</i> network with network objects defined in your network hierarchy that are currently not in use in your network or are used in a honeypot or tarpit installation. Once these have been defined, you must enable the Default-Rule-Anomaly: Potential Honeypot Access rule. You must also add a security/policy sentry to these network objects to generate events based on attempted access.	
Default-BB-Network Definition: NAT Address Range	Network Definition	Event	Edit this BB to define typical Network Address Translation (NAT) range you wish to use in your deployment.	
Default-BB-Network Definition: Server Networks	Network Definition	Event	Edit this BB to include the networks where your servers are located.	
Default-BB-Network Definition: Undefined IP Space	Network Definition	Event	Edit this BB to include areas of your network that does not contain any valid hosts.	
Default-BB-Policy: Application Policy Violation Events	Policy	Event	Edit this BB to define policy application and violation events.	
Default-BB-Policy: IRC/IM Connection Violations	Policy	Event	Edit this BB to define all policy IRC/IM connection violations.	
Default-BB-Policy: Policy P2P	Policy	Event	Edit this BB to include all events that indicate Peer-to-Peer (P2P) events.	
Default-BB-PortDefinition: Database Ports	Port\ Protocol Definition	Event	Edit this BB to include all common database ports.	
Default-BB-PortDefinition: DHCP Ports	Port\ Protocol Definition	Event	Edit this BB to include all common DHCP ports.	
Default-BB-PortDefinition: DNS Ports	Port\ Protocol Definition	Event	Edit this BB to include all common DNS ports.	
Default-BB-PortDefinition: FTP Ports	Port\ Protocol Definition	Event	Edit this BB to include all common FTP ports.	
Default-BB-PortDefinition: Game Server Ports	Port\ Protocol Definition	Event	Edit this BB to include all common game server ports.	

Table B-7 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
Default-BB-PortDefinition: IM Ports	Compliance, Port\ Protocol Definition	Event	Edit this BB to include all common IM ports.	
Default-BB-PortDefinition: IRC Ports	Port\ Protocol Definition	Event	Edit this BB to include all common IRC ports.	
Default-BB-PortDefinition: LDAP Ports	Port\ Protocol Definition	Event	Edit this BB to include all common ports used by LDAP servers.	
Default-BB-PortDefinition: Mail Ports	Port\ Protocol Definition	Event	Edit this BB to include all common ports used by mail servers.	
Default-BB-PortDefinition: P2P Ports	Port\ Protocol Definition	Event	Edit this BB to include all common ports used by Peer-to-Peer (P2P) servers.	
Default-BB-PortDefinition: Proxy Ports	Port\ Protocol Definition	Event	Edit this BB to include all common ports used by proxy servers.	
Default-BB-PortDefinition: RPC Ports	Port\ Protocol Definition	Event	Edit this BB to include all common ports used by RPC servers.	
Default-BB-PortDefinition: SNMP Ports	Port\ Protocol Definition	Event	Edit this BB to include all common ports used by SNMP servers.	
Default-BB-PortDefinition: SSH Ports	Port\ Protocol Definition	Event	Edit this BB to include all common ports used by SSH servers.	
Default-BB-PortDefinition: Syslog Ports	Port\ Protocol Definition	Event	Edit this BB to include all common ports used by the syslog servers.	
Default-BB-PortDefinition: Web Ports	Port\ Protocol Definition	Event	Edit this BB to include all common ports used by Web servers.	
Default-BB-PortDefinition: Windows Ports	Port\ Protocol Definition	Event	Edit this BB to include all common ports used by Windows servers.	
Default-BB-Protocol Definition: Windows Protocols	Port\ Protocol Definition	Event	Edit this BB to include all common protocols (not including TCP) used by Windows servers that will be ignored for false positive tuning rules.	

Table B-7 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
Default-BB-Recon Detected: All Recon Rules	Recon	Event	Define all Juniper default reconnaissance tests. This BB is used to detect a host that has performed reconnaissance such that other follow on tests can be performed. For example, reconnaissance followed by firewall accept.	
Default-BB-Recon Detected: Devices That Merge Recon into Single Event	Recon	Event	Edit this BB to include all devices that accumulate reconnaissance across multiple hosts or ports into a single event. This rule forces these events to become offenses.	
Default-BB-Recon Detected: Host Portscan	Recon	Event	Edit this BB to define reconnaissance scans on hosts in your deployment.	
Default-BB-Recon Detected: Port Scan Detected Across Multiple Hosts	Recon	Event	Edit this BB to indicate port scanning activity across multiple hosts. By default, this BB applies when an attacker is performing reconnaissance against more than 5 hosts within 10 minutes. If internal, this may indicate an exploited machine or a worm scanning for targets.	
User-BB-FalsePositive: User Defined False Positives Tunings	User Tuning	Event	This BB contains any events that you have tuned using the False Positive tuning function. For more information, see the <i>STRM Users Guide</i> .	

A

GLOSSARY

Autonomous System Number	Collection of IP networks that all adhere to the same specific and clearly defined routing policy. An AS number (ASN) is a unique ID number assigned to each Autonomous System.
Address Resolution Protocol (ARP)	A protocol for mapping an Internet Protocol (IP) address to a physical machine address recognized in the local network. For example, in IP Version 4, an address is 32 bits long. In an Ethernet LAN, however, addresses for attached devices are 48 bits long.
anomaly	A deviation from expected behavior of the network.
ARP	See Address Resolution Protocol.
ARP Redirect	ARP allows a host to determine the address of other devices on the LAN or VLAN. A host can use ARP to identify the default gateway (router) or path off to the VLAN. ARP Redirect allows STRM to notify a host if a problem exists with sending traffic to a system. This renders the host and network unusable until the user intervenes.
ASN	See Autonomous System Number.
branding	A reporting option that enables a STRM user to upload custom logos for customized reports.
CIDR	See Classless Inter-Domain Routing.
Classless Inter-Domain Routing (CIDR)	Addressing scheme for the Internet, which allocates and species Internet addresses used in inter-domain routing. With CIDR, a single IP address can be used to designate many unique IP addresses.
client	The host that originates communication.
coalescing interval	The interval for coalescing (bundling) events is 10 seconds, beginning with the first event that does not match any currently coalescing events. Within the interval, the first three matching events are released immediately to the Event Processor and the fourth and subsequent events are coalesced such that the payload and other features are kept from the fourth event. Each arrival of a matching event during the interval increments the event count of the fourth event. At the end of the interval,

the coalesced event is released to the Event Processor and the next interval begins for matching events. If no matching events arrive during this interval, the process restarts. Otherwise, the coalescing continues with all events counted and released in 10 second intervals.

Console	Web interface for STRM. STRM is accessed from a standard web browser (preferably Internet Explorer 6.0 /7.0 or Mozilla Firefox 2.0). When you access the system, a prompt appears for a user name and password, which must be configured in advance by the STRM administrator.
credibility	Indicates the integrity of an event as determined by the credibility rating from source devices. Credibility increases as the multiple sources report the same event.
database leaf objects	The end point objects in a hierarchy. At each point in the hierarchy above this point there would be a parent object that contains the aggregate values of all of the leaf objects below.
datapoint	Any point on the STRM graphs where data is extracted.
DHCP	See Dynamic Host Configuration Protocol.
DNS	See Domain Name System.
Domain Name System (DNS)	An on-line, distributed database used to map human-readable machine names into IP address for resolving machine names to IP addresses.
Dynamic Host Configuration Protocol (DHCP)	A protocol that allows dynamic assignment of IP addresses to customer premise equipment.
Encryption	Encryption provides greater security for all STRM traffic between managed hosts. When encryption is enabled for a managed host, encryption tunnels are created for all client applications on a managed host to provide protected access to the respective servers.
external data views	Require input from external products, such as an IDS engine (for example, SNORT) or firewalls (for example, Cisco PIX or Checkpoint Firewall). These external products provide information to STRM on specified IP addresses that are correlated to the flows responsible. STRM monitors flows between these systems and tags traffic between the hosts for a configured period of time.
event	Record from a device that describes an action on a network or host.
Event Collector	Collects security events from various types of security devices in your network. The Event Collector gathers events from local, remote, and device sources. The Event Collector then normalizes the events and sends the information to the Event Processor.

Event Processor	Processes flows collected from one or more Event Collector(s). The events are bundled once again to conserve network usage. Once received, the Event Processor correlates the information from STRM and distributed to the appropriate area, depending on the type of event.
Fully Qualified Domain Name (FQDN)	The portion of an Internet Uniform Resource Locator (URL) that fully identifies the server program that an Internet request is addressed to.
Fully Qualified Network Name (FQNN)	Full path name of a certain point in the network hierarchy. For example, Company A's hierarchy has a department object that contains a marketing object. Therefore, the FQNN is CompanyA.Department.Marketing.
FQDN	See Fully Qualified Domain Name.
FQNN	See Fully Qualified Network Name.
gateway	A device that communicates with two protocols and translates services between them.
Host Context	Monitors all STRM components to ensure that each component is operating as expected.
ICMP	See Internet Control Message Protocol.
IDS	See Intrusion Detection System.
Internet Control Message Protocol (ICMP)	An Internet network-layer protocol between a host and gateway.
Internet Protocol (IP)	The method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other systems on the Internet. An IP address includes a network address and a host address. An IP address can also be divided by using classless addressing or subnetting.
Internet Service Provider (ISP)	An Internet Service Provider (ISP) provides users access to the Internet and other related services.
interval	The default time period in the system. Affects the update intervals of the graphs and how much time each flow log file contains.
Intrusion Detection System (IDS)	An application or device that identifies suspicious activity on the network.
Intrusion Prevention System (IPS)	Application that reacts to network intrusions. Offense Resolution is an IPS.

IP	See Internet Protocol.
IP Multicast	IP Multicast reduces traffic on a network by delivering a single stream of information to multiple users at one time.
IP network	A group of IP routers that route IP datagrams. These routers are sometimes referred to as Internet gateways. Users access the IP network from a host. Each network in the Internet includes some combination of hosts and IP routers.
IPS	See Intrusion Prevention System.
ISP	See Internet Service Provider.
item	A Dashboard option that creates a customized portal that displays any permissible view for monitoring purposes.
L2L	See Local To Local.
L2R	See Local To Remote.
LAN	See Local Area Network.
LDAP	See Lightweight Directory Access Protocol.
leaves	Children or objects which are part of a parent group.
Lightweight Directory Access Protocol (LDAP)	A set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. And unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access to a directory server.
Local Area Network (LAN)	A non-public data network in which serial transmission is used for direct data communication among data stations located on the user's premises.
Local To Local (L2L)	Internal traffic from one local network to another local network.
Local To Remote (L2R)	Internal traffic from a local network to a remote network.
magnitude	Specifies the relative importance of the event. The magnitude bar provides a visual representation of all the correlated variables of the event. Variables include Relevance, Severity, and Credibility.
NAT	NAT translates an IP address in one network to a different IP address in another network.
Network Address Translation (NAT)	See NAT.

network hierarchy	Contains each component of your network, and identifies which objects belong within other objects. The accuracy and completeness of this hierarchy is essential to traffic analysis functions. The network hierarchy provides for storage of flow logs, databases, and TopN files.
network objects	Components of your network hierarchy. You can add layers to the hierarchy by adding additional network objects and associating them to already defined objects. (Objects that contain other objects are called groups.)
Network Weight	The numerical value applied to each network that signifies the importance of the network. The Network weight is user defined.
Open Systems Interconnection (OSI)	A framework of ISO standards for communication between different systems made by different vendors, in which the communications process is organized into seven different categories that are placed in a layered sequence based on their relationship to the user. Each layer uses the layer immediately below it and provides a service to the layer above. Layers 7 through 4 deal with end-to-end communication between the message source and destination, and layers 3 through 1 deal with network functions.
OSI	See Open Systems Interconnection.
protocol	A set of rules and formats that determines the communication behavior of layer entities in the performance of the layer functions. It may still require an authorization exchange with a policy module or external policy server prior to admission.
QID	STRM Identifier. A mapping of a single event of an external device to a Q1 Labs unique identifier.
STRM Time	The right corner of the STRM interface displays STRM time, which is the time of the STRM Console. This is the time that determines the time of events and offenses.
refresh timer	Dashboard features a dynamic status bar that displays the amount of time until STRM automatically refreshes the current network activity data; built-in refresh can be manually refreshed at any time.
relevance	Relevance determines the significance of an event, category or offense.
reports	A function that creates executive or operational level charting representations of network activity based on time, attackers, offenses, security, and events.
report interval	A configurable time interval at which the Flow Processor must send all captured flow data to the Console.
rule	Collection of conditions and consequent actions. You can configure rules that allow STRM to capture and respond to specific event sequences. The rules allow

you to detect specific, specialized events and forward notifications to either the Offense Manager or log file, e-mail a user, or resolve the event or offense, if the Offense Resolution option is active.

severity	Indicates the amount of threat an attacker poses in relation to how prepared the target is for the attack. This value is mapped to an event category that is correlated to the offense.
Simple Network Management Protocol (SNMP)	A network management protocol used to monitor IP routers, other network devices, and the networks to which they attach.
SNMP	See Simple Network Management Protocol.
subnet	A network subdivided into networks or subnets. When subnetting is used, the host portion of the IP address is divided into a subnet number and a host number. Hosts and routers identify the bits used for the network and subnet number through the use of a subnet mask.
subnet mask	A bit mask that is logically ANDed with the destination IP address of an IP packet to determine the network address. A router routes packets using the network address.
TACACS	Terminal Access Controller Access Control System (TACACS) is an authentication protocol that allows remote server access to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system. TACACS+ uses TCP.
TCP	See Transmission Control Protocol.
TCP flags	A type of marker that can be added to a packet to alert the system of abnormal activity. Only a few specific combinations of flags are valid and typical, in normal traffic. Abnormal combinations of flags often indicate an attack or an abnormal network condition.
TCP resets	For TCP-based applications, STRM can issue a TCP reset to either the client or server in a conversation. This stops the communications between the client and the server.
Time Series	A reporting chart that graphs data based on time. This chart focuses on the networks or IP address data information from the selected networks.
TopN Time Series	A reporting graph option that focuses on the top N networks or IP address data information, based on time, for the data you are graphing.
Transmission Control Protocol (TCP)	A reliable stream service that operates at the transport-layer Internet protocol, which ensures successful end-to-end delivery of data packets without error.

violation	Includes a violation of corporate policy.
Whois	Allows you to look up information about registered Internet names and numbers.

INDEX

A

Administration Console
overview 8

B

branding reports 88
building blocks
about 35
default 101
editing 58

C

conventions 1
customer support
contacting 1

D

dashboard 9
about 9
adding items 13
events 10
events by severity 11
events over time 10
overview 4
reports 12
summary 12
top devices 11
using 10
default rules 91
detaching an item 10

E

Enterprise Vulnerability State 12
event mapping 31
event rule
data/time tests 51
device tests 52
event property tests 47
IP/port tests 50
test 47
event viewer
event mapping 31
false positive tuning 33
overview 5
right-click 16
searching events 27
toolbar 16
using 15

viewing associated offense 31
events
aggregate 21
exporting 33
normalized 17
searching 27
viewing 17
exporting
events 33

F

false positives
tuning 33
functions 35

G

generating a report 87
glossary 115

I

IP addresses
investigating 6

M

mapping events 31

N

normalized events 17

P

pausing the interface 6

Q

STRM Log Management
overview 3
using 6

R

raw events 20
refreshing the interface 6
removing an item 10
report templates
default 86

reports

- about 61
 - brand 88
 - chart type 76
 - container 68
 - content 68
 - creating 68
 - creating a template 69
 - default templates 86
 - distribution channels 73
 - editing 86
 - formatting 73
 - generate 87
 - graph type 85
 - grouping 64
 - assigning 68
 - copying 66
 - creating 65
 - deleting 67
 - editing 66
 - layout 68
 - layout preview 72
 - navigation menu 62
 - overview 5
 - scheduling options 69
 - selecting a container 72
 - selecting the layout 71
 - summary 75
 - template 69
 - time series chart 79
 - toolbar 63
 - using the interface 62
 - viewing 63
- rules 35
- copying 52
 - creating 37
 - deleting 53
 - enabling/disabling 37
 - group 53
 - assigning 58
 - copying 56
 - create 54
 - deleting 57
 - editing 55
 - viewing 36

S

- sorting results 6
-

T

- tests
 - about 35
- time series 79
- TopN time series 82