



Security Threat Response Manager

STRM Log Manager Administration Guide

Release 2009.2

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Published: 2010-04-01

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 Manager Administration Guide
Release 2009.2

Copyright © 2008, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Revision History

April 2010—Revision 1

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

CONTENTS

ABOUT THIS GUIDE

Audience	1
Conventions	1
Technical Documentation	1
Contacting Customer Support	2

1 OVERVIEW

About the Interface	3
Using the Interface	4
Deploying Changes	4
About High Availability	4

2 MANAGING USERS

Managing Roles	7
Viewing Roles	7
Creating a Role	8
Editing a Role	11
Deleting a Role	12
Managing User Accounts	13
Creating a User Account	13
Editing a User Account	14
Disabling a User Account	15
Authenticating Users	16

3 MANAGING THE SYSTEM

Managing Your License Keys	19
Updating your License Key	20
Exporting Your License Key Information	21
Restarting a System	22
Shutting Down a System	22
Configuring Access Settings	22
Configuring Firewall Access	23
Updating Your Host Set-up	25
Configuring Interface Roles	26
Changing Passwords	27
Updating System Time	28

4 MANAGING HIGH AVAILABILITY

- Adding an HA Cluster 34
- Editing an HA Cluster 40
- Setting an HA Host Offline 41
- Setting an HA Host Online 42
- Restoring a Failed Host 42

5 SETTING UP STRM LOG MANAGER

- Creating Your Network Hierarchy 45
 - Considerations 45
 - Defining Your Network Hierarchy 46
- Scheduling Automatic Updates 49
 - Scheduling Automatic Updates 50
 - Updating Your Files On-Demand 53
- Configuring System Settings 54
- Configuring System Notifications 58
- Configuring the Console Settings 60

6 MANAGING BACKUP AND RECOVERY

- Managing Backup Archives 65
 - Viewing Back Up Archives 65
 - Importing an Archive 67
 - Deleting a Backup Archive 67
- Backing Up Your Information 68
 - Scheduling Your Backup 68
 - Initiating a Backup 71
- Restoring Your Configuration Information 72
 - Restoring on a System with the Same IP Address 72
 - Restoring to a System with a Different IP Address 73

7 USING THE DEPLOYMENT EDITOR

- About the Deployment Editor 78
 - Accessing the Deployment Editor 79
 - Using the Editor 79
 - Creating Your Deployment 81
 - Before you Begin 81
 - Editing Deployment Editor Preferences 82
- Building Your Event View 82
 - Adding Components 83
 - Connecting Components 83
 - Forwarding Normalized Events 84
 - Renaming Components 87
- Managing Your System View 87
 - Setting Up Managed Hosts 88
 - Using NAT with STRM Log Manager 93
 - Configuring a Managed Host 97

Assigning a Component to a Host	97
Configuring Host Context	98
Configuring STRM Log Manager Components	100
Configuring an Event Collector	100
Configuring an Event Processor	102

8 FORWARDING SYSLOG DATA

Adding a Syslog Destination	105
Editing a Syslog Destination	106
Delete a Syslog Destination	107

A JUNIPER NETWORKS MIB

B VIEWING AUDIT LOGS

Logged Actions	123
Viewing the Log File	126

INDEX

ABOUT THIS GUIDE

The *STRM Log Manager Administration Guide* provides you with information for managing STRM Log Manager functionality requiring administrative access.




Audience

This guide is intended for the system administrator responsible for setting up STRM Log Manager in your network. This guide assumes that you have STRM Log Manager administrative access and a knowledge of your corporate network and networking technologies.

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 customer support web site at <https://www.juniper.net/support/>. Once you access the Juniper customer 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: techpubs-comments@juniper.net.

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, you can contact customer support as follows:

- Open a support case using the Case Management link at <http://www.juniper.net/support/>.
- Call 1-888-314-JTAC (from the United States, Canada, or Mexico) or 1-408-745-9500 (from elsewhere).

1

OVERVIEW

This chapter provides an overview of the STRM Log Manager administrative functionality including:

- [About the Interface](#)
- [Using the Interface](#)
- [Deploying Changes](#)
- [About High Availability](#)

About the Interface

You must have administrative privileges to access the administrative functions. To access administrative functions, click the **Admin** tab in the STRM Log Manager interface. The Admin tab provides access to the following functions.

- Manage users. See [Chapter 2 Managing Users](#).
- Manage your network settings. See [Chapter 3 Managing the System](#).
- Manage STRM Log Manager settings. See [Chapter 5 Setting Up STRM Log Manager](#).
- Backup and recover your data. See [Chapter 6 Managing Backup and Recovery](#).
- Manage your deployment views. See [Chapter 7 Using the Deployment Editor](#).
- Configure syslog forwarding. See [Chapter 8 Forwarding Syslog Data](#).
- Manage log sources. For more information, see the *Log Sources Users Guide*.

All configuration updates using the Admin tab 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.

Using the Interface

The Admin tab provides several tab and menu options that allow you to configure STRM Log Manager including:

- **System Configuration** - Provides access to administrative functionality, such as user management, automatic updates, license key, network hierarchy, system settings, system notifications, backup and recovery, and Console configuration.
- **Data Sources** - Provides access to log source management, syslog forwarding, and custom event properties.

The Admin Tab also includes several menu options including:

Table 2-1 Admin Tab Menu Options

Menu Option	Sub-Menu	Description
Deployment Editor		Opens the deployment editor interface.
Deploy Changes		Deploys any configuration changes from the current session to your deployment.
Advanced	Deploy Full Configuration	Deploys all changes.

Deploying Changes

Once you update your configuration settings using the Admin tab, you must save those changes to the staging area. You must either manually deploy all changes using the Deploy Changes button or, upon exit, a window appears prompting you to deploy changes before you exit. All deployed changes are then applied throughout your deployment.

Using the Admin tab menu, you can deploy changes as follows:

- **Advanced > Deploy Full Configuration** - Deploys all configuration settings to your deployment.
- **Deploy Changes** - Deploys any configuration changes from the current session to your deployment.

About High Availability

The High Availability (HA) feature ensures availability of STRM Log Manager data in the event of a hardware or network failure. Each HA cluster consists of a primary host and a standby secondary host. The secondary host maintains the same data as the primary host by either replicating the data on the primary host or accessing a shared external storage. At regular intervals, every 10 seconds by default, the secondary host sends a heartbeat ping to the primary host to detect hardware or network failure. If the secondary host detects a failure, the secondary host automatically assumes all responsibilities of the primary host.



Note: HA is not supported in an IPv6 environment.

For more information about managing HA clusters, see [Chapter 4 Managing High Availability](#).

2

MANAGING USERS

You can add or remove user accounts for all users that you want to access STRM Log Manager. Each user is associated with a role, which determines the privileges the user has to functionality and information within STRM Log Manager. You can also restrict or allow access to areas of the network.

This chapter provides information on managing STRM Log Manager users including:

- [Managing Roles](#)
- [Managing User Accounts](#)
- [Authenticating Users](#)

Managing Roles

You must create a role before you can create user accounts. By default, STRM Log Manager provides a default administrative role, which provides access to all areas of STRM Log Manager. A user that is assigned administrative privileges (including the default administrative role) cannot edit their own account. Another administrative user must make any desired changes.

Using the Admin tab, you can:

- View roles. See [Viewing Roles](#).
- Create a role. See [Creating a Role](#).
- Edit a role. See [Editing a Role](#).
- Delete a user role. See [Deleting a Role](#).

Viewing Roles

To view roles:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **System Configuration**.
The System Configuration panel appears.
- Step 3** Click the **User Roles** icon.
The Manage Roles window appears.



The Manage Roles window provides the following information:

Table 3-1 Manage Roles Parameters

Parameter	Description
Role	Specifies the defined user role.
Log Sources	<p>Specifies the log sources you want this role to access. This allows you to restrict or grant access for users assigned to the role to view log and event data received from assigned security and network log sources or log source groups.</p> <p>For non-administrative users, this column indicates a link that allows an administrative user to edit the permissions for the role. For more information on editing a user role, see Editing a Role.</p> <p>To view the list of log sources that have been assigned to this role, move your mouse over the text in the Log Sources column.</p>
Associated Users	Specifies the users associated with this role.
Action	Allows you to edit or delete the user role.

Creating a Role To create a role:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **System Configuration**.
The System Configuration panel appears.
- Step 3** Click the **User Roles** icon.
The Manage User Roles window appears.
- Step 4** Click **Create Role**.
The Manage Role Permissions window appears.

Step 5 Enter values for the parameters. You must select at least one permission to proceed.

Create Roles Parameters

Parameter	Description
Role Name	Specify the name of the role. The name can be up to 15 characters in length and must only contain integers and letters.
Admin	<p>Select the check box if you want to grant this user administrative access to the STRM Log Manager interface. Within the administrator role, you can grant additional access to the following:</p> <ul style="list-style-type: none"> • Administrator Manager - Select this check box if you want to allow users the ability to create and edit other administrative user accounts. If you select this check box, the System Administrator check box is automatically selected. • System Administrator - Select this check box if you want to allow users access to all areas of STRM Log Manager. Users with this access are not able to edit other administrator accounts.

Create Roles Parameters (continued)

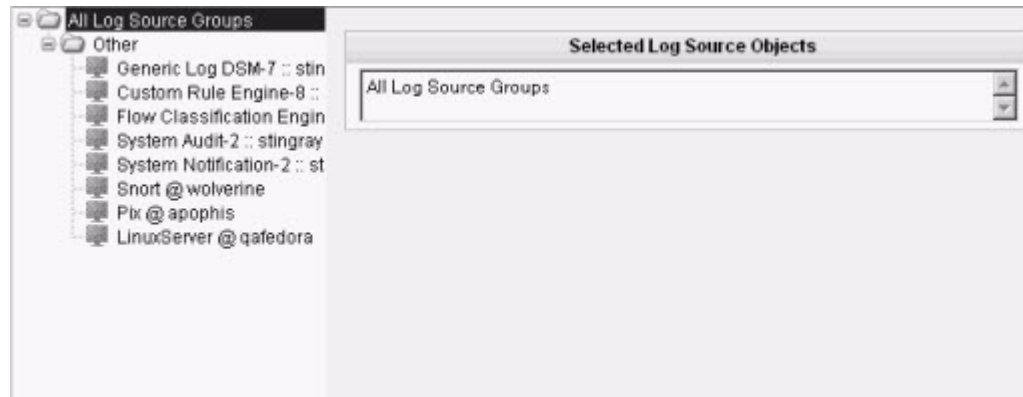
Parameter	Description
Events	<p>Select the check box if you want this user to have access to the Events interface. Within the Events role, you can also grant users additional access to the following:</p> <ul style="list-style-type: none"> • Customized Rule Creation - Select the check box if you want to allow users to create rules using the Events interface. • User Defined Event Properties - Select the check box if you want to allow users the ability to create user-defined event properties. • Event Search Restrictions Override - Select the check box if you want to allow users the ability to override event search restrictions. <p>For more information on the Events interface, see the <i>STRM Log Manager Users Guide</i>.</p>
Reports	<p>Select the check box if you want to grant this user access to Reporting functionality. Within the Reporting functionality, you can grant users additional access to the following:</p> <ul style="list-style-type: none"> • Maintain Templates - Select the check box if you want to allow users to maintain reporting templates. • Distribute Reports via Email - Select the check box if you want to allow users to distribute reports through e-mail. <p>For more information, see the <i>STRM Log Manager Users Guide</i>.</p>
IP Right Click Menu Extensions	Select the check box if you want to grant this user access to options added to the right mouse button (right-click) menu.

Step 6 Click **Next**.

Step 7 Choose one of the following options:

- a If you selected a role that includes the Events permissions role, go to [Step 8](#).
- b If you selected a role that does *not* include the Event permissions, go to [Step 11](#).

The Add Log Sources to User Role window appears.



Step 8 From the menu tree, locate and select a log source that you want user assigned to this role to have access.

The selected device moves to the Selected Log Source Objects field.

Step 9 Repeat for all log sources.

Step 10 Click **Next**.

Step 11 Click **Return**.

Step 12 Close the Manage Roles window.

Step 13 From the Admin tab menu, click **Deploy Changes**.

Editing a Role To edit a role:


Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **System Configuration**.

The System Configuration panel appears.

Step 3 Click the **User Roles** icon.

The Manage Roles window appears.

Step 4 For the role you want to edit, click the edit  icon.

The Manage Role Permissions window appears.

Step 5 Update the permissions (see [Table 3-2](#)), as necessary.

Step 6 Click **Next**.

Step 7 Choose one of the following options:

- a If you selected a role that includes the Events permissions role, go to [Step 8](#).
- b If you selected a role that does *not* include the Event permissions, go to [Step 11](#).

The Add Log Sources to User Role window appears.



- Step 8** Update log source permissions, as desired:
- a To remove a log source permission, select the log source(s) in the Selected Log Source Objects field that you want to remove. Click **Remove Selected Devices**.
 - b To add a log source permission, select an object you want to add from the left panel.
- Step 9** Repeat for all log sources you want to edit for this role.
- Step 10** Click **Next**.
- Step 11** Click **Return**.
- Step 12** Click **Save**.
- Step 13** Close the Manage User Roles window.
The Admin tab appears.
- Step 14** From the Admin tab menu, click **Deploy Changes**.

Deleting a Role To delete a role:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **System Configuration**.
The System Configuration panel appears.
- Step 3** Click the **User Roles** icon.
The Manage Role window appears.
- Step 4** For the role you want to delete, click the delete icon.
A confirmation window appears.
- Step 5** Click **Ok**.
- Step 6** From the Admin tab menu, click **Deploy Changes**.

Managing User Accounts

You can create a STRM Log Manager user account, which allows a user access to selected network components using the STRM Log Manager interface. You can also create multiple accounts for your system that include administrative privileges. Only the main administrative account can create accounts that have administrative privileges.

You can create and edit user accounts to access STRM Log Manager including:

- [Creating a User Account](#)
- [Editing a User Account](#)
- [Disabling a User Account](#)

Creating a User Account

To create an account for a STRM Log Manager user:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **System Configuration**.
The System Configuration panel appears.
- Step 3** Click the **Users** icon.
The Manage Users window appears.
- Step 4** In the Manage Users area, click **Add**.
The User Details window appears.

- Step 5** Enter values for the following parameters:

Table 3-2 User Details Parameters

Parameter	Description
Username	Specify a username for the new user. The username must not include spaces or special characters.
Password	Specify a password for the user to gain access. The password must be at least five characters in length.
Confirm Password	Re-enter the password for confirmation.
Email Address	Specify the user's e-mail address.

Table 3-2 User Details Parameters (continued)

Parameter	Description
Role	Using the drop-down list box, select the role you want this user to assume. For information on roles, see Managing Roles . If you select Admin , this process is complete.

Step 6 Click **Next**.

Step 7 Choose one of the following options:

- a If you selected Admin as the user role, go to [Step 10](#).
- b If you selected a non-administrative user role, go to [Step 8](#).

The Selected Network Objects window appears.



Step 8 From the menu tree, select the network objects you want this user to be able to monitor.

The selected network objects appear in the Selected Network Object panel.

Step 9 Click **Finish**.

Step 10 Close the Manage Users window.

The Admin interface appears.

Editing a User Account To edit a user account:

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **System Configuration**.

The System Configuration panel appears.

Step 3 Click the **Users** icon.

The Manage Users window appears.

Step 4 In the Manage Users area, click the user account you want to edit.

The User Details window appears.

Step 5 Update values (see [Table 3-2](#)), as necessary.

Step 6 Click **Next**.

If you are editing a non-administrative user account, the Selected Network Objects window appears. If you are editing an administrative user account, go to [Step 10](#).

Step 7 From the menu tree, select the network objects you want this user to access.

The selected network objects appear in the Selected Network Object panel.

Step 8 For all network objects you want to remove access, select the object from the Selected Network Objects panel. Click **Remove**.

Step 9 Click **Finish**.

Step 10 Close the Manage Users window.

The Admin interface appears.

Disabling a User Account To disable a user account:

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **System Configuration**.

The System Configuration panel appears.

Step 3 Click the **Users** icon.

The Manage Users window appears.

Step 4 In the Manage Users area, click the user account you want to disable.

The User Details window appears.

Step 5 In the Role drop-down list box, select **Disabled**.

Step 6 Click **Next**.

Step 7 Close the Manage Users window.

The Admin tab appears. This user no longer has access to the STRM Log Manager interface. If this user attempts to log in to STRM Log Manager, the following message appears: **This account has been disabled**.

After you delete a user, items such as saved searches, reports, sentries, and assigned offenses, will remain associated with the deleted user.

Authenticating Users

You can configure authentication to validate STRM Log Manager users and passwords. STRM Log Manager supports the following user authentication types:

- **System Authentication** - Users are authenticated locally by STRM Log Manager. This is the default authentication type.
- **RADIUS Authentication** - Users are authenticated by a Remote Authentication Dial-in User Service (RADIUS) server. When a user attempts to log in, STRM Log Manager encrypts the password only, and forwards the username and password to the RADIUS server for authentication.
- **TACACS Authentication** - Users are authenticated by a Terminal Access Controller Access Control System (TACACS) server. When a user attempts to log in, STRM Log Manager encrypts the username and password, and forwards this information to the TACACS server for authentication.
- **LDAP/ Active Directory** - Users are authenticated by a Lightweight Directory access Protocol) server using Kerberos.

If you want to configure RADIUS, TACACS, or LDAP/Active Directory as the authentication type, you must:

- Configure the authentication server before you configure authentication in STRM Log Manager.
- Make sure the server has the appropriate user accounts and privilege levels to communicate with STRM Log Manager. See your server documentation for more information.
- Make sure the time of the authentication server is synchronized with the time of the STRM Log Manager server. For more information on setting STRM Log Manager time, see [Chapter 5 Setting Up STRM Log Manager](#).
- Make sure all users have appropriate user accounts and roles in STRM Log Manager to allow authentication with the third-party servers.

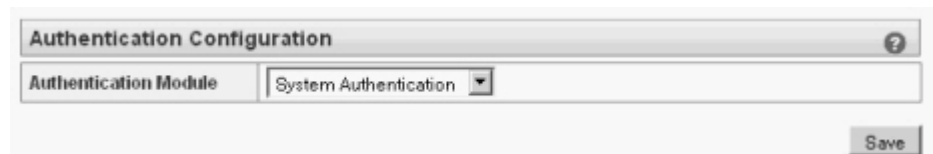
Once authentication is configured and a user enters an invalid username and password combination, a message appears indicating the login was invalid. If the user attempts to access the system multiple times using invalid information, the user must wait the configured amount of time before attempting to access the system again. For more information on configuring system settings for authentication, see [Chapter 5 Setting Up STRM Log Manager - Configuring the Console Settings](#). An administrative user can always access STRM Log Manager through a third-party authentication module or by using the local STRM Log Manager Admin password.

An administrative user can access STRM Log Manager through third-party authentication or the STRM Admin password. The STRM Log Manager Admin password will still function if you have setup and activated a third-party authentication module, however, you can not change the STRM Log Manager Admin password while the authentication module is active. If you want to change the STRM Log Manager admin password, you need to temporarily disable the

third-party authentication module, reset the password, and then reconfigure the third-party authentication module.

To configure authentication:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **System Configuration**.
The System Configuration panel appears.
- Step 3** Click the **Authentication** icon.
The Authentication window appears.



- Step 4** From the Authentication Module drop-down list box, select the authentication type you want to configure.
- Step 5** Configure the selected authentication type:
 - a If you selected **System Authentication**, go to [Step 6](#)
 - b If you selected **RADIUS Authentication**, enter values for the following parameters:

Table 3-3 RADIUS Parameters

Parameter	Description
RADIUS Server	Specify the hostname or IP address of the RADIUS server.
RADIUS Port	Specify the port of the RADIUS server.
Authentication Type	Specify the type of authentication you want to perform. The options are: <ul style="list-style-type: none"> • CHAP (Challenge Handshake Authentication Protocol) - Establishes a Point-to-Point Protocol (PPP) connection between the user and the server. • MSCHAP (Microsoft Challenge Handshake Authentication Protocol) - Authenticates remote Windows workstations. • ARAP (Apple Remote Access Protocol) - Establishes authentication for AppleTalk network traffic. • PAP (Password Authentication Protocol) - Sends clear text between the user and the server.
Shared Secret	Specify the shared secret that STRM Log Manager uses to encrypt RADIUS passwords for transmission to the RADIUS server.

- c If you selected **TACACS Authentication**, enter values for the following parameters:

Table 3-4 TACACS Parameters

Parameter	Description
TACACS Server	Specify the hostname or IP address of the TACACS server.
TACACS Port	Specify the port of the TACACS server.
Authentication Type	Specify the type of authentication you want to perform. The options are: <ul style="list-style-type: none"> • ASCII • PAP (Password Authentication Protocol) - Sends clear text between the user and the server. • CHAP (Challenge Handshake Authentication Protocol) - Establishes a PPP connection between the user and the server. • MSCHAP (Microsoft Challenge Handshake Authentication Protocol) - Authenticates remote Windows workstations. • MSCHAP2 - (Microsoft Challenge Handshake Authentication Protocol version 2)- Authenticates remote Windows workstations using mutual authentication. • EAPMD5 (Extensible Authentication Protocol using MD5 Protocol) - Uses MD5 to establish a PPP connection.
Shared Secret	Specify the shared secret that STRM Log Manager uses to encrypt TACACS passwords for transmission to the TACACS server.

- d If you selected **LDAP/ Active Directory**, enter values for the following parameters:

Table 3-5 LDAP/ Active Directory Parameters

Parameter	Description
Server URL	Specify the URL used to connect to the LDAP server. For example, ldap://<host>:<port>
LDAP Context	Specify the LDAP context you want to use, for example, DC=Q1LABS,DC=INC.
LDAP Domain	Specify the domain you want to use, for example q1labs.inc

Step 6 Click **Save**.

3

MANAGING THE SYSTEM

This chapter provides information for managing your system including:

- [Managing Your License Keys](#)
- [Restarting a System](#)
- [Shutting Down a System](#)
- [Configuring Access Settings](#)

Managing Your License Keys

For your STRM Log Manager Console, a default license key provides you access to the interface for 5 weeks. You must manage your license key using the System and License Management window, which you can access using the Admin tab. This window provides the status of the license key for each system (host) in your deployment including:

- **Valid** - The license key is valid.
- **Expired** - The license key has expired. To update your license key, see [Updating your License Key](#).
- **Override Console License** - This host is using the Console license key. You can use the Console key or apply a license key for this system. If you want to use the Console license for any system in your deployment, click **Default License** in the Manage License window. The license for that system will default to the Console license key.

A license key allows a certain number of log sources to be configured in your system. If you exceed the limit of configured logs sources, as established by the license key, an error message appears. To extend the number of log sources allowed, contact your sales representative.

This section provides information on managing your license keys including:

- [Updating your License Key](#)
- [Exporting Your License Key Information](#)

Updating your License Key

For your STRM Log Manager Console, a default license key provides you access to the interface for 5 weeks. Choose one of the following options for assistance with your license key:

- For a new or updated license key, contact your local sales representative.
- For all other technical issues, please contact Juniper Networks customer support.

If you log in to STRM Log Manager and your Console license key has expired, you are automatically directed to the System and License Management window. You must update the license key before you can continue. However, if one of your non-Console systems includes an expired license key, a message appears when you log in indicating a system requires a new license key. You must navigate to the System and License Management window to update that license key.

To update your license key:

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **System Configuration**.

The System Configuration panel appears.

Step 3 Click the **System and License Management** icon.

The System and License Management window appears providing a list of all hosts in your deployment.

Step 4 Select the host for which you want to view the license key.

Step 5 From the Actions menu, select **Manage License**.

The Current License Details window appears providing the current license key limits. If you want to obtain additional licensing capabilities, please contact your sales representative.

The screenshot shows a window titled "Current License Details" with the following information:

- Host: vm44 : 172.16.77.22
- Activation Key: 2A345S-0R722P-713L6L-010K4Y
- Hardware Serial Number: VMware-56 4d 67 8e 65 9d 10 35-42 51 dd f7 af 33 7b a8
- Customer Name: Q1 Labs / Sales
- Issued To: Sales (sales@q1labs.com)
- Issued Date: Thu May 22 11:49:29 2008
- Start Date: Wed Oct 28 09:57:36 ADT 2009
- Expiry Date: Wed Dec 02 08:57:36 AST 2009
- Technical Contact: Customer Support (welcomeCenter@q1labs.com)
- Offense Manager Enabled: No
- Offense Resolution Enabled: No
- Network Surveillance Enabled: No
- ORadar Log Manager Enabled: Yes
- Active Log Source Limit: 750
- Events per second threshold: 5000
- Flows per interval:
- User Limit: 10
- Network Object Limit: 300

Below the details is a "New License Key File:" field with a "Browse..." button. The "Current Key:" field contains a long alphanumeric string:

```

-----BEGIN REG KEY-----
4MncNOL/PN67gc1XbyEFsdW2zen3RenVax9tvOf02Vh7v+08HL2T/G+FQmor08amrNZAS0QHvfff
YNea4AmdTon2ewHYGPpvjssOPuaesA4Fu3koYKaC6D7jo8VvmgInPC00X8JyOu/2qxvzj6HaN1vn
PA+FvMlXKucGhUTXMObnlTPxmsbcVdTwnvzCckTxadjye2TWPNePr0Eo5Ded7xdkF3/NyYq9ncv
I3fCcsdCFmImrV7NQR3GqsPSXN28JCVTImdkSOCNJtzz1Nc1RaqlR2XAsq7E1YFwQNIrs1LSK1a
dnLXWUL55jjYBT5H5jiTaMOuSGBCYeH5Wa3HltqiFc9T8AP91ER6mkJpph14LLy+ePVf0HQJ1Yb
WV1ZY20t8+4IvbeATpfKzy1uKbePIggv3fhIqQxMaL9/mAMbbFBnesTjaQpFGPRkOdUJlg1MjYgS
zKTTY1X2AC1sN3QtsLABY0PEAhS5/FwCJqp16q487yiTDI3S43JukQrdBBHzqD051HPk4UVS00cW/
P4SEewbli/z+TJ8Xn92hIkibaJCrubenNhaIVRY+6u3TMAHhgGjdXmf1PhjWFu3tLirB4YkzEj7N
synIptBopIcAKB1NCMMb2NFR1aX61vuMQIVZdzqscuLFzRvLewalLruL6T11tehbrVCwnNSCSPOP
zGvP+KVRZ01wGhvEfh5e9uan6dLbWXT84QxqwHirtSULYLn63njLFxuyvNdkce3dDArAdLc1nB
    
```

At the bottom of the window are three buttons: "Revert to Console", "Revert to Deployed", and "Save".

Step 6 Click **Browse** beside the New License Key File and locate the license key.

Step 7 Once you locate and select the license key, click **Open**.

The Current License Details window appears.

Step 8 Click **Save**.



Note: If you want to revert back to the previous license key, click **Revert to Deployed**. If you revert to the license key used by the STRM Log Manager Console system, click **Revert to Console**.

Step 9 In the System and License Management window, click **Deploy License Key**.

The license key information is updated in your deployment.

Exporting Your License Key Information

To export your license key information for all systems in your deployment:

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **System Configuration**.

The System Configuration panel appears.

Step 3 Click the **System and License Management** icon.

The System and License Management window appears providing a list of all hosts in your deployment.

Step 4 Click **Export Licenses**.

The export window appears.

Step 5 Select one of the following options:

- **Open** - Opens the license key data in an Excel spreadsheet.
- **Save** - Allows you to save the file to your desktop.

Step 6 Click **OK**.

Restarting a System

To restart a STRM Log Manager system:

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **System Configuration**.

The System Configuration panel appears.

Step 3 Click the **System and License Management** icon.

The System and License Management window appears.

Step 4 Select the system you want to restart.

Step 5 From the Actions menu, select **Restart System**.

Shutting Down a System

To shutdown a STRM Log Manager system:

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **System Configuration**.

The System Configuration panel appears.

Step 3 Click the **System and License Management** icon.

The System and License Management window appears.

Step 4 Select the system you want to shut down.

Step 5 From the Actions menu, select **Shutdown**.

Configuring Access Settings

The System and License Management window provides access to the web-based system administration interface, which allows you to configure firewall rules, interface roles, passwords, and system time. This section includes:

- Firewall access. See [Configuring Firewall Access](#).
- Update your host set-up. See [Updating Your Host Set-up](#).
- Configure the interface roles for a host. See [Configuring Interface Roles](#).

- Change password to a host. See [Changing Passwords](#).
- Update the system time. See [Updating System Time](#).

Configuring Firewall Access

You can configure local firewall access to enable communications between devices and STRM Log Manager. Also, you can define access to the web-based system administration interface.

To enable STRM Log Manager managed hosts to access specific devices or interfaces:

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **System Configuration**.

The System Configuration panel appears.

Step 3 Click the **System and License Management** icon.

The System and License Management window appears.

Step 4 Select the host for which you want to configure firewall access settings.

Step 5 From the Actions menu, select **Manage System**.

Step 6 Log-in to the System Administration interface. The default is:

Username: **root**

Password: **<your root password>**



Note: *The username and password are case sensitive.*

Step 7 From the menu, select **Managed Host Config > Local Firewall**.

The Local Firewall window appears.

Step 8 In the Device Access box, you must include any STRM Log Manager systems you want to have access to this managed host. Only managed hosts listed will have access. For example, if you enter one IP address, only that one IP address will be granted access to the managed host. All other managed hosts are blocked.

To configure access:

- a In the IP Address field, enter the IP address of the managed host you want to have access.
- b From the Protocol list box, select the protocol you want to enable access for the specified IP address and port:
 - **UDP** - Allows UDP traffic.
 - **TCP** - Allows TCP traffic.
 - **Any** - Allows any traffic.
- c In the Port field, enter the port on which you want to enable communications.
- d Click **Allow**.

Step 9 In the System Administration Web Control box, enter the IP address(es) of managed host(s) that you want to allow access to the web-based system administration interface in the IP Address field. Only IP addresses listed will have access to the interface. If you leave the field blank, all IP addresses will have access. Click **Allow**.



Note: Make sure you include the IP address of your client desktop you want to use to access the interface. Failing to do so may affect connectivity.

- Step 10** Click **Apply Access Controls**.
- Step 11** Wait for the interface to refresh before continuing.

Updating Your Host Set-up You can use the web-based system administration interface to configure the mail server you want STRM Log Manager to use and the global password for STRM Log Manager configuration:

To configure your host set-up:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **System Configuration**.
The System Configuration panel appears.
- Step 3** Click the **System and License Management** icon.
The System and License Management window appears.
- Step 4** Select the host for which you want to update your host set-up.
- Step 5** From the Actions menu, select **Manage System**.
- Step 6** Log in to the System Administration interface. The default is:

Username: **root**

Password: **<your root password>**



Note: The username and password are case sensitive.

- Step 7** From the menu, select **Managed Host Config > STRM Log Manager Setup**.
The STRM Log Manager Setup window appears.

- Step 8** In the **Mail Server** field, specify the address for the mail server you want STRM Log Manager to use. STRM Log Manager uses this mail server to distribute alerts and event messages. To use the mail server provided with STRM Log Manager, enter **localhost**.
- Step 9** In the **Enter the global configuration password**, enter the password you want to use to access the host. Confirm the entered password.



Note: The global configuration password must be the same throughout your deployment. If you edit this password, you must also edit the global configuration password on all systems in your deployment.

Step 10 Click **Apply Configuration**.

Configuring Interface Roles

You can assign specific roles to the network interfaces on each managed host.

Roles

To assign roles:

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **System Configuration**.

The System Configuration panel appears.

Step 3 Click the **System and License Management** icon.

The System and License Management window appears.

Step 4 Select the host for which you want to configure interface roles.

Step 5 From the Actions menu, select **Manage System**.

Step 6 Log-in to the System Administration interface. The default is:

Username: **root**

Password: **<your root password>**



Note: The username and password are case sensitive.

Step 7 From the menu, select **Managed Host Config > Network Interfaces**.

The Network Interfaces window appears with a list of each interface on your managed host.



Note: For assistance with determining the appropriate role for each interface, please contact Juniper Networks customer support.

Network Interfaces

The following network interfaces are installed on this system. Select a role for each interface below. If an interface is to be used as a network interface (eg, for NetFlow™), then address information will be required.

Device	Description	Role
eth0	Broadcom Corporation NetXtreme BCM5703X Gigabit Ethernet (rev 02)	Management
	IP: 10.100.100.32	
	Netmask: 255.255.255.0	
	Gateway: 10.100.100.1	
eth1	Intel Corporation 82545GM Gigabit Ethernet Controller (rev 04)	IPv6 Auto
	IP: N/A (auto-configured)	
eth2	Broadcom Corporation NetXtreme BCM5703X Gigabit Ethernet (rev 02)	IPv6 Auto
	IP: N/A (auto-configured)	

Save Configuration

- Step 8** For each interface listed, select the role you want to assign to the interface using the Role list box.
- Step 9** Click **Save Configuration**.
- Step 10** Wait for the interface to refresh before continuing.

Changing Passwords To change the passwords:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **System Configuration**.
The System Configuration panel appears.
- Step 3** Click the **System and License Management** icon.
The System and License Management window appears.
- Step 4** Select the host for which you want to change passwords.
- Step 5** From the Actions menu, select **Manage System**.
- Step 6** Log-in to the System Administration interface. The default is:
Username: **root**



Password: **<your root password>**

Note: The username and password are case sensitive.

- Step 7** From the menu, select **Managed Host Config > Root Password**.
The Root Passwords window appears.

Step 8 Update the passwords and confirm:



Note: Make sure you record the entered values.

- **New Root Password** - Specify the root password necessary to access the web-based system administration interface.
- **Confirm New Root Password** - Re-enter the password for confirmation.

Step 9 Click **Update Password**.

Updating System Time

You are able to change the time for the following options:

- System time
- Hardware time
- Time Zone
- Time Server



Note: All system time changes must be made within the System Time window. You must change the system time information on the host operating the Console only. The change is then distributed to all managed hosts in your deployment.

You can configure time for your system using one of the following methods:

- [Configuring Your Time Server Using RDATE](#)
- [Configuring Time Settings For Your System](#)

Configuring Your Time Server Using RDATE

To update the time settings using RDATE:

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **System Configuration**.

The System Configuration panel appears.

Step 3 Click the **System and License Management** icon.

The System and License Management window appears.

Step 4 Select the host for which you want to update system time.

Step 5 From the Actions menu, select **Manage System**.

Step 6 Log-in to the System Administration interface. The default is:

Username: **root**

Password: **<your root password>**



Note: *The username and password are case sensitive.*

Step 7 From the menu, select **Managed Host Config > System Time**.

The System Time window appears.

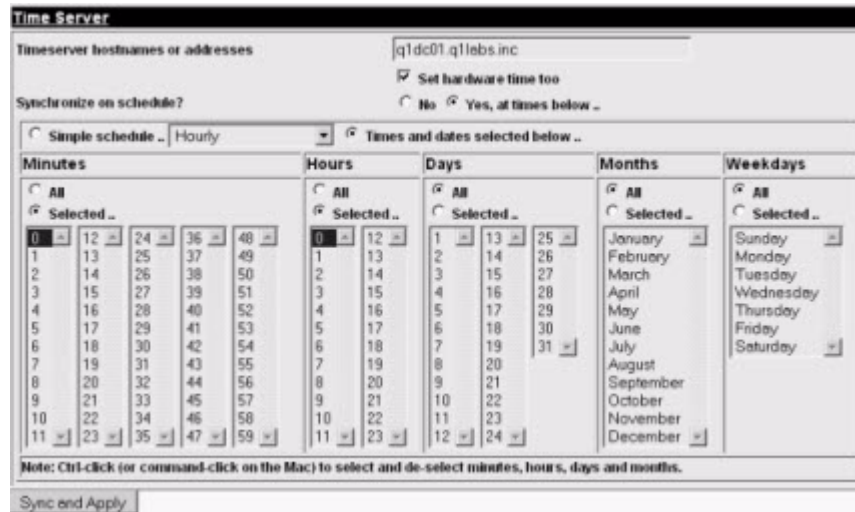


Caution: *The time settings window is divided into four sections. You must save each setting before continuing. For example, when you configure System Time, you must click Apply within the System Time section before continuing.*

Step 8 In the Time Zone box, select the time zone in which this managed host is located using the Change timezone to list box. Click **Save**.

Step 9 In the Time Server box, you must specify the following options:

- **Timeserver hostnames or addresses** - Specify the time server hostname or IP address.
- **Set hardware time too** - Select the check box if you want to set the hardware time as well.
- **Synchronize on schedule?** - Specify one of the following options:
 - **No** - Select the option if you do not want to synchronize the time specified in the Run at selected time below options. Go to [Step 10](#).
 - **Yes** - Select the option if you want to synchronize the time. See options below.
- **Simple Schedule** - Specify if you want the time update to occur at a specific time. If not, select the Run at times selected below option.
- **Times and dates are selected below** - Specify the time you want the time update to occur.



Step 10 Click **Sync and Apply**.

Configuring Time Settings For Your System

To update the time settings for your system:

Step 1 From the System View, use the right mouse button (right-click) on the managed host you want to update the time settings and select **Config Management**.

The web-based system administration interface login appears.

Step 2 Log-in to the System Administration interface. The default is:

Username: **root**

Password: **<your root password>**



Note: The username and password are case sensitive.

Step 3 From the menu, select **Managed Host Config > System Time**.

The System Time window appears.



Caution: The time settings window is divided into four sections. You must save each setting before continuing. For example, when you configure System Time, you must click **Apply** within the System Time section before continuing.

Step 4 In the System Time box, you must specify the current date and time you want to assign to the managed host. Click **Apply**.

If you want to set the System Time to the same as the Hardware time, click **Set system time to hardware time**.



Step 5 In the Hardware Time box, you must specify the current date and time you want to assign to the managed host. Click **Save**.

If you want to set the System Time to the same as the Hardware time, click **Set hardware time to system time**.

Hardware Time				
Day	Date	Month	Year	Hour
Friday				: :
Save		Set hardware time to system time		

Step 6 In the Time Zone box, select the time zone in which this managed host is located using the Change timezone to list box. Click **Save**.

Time Zone	
Change timezone to	America/Halifax (Atlantic Time - Nova Scotia (most places), PEI)
Save	

4

MANAGING HIGH AVAILABILITY

The High Availability (HA) feature ensures availability of STRM Log Manager data in the event of a hardware or network failure. Each HA cluster consists of a primary host and a secondary host that acts as a standby for the primary. The secondary host maintains the same data as the primary host by one of two methods: data replication or shared external storage. At regular intervals, every 10 seconds by default, the secondary host sends a heartbeat ping to the primary host to detect hardware and network failure. If the secondary host detects a failure, the secondary host automatically assumes all responsibilities of the primary host.

For more information about Primary and Secondary HA, see *Installation Procedures* in the *STRM Log Manager Installation Guide*.

An HA cluster consists of the following:

- **Primary host** - The primary host is the host for which you want to configure HA. You can configure HA for any system (Console or non-Console) in your deployment. When you configure HA, the IP address of the primary host becomes the virtual cluster IP address; therefore, you must configure a new IP address for the primary host.
- **Secondary host** - The secondary host is the standby for the primary host. If the primary host fails, the secondary host automatically assumes all responsibilities of the primary host.
- **Virtual Cluster IP address** - When you configure HA, the IP address of the primary host becomes the Virtual Cluster IP address. In the event that the primary host fails, the Virtual Cluster IP address will be assumed by the secondary host.

This section includes:

- [Adding an HA Cluster](#)
- [Editing an HA Cluster](#)
- [Setting an HA Host Offline](#)
- [Setting an HA Host Online](#)
- [Restoring a Failed Host](#)

Adding an HA Cluster

The System and License Management window allows you to manage your HA clusters.

Before adding an HA cluster, confirm the following:

- The secondary host you want to add must have a valid HA activation key.
- The secondary host you want to add must not already be a component in another HA cluster.
- The primary and secondary host must have the same STRM Log Manager software version installed.
- The primary and secondary host must be the same type: Console or non-Console. For example, if the primary host is a Console, the secondary host must also be a Console.
- The secondary host is located on the same subnet as the primary host.
- The new primary host IP address is set up on the same subnet.
- The secondary host must be configured with the same external iSCSI devices (if any) as the primary host.
- The /store partition on the secondary host must be larger than the /store partition on the primary host.
- The secondary host must use the same management interface specified as the primary host. For example, if the primary host uses ETH0 as the management interface, the secondary host must also use ETH0.
- If you plan to enable disk replication, we recommend that there is at least a 1 GB connection between the primary host and secondary host.

To add an HA cluster:

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **System Configuration**.

The System Configuration panel appears.

Step 3 Click the **System and License Management** icon.

The System and License Management window appears.

Step 4 Select the host for which you want to configure HA.

Step 5 From the Actions menu, select **Add HA Host**.



Note: If the primary host is a Console, a warning message appears to indicate that user interface will restart after you add an HA host. Click **OK** to proceed.

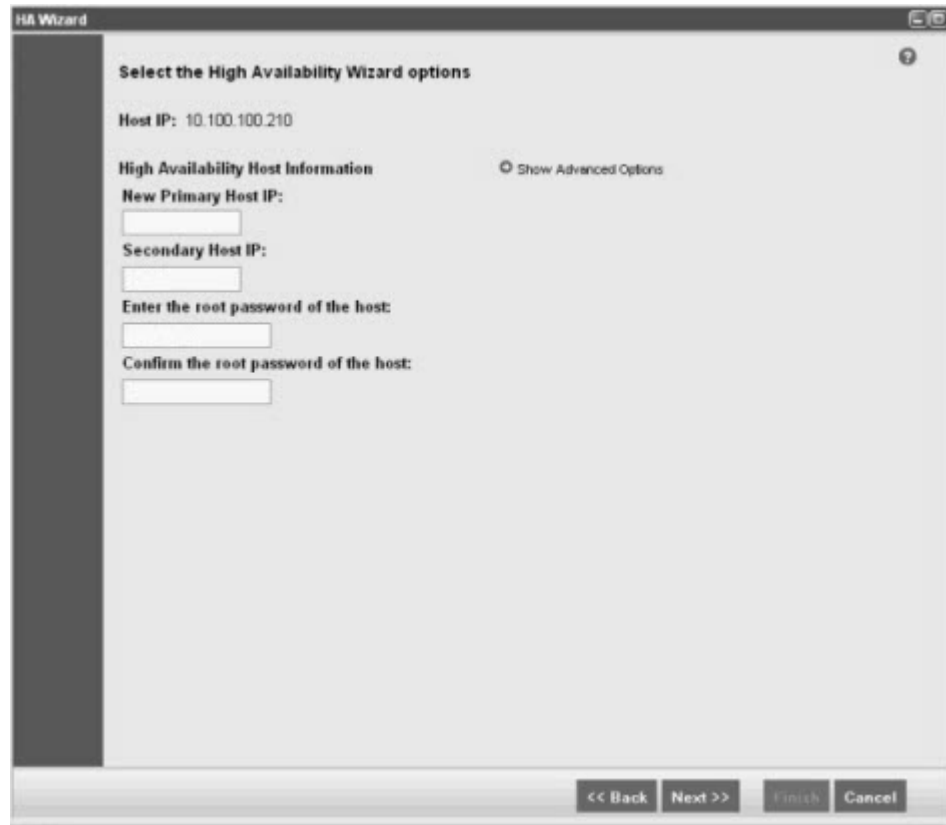
The HA Wizard appears.



Note: If you do not want to view the Welcome to the High Availability window again, select the Skip this page when running the High Availability wizard check box.

Step 6 Read the introductory text. Click **Next**.

The Select the High Availability Wizard Options window appears, automatically displaying the IP address of the primary host (Host IP).



Step 7 To configure the HA host information, configure the following parameters:

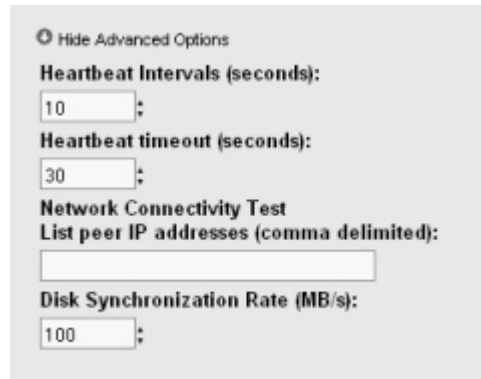
Table 5-1 HA Host Information Parameters

Parameter	Description
New Primary Host IP	Specify a new primary host IP address. The new primary host IP is assigned to the primary host. The previous IP address of the primary host becomes the Cluster Virtual IP address. If the primary host fails and the secondary host becomes active, the Cluster Virtual IP address is assigned to the secondary host. <i>Note:</i> The new primary host IP address must be on the same subnet as the Host IP.
Secondary Host IP	Specify the IP address of the secondary host you want to add. The secondary host must be in the same subnet as the primary host.
Enter the root password of the host	Specify the root password for the secondary host.
Confirm the root password of the host	Confirm the root password for the secondary host.

Step 8 Optional. To configure advanced parameters:

- a To display the advanced option parameters, click the arrow beside Show Advanced Options.

The advanced option parameters appear.



- b Configure the following parameters:


Table 5-2 Advanced Options Parameters

Parameter	Description
Heartbeat Intervals (seconds)	Specify the time, in seconds, you want to elapse between heartbeat messages. The default is 10 seconds.
Heartbeat Timeout (seconds)	Specify the time, in seconds, you want to elapse before the primary host is considered unavailable if there is no heartbeat detected. The default is 30 seconds.
Network Connectivity Test List peer IP addresses (comma delimited)	Specify the IP address(es) of the host(s) you want to ping to test the secondary host's network connection. The default is all other hosts in your deployment.
Disk Synchronization Rate (MB/s)	Specify or select the disk synchronization rate. The default is 100 MB/s.
Disable Disk Replication	Select this option if you want to disable disk replication. Note: This option is only visible for non-Console hosts.


- c Click **Next**.


The Confirm the High Availability Wizard Options window appears.



 **Caution:** If the primary host is configured with external storage, you must configure the secondary host with the same external storage before continuing.

Step 9 Review the information. Click **Finish**.

 **Note:** If Disk Synchronization is enabled, it can take 4 to 6 hours for the data to initially synchronize.

 **Note:** If required, click Back to return to the Confirm the High Availability Wizard options window to edit the information.

The System and License Management window displays the HA cluster you added. Use the Arrow icon to display or hide the secondary host.

Host Name	License	Serial Number	Status
stingray (console) (HA)	Valid	9256LF1	Active
stingray-primary.q1labs inc (console)	Valid	9268LF1	Active
g4b.q1labs inc (console) (secondary)	Expired		Needs License
mustang (HA)	Valid,Override Console License	G4ZMP61	Active
mustang-primary.q1labs inc (primary)	Valid,Override Console License	G4ZMP61	Active
integra.q1labs inc (secondary)	Expired		Needs License

The System and License Management window provides the status of your HA clusters including:

Table 5-3 HA Status Descriptions

Status	Description
Active	Specifies that the host is acting as the active system with all services running. Either the primary or secondary host can display the Active status. If the secondary host is displaying the Active status, failover has occurred.
Standby	Specifies that the host is acting as the standby system. This status will only display for a secondary host. The standby system has no services running. If disk replication is enabled, the standby system is replicating data from the primary host. If the primary host fails, the standby system automatically assumes the active role.
Failed	<p>Specifies that the host is in a failed state. Both the primary or secondary host can display the Failed status:</p> <ul style="list-style-type: none"> • If the primary host displays the Failed status, the secondary host takes over the services and should now display the Active status. • If the secondary host displays the Failed status, the primary host remains active, but is not protected by HA. <p>A system in the failed state must be manually repaired (or replaced), and then restored. See Restoring a Failed Host.</p> <p>Note: You may not be able to access a failed system from the Console.</p>
Synchronizing	<p>Specifies that host is synchronizing data on the local disk of the host to match the currently active system.</p> <p>Note: This status only appears if disk replication is enabled.</p>
Online	Specifies that the host is online.
Offline	Specifies that the host is offline. All processes are stopped and the host is not monitoring the heartbeat from the active system. Both the primary or the secondary can display the Offline status. While in the Offline state, disk replication continues if it is enabled.
Restoring	Once you select High Availability > Restore System to restore a failed host (see Restoring a Failed Host), this status specifies that system is in the process of restoring.
Needs License	Specifies that a license key is required. See Updating your License Key . In the Needs License state, no processes are running.

Editing an HA Cluster

Using the Edit HA Host feature, you can edit the advanced options for your HA cluster.

To edit an HA cluster:

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **System Configuration**.

The System Configuration panel appears.

Step 3 Click the **System and License Management** icon.

The System and License Management window appears.

Step 4 Select the row for the HA cluster you want to edit.

Step 5 From the High Availability menu, select **Edit HA Host**.

The HA Wizard appears, displaying the Select the High Availability Wizard Options window.

The screenshot shows the 'HA Wizard' window with the title 'Select the High Availability Wizard options'. The window contains the following fields and options:

- Host IP:** 10.100.100.210
- High Availability Host Information:**
 - New Primary Host IP:** 10.100.100.216
 - Secondary Host IP:** 10.100.100.20
- Advanced Options:**
 - Hide Advanced Options
 - Heartbeat Intervals (seconds):** 10
 - Heartbeat timeout (seconds):** 30
 - Network Connectivity Test:** List peer IP addresses (comma delimited):
 - Disk Synchronization Rate (MB/s):** 100

At the bottom of the window, there are four buttons: '<< Back', 'Next >>', 'Finish', and 'Cancel'.

Step 6 Edit the parameters in the advanced options section. See [Table 5-2](#).

Step 7 Click **Next**.

The Confirm the High Availability Wizard Options window appears.



Step 8 Review the information. Click **Finish**.

The secondary host restarts and your HA cluster continues functioning.

Setting an HA Host Offline

To set an HA host offline:

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **System Configuration**.

The System Configuration panel appears.

Step 3 Click the **System and License Management** icon.

The System and License Management window appears.

Step 4 Select the HA host you want to set to offline.

Step 5 From the High Availability menu, select **Set System Offline**.

The status for the host changes to Offline. If you set the active system to offline, the standby system becomes the active system. If you set the standby system to offline, the standby system no longer monitors the heartbeat of the active system, however, continues to synchronize data from the active system.

Setting an HA Host Online

To set an HA host online:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **System Configuration**.
The System Configuration panel appears.
- Step 3** Click the **System and License Management** icon.
The System and License Management window appears.
- Step 4** Select the offline HA host you want to set to online.
- Step 5** From the High Availability menu, select **Set System Online**.

The status for the host changes to Online. When you set the secondary host to online, the secondary host becomes the standby system. If you set the primary host to online while the secondary system is currently the active system, the primary host becomes the active system and the secondary host automatically becomes the standby system.

Restoring a Failed Host

If a host displays a status of Failed, a hardware or network failure occurred for that host.



Note: Before you can restore the host using the user interface, you must manually repair the host. For more information, see your network administrator.

To restore a failed system:

- Step 1** Recover the failed host.



Note: Recovering a failed host involves re-installing STRM Log Manager. For more information about recovering a failed host, see the STRM Log Manager Installation Guide. If you are recovering a primary host and your HA cluster uses shared storage, you must manually configure iSCSI. For more information about configuring iSCSI, see the Configuring iSCSI technical note.

- Step 2** Click the **Admin** tab.
- Step 3** In the navigation menu, click **System Configuration**.
The System Configuration panel appears.
- Step 4** Click the **System and License Management** icon.
The System and License Management window appears.
- Step 5** Select the failed HA host you want to restore.
- Step 6** From the High Availability menu, select **Restore System**.

The system restores the HA configuration on the failed host. The status of the host changes through the following sequence:

- a Restoring

- b Synchronizing (if disk synchronization is enabled)
- c Standby (secondary host) or Offline (primary host)

If the restored host is the primary system, you must set the primary system to the Online state. See [Setting an HA Host Online](#).

5

SETTING UP STRM LOG MANAGER

This chapter provides information on setting up STRM Log Manager including:

- [Creating Your Network Hierarchy](#)
- [Scheduling Automatic Updates](#)
- [Configuring System Settings](#)
- [Configuring System Notifications](#)
- [Configuring the Console Settings](#)

Creating Your Network Hierarchy

STRM Log Manager uses the network hierarchy to understand your network and provide you with the ability to view network information for your entire deployment.

When you develop your network hierarchy, you should consider the most effective method for viewing network activity. Note that the network you configure in STRM Log Manager does not have to resemble the physical deployment of your network. STRM Log Manager supports any network hierarchy that can be defined by a range of IP addresses. You can create your network based on many different variables, including geographical or business units.

Considerations

Consider the following when defining your network hierarchy:

- Group together systems and user groups that have similar behavior. This provides you with a clear view of your network.
- Do not group together servers that have unique behavior with other servers on your network. For example, placing a unique server alone provides the server greater visibility in STRM Log Manager allowing you to enact specific policies.
- Combine multiple Classless Inter-Domain Routings (CIDRs) or subnets into a single network/group to conserve disk space. For example:

Group	Description	IP Address
1	Marketing	10.10.5.0/24
2	Sales	10.10.8.0/21

Group	Description	IP Address
3	Database Cluster	10.10.1.3/32 10.10.1.4/32 10.10.1.5/32



Note: We recommend that you do not configure a network group with more than 15 objects. This may cause you difficulty in viewing detailed information for each group.

You may also want to define an all-encompassing group so when you define new networks, the appropriate policies and behavioral monitors are applied. For example:

Group	Subgroup	IP Address
Cleveland	Cleveland misc	10.10.0.0/16
Cleveland	Cleveland Sales	10.10.8.0/21
Cleveland	Cleveland Marketing	10.10.1.0/24

Defining Your Network Hierarchy

To define your network hierarchy:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **System Configuration**.
The System Configuration panel appears.
- Step 3** Click the **Network Hierarchy** icon.
The Network Views window appears.
- Step 4** From the menu tree, select the areas of the network you want to add a network component.
The Manage Group window appears for the selected network component.
- Step 5** Click **Add**.
The Add Network Object window appears.
- Step 6** Enter your network object values:

Table 6-1 Add New Object Parameters

Parameter	Action
Group	Specify the group for the new network object. Click Add Group to specify the group.
Name	Specify the name for the object.
Weight	Specify the weight of the object. The range is 0 to 100 and indicates the importance of the object in the system.
IP/CIDR(s)	Specify the CIDR range(s) for this object. For more information on CIDR values, see Accepted CIDR Values .

Table 6-1 Add New Object Parameters (continued)

Parameter	Action
Description	Specify a description for this network object.
Color	Specify a color for this object.
Database Length	Specify the database length.

Step 7 Click **Save**.

Step 8 Repeat for all network objects.

Step 9 Click **Re-Order**.

The Reorder Group window appears.

Step 10 Order the network objects in the desired order.

Step 11 Click **Save**.



Note: We recommend adding key servers as individual objects and grouping other major but related servers into multi-CIDR objects.

Accepted CIDR Values

The following table provides a list of the CIDR values that STRM Log Manager accepts:

Table 6-2 Accepted CIDR Values

CIDR Length	Mask	Number of Networks	Hosts
/1	128.0.0.0	128 A	2,147,483,392
/2	192.0.0.0	64 A	1,073,741,696
/3	224.0.0.0	32 A	536,870,848
/4	240.0.0.0	16 A	268,435,424
/5	248.0.0.0	8 A	134,217,712
/6	252.0.0.0	4 A	67,108,856
/7	254.0.0.0	2 A	33,554,428
/8	255.0.0.0	1 A	16,777,214
/9	255.128.0.0	128 B	8,388,352
/10	255.192.0.0	64 B	4,194,176
/11	255.224.0.0	32 B	2,097,088
/12	255.240.0.0	16 B	1,048,544
/13	255.248.0.0	8 B	524,272
/14	255.252.0.0	4 B	262,136
/15	255.254.0.0	2 B	131,068
/16	255.255.0.0	1 B	65,534
/17	255.255.128.0	128 C	32,512

Table 6-2 Accepted CIDR Values (continued)

CIDR Length	Mask	Number of Networks	Hosts
/18	255.255.192.0	64 C	16,256
/19	255.255.224.0	32 C	8,128
/20	255.255.240.0	16 C	4,064
/21	255.255.248.0	8 C	2,032
/22	255.255.252.0	4 C	1,016
/23	255.255.254.0	2 C	508
/24	255.255.255.0	1 C	254
/25	255.255.255.128	2 subnets	124
/26	255.255.255.192	4 subnets	62
/27	255.255.255.224	8 subnets	30
/28	255.255.255.240	16 subnets	14
/29	255.255.255.248	32 subnets	6
/30	255.255.255.252	64 subnets	2
/31	255.255.255.254	none	none
/32	255.255.255.255	1/256 C	1

For example, a network is called a supernet when the prefix boundary contains fewer bits than the network's natural (such as, classful) mask. A network is called a subnet when the prefix boundary contains more bits than the network's natural mask:

- 209.60.128.0 is a class C network address with a mask of /24.
- 209.60.128.0 /22 is a supernet that yields:
 - 209.60.128.0 /24
 - 209.60.129.0 /24
 - 209.60.130.0 /24
 - 209.60.131.0 /24
- 192.0.0.0 /25
 - Subnet Host Range
 - 0 192.0.0.1-192.0.0.126
 - 1 192.0.0.129-192.0.0.254
- 192.0.0.0 /26
 - Subnet Host Range
 - 0 192.0.0.1 - 192.0.0.62
 - 1 192.0.0.65 - 192.0.0.126
 - 2 192.0.0.129 - 192.0.0.190

- 3 192.0.0.193 - 192.0.0.254
- 192.0.0.0 /27
 - Subnet Host Range
 - 0 192.0.0.1 - 192.0.0.30
 - 1 192.0.0.33 - 192.0.0.62
 - 2 192.0.0.65 - 192.0.0.94
 - 3 192.0.0.97 - 192.0.0.126
 - 4 192.0.0.129 - 192.0.0.158
 - 5 192.0.0.161 - 192.0.0.190
 - 6 192.0.0.193 - 192.0.0.222
 - 7 192.0.0.225 - 192.0.0.254

Scheduling Automatic Updates

STRM Log Manager uses system configuration files to provide useful characterizations of network data flows. You can update your configuration files automatically or manually using the STRM Log Manager interface to make sure your configuration files contain the latest network security information. The updates, located on the Juniper customer support web site, include threats, vulnerabilities, and geographic information from various security related web sites.



Note: *In an HA deployment, once you update your configuration files on the primary host and deploy your changes, the updates are automatically performed on the secondary host. If you do not deploy your changes, the updates are performed on the secondary host through an automated process that runs hourly.*

You can configure the automatic updates to include minor updates (such as on-line Help or updated scripts), major updates (such as updated JAR files), or DSM updates. You can configure the automatic updates function to download and install minor updates. Major updates and DSM updates must be downloaded and installed manually. The Console must be connected to the Internet to receive the updates.



Note: *We do not guarantee the accuracy of the third-party information contained on the above-mentioned web sites.*

STRM Log Manager allows you to either replace your existing configuration files or integrate the updates with your existing files to maintain the integrity of your current configuration and information.

You can also update the configuration files for all systems in your STRM Log Manager deployment. However, the views must currently exist in your deployment editor. For more information on using the deployment editor, see [Chapter 7 Using the Deployment Editor](#).



Caution: Failing to build your deployment map before you configure automatic or manual updates results in your remote systems not being updated.

This section includes:

- [Scheduling Automatic Updates](#)
- [Updating Your Files On-Demand](#)

Scheduling Automatic Updates

To schedule automatic updates:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **System Configuration**.
The System Configuration panel appears.
- Step 3** Click the **Auto Update** icon.
The Auto Update Configuration window appears.
- Step 4** Configure the update method and types of updates you want to receive using the Choose Updates box:

Table 6-3 Choose Updates Configuration Parameters

Parameter	Description
Update Method	Using the drop-down list box, select the method you want to use for updating your system including: <ul style="list-style-type: none"> • Auto Integrate - Integrates the new configuration files with your existing files to maintain the integrity of your information. This is the default. • Auto Update - Replaces your existing configuration files with the new configuration files.
Weekly Updates	Weekly updates include vulnerability, QID map updates, and security threat information. Using the drop-down list box, select one of the following: <ul style="list-style-type: none"> • Enabled - Allows weekly updates for your system. This is the default. • Disabled - Disables the option for your system to receive weekly updates.

Table 6-3 Choose Updates Configuration Parameters (continued)

Parameter	Description
Minor Updates	<p>Minor updates include such items as additional on-line Help content or updated scripts. Using the drop-down list box, select one of the following options for minor updates:</p> <ul style="list-style-type: none"> • Disabled - Disables the option for your system to receive minor updates. • Download - Downloads the minor updates to the designated download path location. See the readme file in the download files for installation instructions. • Install - Automatically installs minor updates on your system. This is the default.
Major Updates	<p>Major updates require service interruptions to install. Major updates include such items as updated JAR files. Using the drop-down list box, select one of the following options for major updates:</p> <ul style="list-style-type: none"> • Disabled - Disables the option for your system to receive major updates. This is the default. • Download - Downloads the major updates to the designated download path location. See the readme file in the download files for installation instructions.
DSM Updates	<p>Using the drop-down list box, select one of the following options for DSM updates:</p> <ul style="list-style-type: none"> • Disabled - Disables the option for your system to receive DSM updates. • Download - Downloads the DSM updates to the designated download path location. This is the default. See the readme file in the download files for installation instructions.
Download Path	Specify the directory path location to which you want to store DSM, minor, and major updates.

Step 5 Configure the server settings:

Server Configuration	
Webserver	<input type="text" value="https://qmmunity.q1labs.com/"/>
Directory	<input type="text" value="autoupdates/"/>
Proxy Server	<input type="text"/>
Proxy Port	<input type="text"/>
Proxy Username	<input type="text"/>
Proxy Password	<input type="text"/>

Table 6-4 Server Configuration Parameters

Parameter	Description
Webserver	Specify the web server from which you want to obtain the updates. The default web site is: http://www.juniper.net/support/
Directory	Specify the directory location on which you want to store the updates. The default is autoupdates/.
Proxy Server	Specify the URL for the proxy server.
Proxy Port	Specify the port for the proxy server.
Proxy Username	Specify the necessary username for the proxy server. A username is only required if you are using an authenticated proxy.
Proxy Password	Specify the necessary password for the proxy server. A password is only required if you are using an authenticated proxy.

Step 6 Configure the update settings:

Table 6-5 Update Settings Parameters

Parameter	Description
Deploy changes	Select the check box if you want to deploy update changes automatically. If the check box is clear, a system notification appears in the Dashboard indicating that you must deploy changes. By default, the check box is clear.
Send feedback	Select the check box if you want to send feedback to Juniper Networks regarding the update. Feedback is sent automatically using a web form if any errors occur with the update. By default, the check box is clear.
Backup Retention Period (days)	Specify the length of time, in days, that you want to store files that may be replaced during the update process. The files will be stored in the location specified in the Backup Location parameter.
Backup Location	Specify the location that you want to store backup files.

Step 7 Configure the schedule for updates:

Table 6-6 Schedule Update Parameters

Parameter	Description
Schedule Update Frequency	Using the drop-down list box, select the frequency you want to receive updates. The options are Disabled, Weekly, Monthly, or Daily. The default is Weekly.
Hour	Using the drop-down list box, select the time of day you want your system to update. The default is 1 am.
Week Day	This option is only available if you select Weekly as the update frequency. Using the drop-down list box, select the day of the week you want to receive updates. The default is Monday.
Month Day	This option is only active when you select Monthly as the update frequency. Using the drop-down list box, select the day of the month you want to receive updates.

Step 8 Click **Save**.

If you selected the Deploy Changes check box in [Step 6](#), the updates are enforced through your deployment. Once the automatic update process is complete, a system notification appears in the Dashboard. For more information, see the *STRM Log Manager Users Guide*.

Updating Your Files On-Demand

You can update your files, whenever necessary, using the Auto Update window.

To update your files:

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **System Configuration**.

The System Configuration panel appears.

Step 3 Click the **Auto Update icon**.

The Auto Update Configuration window appears.

Step 4 In the Update Method drop-down list box, select the method you want to use for updating your files:

- **Auto Integrate** - Integrates the new configuration files with your existing files to maintain the integrity of your information.
- **Auto Update** - Replaces your existing configuration files with the new configuration files.

Step 5 Click **Save and Update Now**.

Step 6 From the Admin tab menu, click **Deploy Changes**.

If you selected the Deploy Changes check box in the Update Settings box, the updates are enforced through your deployment. Once the automatic update process is complete, a system notification appears in the Dashboard. For more information, see the *STRM Log Manager Users Guide*.

Configuring System Settings

Using the Admin tab, you can configure the system, database, and sentry settings.

To configure system settings:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **System Configuration**.

The System Configuration panel appears.

- Step 3** Click the **System Settings** icon.

The System Settings window appears.

- Step 4** Enter values for the parameters:

Table 6-7 System Settings Parameters

Parameter	Description
System Settings	
Administrative Email Address	Specify the e-mail address of the designated system administrator. The default is root@localhost.
Alert Email From Address	Specify the e-mail address from which you want to receive e-mail alerts.
Delete Root Mail	Root mail is the default location for host context messages. Specify one of the following: <ul style="list-style-type: none"> Yes - Delete the local administrator e-mail. This is the default. No - Do not delete local administrator e-mail.
Temporary Files Retention Period	Specify the time period the system stores temporary files. The default is 6 hours.
Audit Log Enable	Enables or disables the ability to collect audit logs. You can view audit log information using the Events interface. The default is Yes.
Coalescing Events	Enables or disables the ability for a log source to coalesce (bundle) events. This value applies to all log sources. However, if you want to alter this value for a specific log source, edit the Coalescing Event parameter in the log source configuration. For more information, see the <i>Log Sources Users Guide</i> . The default is Yes.
Store Event Payload	Enables or disables the ability for a log source to store event payload information. This value applies to all auto detected log sources. However, if you want to alter this value for a specific log source, edit the Event Payload parameter in the log source configuration. For more information, see the <i>Log Sources Users Guide</i> . The default is Yes.

Table 6-7 System Settings Parameters (continued)

Parameter	Description
Global Iptables Access	Specify the IP address of a non-Console system that does not have IP tables configuration to which you want to enable direct access. To enter multiple systems, enter a comma-separated list of IP addresses.
Syslog Event Timeout (minutes)	Specify the amount of time, in minutes, that the status of a syslog device is recorded as error if no events have been received within the timeout period. The status appears in the Log Sources window (for more information, see the <i>Log Sources Users Guide</i>). The default is 720 minutes (12 hours).
Database Settings	
User Data Files	Specify the location of the user profiles. The default is /store/users.
Database Storage Location	Specify the location of the database files. The default location is /store/db.
Ariel Database Settings	
Log Source Storage Location	Specify the location that you want to store the log source information. The default location is /store/ariel/events.
Log Source Data Retention Period	Specify the amount of time that you want to store the log source data. The default is 30 days.
Search Results Retention Period	Using the drop-down list box, select the amount of time you want to store event search results. The default is 1 day.
Maximum Real Time Results	Specify the maximum number of results you want to view in the Events interface. The default is 10,000.
Reporting Max Matched Results	Specify the maximum number of results you want a report to return. This value applies to the search results in the Events interface. The default is 1,000,000.
Command Line Max Matched Results	Specify the maximum number of results you want the command line to return. The default is 0.
Web Execution Time Limit	Specify the maximum amount of time, in seconds, you want a query in the interface to process before a time-out occurs. This value applies to the search results in the Events interface. The default is 600 seconds.
Reporting Execution Time Limit	Specify the maximum amount of time, in seconds, you want a reporting query to process before a time-out occurs. The default is 57,600 seconds.
Command Line Execution Time Limit	Specify the maximum amount of time, in seconds, you want a query in the command line to process before a time-out occurs. The default is 0 seconds.
Event Log Hashing	Enables or disables the ability for STRM Log Manager to store a hash file for every stored event log file. The default is No.

Table 6-7 System Settings Parameters (continued)

Parameter	Description
Hashing Algorithm	<p>You can use a hashing algorithm for database storage and encryption. You can use one of the following hashing algorithms:</p> <ul style="list-style-type: none"> • Message-Digest Hash Algorithm - Transforms digital signatures into shorter values called Message-Digests (MD). • Secure Hash Algorithm (SHA) Hash Algorithm - Standard algorithm that creates a larger (60 bit) MD. <p>Specify the log hashing algorithm you want to use for your deployment. The options are:</p> <ul style="list-style-type: none"> • MD2 - Algorithm defined by RFC 1319. • MD5 - Algorithm defined by RFC 1321. • SHA-1 - Default. Algorithm defined by Secure Hash Standard (SHS), NIST FIPS 180-1. • SHA-256 - Algorithm defined by the draft Federal Information Processing Standard 180-2, SHS. SHA-256 is a 256 bit hash algorithm intended for 128 bits of security against security attacks. • SHA-384 - Algorithm defined by the draft Federal Information Processing Standard 180-2, SHS. SHA-384 is a bit hash algorithm is provided by truncating the SHA-512 output. • SHA-512 - Algorithm defined by the draft Federal Information Processing Standard 180-2, SHS. SHA-512 is a bit hash algorithm intended to provide 256 bits of security.
Transaction Sentry Settings	
Transaction Max Time Limit	<p>A transaction sentry detects unresponsive applications using transaction analysis. If an unresponsive application is detected, the transaction sentry attempts to return the application to a functional state.</p> <p>Using the drop-down list box, select the length of time you want the system to check for transactional issues in the database. The default is 10 minutes.</p>
Resolve Transaction on Non-Encrypted Host	<p>Using the drop-down list box, select whether you want the transaction sentry to resolve all erroneous conditions detected on the Console or non-encrypted managed hosts.</p> <p>If you select No, the conditions are detected and logged but you must manually intervene and correct the error. The default is Yes.</p>

Table 6-7 System Settings Parameters (continued)

Parameter	Description
Resolve Transaction on Encrypted Host	Using the drop-down list box, select whether you want the transaction sentry to resolve all erroneous conditions detected on the encrypted managed host. If you select No, the conditions are detected and logged but you must manually intervene and correct the error. The default is Yes.
SNMP Settings	
SNMP Version	Using the drop-down list box, choose one of the following options: <ul style="list-style-type: none"> • Disabled - Specify if you do not want SNMP responses in the STRM Log Manager custom rules engine. Disabling SNMP indicates that you do not want to accept events using SNMP. • SNMPv3 - Specify if you want to use SNMP version 3 in your deployment. • SNMPv2c - Specify if you want to use SNMP version 2 in your deployment.
SNMPv2c Settings	
Destination Host	Specify the IP address to which you want to send SNMP notifications.
Destination Port	Specify the port to which you want to send SNMP notifications. The default is 162.
Community	Specify the SNMP community, such as public.
SNMPv3 Settings	
Destination Host	Specify the IP address to which you want to send SNMP notifications.
Destination Port	Specify the port to which you want to send SNMP notifications. The default is 162.
User Name	Specify the name of the user you want to access SNMP related properties.
Security Level	Specify the security level for SNMP. The options are: <ul style="list-style-type: none"> • NOAUTH_NOPRIV - Indicates no authorization and no privacy. This the default. • AUTH_NOPRIV - Indicates authorization is permitted but no privacy. • AUTH_PRIV - Allows authorization and privacy.
Authentication Protocol	Specify the algorithm you want to use to authenticate SNMP traps.
Authentication Password	Specify the password you want to use to authenticate SNMP.
Privacy Protocol	Specify the protocol you want to use to decrypt SNMP traps.

Table 6-7 System Settings Parameters (continued)

Parameter	Description
Privacy Password	Specify the password used to decrypt SNMP traps.

Step 5 Click **Save**.

The STRM Log Manager Admin tab appears.

Step 6 From the Admin tab menu, select **Advanced > Deploy Full Configuration**.

Configuring System Notifications

You can configure global system performance alerts for thresholds using the STRM Log Manager Admin tab. This section provides information for configuring your global system thresholds.

To configure global system thresholds:

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **System Configuration**.

The System Configuration panel appears.

Step 3 Click the **Global System Notifications** icon.

The Global System Notifications window appears.

Step 4 Enter values for the parameters. For each parameter, you must select the following options:

- **Enabled** - Select the check box to enable the option.
- **Respond if value is** - Specify one of the following options:
 - **Greater Than** - An alert occurs if the parameter value exceeds the configured value.
 - **Less Than** - An alert occurs if the parameter value is less than the configured value.

Table 6-8 Global System Notifications Parameters

Parameter	Description
User CPU usage	Specify the threshold percentage of user CPU usage.
Nice CPU usage	Specify the threshold percentage of user CPU usage at the nice priority.
System CPU usage	Specify the threshold percentage of CPU usage while operating at the system level.
Idle CPU usage	Specify the threshold percentage of idle CPU time.
Percent idle time	Specify the threshold percentage of idle time.
Run queue length	Specify the threshold number of processes waiting for run time.
Number of processes in the process list	Specify the threshold number of processes in the process list.

Table 6-8 Global System Notifications Parameters (continued)

Parameter	Description
System load over 1 minute	Specify the threshold system load average over the last minute.
System load over 5 minutes	Specify the threshold system load average over the last 5 minutes.
System load over 15 minutes	Specify the threshold system load average over the last 15 minutes.
Kilobytes of memory free	Specify the threshold amount, in kilobytes, of free memory.
Kilobytes of memory used	Specify the threshold amount, in kilobytes, of used memory. This does not consider memory used by the kernel.
Percentage of memory used	Specify the threshold percentage of used memory.
Kilobytes of cached swap memory	Specify the threshold amount of memory, in kilobytes, shared by the system.
Kilobytes of buffered memory	Specify the threshold amount of memory, in kilobytes, used as a buffer by the kernel.
Kilobytes of memory used for disc cache	Specify the threshold amount of memory, in kilobytes, used to cache data by the kernel.
Kilobytes of swap memory free	Specify the threshold amount of free memory, in kilobytes.
Kilobytes of swap memory used	Specify the threshold amount of free swap memory, in kilobytes.
Percentage of swap used	Specify the threshold percentage of used swap space.
Number of interrupts per second	Specify the threshold number of received interrupts per second.
Received packets per second	Specify the threshold number of packets received per second.
Transmitted packets per second	Specify the threshold number of packets transmitted per second.
Received bytes per second	Specify the threshold number of bytes received per second.
Transmitted bytes per second	Specify the threshold number of bytes transmitted per second.
Received compressed packets	Specify the threshold number of compressed packets received per second.
Transmitted compressed packets	Specify the threshold number of compressed packets transmitted per second.
Received multicast packets	Specify the threshold number of received Multicast packets per second.
Receive errors	Specify the threshold number of corrupt packets received per second.

Table 6-8 Global System Notifications Parameters (continued)

Parameter	Description
Transmit errors	Specify the threshold number of corrupt packets transmitted per second.
Packet collisions	Specify the threshold number of collisions that occur per second while transmitting packets.
Dropped receive packets	Specify the threshold number of received packets that are dropped per second due to a lack of space in the buffers.
Dropped Transmit packets	Specify the threshold number of transmitted packets that are dropped per second due to a lack of space in the buffers.
Transmit carrier errors	Specify the threshold number of carrier errors that occur per second while transmitting packets.
Receive frame errors	Specify the threshold number of frame alignment errors that occur per second on received packets.
Receive fifo overruns	Specify the threshold number of First In First Out (FIFO) overrun errors that occur per second on received packets.
Transmit fifo overruns	Specify the threshold number of First In First Out (FIFO) overrun errors that occur per second on transmitted packets.
Transactions per second	Specify the threshold number of transfers per second sent to the system.
Sectors written per second	Specify the threshold number of sectors transferred to or from the system

Step 5 Click **Save**.

The STRM Log Manager Admin tab appears.

Step 6 From the Admin tab menu, click **Deploy Changes**.

Configuring the Console Settings

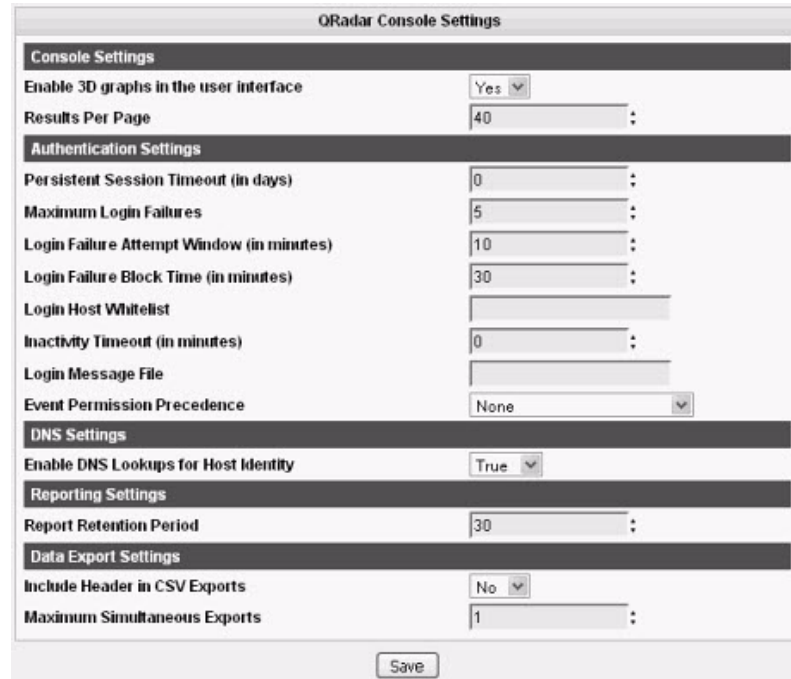
The STRM Log Manager Console provides the interface for STRM Log Manager. This Console is also used to manage distributed STRM Log Manager deployments.

The Console is accessed from a standard web browser. When you access the system, a prompt appears for a user name and password, which must be configured in advance by the STRM Log Manager administrator. STRM Log Manager supports the following web browsers:

- Internet Explorer 7.0
- Mozilla Firefox 3.0

To configure STRM Log Manager Console settings:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **System Configuration**.
The System Configuration panel appears.
- Step 3** Click the **Console** icon.
The Console Settings window appears.



- Step 4** Enter values for the parameters:

Table 6-9 STRM Log Manager Console Management Parameters

Parameter	Description
Console Settings	
Enable 3D graphs in the user interface	Using the drop-down list box, select one of the following: <ul style="list-style-type: none"> • Yes - Displays Dashboard graphics in 3-dimensional format. • No - Displays Dashboard graphics in 2-dimensional format.
Results Per Page	Specify the maximum number of results you want to display in the main STRM interface. This parameter applies to the Events and Reports interfaces. For example, if the Default Page Size parameter is configured to 50, the Events interface displays a maximum of 50 events. The default is 40.

Table 6-9 STRM Log Manager Console Management Parameters (continued)

Parameter	Description
Authentication Settings	
Persistent Session Timeout (in days)	Specify the length of time, in days, that a user system will be persisted, in days. The default is 0, which disables this features and the remember me option upon login.
Maximum Login Failures	Specify the number of times a login attempt may fail. The default is 5.
Login Failure Attempt Window (in minutes)	Specify the length of time during which a maximum login failures may occur before the system is locked. The default is 10 minutes.
Login Failure Block Time (in minutes)	Specify the length of time that the system is locked if the the maximum login failures value is exceeded. The default is 30 minutes.
Login Host Whitelist	Specify a list of hosts who are exempt from being locked out of the system. Enter multiple entries using a comma-separated list.
Inactivity Timeout (in minutes)	Specify the amount of time that a user will be automatically logged out of the system if no activity occurs.
Login Message File	Specify the location and name of a file that includes content you want to appear on the STRM Log Manager log in window. This file may be in text or HTML format and the contents of the file appear below the current log in window.
Event Permission Precedence	<p>Using the drop-down list box, specify the level of network permissions you want to assign to users. This affects the events that appear in the Events interface. The options include:</p> <ul style="list-style-type: none"> • Network Only - A user must have access to either the source network or the destination network of the event to have the event appear in the Events interface. • Devices Only - A user must have access to either the device or device group that created the event to have the event appear in the Events interface. • Networks and Devices - A user must have access to both the source or the destination network and the device or device group to have an event appear in the Events interface. • None - All events appear in the Events interface. Any user with Events role permissions are able to view all events. <p>Note: For more information on managing users, see Chapter 2 Managing Users.</p>
DNS Settings	

Table 6-9 STRM Log Manager Console Management Parameters (continued)

Parameter	Description
Enable DNS Lookups for Host Identity	Enable or disable the ability for STRM Log Manager to search for host identity information. When enabled, this information is available using the right-mouse button (right-click) on any IP address or asset name in the interface. The default is True.
Reporting Settings	
Report Retention Period	Specify the period of time, in days, that you want the system to maintain reports. The default is 30 days.
Data Export Settings	
Include Header in CSV Exports	Specify whether you want to include a header in a CSV export file.
Maximum Simultaneous Exports	Specify the maximum number of exports you want to occur at one time.

Step 5 Click **Save**.

Step 6 From the Admin tab menu, click **Deploy Changes**.

6

MANAGING BACKUP AND RECOVERY

You can backup and recover configuration information and data for STRM Log Manager.



Note: *The restore process only restores your configuration information. For assistance in restoring your data, see the Restoring Your Data Technical Note.*

This chapter provides information on managing backup and recovery of including:

- [Managing Backup Archives](#)
- [Backing Up Your Information](#)
- [Restoring Your Configuration Information](#)

Managing Backup Archives

Using the Admin tab, you can:

- View your successful backup archives. See [Viewing Back Up Archives](#).
- Import an archive file. See [Importing an Archive](#).
- Delete an archive file. See [Deleting a Backup Archive](#).

Viewing Back Up Archives

To view all successful backups:

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **System Configuration**.

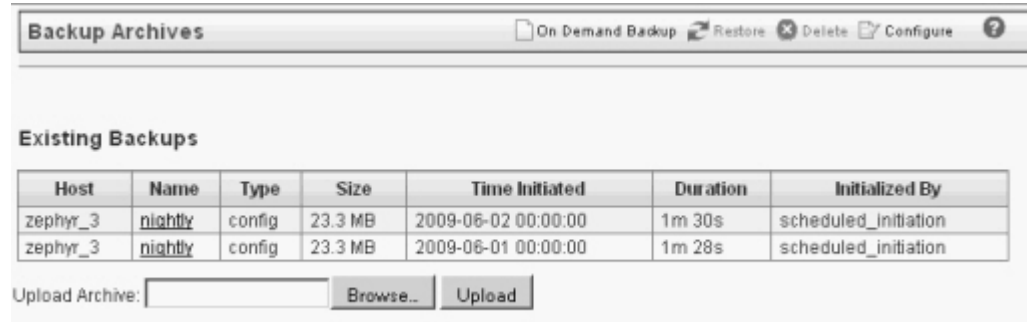
The System Configuration panel appears.

Step 3 Click the **Backup and Recovery** icon.

The Backup Archives window appears providing the following information, depending on the status of the backup processes:

- If there are no backup archives, a message appears indicating no backup archives have been created.
- If a backup is in progress, a status window appears to indicate the duration of the current backup, which user/process initiated the backup, and provides you with the option to cancel the backup.

- If there are existing backup archives, the list of the successful backup archives that exists in the database appears. If a backup file is deleted, it is removed from the disk and from the database. Also, the entry is removed from this list and an audit event is generated to indicate the removal. Each archive file includes the data from the previous day. The list of archive is sorted by the Time Initiated column in descending order.



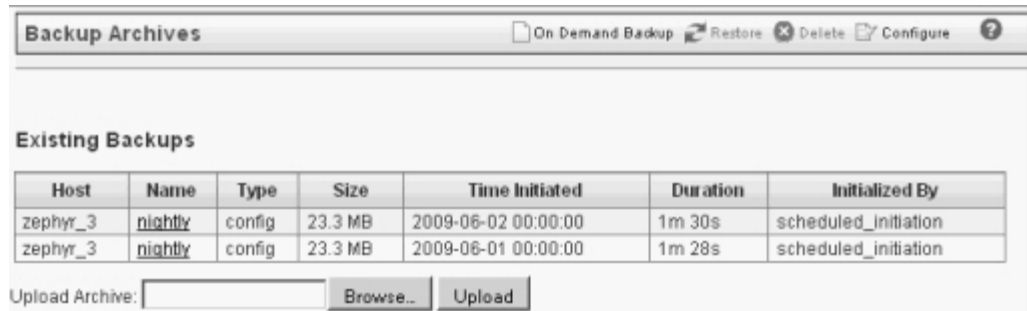
The Backup Archives window provides the following information for each backup archive.

Table 7-1 Backup Archive Window Parameters

Parameter	Description
Host	Specifies the host that initiated the backup process.
Name	Specifies the name of the backup archive. To view the backup file, click the name of the backup. You can only download a backup created on a Console.
Type	Specifies the type of backup. The options are: <ul style="list-style-type: none"> • config (configuration data) • data (events information)
Size	Specifies the size of the archive file.
Time Initiated	Specifies the time that the backup file was initiated.
Duration	Specifies the time to complete the backup process.
Initialized By	Specifies whether the backup file was created by a user or through a scheduled process.

Importing an Archive To import a STRM Log Manager backup archive file:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **System Configuration**.
The System Configuration panel appears.
- Step 3** Click the **Backup and Recovery** icon.
The Backup Archives window appears.



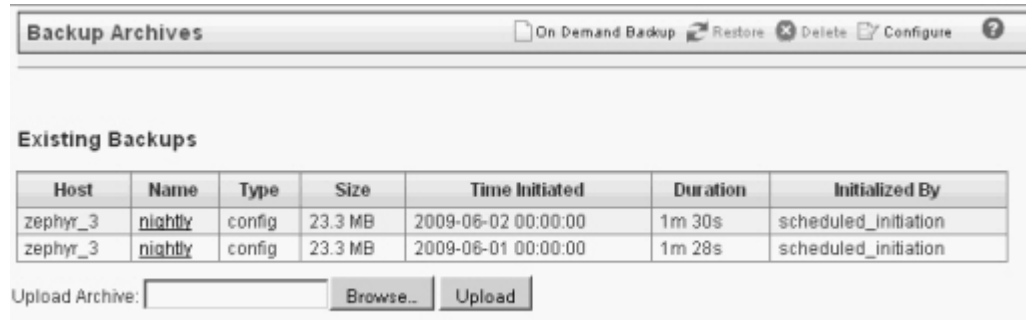
- Step 4** In the Upload Archive field, click **Browse**.
The File Upload window appears.
- Step 5** Select the archive file you want to upload. The archive file must include a .tgz extension. Click **Open**.
- Step 6** Click **Upload**.

Deleting a Backup Archive To delete a backup archive:



Note: To delete a backup archive file, the backup archive file and the Host Context component must reside on the same system. The system must also be in communication with the Console and no other backup can be in progress.

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **System Configuration**.
The System Configuration panel appears.
- Step 3** Click the **Backup and Recovery** icon.
The Backup Archives window appears.



- Step 4** Select the archive you want to delete.
- Step 5** Click **Delete**.
- Step 6** A confirmation window appears.
- Step 7** Click **Ok**.

Backing Up Your Information

You can backup your configuration information and data using the Backup Recovery Configuration window. By default, STRM Log Manager creates a backup archive of your configuration information every night at midnight and the backup includes configuration and/or data from the previous day.

You can backup your information using one of the following methods:

- Creating a configuration only backup. See [Initiating a Backup](#).
- Scheduling a nightly backup. See [Scheduling Your Backup](#).
- Copying a backup archive file to the system on which you want to restore the archive. You can then restore the data. See [Restoring Your Configuration Information](#).

This section provides information on both methods of backing up your data including:

- [Scheduling Your Backup](#)
- [Initiating a Backup](#)

Scheduling Your Backup

To schedule your backup process:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **System Configuration**.
The System Configuration panel appears.
- Step 3** Click the **Backup and Recovery** icon.
The Backup Archives window appears.
- Step 4** Click **Configure**.

The Backup Recovery Configuration window appears.

Step 5 Enter values for the parameters:

Table 7-2 Backup Recovery Configuration Parameters

Parameter	Description
General Backup Configuration	
Backup Repository Path	Specifies the location you want to store your backup file. This path must exist before the backup process is initiated. If this path does not exist, the backup process aborts. The default is /store/backup.
Backup Retention Period	Specify the length of time, in days, that you want to store backup files. The default is 2 days. Note: This period of time only affects backup files generated as a result of a scheduled process. Manually initiated or imported backup files are not affected by this value.

Table 7-2 Backup Recovery Configuration Parameters (continued)

Parameter	Description
Nightly Backup Schedule	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • No Nightly Backups - Disables the creation of a backup archive on a daily basis. • Configuration Backup Only - Enables the creation of a daily backup at midnight that includes configuration information only. • Configuration and Data Backups - Enables the creation of a daily backup at midnight that includes configuration information and data. If you select the Configuration and Data Backups option, you can select the hosts you want to backup. <p>Configuration backups includes the following components:</p> <ul style="list-style-type: none"> • Custom rules • Event searches • Log sources • Groups • Event categories • Device Support Modules (DSMs) • User and user roles information • License key information <p>Data backups includes the following information:</p> <ul style="list-style-type: none"> • Event data • Report data • Audit log information
Configuration Only Backup	
Backup Time Limit	Specify the length of time, in minutes, that you want to allow the backup to process. The default is 180 minutes. If the backup process exceeds the configured time limit, the backup will automatically be canceled.
Backup Priority	Specify the level of importance (LOW, MEDIUM, HIGH) that you want the system to place on the configuration information backup process compared to other processes. A priority of medium or high will have a greater impact on system performance.
Data Backup	
Backup Time Limit (min)	Specify the length of time, in minutes, that you want to allow the backup to process. The default is 1020 minutes. If the backup process exceeds the configured time limit, the backup will automatically be canceled.
Backup Priority	Specify the level of importance (LOW, MEDIUM, HIGH) you want the system to place on the data backup process compared to other processes. A priority of medium or high will have a greater impact on system performance.

Step 6 Click **Save**.

Step 7 From the Admin tab menu, click **Deploy Changes**.

Initiating a Backup To manually initiate a backup of your configuration information:

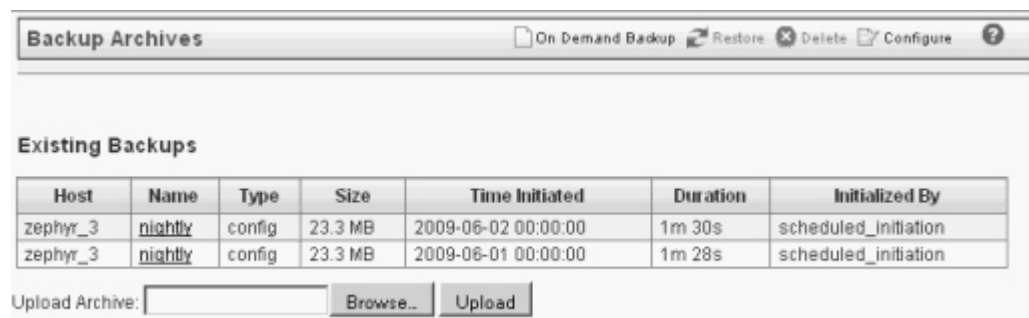
Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **System Configuration**.

The System Configuration panel appears.

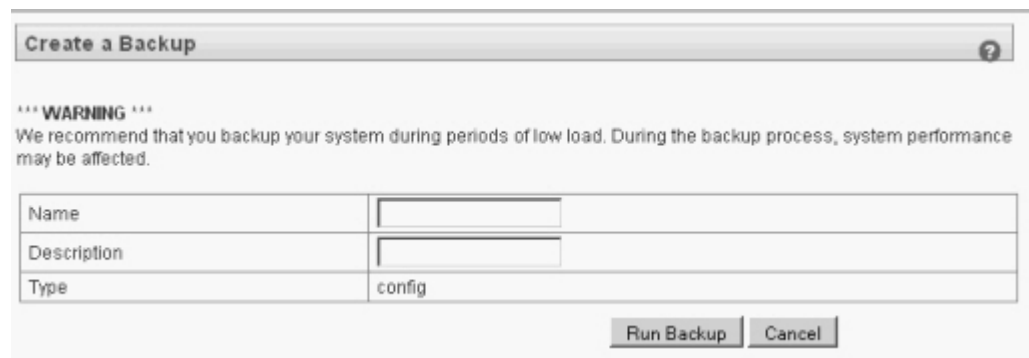
Step 3 Click the **Backup and Recovery** icon.

The Backup Archives window appears.



Step 4 Click **On Demand Backup**.

The Create a Backup window appears.



Step 5 Enter values for the following parameters:

- **Name** - Specify a unique name you want to assign to this backup file. The name must be a maximum of 100 alphanumeric characters. Also, the name may contain following characters: underscore (_), dash (-), or period (.).
- **Description** - Specify a description for this backup. The name can be up to 255 characters in length.

Step 6 Click **Run Backup**.

A confirmation window appears.

Step 7 Click **OK**.

Restoring Your Configuration Information

You can restore configuration information from existing backup archives using the Restore a Backup window. You can only restore a backup archive created within the same release of software. For example, if you are running STRM Log Manager 2009.2, the backup archive must of been created in STRM Log Manager 2009.2.

You can restore configuration information in the following scenarios:

- Restore backup archive on a system that has the same IP address as the backup archive. See [Restoring on a System with the Same IP Address](#).
- Restore backup archive on system with a different IP address than the backup archive. See [Restoring to a System with a Different IP Address](#).



Note: *If the backup archive originated on a NATed Console system, you can only restore that backup archive on a NATed system.*

Restoring on a System with the Same IP Address

To restore your configuration information on a system that has the same IP address as the backup archive:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **System Configuration**.
The System Configuration panel appears.
- Step 3** Click the **Backup and Recovery** icon.
The Backup Archives window appears.
- Step 4** Select the archive you want to restore.
- Step 5** Click **Restore**.
The Restore a Backup window appears.

Restore a Backup [?]

*** WARNING ***
During the restore process all processes cease functioning, you will not be able to access your data, and no data will be collected.

Name	nightly
Description	nightly_backup
Type	config

All Items

Restore Cancel

- Step 6** To restore specific items in the archive:
 - a Clear the All Items check box.
The list of archived items appears.
 - b Select the check box for each item you want to restore.

Step 7 Click **Restore**.

A confirmation window appears. Each backup archive includes IP address information of the system from which the backup archive was created.

Step 8 Click **Ok**.

The restore process begins. This process may take an extended period of time. When complete, a message appears.

Step 9 Click **Ok**.**Step 10** Choose one of the following options:

- a If the STRM Log Manager interface was closed during the restore process, open a browser and log in to STRM Log Manager.
- b If the STRM Log Manager interface was not closed, refresh your browser.

A window appears providing the status of the restore process. This window provides any errors for each host. This window also provides instructions for resolving errors that have occurred.

Step 11 Follow the instructions on the status window.

Note: The restore process only restores your configuration information. For assistance in restoring your data, see the *Restoring Your Data Technical Note*.



Note: If the backup archive originated on an HA cluster, you must click **Deploy Changes** to restore the HA cluster configuration after the restore is complete. If disk replication is enabled, the secondary host immediately synchronizes data once the system is restored. If the secondary host was removed from the deployment after backup was performed, the secondary host displays a Failed status in the System and License Management window.

Restoring to a System with a Different IP Address

To restore your configuration information on a system with a different IP address than the backup archive:

Step 1 Click the **Admin** tab.**Step 2** In the navigation menu, click **System Configuration**.

The System Configuration panel appears.

Step 3 Click the **Backup and Recovery** icon.

The Backup Archives window appears.

Step 4 Select the archive you want to restore.**Step 5** Click **Restore**.

The Restore a Backup window appears. Since the IP address of the system on which you want to restore the information does not match the IP address of the backup archive, a message appears indicating that you must stop iptables on each managed host in your deployment



Step 6 To restore specific items in the archive:

- a Clear the All Items check box.
The list of archived items appears.
- b Select the check box for each item you want to restore.

Step 7 Stop IP tables:

- a Log into the managed host, as root.
- b Enter the following command:
`service iptables stop`
- c Repeat for all managed hosts in your deployment.

Step 8 In the Restore a Backup window, click **Test Host Access**.

The Restore a Backup (Managed Hosts Accessibility) window appears.

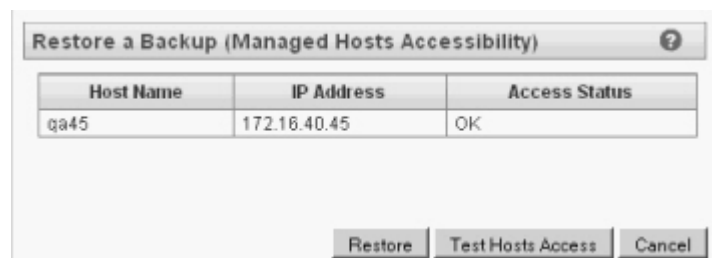


Table 7-3 provides the following information:

Table 7-3 Restore a Backup (Managed Host Accessibility Parameters)

Parameter	Description
Host Name	Specifies the managed host name.
IP Address	Specifies the IP address of the managed host.

Table 7-3 Restore a Backup (Managed Host Accessibility Parameters (continued))

Parameter	Description
Access Status	<p>Specifies the access status to the managed host. The options include:</p> <ul style="list-style-type: none"> • Testing Access - The test to determine access status is not complete. • No Access - The managed host can not be accessed. • OK - The managed host is accessible.

Step 9 When the accessibility of all hosts is determined and the status in the Access Status column indicates OK or No Access, click **Restore**.

The restore process begins.



Note: If the Access Status column indicates No Access for a host, stop iptables (see [Step 7](#)) again and click Test Host Access to attempt a connection.

Step 10 Click **Ok**.

The restore process begins. This process may take an extended period of time.

Step 11 Click **Ok**.

Step 12 Choose one of the following options:

- a If the STRM Log Manager interface has been closed during the restore process, open a browser and log in to STRM Log Manager.
- b If the STRM Log Manager interface has not been closed, refresh your browser.

A window appears providing the status of the restore process. This window provides any errors for each host. This window also provides instructions for resolving errors that have occurred.

Step 13 Follow the instructions on the status window.



Note: The restore process only restores your configuration information. For assistance in restoring your data, see the *Restoring Your Data Technical Note*.



Note: If the backup archive originated on an HA cluster, you must click **Deploy Changes** to restore the HA cluster configuration after the restore is complete. If disk replication is enabled, the secondary host immediately synchronizes data once the system is restored. If the secondary host was removed from the deployment after backup was performed, the secondary host displays a Failed status in the System and License Management window.

7

USING THE DEPLOYMENT EDITOR

The deployment editor allows you to manage the individual components of your STRM Log Manager deployment. Once you configure your Event, and System Views, you can access and configure the individual components of each managed host.



Note: *The Deployment Editor requires Java Runtime Environment. Download JRE5.0 at www.java.sun.com. Also, If you are using the Firefox browser, you must configure your browser to accept Java Network Language Protocol (JNLP) files.*



Caution: *Many third-party web browsers that use the Internet Explorer engine, such as Maxthon or MyIE, install components that may be incompatible with the STRM Log Manager Admin tab. You must disable any third-party web browsers installed on your system. For further assistance, please contact customer support.*

If you want to access the deployment editor from behind a proxy server or firewall, you must configure the appropriate proxy settings on your desktop. This allows the software to automatically detect the proxy settings from your browser. To configure the proxy settings, open the Java configuration located in your Control Panel and configure the IP address of your proxy server. For more information on configuring proxy settings, see your Microsoft documentation.

This chapter provides information on managing your views including:

- [About the Deployment Editor](#)
- [Editing Deployment Editor Preferences](#)
- [Building Your Event View](#)
- [Managing Your System View](#)
- [Configuring STRM Log Manager Components](#)

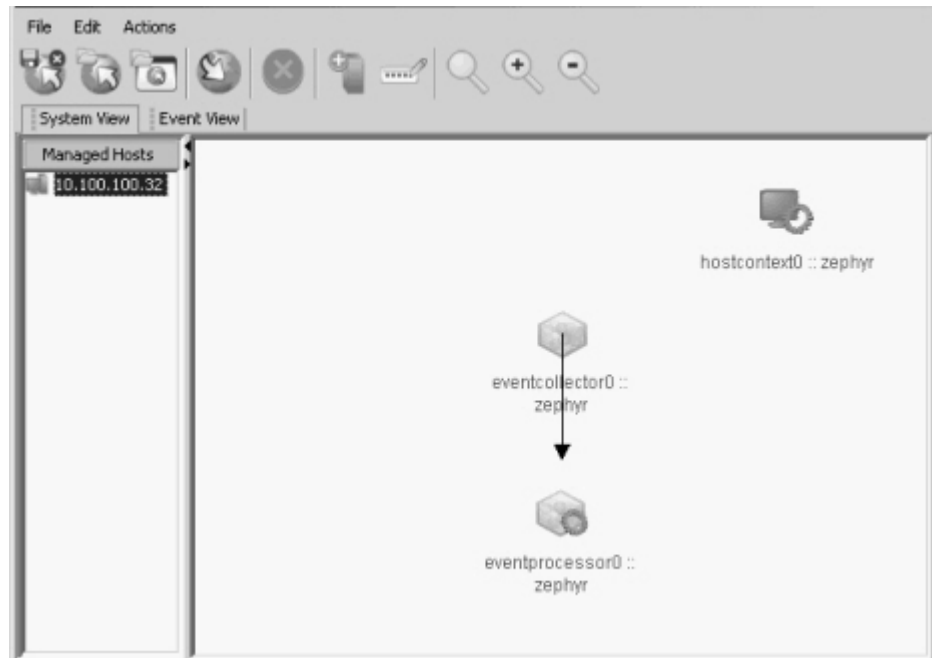
About the Deployment Editor

You can access the deployment editor using Admin tab. You can use the deployment editor to create your deployment, assign connections, and configure each component.

The deployment editor provides the following views of your deployment:

- **System View** - Allows you to assign software components to systems (managed hosts) in your deployment. The System View includes all managed hosts in your deployment. A managed host is a system in your deployment that providing additional event processing. By default, the System View also includes the Host Context component, which monitors all STRM Log Manager components to ensure that each component is operating as expected.
- **Event View** - Allows you to create a view for your SIM components including Event Processor, and Event Collector components.

Each view is divided into two panels.



In the Event View, the left panel provides a list of SIM components you can add to the view and the right panel provides an existing view of your SIM deployment.

In the System View, the left panel provides a list of managed hosts, which you can view and configure. The deployment editor polls your deployment for updates to managed hosts. If the deployment editor detects a change to a managed host in your deployment, a message appears notifying you of the change. For example, if you remove a managed host, a message appears indicating that the assigned components to that host must be re-assigned to another host. Also, if you add a managed host to your deployment, the deployment editor displays a message indicating that the managed host has been added.

Accessing the Deployment Editor

In the Admin tab, click Deployment Editor. The deployment editor appears. Once you update your configuration settings using the deployment editor, you must save those changes to the staging area. You must either manually deploy all changes using the Admin tab menu options. All deployed changes are then enforced throughout your deployment.

Using the Editor

The deployment editor provides you with several menu and toolbar options when configuring your views including:

- [Menu Options](#)
- [Toolbar Options](#)

Menu Options

The menu options that appear depend on the selected component in your view. [Table 8-1](#) provides a list of the menu options and the component for which they appear.

Table 8-1 Deployment Editor Menu Options

Menu Option	Sub Menu Option	Description
File	Save to staging	Saves deployment to the staging area.
	Save and close	Save deployment to the staging area and closes the deployment editor.
	Open staged deployment	Opens a deployment that was previously saved to the staging area.
	Open production deployment	Opens a deployment that was previously saved.
	Close current deployment	Closes the current deployment.
	Revert	Reverts current deployment to the previously saved deployment.
	Edit Preferences	Opens the preferences window.
Edit	Close editor	Closes the deployment editor.
	Delete	Deletes a component, host, or connection.
Actions	Add a managed host	Opens the Add a Managed Host wizard.
	Manage NATed Networks	Opens the Manage NATed Networks window, which allows you to manage the list of NATed networks in your deployment.
	Rename component	Renames an existing component. This option is only available when a component is selected.
	Configure	Configure a STRM Log Manager components. This option is only available when Event Collector or Event Processor is selected.

Table 8-1 Deployment Editor Menu Options (continued)

Menu Option	Sub Menu Option	Description
	Assign	Assigns a component to a managed host. This option is only available when Event Collector or Event Processor is selected.
	Unassign	Unassigns a component from a managed host. This option is only available when the selected component has a managed host running a compatible version of STRM Log Manager software. This option is only available when Event Collector or Event Processor is selected.

Toolbar Options

The toolbar options include:

Table 8-2 Toolbar Options











Button	Description
	Saves deployment to the staging area and closes the deployment editor.
	Opens current production deployment.
	Opens a deployment that was previously saved to the staging area.
	Discards recent changes and reloads last saved model.
	Deletes selected item from the deployment view. This option is only available when the selected component has a managed host running a compatible version of STRM Log Manager software.
	Opens the Add a Managed Host wizard, which allows you to add a managed host to your deployment.
	Opens the Manage NATed Networks window, which allows you to manage the list of NATed networks in your deployment.
	Resets the zoom to the default.
	Zooms in.

Table 8-2 Toolbar Options (continued)

Button	Description
	Zooms out.

Creating Your Deployment

To create your deployment, you must:

- Step 1** Build your System View. See [Managing Your System View](#).
- Step 2** Configure added components. See [Configuring STRM Log Manager Components](#).
- Step 3** Build your Event View. See [Building Your Event View](#).
- Step 4** Stage the deployment. From the deployment editor menu, select **File > Save to Staging**.
- Step 5** Deploy all configuration changes. From the Admin tab menu, select **Advanced > Deploy Full Configuration**.

For more information on the Admin tab, see [Chapter 1 Overview](#).

Before you Begin

Before you begin, you must:

- Install all necessary hardware and STRM Log Manager software.
- Install Java Runtime Environment. You can download Java version 1.6.0_13 x 86 at the following web site: <http://java.com/en/download/index.jsp>
- If you are using the Firefox browser, you must configure your browser to accept Java Network Language Protocol (JNLP) files.
- Plan your STRM Log Manager deployment including the IP addresses and login information for all devices in your STRM Log Manager deployment.

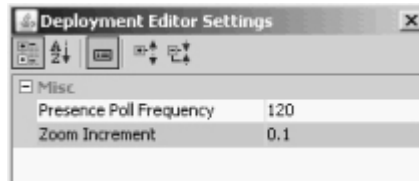


Note: *If you require assistance with the above, please contact Juniper Networks customer support.*

Editing Deployment Editor Preferences

To edit the deployment editor preferences:

- Step 1** From the deployment editor main menu, select **File > Edit Preferences**.
The Deployment Editor Setting window appears.



- Step 2** Enter values for the following parameters:
- **Presence Poll Frequency** - Specify how often, in milliseconds, that the managed host monitors your deployment for updates, for example, a new or updated managed host.
 - **Zoom Increment** - Specify the increment value when the zoom option is selected. For example, 0.1 indicates 10%.
- Step 3** Close the window
The Deployment Editor appears.

Building Your Event View

The Event View allows you to create and manage the SIM components for your deployment including:

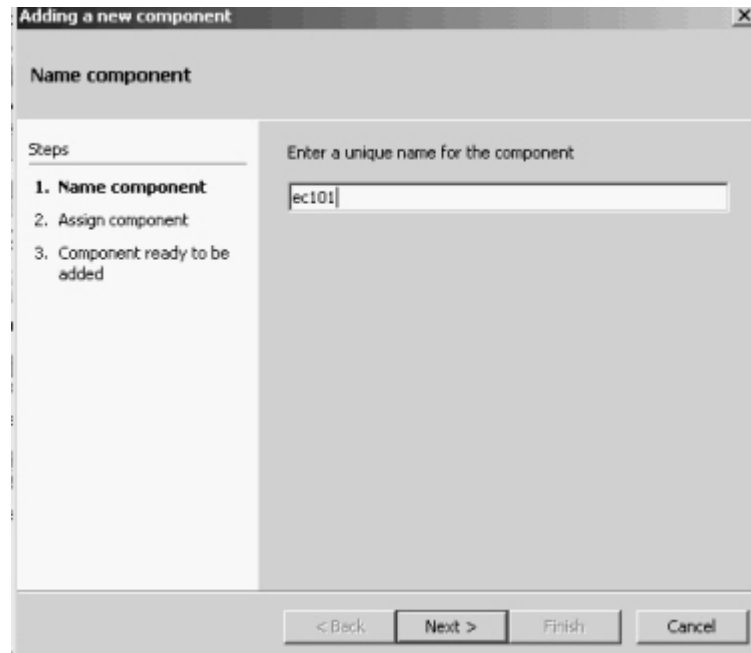
- **Event Collector** - Collects security events from various types of security devices in your network. The Event Collector gathers events from local, remote, and device sources. The Event Collector then normalizes the events and sends the information to the Event Processor. The Event Collector also bundles all virtually identical events to conserve system usage.
- **Event Processor** - An Event Processor processes events 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 Log Manager and distributes to the appropriate area, depending on the type of event. The Event Processor also includes information gathered by STRM Log Manager to indicate any behavioral changes or policy violations for that event. Rules are then applied to the events that allow the Event Processor to process according to the configured rules.

To build your Event View, you must:

- Step 1** Add SIM components to your view. See [Adding Components](#).
- Step 2** Connect the components. See [Connecting Components](#).
- Step 3** Forward normalized events. See [Forwarding Normalized Events](#).
- Step 4** Rename the components so each component has a unique name. See [Renaming Components](#).

Adding Components To add components to your Event View:

- Step 1** In the deployment editor, click the **Event View** tab.
The Event View appears.
- Step 2** In the Event Tools panel, select a component you want to add to your deployment.
The Adding a New Component Wizard appears.



- Step 3** Enter a unique name for the component you want to add. The name can be up to 15 characters in length and may include underscores or hyphens. Click **Next**.
The Assign Component window appears.
- Step 4** From the Select a host to assign to list box, select a managed host to which you want to assign the new component. Click **Next**.
- Step 5** Click **Finish**.
- Step 6** Repeat for each component you want to add to your view.
- Step 7** From the main menu, select **File > Save to staging**.

Connecting Components Once you add all the necessary components in your Event View, you must connect your Event Processor(s) and Event Collector(s).

To connect components:

- Step 1** In the Event View, select the component for which you want to establish a connection.
- Step 2** From the menu, select **Actions > Add Connection**.



Note: You can also use the right mouse button (right-click) to access the Action menu item.

An arrow appears in your map.

Step 3 Drag the end of the arrow to the component on which you want to establish a connection. You can only connect Event Collectors to Event Processors.

The arrow connects the two components.

Step 4 Repeat for all remaining components that you want to establish a connection.

Step 5 Specify a unique name for the source or target. The name can be up to 15 characters in length and may include underscores or hyphens. Click **Next**.

The event source/target information window appears.

Step 6 Enter values for the parameters:

- **Enter a name for the off-site host** - Specify the name of the off-site host. The name can be up to 15 characters in length and may include underscores or hyphens.
- **Enter the IP address of the server** - Specify the IP address of the managed host to which you want to connect.
- **Encrypt traffic from off-site source** - Select the check box if you want to encrypt traffic from an off-site source. To enable encryption, you must select this check box on the associated off-site source and target.

Step 7 Click **Next**.

Step 8 Click **Finish**.

Step 9 Repeat for all remaining off-site sources and targets.

Step 10 From the main menu, select **File > Save to staging**.



Note: If you update your Event Collector configuration or the monitoring ports, you must manually update your source and target configurations to maintain the connection between deployments.

Forwarding Normalized Events

To forward normalized events, you must configure an off-site Event Collector (target) in your current deployment and the associated off-site Event Collector in the receiving deployment (source).

You can add the following components to your Event View:

- **Off-site Source** - Indicates an off-site Event Collector from which you want to receive data. The source must be configured with appropriate permissions to send events to the off-site target.
- **Off-site Target** - Indicates an off-site Event Collector to which you want to send data.

For example, if you want to forward normalized events between two deployments (A and B), where deployment B wants to receive events from deployment A you

must configure deployment A with an off-site target to provide the IP address of the managed host that includes Event Collector B. You must then connect Event Collector A to the off-site target. In deployment B, you must configure an off-site source with the IP address of the managed host that includes Event Collector A and the port to which Event Collector A is monitoring.

If you want to disconnect the off-site source, you must remove the connections from both deployments. From deployment A, you must remove the off-site target and in deployment B, you must remove the off-site source.

If you want to enable encryption between deployments, you must enable encryption on both off-site source and target. Also, you must ensure the SSH public key for the off-site source (client) is available to the target (server) to ensure appropriate access. For example, in the example below, if you want to enable encryption between the off-site source and Event Collector B, you must copy the public key (located at `/root/.ssh/id_rsa.pub`) from the off-site source to Event Collector B (add the contents of the file to `/root/.ssh/authorized_keys`).

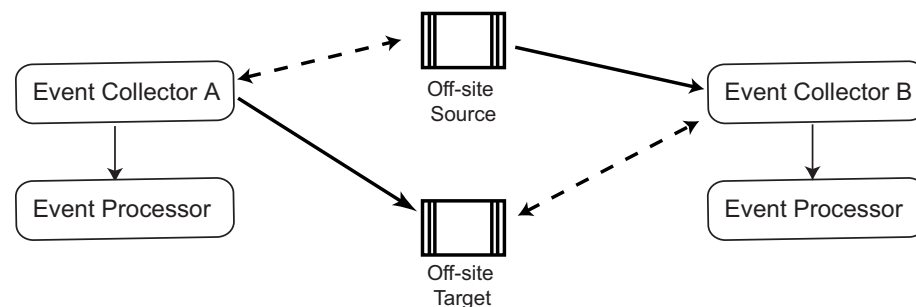


Figure 8-1 Example of Connecting Deployments



Note: If the off-site source/target is an all-in-one system, the public key is not automatically generated, therefore, you must manually generate the public key. For more information on generating public keys, see your Linux documentation.

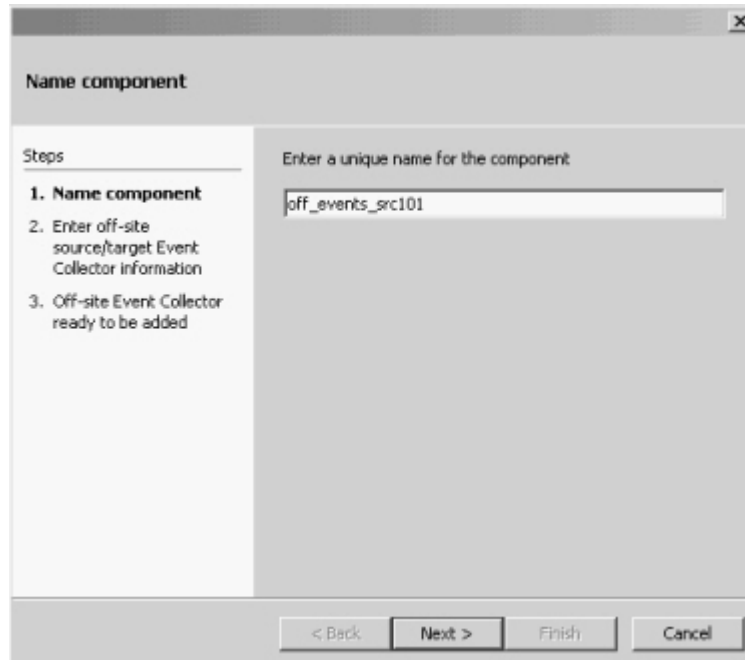
To forward normalized events:

Step 1 In the deployment editor, click the **Event View** tab.

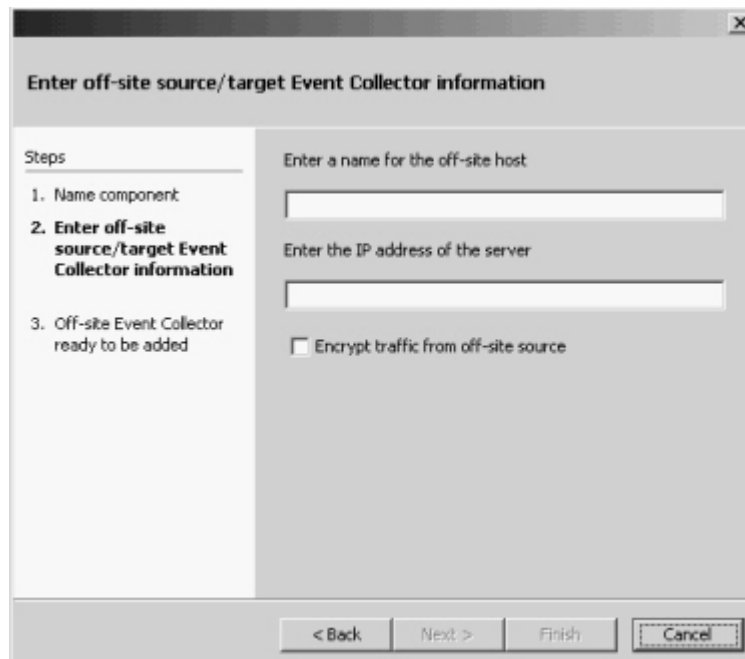
The Event View appears.

Step 2 In the Components panel, select either **Add Off-site Source** or **Add Off-site Target**.

The Adding a New Component Wizard appears.



Step 3 Specify a unique name for the source or target. The name can be up to 15 characters in length and may include underscores or hyphens. Click **Next**. The event source/target information window appears.



Step 4 Enter values for the parameters:

- **Enter a name for the off-site host** - Specify the name of the off-site host. The name can be up to 15 characters in length and may include underscores or hyphens.
- **Enter the IP address of the server** - Specify the IP address of the managed host to which you want to connect.
- **Encrypt traffic from off-site source** - Select the check box if you want to encrypt traffic from an off-site source. To enable encryption, you must select this check box on the associated off-site source and target.

Step 5 Click **Next**.

Step 6 Click **Finish**.

Step 7 Repeat for all remaining off-site sources and targets.

Step 8 From the main menu, select **File > Save to staging**.



Note: If you update your Event Collector configuration or the monitoring ports, you must manually update your source and target configurations to maintain the connection between deployments.

Renaming Components

You may want to rename a component in your view to uniquely identify components through your deployment.

To rename a component:

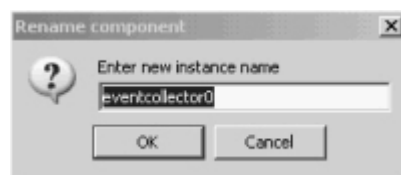
Step 1 Select the component you want to rename.

Step 2 From the menu, select **Actions > Rename Component**.



Note: You can also use the right mouse button (right-click) to access the Action menu items.

The Rename component window appears.



Step 3 Enter a new name for the component. The name must be alphanumeric with no special characters.

Step 4 Click **Ok**.

Managing Your System View

The System View allows you to manage all managed hosts in your network. A managed host is a component in your network that includes STRM Log Manager software. If you are using a STRM Log Manager appliance, the components for that appliance model appear. If your STRM Log Manager software is installed on your own hardware, the System View includes a Host Context component. The

System View allows you to select which component(s) you want to run on each managed host.

Using the System View, you can:

- Set up managed hosts in your deployment. See [Setting Up Managed Hosts](#).
- Use STRM Log Manager with NATed networks in your deployment. See [Using NAT with STRM Log Manager](#).
- Update the managed host port configuration. See [Configuring a Managed Host](#).
- Assign a component to a managed host. See [Assigning a Component to a Host](#).
- Configure Host Context. See [Configuring Host Context](#).

Setting Up Managed Hosts

Using the deployment editor, you can manage all hosts in your deployment including:

- Add a managed host to your deployment. See [Adding a Managed Host](#).
- Edit an existing managed host. See [Editing a Managed Host](#).
- Remove a managed host. See [Removing a Managed Host](#).

You also can not assign or configure components on a non-Console managed host when the STRM Log Manager software version is incompatible with the software version that the Console is running. If a managed host has previously assigned components and is running an incompatible software version, you can still view the components, however, you are not able to update or delete the components.

Encryption provides greater security for all STRM Log Manager traffic between managed hosts. To provide enhanced security, STRM Log Manager also provides integrated support for OpenSSH and attachmateWRQ® Reflection SSH software. Reflection SSH software provides a FIPS 140-2 certified encryption solution. When integrated with STRM Log Manager, Reflection SSH provides secure communication between STRM Log Manager components. For information on Reflection SSH, your product documentation.:



Note: You must have Reflection SSH installed on each managed host you want to encrypt using Reflection SSH. Also, Reflection SSH is not compatible with other SSH software, such as, OpenSSH.

Since encryption occurs between managed hosts in your deployment, your deployment must consist of more than one managed host before encryption is possible. Encryption is enabled using SSH tunnels (port forwarding) initiated from the client. A client is the system that initiates a connection in a client/server relationship. 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. If you enable encryption on a non-Console managed host, encryption tunnels are automatically created for databases and other support service connections to the Console.



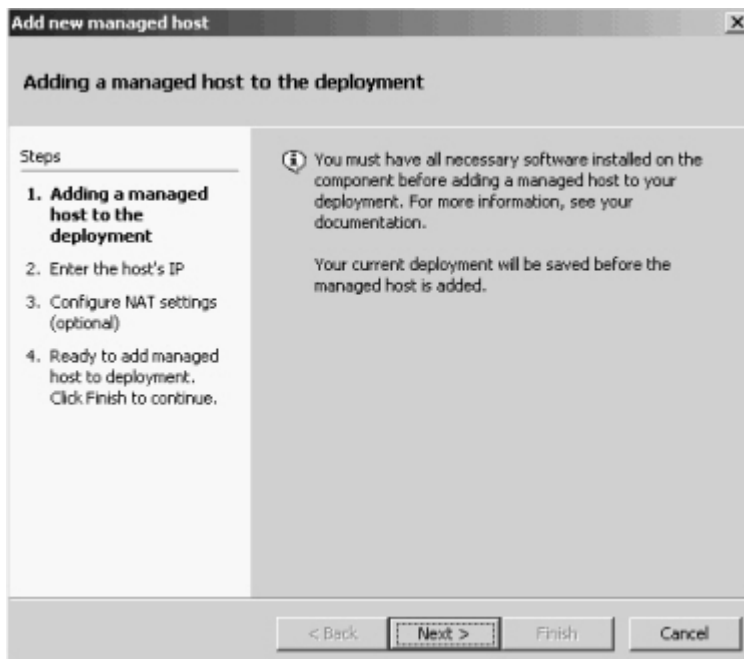
Note: Enabling encryption reduces the performance of a managed host by at least 50%.

Adding a Managed Host

To add a managed host:

Step 1 From the menu, select **Actions > Add a managed host**.

The Add new host wizard appears.



Step 2 Click **Next**.

The Enter the host's IP window appears.

Step 3 Enter values for the parameters:

- **Enter the IP of the server or appliance to add** - Specify the IP address of the host you want to add to your System View.
- **Enter the root password of the host** - Specify the root password for the host.
- **Confirm the root password of the host** - Specify the password again, for confirmation.
- **Host is NATed** - Select the check box if you want to use an existing Network Address Translation (NAT) on this managed host. For more information on NAT, see [Using NAT with STRM Log Manager](#).



Note: If you want to enable NAT for a managed host, the NATed network must be using static NAT translation. For more information on using NAT, see [Using NAT with STRM Log Manager](#).

- **Enable Encryption** - Select the check box if you want to create an encryption tunnel for the host.

If you selected the Host is NATed check box, the Configure NAT settings window appears. Go to [Step 4](#). Otherwise, go to [Step 5](#).



Note: If you want to add a non-NATed managed host to your deployment when the Console is NATed, you must change the Console to a NATed host (see [Changing the NAT Status for a Managed Host](#)) before adding the managed host to your deployment.

Step 4 To select a NATed network, enter values for the following parameters:

- **Enter public IP of the server or appliance to add** - Specify the public IP address of the managed host. The managed host uses this IP address to

communicate with another managed host that belongs to a different network using NAT.

- **Select NATed network** - Using the drop-down list box, select the network you want this managed host to use.
 - If the managed host is on the same subnet as the Console, make sure you select the Console of the NATed network.
 - If the managed host is not on the same subnet as the Console, make sure select managed host of the NATed network.



Note: For information on managing your NATed networks, see [Using NAT with STRM Log Manager](#).

Step 5 Click **Next**.

Step 6 Click **Finish**.



Note: If your deployment included undeployed changes, a window appears enabling you to deploy all changes.

The System View appears with the host in the Managed Hosts panel.

Editing a Managed Host

To edit an existing managed host:

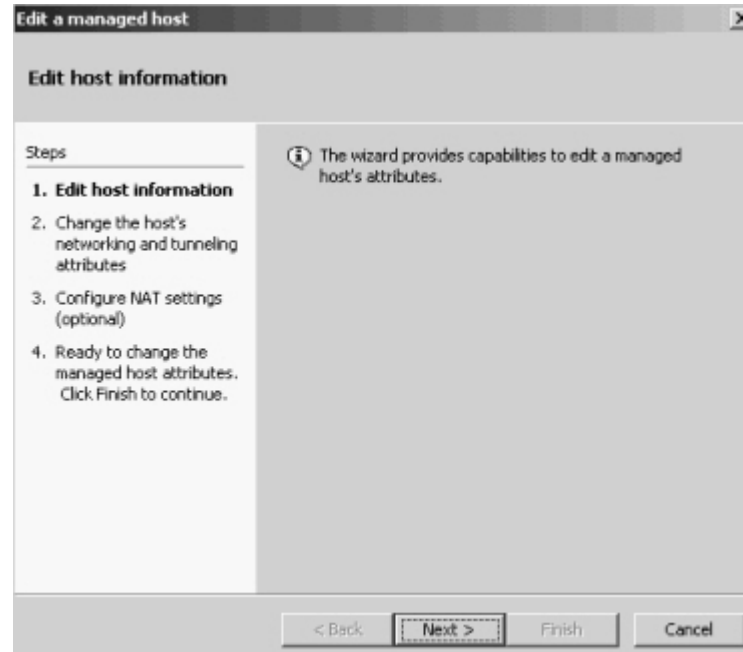
Step 1 Click the **System View** tab.

Step 2 Use the right mouse button (right-click) on the managed host you want to edit and select **Edit Managed Host**.

The Edit a managed host wizard appears.

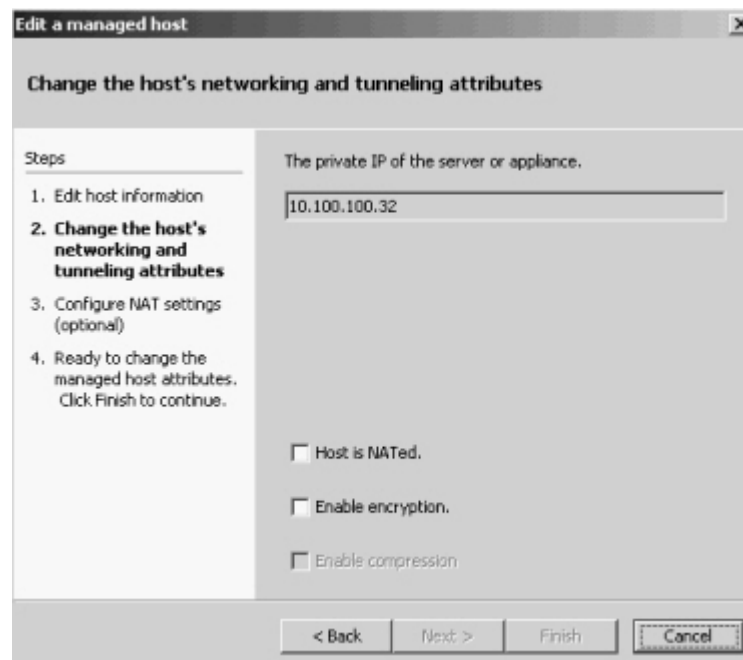


Note: This option is only available when the selected component has a managed host running a compatible version of STRM Log Manager software.



Step 3 Click **Next**.

The attributes window appears.



Step 4 Edit the following values, as necessary:

- **Host is NATed** - Select the check box if you want to use existing Network Address Translation (NAT) on this managed host. For more information on NAT, see [Using NAT with STRM Log Manager](#).



Note: If you want to enable NAT for a managed host, the NATed network must be using static NAT translation. For more information on using NAT, see [Using NAT with STRM Log Manager](#).

- **Enable Encryption** - Select the check box if you want to create an encryption tunnel for the host.

If you selected the Host is NATed check box, the Configure NAT settings window appears. Go to [Step 5](#). Otherwise, go to [Step 6](#).

Step 5 To select a NATed network, enter values for the following parameters:

- **Enter public IP of the server or appliance to add** - Specify the public IP address of the managed host. The managed host uses this IP address to communicate with another managed host that belongs to a different network using NAT.
- **Select NATed network** - Using the drop-down list box, select the network you want this managed host to use.



Note: For information on managing your NATed networks, see [Using NAT with STRM Log Manager](#).

Step 6 Click **Next**.

Step 7 Click **Finish**.

The System View appears with the updated host in the Managed Hosts panel.

Removing a Managed Host

You can only remove non-Console managed hosts from your deployment. You can not remove a managed host that is hosting the STRM Log Manager Console.

To remove a managed host:

Step 1 Click the **System View** tab.

Step 2 Use the right mouse button (right-click) on the managed host you want to delete and select **Remove host**.



Note: This option is only available when the selected component has a managed host running a compatible version of STRM Log Manager software.

A confirmation window appears.

Step 3 Click **Ok**.

Step 4 From the Admin tab menu, select **Advanced > Deploy Full Configuration**.

Using NAT with STRM Log Manager

Network Address Translation (NAT) translates an IP address in one network to a different IP address in another network. NAT provides increased security for your deployment since requests are managed through the translation process and essentially hides internal IP addresses.

Before you enable NAT for a STRM Log Manager managed host, you must set up your NATed networks using static NAT translation. This ensures communications between managed hosts that exist within different NATed networks.



Note: Your static NATed networks must be setup and configured on your network before you enable NAT using STRM Log Manager. For more information, see your network administrator.

You can add a non-NATed managed host using inbound NAT for a public IP address. You can also use a dynamic IP address for outbound NAT. However, both must be located on the same switch as the Console or managed host. You must configure the managed host to use the same IP address for the public and private IP addresses.

When adding or editing a managed host, you can enable NAT for that managed host. You can also use the deployment editor to manage your NATed networks including:

- [Adding a NATed Network to STRM Log Manager](#)
- [Editing a NATed Network](#)
- [Deleting a NATed Network From STRM Log Manager](#)
- [Changing the NAT Status for a Managed Host](#)

Adding a NATed Network to STRM Log Manager

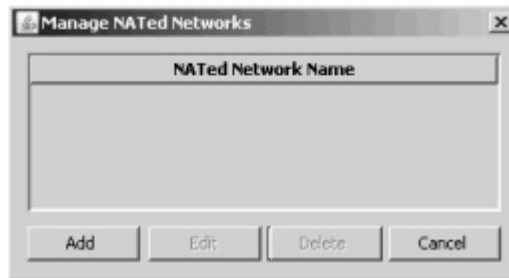
To add a NATed network to your STRM Log Manager deployment:

Step 1 In the deployment editor, click the  NATed networks button.



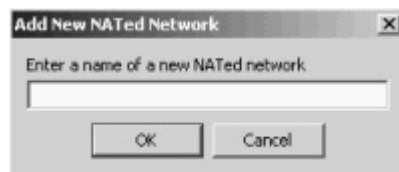
Note: You can also use the **Actions > Managed NATed Networks** menu option to access the *Managed NATed Networks* window.

The Manage NATed Networks window appears.



Step 2 Click **Add**.

The Add New NATed Network window appears.



Step 3 Enter a name of a network you want to use for NAT.

Step 4 Click **Ok**.

The Manage NATed Networks window appears.

- Step 5** Click **Ok**.
A confirmation window appears.

- Step 6** Click **Yes**.

Editing a NATed Network

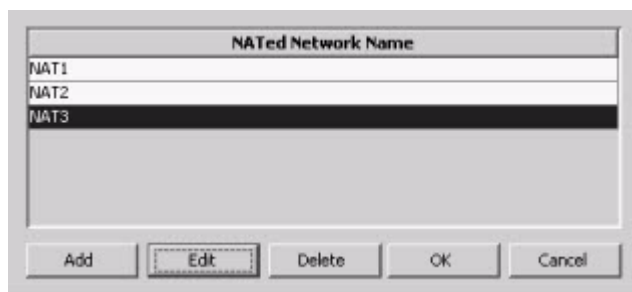
To edit a NATed network:

- Step 1** In the deployment editor, click the  NATed networks icon.



Note: You can also use the **Actions > Managed NATed Networks** menu option to access the Managed NATed Networks window.

The Manage NATed Networks window appears.



- Step 2** Select the NATed network you want to edit. Click **Edit**.
The Edit NATed Network window appears.
- Step 3** Update the name of the network you want to use for NAT.

- Step 4** Click **Ok**.
The Manage NATed Networks window appears.

- Step 5** Click **Ok**.
A confirmation window appears.

- Step 6** Click **Yes**.

Deleting a NATed Network From STRM Log Manager

To delete a NATed network from your deployment:

- Step 1** In the deployment editor, click the  NATed networks icon.



Note: You can also use the **Actions > Managed NATed Networks** menu option to access the Managed NATed Networks window.

The Manage NATed Networks window appears.

- Step 2** Select the NATed network you want to delete.
- Step 3** Click **Delete**.
A confirmation window appears.

- Step 4** Click **Ok**.

Step 5 Click **Yes**.

Changing the NAT Status for a Managed Host

To change your NAT status for a managed host, make sure you update the managed host configuration within STRM Log Manager before you update the device. This prevents the host from becoming unreachable and allows you to deploy changes to that host.

To change the status of NAT (enable or disable) for an existing managed host:

Step 1 In the deployment editor, click the **System View** tab.

Step 2 Use the right mouse button (right-click) on the managed host you want to edit and select **Edit Managed Host**.

The Edit a managed host wizard appears.

Step 3 Click **Next**.

The networking and tunneling attributes window appears.

Step 4 Choose one of the following:

a If you want to enable NAT for the managed host, select the check box. Go to [Step 5](#).



Note: *If you want to enable NAT for a managed host, the NATed network must be using static NAT translation.*

b If you want to disable NAT for the managed host, clear the check box. Go to [Step 6](#).

Step 5 To select a NATed network, enter values for the following parameters:

- **Change public IP of the server or appliance to add** - Specify the public IP address of the managed host. The managed host uses this IP address to communicate with another managed host that belongs to a different network using NAT.
- **Select NATed network** - Using the drop-down list box, select network you want this managed host to use.
- **Manage NATs List** - Update the NATed network configuration. For more information, see [Using NAT with STRM Log Manager](#).

Step 6 Click **Next**.

Step 7 Click **Finish**.

The System View appears with the updated host in the Managed Hosts panel.



Note: *Once you change the NAT status for an existing managed host error messages may appear. Ignore all error messages.*

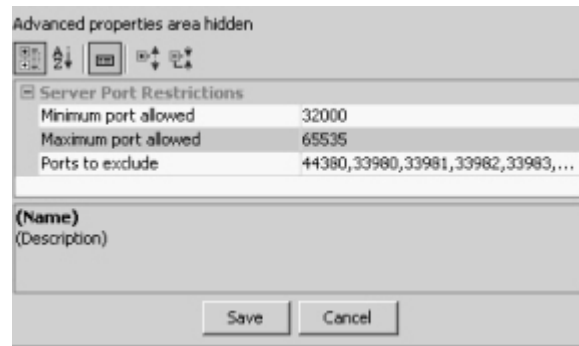
Step 8 Update the configuration for the device (firewall) to which the managed host is communicating.

Step 9 From the Admin tab menu, select **Advanced > Deploy Full Configuration**.

Configuring a Managed Host

- To configure a managed host:
- Step 1** From the System View, use the right mouse button (right-click) on the managed host you want to configure and select **Configure**.

The Configure host window appears.



- Step 2** Enter values for the parameters:
- **Minimum port allowed** - Specify the minimum port for which you want to establish communications.
 - **Maximum port allowed** - Specify the maximum port for which you want to establish communications.
 - **Ports to exclude** - Specify the port you want to exclude from communications. You can enter multiple ports you want to exclude. Separate multiple ports using a comma.
- Step 3** Click **Save**.

Assigning a Component to a Host

You can assign the STRM Log Manager components added in the Event Views to the managed hosts in your deployment. This section provides information on assigning a component to a host using the System View, however, you can also assign components to a host in the Event Views.

To assign a host:

- Step 1** Click the **System View** tab.
- Step 2** From the Managed Host list, select the managed host to which you want to assign a STRM Log Manager component.
- The System View of the host appears.
- Step 3** Select the component you want to assign to a managed host.
- Step 4** From the menu, select **Actions > Assign**.



Note: You can also use the right mouse button (right-click) to access the Actions menu items.

The Assign component wizard appears.

Step 5 From the Select a host to assign to drop-down list box, select the host that you want to assign to this component. Click **Next**.



Note: The drop-down list box only displays managed hosts that are running a compatible version of STRM Log Manager software.

Step 6 Click **Finish**.

Configuring Host Context

The Host Context component monitors all STRM Log Manager components to make sure that each component is operating as expected.

To configure Host Context:

Step 1 In the Deployment Editor, click the **System View** tab.

The System View appears.

Step 2 Select the Managed Host that includes the Host Context you want to configure.

Step 3 Select the Host Context component.

Step 4 From the menu, select **Actions > Configure**.



Note: You can also use the right mouse button (right-click) to access the Actions menu item.

The Host Context Configuration window appears.



Step 5 Enter values for the parameters:

Table 8-3 Host Context Parameters

Parameter	Description
Disk Usage Sentinel Settings	

Table 8-3 Host Context Parameters (continued)

Parameter	Description
Warning Threshold	<p>When the configured threshold of disk usage is exceeded, an e-mail is sent to the administrator indicating the current state of disk usage. The default is 0.75, therefore, when disk usage exceeds 75%, an e-mail is sent indicating that disk usage is exceeding 75%. If disk usage continues to increase above the configured threshold, a new e-mail is sent after every 5% increase in usage. By default, Host Context monitors the below partitions for disk usage:</p> <ul style="list-style-type: none"> • / • /store • /store/tmp <p>Specify the desired warning threshold for disk usage.</p> <p>Note: Notification e-mails are sent to the Administrative Email Address and are sent from the Alert Email From Address, which is configured in the System Settings. For more information, see Chapter 5 Setting Up STRM Log Manager.</p>
Recovery Threshold	<p>Once the system has exceeded the shutdown threshold, disk usage must fall below the recovery threshold before STRM Log Manager processes are restarted. The default is 0.90, therefore, processes will not be restarted until the disk usage is below 90%.</p> <p>Specify the recovery threshold.</p> <p>Note: Notification e-mails are sent to the Administrative Email Address and are sent from the Alert Email From Address, which is configured in the System Settings. For more information, see Chapter 5 Setting Up STRM Log Manager.</p>
Shutdown Threshold	<p>When the system exceeds the shutdown threshold, all STRM Log Manager processes are stopped. An e-mail is sent to the administrator indicating the current state of the system. The default is 0.95, therefore, when disk usage exceeds 95%, all STRM Log Manager processes stop.</p> <p>Specify the shutdown threshold.</p> <p>Note: Notification e-mails are sent to the Administrative Email Address and are sent from the Alert Email From Address, which is configured in the System Settings. For more information, see Chapter 5 Setting Up STRM Log Manager.</p>
Inspection Interval	Specify the frequency, in milliseconds, that you want to determine disk usage.
SAR Sentinel Settings	
Inspection Interval	Specify the frequency, in milliseconds, that you want to inspect SAR output. The default is 300,000 ms.

Table 8-3 Host Context Parameters (continued)

Parameter	Description
Alert Interval	Specify the frequency, in milliseconds, that you want to be notified that the thresholds have been exceeded. The default is 7,200,000 ms.
Time Resolution	Specify the time, in seconds, that you want the SAR inspection to be engaged. The default is 60 seconds.
Log Monitor Settings	
Inspection Interval	Specify the frequency, in milliseconds, that you want to monitor the log files. The default is 60,000 ms.
Monitored SYSLOG File Name	Specify a filename for the SYSLOG file. The default is /var/log/qradar.error.
Alert Size	Specify the maximum number of lines you want to monitor from the log file. The default is 1000.

Step 6 Click **Save**.

The System View appears.

Configuring STRM Log Manager Components

This section provides information on configuring STRM Log Manager components and includes:

- [Configuring an Event Collector](#)
- [Configuring an Event Processor](#)

Configuring an Event Collector

The Event Collector collects security events from various types of security devices in your network.

To configure an Event Collector:

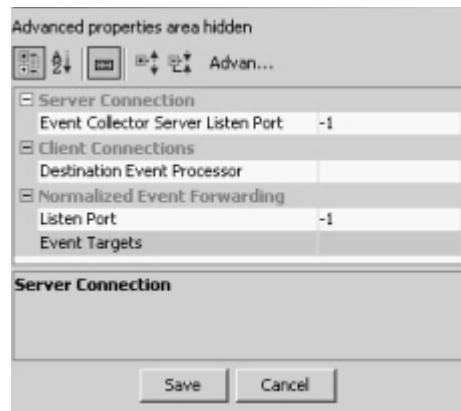
Step 1 From either the Event View or System View, select the Event Collector you want to configure.

Step 2 From the menu, select **Actions > Configure**.



Note: You can also use the right mouse button (right-click) to access the Action menu items.

The Event Collector Configuration window appears.

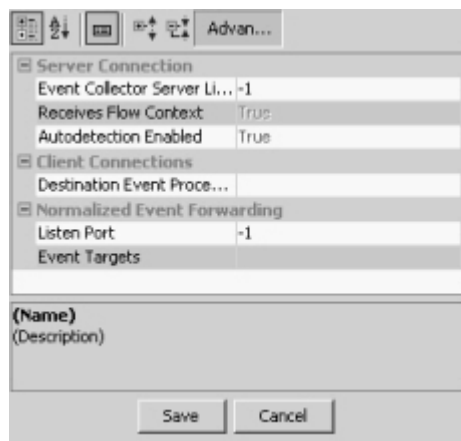


Step 3 Enter values for the parameters:

Table 8-4 Event Collector Parameters

Parameter	Description
Event Collector Server Listen Port	The Event Collector monitors at least one device per instance of the component.
Destination Event Processor	Specify the destination Event Processor for communications.
Listen Port	Specifies the listening port for event forwarding.
Event Targets	If the Event Collector includes an off-site target, this parameter specifies the normalized event forwarding device, separated by commas, using the following format: <device>:<type> This parameter is for informational purposes only and is not amendable.

Step 4 In the toolbar, click **Advanced** to display the advanced parameters. The advanced configuration parameter appear.



Step 5 Enter values for the parameters:

Table 8-5 Event Collector Advanced Parameters

Parameter	Description
Receives Flow Context	Specifies the first Event Collector installed in your deployment. This parameter is for informational purposes only and is not amendable.
Auto Detection Enabled	Specify if you want the Event Collector to auto analyze and accept traffic from previously unknown log sources. The default is true, which means that the Event Collector detects log sources in your network. Also, when set to True, the appropriate firewall ports are opened to enable auto detection to receive events. For more information on configuring log sources, see the <i>Managing Log Sources Guide</i> .

Step 6 Click **Save**.

The deployment editor appears.

Step 7 Repeat for all Event Collectors in your deployment you want to configure.

Configuring an Event Processor

The Event Processor processes events collected from one or more Event Collector(s).

To configure an Event Processor:

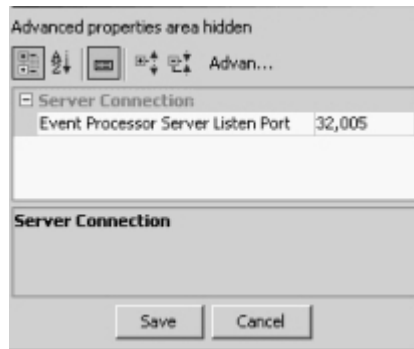
Step 1 From either the Event View or System View, select the Event Processor you want to configure.

Step 2 From the menu, select **Actions > Configure**.



Note: You can also use the right mouse button (right-click) to access the Action menu items.

The Event Processor Configuration window appears.

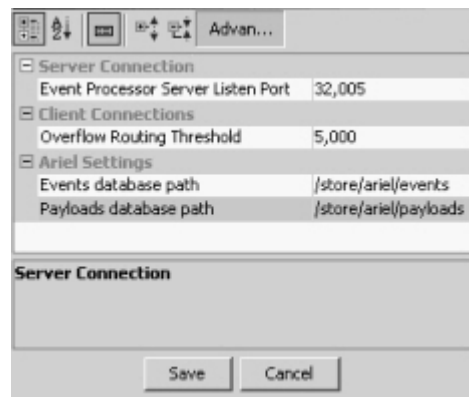


Step 3 Enter values for the parameters:

Table 8-6 Event Processor Parameters

Parameter	Description
Event Processor Server Listen Port	Specify the port that the Event Processor monitors for incoming connections. The default range is from 32,000 to 65,535.

- Step 4** In the toolbar, click **Advanced** to display the advanced parameters.
The advanced configuration parameters appear.



- Step 5** Enter values for the parameters, as necessary:

Table 8-7 Event Processor Parameters

Parameter	Description
Overflow Routing Threshold	Specify the events per second threshold that the Event Processor can manage events. Events over this threshold are placed in the cache.
Events database path	Specify the location you want to store events. The default is <code>/store/ariel/events</code> .
Payloads database path	Specify the location you want to store payload information. The default is <code>/store/ariel/payloads</code> .

- Step 6** Click **Save**.
The deployment editor appears.
- Step 7** Repeat for all Event Processors in your deployment you want to configure.

8

FORWARDING SYSLOG DATA

STRM Log Manager allows you to forward received log data to other products. You can forward syslog data (raw log data) received from devices as well as STRM Log Manager normalized event data. You can forward data on a per Event Collector/ Event Processor basis and you can configure multiple forwarding destinations. Also, STRM Log Manager ensures that all data that is forwarded is unaltered.

This chapter includes:

- [Adding a Syslog Destination](#)
- [Editing a Syslog Destination](#)
- [Delete a Syslog Destination](#)

Adding a Syslog Destination

To add a syslog forwarding destination:

- Step 1** Click the **Admin** tab.
- Step 2** In the navigation menu, click **Data Sources**.
The Data Sources panel appears.
- Step 3** Click the **Syslog Forwarding Destinations** icon.
The Syslog Forwarding Destinations window appears.



- Step 4** Click **Add**.
The Syslog Forwarding Destinations window appears.

Step 5 Enter values for the parameters:

- **Forwarding Event Collector** - Using the drop-down list box, select the deployed Event Collector from which you want to forward log data.
- **IP** - Enter the IP address of the system to which you want to forward log data.
- **Port** - Enter the port number on the system to which you want to forward log data.

Step 6 Click **Save**.

Editing a Syslog Destination

To edit a syslog forwarding destination:

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **Data Sources**.

The Data Sources panel appears.

Step 3 Click the **Syslog Forwarding Destinations** icon.

The Syslog Forwarding Destinations window appears.

Step 4 Select the entry you want to edit.

Step 5 Click **Edit**.

The Syslog Forwarding Destinations window appears.

Step 6 Update values, as necessary:

- **Forwarding Event Collector** - Using the drop-down list box, select the deployed Event Collector from which you want to forward log data.
- **IP** - Enter the IP address of the system to which you want to forward log data.
- **Port** - Enter the port number on the system to which you want to forward log data.

Step 7 Click **Save**.

Delete a Syslog Destination

To delete a syslog forwarding destination:

Step 1 Click the **Admin** tab.

Step 2 In the navigation menu, click **Data Sources**.

The Data Sources panel appears.

Step 3 Click the **Syslog Forwarding Destinations** icon.

The Syslog Forwarding Destinations window appears.

Step 4 Select the entry you want to delete.

Step 5 Click **Delete**.

A confirmation window appears.

Step 6 Click **Ok**.

A

JUNIPER NETWORKS MIB

This appendix provides information on the Juniper Networks Management Information Base (MIB). The Juniper Networks MIB allows you to send SNMP traps to other network management systems. The Juniper Networks OID is 1.3.6.1.4.1.20212.



Note: *STRM does not support outbound SNMP traps. For assistance with the Juniper Networks MIB, please contact Juniper Networks customer support.*

```
--  
-- Juniper Enterprise Specific MIB: Security Threat Response  
-- Manager (STRM) trap MIB.  
--  
-- Copyright (c) 2002-2006, Juniper Networks, Inc.  
-- All rights reserved.  
--  
-- The contents of this document are subject to change without  
-- notice.  
--
```

```
JUNIPER-STRM-TRAPS DEFINITIONS ::= BEGIN
```

```
IMPORTS
```

```
    MODULE-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE,  
    IPAddress  
        FROM SNMPv2-SMI  
    jnxStrm  
        FROM JUNIPER-SMI  
    DisplayString, DateAndTime, TruthValue,  
TEXTUAL-CONVENTION  
        FROM SNMPv2-TC;
```

```
strmTrapInfo MODULE-IDENTITY
```

```

LAST-UPDATED "200811101100Z"
  ORGANIZATION "Juniper Networks, Inc"
  CONTACT-INFO
    "      Juniper Technical Assistance Center
      Juniper Networks, Inc.
      1194 N. Mathilda Avenue
      Sunnyvale, CA 94089
      E-mail: support@juniper.net"
  DESCRIPTION "Security Threat Response Manger trap
definitions for STRM"
    ::= { jnxStrm 1 }

strmTrap OBJECT IDENTIFIER ::= { jnxStrm 0 }

---
--- Variables within the STRM Trap Info
--- .2636.7.1.*
---

strmLocalHostAddress OBJECT-TYPE
  SYNTAX IPAddress
  MAX-ACCESS accessible-for-notify
  STATUS current
  DESCRIPTION "IP address of the local machine where the
notification originated"
  ::= { strmTrapInfo 1 }

strmTimeString OBJECT-TYPE
  SYNTAX DisplayString (SIZE(0..64))
  MAX-ACCESS accessible-for-notify
  STATUS current
  DESCRIPTION "Time offense was created or time the event rule
fired. Example 'Mon Apr 28 10:14:49 GMT 2008'"
  ::= { strmTrapInfo 2 }

strmTimeInMillis OBJECT-TYPE
  SYNTAX Counter64

```

```

MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Time offense was created or time the event rule
fired in milliseconds"
::= { strmTrapInfo 3 }

---
--- Offense Properties
---

strmOffenseID OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Offense ID"
::= { strmTrapInfo 4 }

strmOffenseDescription OBJECT-TYPE
SYNTAX DisplayString (SIZE(0..1024))
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Description of the Offense"
::= { strmTrapInfo 6 }

strmOffenseLink OBJECT-TYPE
SYNTAX DisplayString (SIZE(0..1024))
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "HTTP link to the offense"
::= { strmTrapInfo 7 }

strmMagnitude OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Offense magnitude"
::= { strmTrapInfo 8 }

strmSeverity OBJECT-TYPE

```

```

SYNTAX Integer32
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Offense severity"
 ::= { strmTrapInfo 9 }

strmCreditibility OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Offense creditibility"
 ::= { strmTrapInfo 10 }

strmRelevance OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Offense relevance"
 ::= { strmTrapInfo 11 }

---
--- Attacker Properties
---

strmAttackerIP OBJECT-TYPE
    SYNTAX IpAddress
    MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Attacker IP"
 ::= { strmTrapInfo 12 }

strmAttackerUserName OBJECT-TYPE
SYNTAX DisplayString (SIZE(0..1024))
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Attacker's User Name"
 ::= { strmTrapInfo 13 }

strmAttackerCount OBJECT-TYPE

```

```

SYNTAX Counter64
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Total Number of Attackers"
 ::= { strmTrapInfo 14 }

strmTop5AttackerIPs OBJECT-TYPE
SYNTAX DisplayString (SIZE(0..1024))
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Top 5 Attackers by Magnitude(comma separated)"
 ::= { strmTrapInfo 15 }

strmTopAttackerIP OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Top Attacker IPs"
 ::= { strmTrapInfo 16 }

strmTop5AttackerUsernames OBJECT-TYPE
SYNTAX DisplayString (SIZE(0..1024))
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Top 5 Attackers by Magnitude(comma separated)"
 ::= { strmTrapInfo 48 }

strmTopAttackerUsername OBJECT-TYPE
SYNTAX DisplayString (SIZE(0..32))
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Top Attacker IPs"
 ::= { strmTrapInfo 49 }

strmAttackerNetworks OBJECT-TYPE
SYNTAX DisplayString (SIZE(0..1024))
MAX-ACCESS accessible-for-notify
STATUS current

```

```

DESCRIPTION "Attacker Networks(comma separated)"
 ::= { strmTrapInfo 17 }

---
--- Target Properties
---
strmTargetIP OBJECT-TYPE
    SYNTAX IPAddress
    MAX-ACCESS accessible-for-notify
    STATUS current
    DESCRIPTION "Target IP"
    ::= { strmTrapInfo 18 }

strmTargetUserName OBJECT-TYPE
    SYNTAX DisplayString (SIZE(0..64))
    MAX-ACCESS accessible-for-notify
    STATUS current
    DESCRIPTION "Target's User Name"
    ::= { strmTrapInfo 19 }

strmTargetCount OBJECT-TYPE
    SYNTAX Counter64
    MAX-ACCESS accessible-for-notify
    STATUS current
    DESCRIPTION "Total Number of Targets"
    ::= { strmTrapInfo 20 }

strmTop5TargetIPs OBJECT-TYPE
    SYNTAX DisplayString (SIZE(0..1024))
    MAX-ACCESS accessible-for-notify
    STATUS current
    DESCRIPTION "Top 5 Target IPs by Magnitude"
    ::= { strmTrapInfo 21 }

strmTopTargetIP OBJECT-TYPE
    SYNTAX IPAddress
    MAX-ACCESS accessible-for-notify
    STATUS current

```

```

DESCRIPTION "Top Target"
::= { strmTrapInfo 22 }

strmTop5TargetUsernames OBJECT-TYPE
SYNTAX DisplayString (SIZE(0..1024))
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Top 5 Target Usernames by Magnitude"
::= { strmTrapInfo 50 }

strmTopTargetUsername OBJECT-TYPE
SYNTAX DisplayString (SIZE(0..32))
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Top Target"
::= { strmTrapInfo 51 }

strmTargetNetworks OBJECT-TYPE
SYNTAX DisplayString (SIZE(0..1024))
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Target Networks(comma separated)"
::= { strmTrapInfo 23 }

---
--- Category properties
---

strmCategoryCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Total Number of Categories"
::= { strmTrapInfo 24 }

strmTop5Categories OBJECT-TYPE
SYNTAX DisplayString (SIZE(0..1024))
MAX-ACCESS accessible-for-notify
STATUS current

```

```

DESCRIPTION "Top 5 Categories(comma separated)"
 ::= { strmTrapInfo 25 }

strmTopCategory OBJECT-TYPE
SYNTAX DisplayString (SIZE(0..64))
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Top Category"
 ::= { strmTrapInfo 26 }

strmCategoryID OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Category ID of Event that triggered the Event CRE
Rule"
 ::= { strmTrapInfo 27 }

strmCategory OBJECT-TYPE
SYNTAX DisplayString (SIZE(0..64))
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Category of the Event that triggered the Event CRE
Rule"
 ::= { strmTrapInfo 28 }

---
--- Annotation Properties
---

strmAnnotationCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Total Number of Annotations"
 ::= { strmTrapInfo 29 }

strmTopAnnotation OBJECT-TYPE
SYNTAX DisplayString (SIZE(0..1024))

```

```

MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Top Annotation"
 ::= { strmTrapInfo 30 }

---
--- Rule Properties
---

strmRuleCount OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Total Number of Rules contained in the Offense"
 ::= { strmTrapInfo 31 }

strmRuleNames OBJECT-TYPE
SYNTAX DisplayString (SIZE(0..1024))
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Names of the Rules that contributed to the
Offense(comma separated)"
 ::= { strmTrapInfo 32 }

strmRuleID OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "ID of the Rule that was triggered in the CRE"
 ::= { strmTrapInfo 33 }

strmRuleName OBJECT-TYPE
SYNTAX DisplayString (SIZE(0..256))
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Name of the Rules that was triggered in the CRE"
 ::= { strmTrapInfo 34 }

strmRuleDescription OBJECT-TYPE

```

```

SYNTAX DisplayString (SIZE(0..1024))
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Description/Notes of the Rules that was triggered
in the CRE"
 ::= { strmTrapInfo 35 }

---
--- Event Properties
---

strmEventCount OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Total Number of Events contained in the Offense"
 ::= { strmTrapInfo 36 }

strmEventID OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "ID of the Event that triggered the Event CRE Rule"
 ::= { strmTrapInfo 37 }

strmQid OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "QID of the Event that triggered the Event CRE Rule"
 ::= { strmTrapInfo 38 }

strmEventName OBJECT-TYPE
SYNTAX DisplayString (SIZE(0..256))
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Name of the Event that triggered the Event CRE
Rule"
 ::= { strmTrapInfo 39 }

```

```

strmEventDescription OBJECT-TYPE
  SYNTAX DisplayString (SIZE(0..1024))
  MAX-ACCESS accessible-for-notify
  STATUS current
  DESCRIPTION "Description/Notes of the Event that triggered the
  Event CRE Rule"
  ::= { strmTrapInfo 40 }

---
--- IP Properties
---

strmSourceIP OBJECT-TYPE
  SYNTAX IpAddress
  MAX-ACCESS accessible-for-notify
  STATUS current
  DESCRIPTION "Source IP of the Event that triggered the Event CRE
  Rule"
  ::= { strmTrapInfo 41 }

strmSourcePort OBJECT-TYPE
  SYNTAX Integer32
  MAX-ACCESS accessible-for-notify
  STATUS current
  DESCRIPTION "Source Port of the Event that triggered the Event
  CRE Rule"
  ::= { strmTrapInfo 42 }

strmDestinationIP OBJECT-TYPE
  SYNTAX IpAddress
  MAX-ACCESS accessible-for-notify
  STATUS current
  DESCRIPTION "Destination IP of the Event that triggered the
  Event CRE Rule"
  ::= { strmTrapInfo 43 }

strmDestinationPort OBJECT-TYPE
  SYNTAX Integer32
  MAX-ACCESS accessible-for-notify

```

```

STATUS current
DESCRIPTION "Destination Port of the Event that triggered the
Event CRE Rule"
::= { strmTrapInfo 44 }

strmProtocol OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Protocol of the Event that triggered the Event CRE
Rule"
::= { strmTrapInfo 45 }

strmAttackerPort OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Source Port of the Event that triggered the Event
CRE Rule"
::= { strmTrapInfo 46 }

strmTargetPort OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS accessible-for-notify
STATUS current
DESCRIPTION "Destination Port of the Event that triggered the
Event CRE Rule"
::= { strmTrapInfo 47 }

---
--- STRM Trap Notifications
--- .2636.7.0.*
---

strmEventCRENotification NOTIFICATION-TYPE
OBJECTS {
strmLocalHostAddress,
strmTimeString,
strmRuleName,
strmRuleDescription,

```

```

strmAttackerIP,
strmAttackerPort,
strmAttackerUserName,
strmAttackerNetworks,
strmTargetIP,
strmTargetPort,
strmTargetUserName,
strmTargetNetworks,
strmProtocol,
strmQid,
strmEventName,
strmEventDescription,
strmCategory
}
STATUS current
DESCRIPTION "Event CRE Notification"
::= { strmTrap 1 }

```

```

strmOffenseCRENotification NOTIFICATION-TYPE
OBJECTS {
strmLocalHostAddress,
strmTimeString,
strmRuleName,
strmRuleDescription,
strmOffenseID,
strmOffenseDescription,
strmOffenseLink,
strmMagnitude,
strmSeverity,
strmCreditibility,
strmRelevance,
strmEventCount,
strmCategoryCount,
strmTop5Categories,
strmAttackerIP,
strmAttackerUserName,
strmAttackerNetworks,
strmAttackerCount,

```

```
    strmTop5AttackerIPs,  
    strmTargetIP,  
    strmTargetUserName,  
    strmTargetNetworks,  
    strmTargetCount,  
    strmTop5TargetIPs,  
    strmRuleCount,  
    strmRuleNames,  
    strmAnnotationCount,  
    strmTopAnnotation.1,  
    strmTopAnnotation.2,  
    strmTopAnnotation.3,  
    strmTopAnnotation.4,  
    strmTopAnnotation.5,  
  }  
  STATUS current  
  DESCRIPTION "Offense CRE Notification"  
  ::= { strmTrap 2 }  
  
END
```

B

VIEWING AUDIT LOGS

Changes made by STRM Log Manager users are recorded in the audit logs. You can view the audit logs to monitor changes to STRM Log Manager and the users performing those changes.

All audit logs are stored in plain text and are archived and compressed once the audit log file reaches a size of 200 MB. The current log file is named `audit.log`. Once the file reaches a size of 200 MB, the file is compressed and renamed as follows: `audit.1.gz`, `audit.2.gz`, etc with the file number incrementing each time a log file is archived. STRM Log Manager stores up to 50 archived log files.

This appendix provides information on using the audit logs including:

- [Logged Actions](#)
- [Viewing the Log File](#)

Logged Actions

STRM Log Manager logs the following categories of actions in the audit log file:

Table 2-1 Logged Actions

Category	Action
User Authentication	Log in to STRM Log Manager.
	Log out of STRM Log Manager.
Administrator Authentication	Log in to the STRM Log Manager Admin tab.
	Log out of the STRM Log Manager Admin tab.
System Management	Shutdown a system.
	Restart a system.
Session Authentication	Create a new administration session.
	Terminate an administration session.
	Deny an invalid authentication session.
	Expire a session authentication.
	Create an authentication session.
Terminate an authentication session.	

Table 2-1 Logged Actions (continued)

Category	Action
User Authentication Ariel	Deny a login attempt.
	Add an Ariel property.
	Delete an Ariel property.
	Edit an Ariel property.
	Add an Ariel property extension.
	Delete an Ariel property extension.
	Edit an Ariel property extension.
Root Login	Log in to STRM Log Manager, as root.
	Log out of STRM Log Manager, as root.
Rules	Add a rule.
	Delete a rule.
	Edit a rule.
User Accounts	Add an account.
	Edit an account.
	Delete an account.
User Roles	Add a role.
	Edit a role.
	Delete a role.
Log Sources	Add a log source.
	Edit a log source.
	Delete a log source.
	Add a log source group.
	Edit a log source group.
	Delete a log source group.
	Edit the DSM parsing order.
Log Source Extension	Add an log source extension.
	Edit the log source extension.
	Delete a log source extension.
	Upload a log source extension.
	Upload a log source extension successfully.
	Upload an invalid log source extension.
	Download a log source extension.
	Report a log source extension.
	Modify a log sources association to a log source or log source type.

Table 2-1 Logged Actions (continued)

Category	Action
Log Source Extension	Add an log source extension.
	Edit the log source extension.
	Delete a log source extension.
	Upload a log source extension.
	Upload a log source extension successfully.
	Upload an invalid log source extension.
	Download a log source extension.
	Report a log source extension.
	Modify a log sources association to a log source or log source type.
Protocol Configuration	Add a protocol configuration.
	Delete a protocol configuration.
	Edit a protocol configuration.
Reports	Add a template.
	Delete a template.
	Edit a template.
	Execute a template.
	Delete a report.
Groups	Add a group.
	Delete a group.
	Edit a group.
Backup and Recovery	Edit the configuration.
	Initiate the backup.
	Complete the backup.
	Fail the backup.
	Delete the backup.
	Synchronize the backup.
	Cancel the backup.
	Initiate the restore.
	Upload a backup.
	Upload an invalid backup.
	Delete the backup.
Purge the backup.	
Asset	Delete all assets.

Table 2-1 Logged Actions (continued)

Category	Action
High Availability	Add an HA host.
	Remove an HA host.
	Set an HA system offline.
	Set an HA system online.
	Restore an HA system.
QIDmap	Add a QID map entry.
	Edit a QID map entry.
Ariel Properties	Add a custom event property.
	Edit a custom event property.
	Delete a custom property.
Ariel Property Extensions	Add a custom event property expression.
	Edit a custom event property expression.
	Delete a custom event property expression.
Installation	Install a .rpm package, such as a DSM update.
License	Add a license key.
	Edit a license key.

Viewing the Log File

To view the audit logs:

Step 1 Log in to STRM Log Manager as root.

Step 2 Go to the following directory:

```
/var/log/audit
```

Step 3 Open the desired audit log file.

Each entry in the log file displays using the following format:



Note: The maximum size of any audit message (not including date, time, and host name) is 1024 characters.

```
<date_time> <host name> <user>@<IP address> (thread ID)
[<category>] [<sub-category>] [<action>] <payload>
```

Where:

<date_time> is the date and time of the activity in the format: Month Date HH:MM:SS.

<host name> is the host name of the Console where this activity was logged.

<user> is the name of the user that performed the action.

<IP address> is the IP address of the user that performed the action.

(thread ID) is the identifier of the Java thread that logged this activity.

<category> is the high-level category of this activity.

<sub-category> is the low-level category of this activity.

<action> is the activity that occurred.

<payload> is the complete record that has changed, if any. This may include a user record or an event rule.

For example:

```
Nov  6 12:22:31 localhost.localdomain admin@10.100.100.15
(Session) [Authentication] [User] [Login]

Nov  6 12:22:31 localhost.localdomain jsam@10.100.100.15 (0)
[Configuration] [User Account] [Account Modified]
username=james, password=/oJDuxP7YXUYQ, networks=ALL,
email=sam@qllabs.com, userrole=Admin

Nov 13 10:14:44 localhost.localdomain admin@10.100.45.61 (0)
[Configuration] [FlowSource] [FlowSourceModified] Flowsource(
name="tim", enabled="true", deployed="false",
asymmetrical="false", targetQflow=DeployedComponent(id=3),
flowsourceType=FlowsourceType(id=6),
flowsourceConfig=FlowsourceConfig(id=1))
```


INDEX

A

- Admin tab
 - about 3
 - using 4
- administrator role 9
- Ariel database 103
- audience 1
- audit log
 - viewing 126
- authentication
 - configuring 17
 - LDAP 16
 - RADIUS 16
 - system 16
 - TACACS 16
 - user 16
- auto detection 102
- automatic update
 - about 49
 - on demand 53
 - scheduling 50

B

- backup and recovery 65

C

- changes
 - deploying 4
- command line max matched results 55
- components 100
- console
 - settings 60
- conventions 1
- customer support
 - contacting 2

D

- database settings 55
- deploying changes 4
- deployment editor 77
 - about 77
 - accessing 79
 - creating your deployment 81
 - event view 82
 - preferences 82
 - STRM Log Manager components 100
 - requirements 81
 - system view 87
 - toolbar 80
 - using 79

- device access 23
- device management 26

E

- encryption 84, 85, 87
- Event Collector
 - about 82
 - configuring 100
- Event Processor
 - about 82
 - configuring 102
- event view
 - about 78
 - adding components 83
 - building 82
 - connecting components 83
 - renaming components 87
- events role 10

F

- firewall access 23

H

- hashing
 - algorithm 56
- high availability 33
 - adding 34
 - editing 40
 - restoring a failed host 42
 - setting HA host offline 41
 - setting HA host online 42
- host
 - adding 89
- host context 78, 98

I

- interface roles 26
- IP right click menu extension role 10

L

- LDAP/Active directory 16
- license key
 - exporting 21
 - managing 19

M

managed host
 adding 89
 assigning components 97
 editing 91
 removing 93
 set-up 25
 maximum real-time results 55
 MIB 109

N

NAT
 editing 95
 enabling 93
 removing 95
 using with STRM Log Manager 93
 Network Address Translation. See NAT
 network hierarchy
 creating 45
 NTP 30

O

off-site source 85
 off-site target 85

P

passwords
 changing 27

R

RADIUS authentication 16
 RDATE 28
 recovery 65
 role 7
 Admin 9
 creating 8
 editing 11
 events 10
 IP right click menu extension 10
 managing 7
 reporting 10

S

search results retention period 55
 SNMP agent
 accessing 22
 SNMP settings 57
 source
 off-site 84, 85
 syslog
 forwarding 105
 adding 105
 deleting 107
 editing 106
 system authentication 16

system settings 54
 configuring 54, 61
 system thresholds 58
 system time 28
 system view
 about 78
 assigning components 97
 Host Context 98
 managed host 97
 managing 88

T

TACACS authentication 16
 target
 off-site 84, 85
 thresholds 58
 time 28
 time limit
 command like execution 55
 reporting execution 55
 web execution 55
 transaction sentry 56

U

user
 creating account 13
 editing account 14, 15
 managing 7
 roles 7
 users
 authentication 16