



Security Threat Response Manager

STRM Log Management Administration Guide

Release 2008.2 R2

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 530-027298-01, Revision 1

Copyright Notice

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

FCC Statement

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

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

Disclaimer

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

STRM Log Management Administration Guide
Release 2008.2 R2

Copyright © 2008, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Revision History

September 2008—Revision 1

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

CONTENTS

ABOUT THIS GUIDE

Audience	1
Conventions	1
Technical Documentation	1
Contacting Customer Support	2

1 OVERVIEW

About the Interface	3
Accessing the Administration Console	4
Using the Interface	4
Deploying Changes	5
Viewing STRM Log Management Audit Logs	5
Logged Actions	6
Viewing the Log File	7

2 MANAGING USERS

Managing Roles	9
Creating a Role	9
Editing a Role	11
Managing User Accounts	12
Creating a User Account	12
Editing a User Account	13
Disabling a User Account	14
Authenticating Users	15

3 SETTING UP STRM LOG MANAGEMENT

Managing Your License Keys	19
Updating your License Key	20
Exporting Your License Key Information	21
Creating Your Network Hierarchy	22
Considerations	22
Defining Your Network Hierarchy	23
Scheduling Automatic Updates	26
Configuring System Settings	27
Configuring System Notifications	31
Configuring the Console Settings	33

Starting and Stopping STRM Log Management	35
Accessing the Embedded SNMP Agent	35
Configuring Access Settings	36
Configuring Firewall Access	36
Updating Your Host Set-up	38
Configuring Interface Roles	39
Changing Passwords	40
Updating System Time	40

4 MANAGING BACKUP AND RECOVERY

Managing Backup Archives	45
Viewing Back Up Archives	45
Importing an Archive	46
Deleting a Backup Archive	47
Backing Up Your Information	48
Scheduling Your Backup	48
Initiating a Backup	49
Restoring Your Configuration Information	50

5 USING THE DEPLOYMENT EDITOR

About the Deployment Editor	54
Accessing the Deployment Editor	55
Using the Editor	55
Creating Your Deployment	57
Before you Begin	57
Editing Deployment Editor Preferences	58
Building Your Event View	58
Adding Components	59
Connecting Components	60
Forwarding Normalized Events	61
Renaming Components	63
Managing Your System View	63
Setting Up Managed Hosts	64
Using NAT with STRM Log Management	68
Configuring a Managed Host	72
Assigning a Component to a Host	72
Configuring Host Context	73
Configuring STRM Log Management Components	76
Configuring an Event Collector	76
Configuring an Event Processor	77

6 FORWARDING SYSLOG DATA

Adding a Syslog Destination	79
Editing a Syslog Destination	80
Delete a Syslog Destination	81

A Q1 LABS MIB

INDEX




ABOUT THIS GUIDE

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

Audience This guide is intended for the system administrator responsible for setting up STRM Log Management in your network. This guide assumes that you have STRM Log Management 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 Networks support web site at <https://juniper.net/support>. Once you access the Juniper Networks support web site, locate the product and software release for which you require documentation.

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

documentation@juniper.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 Log Management, you can contact Customer Support as follows:

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

1

OVERVIEW

This chapter provides an overview of the STRM Log Management Administration Console and STRM Log Management administrative functionality including:

- [About the Interface](#)
- [Accessing the Administration Console](#)
- [Using the Interface](#)
- [Deploying Changes](#)
- [Viewing STRM Log Management Audit Logs](#)

About the Interface

You must have administrative privileges to access the Administration Console. The STRM Log Management Administration Console provides access to following administrative functionality:

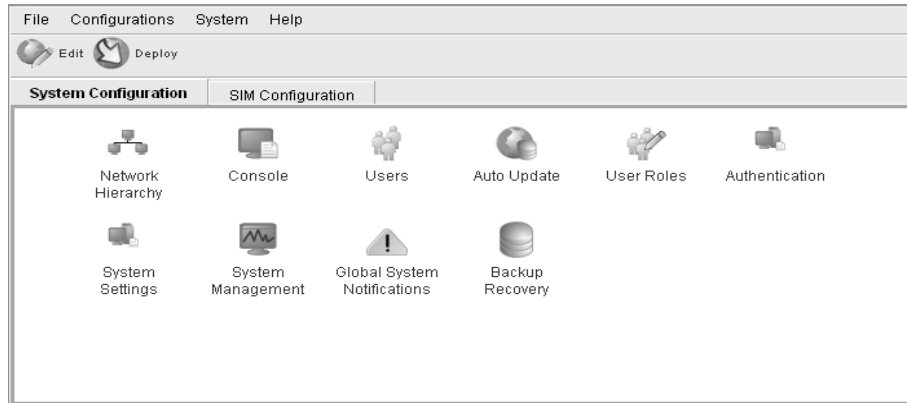
- Manage users. See [Chapter 2 Managing Users](#).
- Manage STRM Log Management. See [Chapter 3 Setting Up STRM Log Management](#).
- Backup and recover your data. See [Chapter 4 Managing Backup and Recovery](#).
- Manage your deployment views. See [Chapter 5 Using the Deployment Editor](#).
- Configure syslog forwarding. See [Chapter 6 Forwarding Syslog Data](#).

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

Accessing the Administration Console

You can access the STRM Log Management Administration Console through the main STRM Log Management interface. Also, you can create a shortcut on your desktop that allows you to access the Administration Console directly.

To access the Administration Console, click **Config** in the main STRM Log Management interface. The Administration Console appears.



Using the Interface

The Administration Console provides several tab and menu options that allow you to configure STRM Log Management including:

- **System Configuration** - Provides access to administrative functionality, such as, user management, automatic updates, license key, network hierarchy, system settings, system thresholds, backup and recovery and Console configuration.
- **SIM Configuration** - Provides access to sensor device management and syslog forwarding.

The Administration Console also includes several menu options including:

Table 1-1 Administrative Console Menu Options



Menu Option	Sub-Menu	Description
File	Close	Closes the Administration Console.
Configurations	Deployment Editor	Opens the deployment editor interface.
	Deploy configuration changes	Deploys any configuration changes from the current session to your deployment.
	Deploy All	Deploys all configuration settings to your deployment.
System	STRM Start	Starts the STRM Log Management application.

Table 1-1 Administrative Console Menu Options (continued)

Menu Option	Sub-Menu	Description
	STRM Stop	Stops the STRM Log Management application.
	STRM Restart	Restarts the STRM Log Management application.
Help	Help and Support	Opens user documentation.
	About STRM	Displays version information.

The Administration Console provides several toolbar options including:

Table 1-2 Administration Console Toolbar Options

Icon	Description
 Edit	Opens the deployment editor interface.
 Deploy	Deploys all changes made through the Administration Console.

Deploying Changes

Once you update your configuration settings using the Administration Console, you must save those changes to the staging area. You must either manually deploy all changes using the Deploy menu option or, upon exit, a window appears prompting you to deploy changes before you exit. All deployed changes are then enforced throughout your deployment.

Using the Administration Console menu, you can deploy changes as follows:

- **Deploy All** - Deploys all configuration settings to your deployment.
- **Deploy configuration changes** - Deploys any configuration changes from the current session to your deployment.

Viewing STRM Log Management Audit Logs

Changes made by STRM Log Management users are recorded in the audit logs. You can view the audit logs to monitor changes to STRM Log Management 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 Management stores up to 50 archived log files.

This section provides information on using the audit logs including:

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

Logged Actions STRM Log Management logs the following categories of actions in the audit log file:

Table 1-3 Logged Actions

Category	Action
User Authentication	Log in to STRM Log Management
User Authentication	Log out of STRM Log Management
Administrator Authentication	Log in to the STRM Log Management Administration Console
Administrator Authentication	Log out of the STRM Log Management Administration Console
Root Login	Log in to STRM Log Management, as root
	Log out of STRM Log Management, as root
User Accounts	Adding an account
	Editing an account
	Deleting an account
User Roles	Adding a role
	Editing a role
	Deleting a role
Sensor Devices	Adding a sensor device
	Editing a sensor device
	Deleting a sensor device
	Adding a sensor device group
	Editing a sensor device group
	Deleting a sensor device group
Protocol Configuration	Adding a protocol configuration
	Deleting a protocol configuration
	Editing a protocol configuration
Syslog Forwarding	Adding a syslog forwarding
	Deleting a syslog forwarding
	Editing a syslog forwarding
Reports	Adding a template
	Deleting a template
	Editing a template
	Executing a template
	Deleting a report
Groups	Adding a group
	Deleting a group
	Editing a group

Table 1-3 Logged Actions

Category	Action
Sensor Device Extension	Adding an sensor device extension
	Editing the sensor device extension
	Deleting a sensor device extension
	Uploading a sensor device extension
	Uploading a sensor device extension successfully
	Downloading a sensor device extension
	Reporting a sensor device extension
	Modifying a sensor devices association to a device or device type.
Backup and Recovery	Editing the configuration
	Initiating the backup
	Completing the backup
	Failing the backup
	Deleting the backup
	Synchronizing the backup
	Cancelling the backup
	Initiating the restore
	Uploading a backup
	Uploading an invalid backup
	Deleting the backup
License	Adding a license key.
	Editing a license key.

Viewing the Log File To view the audit logs:

Step 1 Log in to STRM Log Management 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))
```

2

MANAGING USERS

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

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

You can add or remove user accounts for all users that you wish to access STRM Log Management. Each user is associated with a role, which determines the privileges the user has to functionality and information within STRM Log Management. You can also restrict or allow access to areas of the network. By default, the STRM Log Management Administrative (admin) user has unrestricted access to all components of your deployment. You can create multiple admin accounts for your STRM Log Management system.

Managing Roles

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

- Create a role. See [Creating a Role](#).
- Edit a role. See [Editing a Role](#)

Creating a Role

To create a role:

- Step 1** In the Administration Console, click the **System Configuration** tab.
The System Configuration panel appears.
- Step 2** Click the **User Roles** icon.
The Manage User Roles window appears.
- Step 3** Click **Create Role**.

Manage Role Permissions

Role Name

Select the permissions associated with this role.

Administrator Event Viewer

System Administrator Event Search Restrictions Override

Administrator Manager Customized Rule Creation

Reporting

Distribute Reports via Email

Maintain Templates

Step 4 Enter values for the parameters. You must select at least one permission to proceed.

Table 2-1 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.
Administrator	Select the check box if you wish to grant this user administrative access to the STRM Log Management interface. Within the administrator role, you can grant additional access to the following: <ul style="list-style-type: none"> • System Administrator - Select this check box if you wish to allow users access to all areas of STRM Log Management. Also users with this access are not able to edit other administrator accounts. • Administrator Manager - Select this check box if you wish 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.
Event Viewer	Select the check box if you wish this user to have access to the Event Viewer. Within the Event Viewer, you can also grant users additional access to the following: <ul style="list-style-type: none"> • Event Search Restrictions Override - Select the check box if you wish to allow users the ability to override event search restrictions. • Customized Rule Creation functionality - Select the check box if you wish to allow users to create rules using the Event Viewer. <p>For more information on the Event Viewer, see the <i>STRM Log Management Users Guide</i>.</p>

Table 2-1 Create Roles Parameters (continued)

Parameter	Description
Reporting	<p>Select the check box if you wish 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"> • Distribute Reports via Email - Select the check box if you wish to allow users to distribute reports through e-mail. • Maintain Templates - Select the check box if you wish to allow users to maintain reporting templates. <p>For more information, see the <i>STRM Log Management Users Guide</i>.</p>

Step 5 Click **Save**.

Step 6 Click **Return**.

Step 7 Close the Manage Roles window.

The STRM Log Management Administration Console appears.

Step 8 From the menu, select **Configurations > Deploy configuration changes**.

Editing a Role To edit a role:

Step 1 In the Administration Console, click the **System Configuration** tab.

The System Configuration panel appears.

Step 2 Click the **User Roles** icon.

The Manage Role window appears.

Step 3 For the role you wish to edit, click the edit icon.

The Permissions for Role window appears.

Step 4 Update the permissions (see [Table 2-1](#)), as necessary.

Step 5 Click **Return**.

Step 6 Click **Save**.

Step 7 Close the Manage User Roles window.

The STRM Log Management Administration Console appears.

Step 8 From the menu, select **Configurations > Deploy configuration changes**.

Managing User Accounts

You can create a STRM Log Management user account, which allows a user access to selected network components using the STRM Log Management 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 Management 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 Management user:

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

The screenshot shows a 'User Details' form with the following fields: Username, Password, Confirm password, Email Address, and a dropdown menu for Select Role. At the bottom of the form are 'Cancel' and 'Next' buttons.

- Step 4** Enter values for the following parameters:

Table 2-2 User Details Parameters

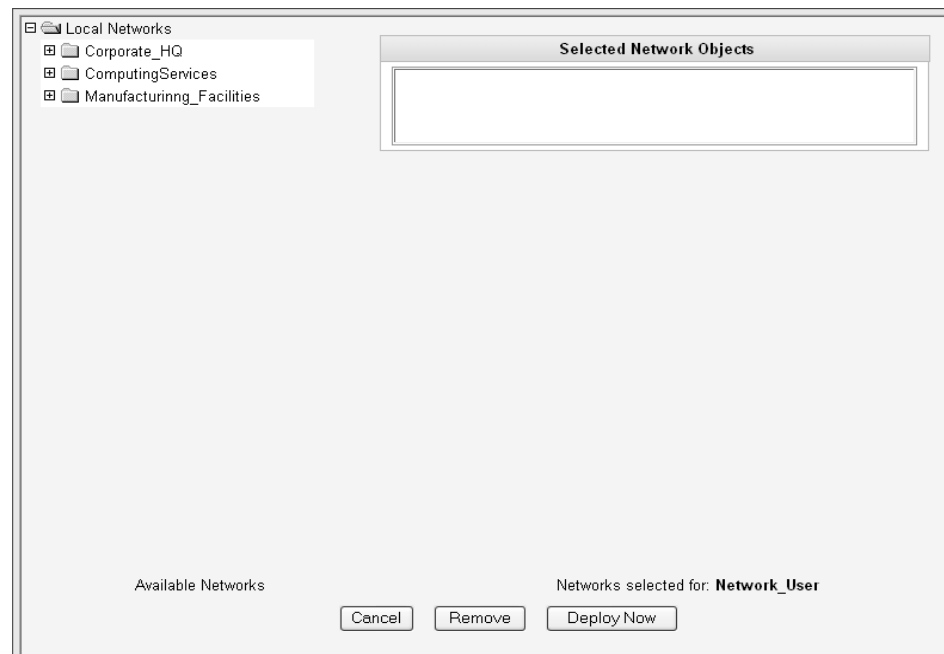
Parameter	Description
Username	Specify a username for the new user. The username must not include spaces or special characters.
Password	Specify a password for the user to gain access. The password must be at least 5 characters in length.
Confirm Password	Re-enter the password for confirmation.
Email Address	Specify the user's e-mail address.

Table 2-2 User Details Parameters (continued)

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

Step 5 Click **Next**.

The Selected Network Objects window appears.



Step 6 From the menu tree, select the network objects you wish this user to be able to monitor.

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

Step 7 Choose one of the following options:

- a Click **Deploy Now** to deploy new user information immediately.
- b Click **Cancel** to cancel all updates and return to the Manage Users window.

Step 8 Close the Manage Users window.

The STRM Log Management Administration Console appears.

Editing a User Account To edit a user account:

Step 1 In the Administration Console, click the **System Configuration** tab.

The System Configuration panel appears.

Step 2 Click the **Users** icon.

The Manage Users window appears.

Step 3 In the Manage Users area, click the user account you wish to edit.

The User Details window appears.

Step 4 Update values (see [Table 2-2](#)), as necessary.

Step 5 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 9](#).

Step 6 From the menu tree, select the network objects you wish this user to access.

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

Step 7 For all network objects you wish to remove access, select the object from the Selected Network Objects panel and click **Remove**.

Step 8 Choose one of the following options:

a Click **Deploy Now** to deploy new user information immediately.

b Click **Cancel** to return to cancel all updates and return to the Manage Users window.

Step 9 Close the Manage Users window.

The STRM Log Management Administration Console appears.

Disabling a User Account To disable a user account:

Step 1 In the Administration Console, click the **System Configuration** tab.

The System Configuration panel appears.

Step 2 Click the **Users** icon.

The Manage Users window appears.

Step 3 In the Manage Users area, click the user account you wish to disable.

The User Details window appears.

Step 4 In the Role drop-down list box, select **Disabled**.

Step 5 Click **Next**.

Step 6 Close the Manage Users window.

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

Authenticating Users

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

- **System Authentication** - Users are authenticated locally by STRM Log Management. 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 login, STRM Log Management 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 login, STRM Log Management 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 wish 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 Management.
- Make sure the server has the appropriate user accounts and privilege levels to communicate with STRM Log Management. See your server documentation for more information.
- Make sure the time of the authentication server is synchronized with the time of the STRM Log Management server. For more information on setting STRM Log Management time, see [Chapter 3 Setting Up STRM Log Management](#).

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 3 Setting Up STRM Log Management - Configuring the Console Settings](#). An administrative user can always access STRM Log Management through a third party authentication module or by using the local STRM Log Management Admin password

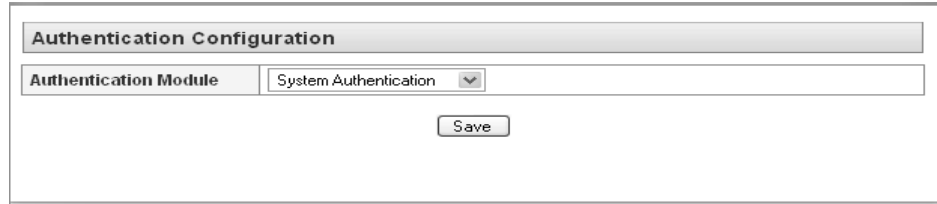
To configure authentication:

Step 1 In the Administration Console, click the **System Configuration** tab.

The System Configuration panel appears.

Step 2 Click the **Authentication** icon.

The Authentication window appears.



Step 3 From the Authentication Module drop-down list box, select the authentication type you wish to configure.

Step 4 Configure the selected authentication type:

- a If you selected **System Authentication**, go to [Step 5](#)
- b If you selected **RADIUS Authentication**, enter values for the following parameters:

Table 2-3 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 wish 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. • ASCII • PAP (Password Authentication Protocol) - Sends clear text between the user and the server.
Shared Secret	Specify the shared secret that STRM Log Management uses to encrypt RADIUS passwords for transmission to the RADIUS server.

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

Table 2-4 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.

Table 2-4 TACACS Parameters (continued)

Parameter	Description
Authentication Type	Specify the type of authentication you wish to perform. The options are: <ul style="list-style-type: none"> • 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 Management 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 2-5 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 wish to use, for example, DC=Q1LABS,DC=INC.
LDAP Domain	Specify the domain you wish to use, for example q1labs.inc

Step 5 Click **Save**.

3

SETTING UP STRM LOG MANAGEMENT

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

- [Managing Your License Keys](#)
- [Creating Your Network Hierarchy](#)
- [Scheduling Automatic Updates](#)
- [Configuring System Settings](#)
- [Configuring System Notifications](#)
- [Configuring the Console Settings](#)
- [Starting and Stopping STRM Log Management](#)
- [Accessing the Embedded SNMP Agent](#)
- [Configuring Access Settings](#)

Managing Your License Keys

For your STRM Log Management Console, a default license key provides you access to the interface for 5 weeks. You must manage your license key using the System Management window in the Administration Console. This interface 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 wish 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.

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 Management 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, please contact your local sales representative.
- For all other technical issues, please contact Juniper Customer Support.

If you log in to STRM Log Management and your Console license key has expired, you are automatically directed to the System 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 Management window to update that license key.

To update your license key:

Step 1 In the Administration Console, click the **System Configuration** tab.

The System Configuration panel appears.

Step 2 Click the **System Management** icon.

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

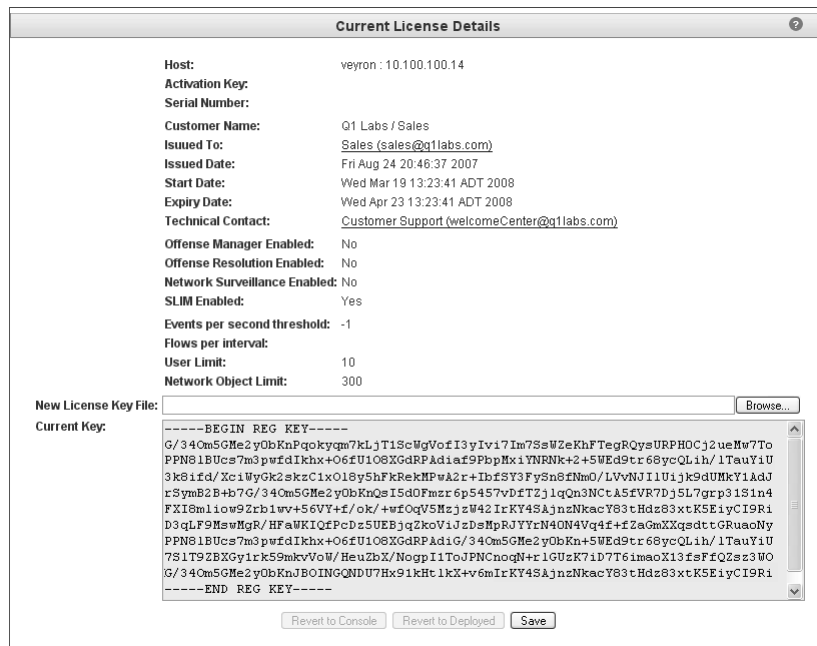
Step 3 For the host that on which you wish to update the license key, click the value that appears in the License column.



Note: *If you update the license key for your Console, all systems in your deployment default to the Console license key at that time.*

The Current License Details window appears.

Step 4 Click **Browse** beside the New License Key File and locate the license key.



Step 5 Once you locate and select the license key, click **Open**.

The Current License Details window appears.

Step 6 Click **Save**.

A message appears indicating the license key was successfully updated.



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

Step 7 Close the license key window.

The Administration Console appears.

Step 8 From the menu, select **Configurations > Deploy All**.

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 In the Administration Console, click the **System Configuration** tab.

The System Configuration panel appears.

Step 2 Click the **System Management** icon.

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

System Management	 Export Licenses 
--------------------------	---

Host Name	View Agent	Manage System	License	Serial Number
veyron (console)	View Agent	Manage System	Valid	

Step 3 Click **Export Licenses**.

The export window appears.

Step 4 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 5 Click **OK**.

Creating Your Network Hierarchy

STRM Log Management uses the network hierarchy to understand your network traffic and provide you with the ability to view network activity 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 Management does not have to resemble the physical deployment of your network. STRM Log Management 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 Management 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
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 wish 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** In the Administration Console, click the **System Configuration** tab.
The System Configuration panel appears.
- Step 2** Click the **Network Hierarchy** icon.
The Network Views window appears.
- Step 3** From the menu tree, select the areas of the network you wish to add a network component.
The Manage Group window appears for the selected network component.
- Step 4** Click **Add**.
The Add Network Object window appears.
- Step 5** Enter your network object values:

Table 3-1 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 1 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 .
Description	Specify a description for this network object.
Color	Specify a color for this object.
Database Length	Specify the database length.

- Step 6** Click **Save**.
- Step 7** Repeat for all network objects.

Step 8 Click **Re-Order**.

The Reorder Group window appears.

Step 9 Order the network objects in the desired order.**Step 10** Click **Save**.

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

Accepted CIDR Values

[Table 3-2](#) provides a list of the CIDR values that STRM Log Management accepts:

Table 3-2 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
/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

Table 3-2 Accepted CIDR Values (continued)

CIDR Length	Mask	Number of Networks	Hosts
/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 natural mask of /24.
- 209.60.128.0 /22 is a supernet which 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 Management uses system configuration files to provide useful characterizations of network data flows. You can now update your configuration files automatically or manually using the STRM Log Management interface to make sure your configuration files contain the latest network security information. The updates, located on the Juniper Networks support web site, include threats, vulnerabilities, and geographic information from various security related web sites. The managed host 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 Management 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 Management deployment. However, you must have the views created in your deployment editor. For more information on using the deployment editor, see [Chapter 5 Using the Deployment Editor](#).



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

To schedule automatic updates:

Step 1 In the Administration Console, click the **System Configuration** tab.

The System Configuration panel appears.

Step 2 Click the **Auto Update** icon.

The Auto Update Configuration window appears.

Step 3 In the Schedule Autoupdates section, select the check box to enable automatic updates.

Step 4 In the Frequency list box, select the frequency of the updates in the Frequency list box:

- **Daily** - Updates are downloaded every day at 1 am.
- **Weekly** - Updates are downloaded every Sunday at 1 am.
- **Monthly** - Updates are downloaded on the first day of every month at 1 am.

Step 5 Click **Save** save your settings or click **Save and Update Now** to initiate the update process immediately.

Step 6 From the menu, select **Configurations > Deploy Configuration Changes**.

The updates are enforced through your deployment.



Note: STRM automatic updates are not enforced through your deployment automatically. After each automatic update, you must log in to STRM and from the Administration Console menu, select **Configurations > Deploy Configuration Changes**.

Configuring System Settings

Using the Administration Console, you can configure the system, database, and sentry settings.

To configure system settings:

Step 1 In the Administration Console, click the **System Configuration** tab.

The System Configuration panel appears.

Step 2 Click the **System Settings** icon.

The System Management window appears.

Step 3 Enter values for the parameters:

Table 3-3 System Settings Parameters

Parameter	Description
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 wish 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.

Table 3-3 System Settings Parameters (continued)

Parameter	Description
Audit Log Enable	Enables or disables the ability to collect audit logs. You can view audit log information using the Event Viewer. The default is Yes.
Coalescing Events	Enables or disables the ability for a sensor device to coalesce (bundle) events. This value applies to all sensor devices. However, if you wish to alter this value for a specific sensor device, edit the Coalescing Event parameter in the sensor device configuration. For more information, see the <i>Managing Sensor Devices Guide</i> . The default is Yes.
Store Event Payload	Enables or disables the ability for a sensor device to store event payload information. This value applies to all auto detected sensor devices. However, if you wish to alter this value for a specific sensor device, edit the Event Payload parameter in the sensor device configuration. For more information, see the <i>Managing Sensor Devices Guide</i> . The default is Yes.
Global Iptables Access	Specify the IP address of a non-Console system that does not have IP tables configuration to which you wish to enable direct access. To enter multiple systems, enter a comma separated list of IP addresses.
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	
Device Log Storage Location	Specify the location that you wish to store the device log information. The default location is /store/ariel/events.
Device Log Data Retention Period	Specify the amount of time that you wish to store the device log data. The default is 30 days.
Maximum Real Time Results	Specify the maximum number of results you wish to view in the Event Viewer and Flow Viewer. The default is 10000.
Reporting Max Matched Results	Specify the maximum number of results you wish a report to return. This value applies to the search results in the Event Viewer. The default is 1000000.
Command Line Max Matched Results	Specify the maximum number of results you wish the command line to return. The default is 0.
Web Execution Time Limit	Specify the maximum amount of time, in seconds, you wish a query in the interface to process before a time out occurs. This value applies to the search results in the Event Viewer and Flow Viewer. The default is 600 seconds.

Table 3-3 System Settings Parameters (continued)

Parameter	Description
Reporting Execution Time Limit	Specify the maximum amount of time, in seconds, you wish a reporting query to process before a time out occurs. The default is 57600 seconds.
Command Line Execution Time Limit	Specify the maximum amount of time, in seconds, you wish 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 Management to store a hash file for every stored event log file. The default is No.
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 wish 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, NIST FIPS 180-1. • SHA-256 - Algorithm defined by the draft Federal Information Processing Standard 180-2, Secure Hashing Standard (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, Secure Hashing Standard (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, Secure Hashing Standard (SHS). SHA-512 is a bit hash algorithm intended to provide 256 bits of security.
SNMP Settings	
Enable	Enables or disables SNMP responses in the STRM Log Management custom rules engine. The default is No, which means you do not wish to accept events using SNMP.
Destination Host	Specify the IP address to which you wish to send SNMP notifications.

Table 3-3 System Settings Parameters (continued)

Parameter	Description
Destination Port	Specify the port to which you wish to send SNMP notifications. The default is 162.
Community (V2)	Specify the SNMP community, such as public. This parameter only applies if you are using SNMPv2.
User Name	Specify the name of the user you wish 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 wish to use to authenticate SNMP traps.
Authentication Password	Specify the password you wish to use to authenticate SNMP.
Privacy Protocol	Specify the protocol you wish to use to decrypt SNMP traps.
Privacy Password	Specify the password used to decrypt SNMP traps.
Embedded SNMP Agent Settings	
Enabled	Enables or disables access to data from the SNMP Agent using SNMP requests. The default is No.
Community String	Specify the SNMP community, such as public. This parameter only applies if you are using SNMPv2 and SNMPv3.
IP Access List	Specify the systems that can access data from the SNMP agent using SNMP request. If the Enabled option is set to Yes, this option is enforced.

Step 4 Click **Save**.

The STRM Log Management Administration Console appears.

Step 5 From the menu, select **Configurations > Deploy All**.

Configuring System Notifications

You can configure global system performance alerts for thresholds using the STRM Log Management Administration Console. This section provides information for configuring your global system thresholds.

To configure global system thresholds:

- Step 1** In the Administration Console, click the **System Configuration** tab.
The System Configuration panel appears.
- Step 2** Click the **Global System Notifications** icon.
The Global System Notifications window appears.
- Step 3** 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.
 - **Resolution Message** - Specify a description of the preferred resolution to the alert.

Table 3-4 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.
System load over 1 minute	Specify the threshold system load average over the last minute.
System load over 5 minute	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.

Table 3-4 Global System Notifications Parameters (continued)

Parameter	Description
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 cache 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, in kilobytes, of used swap memory.
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.
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.

Table 3-4 Global System Notifications Parameters (continued)

Parameter	Description
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 4 Click **Save**.

The STRM Log Management Administration Console appears.

Step 5 From the menu, select **Configurations > Deploy configuration changes**.

Configuring the Console Settings

The STRM Log Management Console provides the interface for STRM Log Management. This Console is also used to manage distributed STRM Log Management 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 Management administrator. STRM Log Management supports the following web browsers:

- Internet Explorer 6.0 or 7.0
- Mozilla Firefox 2.0

To configure STRM Log Management Console settings:

Step 1 In the Administration Console, click the **System Configuration** tab.

The System Configuration panel appears.

Step 2 Click the **Console** icon.

The Console Management window appears.

The screenshot shows the QRadar Console Management interface with the following settings:

- Console Settings:**
 - Enable 3D graphs in the user interface: No
- Authentication Settings:**
 - Persistent Session Timeout (in days): 0
 - Maximum Login Failures: 5
 - Login Failure Attempt Window (in minutes): 10
 - Login Failure Block Time (in minutes): 30
 - Login Host Whitelist: (empty text field)
 - Inactivity Timeout (in minutes): 0
 - Login Message File: (empty text field)
- DNS Settings:**
 - Enable DNS Lookups for Host Identity: True
- Data Export Settings:**
 - Include Header in CSV Exports: No
 - Maximum Simultaneous Exports: 1

A "Save" button is located at the bottom of the settings area.

Step 3 Enter values for the parameters:

Table 3-5 STRM Log Management 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.
Authentication Settings	
Persistent Session Timeout	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 delimited 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.

Table 3-5 STRM Log Management Console Management Parameters (continued)

Parameter	Description
Login Message File	Specify the location and name of a file that includes content you wish to appear on the STRM Log Management 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.
DNS Settings	
Enable DNS Lookups for Host Identity	Enable or disable the ability for STRM Log Management 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.
Data Export Settings	
Include Header in CSV Exports	Specify whether you wish to include a header in a CSV export file.
Maximum Simultaneous Exports	Specify the maximum number of exports you wish to occur at one time.

Step 4 Click **Save**.

Step 5 From the Administration Console menu, select **Configurations > Deploy configuration changes**.

Starting and Stopping STRM Log Management

To start, stop, or restart STRM Log Management:

- Step 1** In the main STRM Log Management interface, click **Config**.
The STRM Log Management Administration Console appears.
- Step 2** From the System menu, select one of the following options:
- a STRM Start
 - b STRM Stop
 - c STRM Restart

Accessing the Embedded SNMP Agent

To access the SNMP agent:

- Step 1** In the Administration Console, click the **System Configuration** tab.
The System Configuration panel appears.
- Step 2** Click the **System Management** icon.
The System Management window appears.

System Management Export Licenses ?				
Host Name	View Agent	Manage System	License	Serial Number
veyron (console)	View Agent	Manage System	Valid	

Step 3 In the View Agent column, click **View Agent** for the SNMP agent you wish to access.

The SNMP Agent appears.

Configuring Access Settings

The System Configuration tab provides access 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 Management. Also, you can define access to the web-based system administration interface.

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

Step 1 In the Administration Console, click the **System Configuration** tab.

The System Configuration panel appears.

Step 2 Click the **System Management** icon.

The System Management window appears.

Step 3 For the host you wish to configure firewall access, click **Manage System**.

Step 4 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 5 From the menu, select **Managed Host Config > Local Firewall**.

The Local Firewall window appears.

Local Firewall

Device Access

Enter the IP addresses of the systems that should be allowed to connect to this device below, along with the ports they require access to.

If the list is empty, all device access will be disabled.

IP Address: Protocol: Any Port: Allow

Remove Selected

System Administration Web Control

Enter the IP addresses that should be allowed to connect to this administration interface below.

If the list is empty, access controls will be disabled.

IP Address: Allow

Remove Selected

Apply Access Controls

Step 6 In the Device Access box, you must include any STRM Log Management systems you wish 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 wish to have access.
- b From the Protocol list box, select the protocol you wish 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 wish to enable communications.



Note: If you change your External Flow Source Monitoring Port parameter in the QFlow Configuration, you must also update your firewall access configuration.

- d Click **Allow**.

Step 7 In the System Administration Web Control box, enter the IP address of managed hosts that you wish 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 wish to access the interface. Failing to do so may affect connectivity.

Step 8 Click **Apply Access Controls**.

Step 9 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 wish STRM Log Management to use, the global password for STRM Log Management configuration, and the IP address for the STRM Log Management Console:

To configure your host set-up:

Step 1 In the Administration Console, click the **System Configuration** tab.

The System Configuration panel appears.

Step 2 Click the **System Management** icon.

The System Management window appears.

Step 3 For the host you wish to update your host set-up, click **Manage System**.

Step 4 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 5 From the menu, select **Managed Host Config > STRM Log Management Setup**.

The STRM Log Management Setup window appears.

QRadar-SLIM Setup

Console Information
Enter the IP address of the QRadar-SLIM console:

Enter the address of the mail server QRadar-SLIM should use.
Mail server:

Global QRadar-SLIM Configuration Password
Enter the global configuration password:
Confirm the global configuration password:

Web Address
Enter the web address of the console:

Step 6 You must enable communications between the STRM Log Management Console and the current host. In the **Enter the IP address of the STRM Log Management console** field, enter the IP address of the managed host operating the STRM Log Management Console.

Step 7 In the **Mail Server** field, specify the address for the mail server you wish STRM Log Management to use. STRM Log Management uses this mail server to

distribute alerts and event messages. To use the mail server provided with STRM Log Management, enter **localhost**.

Step 8 In the **Enter the global configuration password**, enter the password you wish 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 9 In the **Enter the web address of the console** field, enter the IP address of the managed host operating the STRM Log Management Console.

Step 10 Click **Apply Configuration**.

Configuring Interface Roles

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

To assign roles:

Step 1 In the Administration Console, click the **System Configuration** tab.

The System Configuration panel appears.

Step 2 Click the **System Management** icon.

The System Management window appears.

Step 3 For the host you wish to configure interface roles, click **Manage System**.

Step 4 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 5 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 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	PCI device 8086:1076 (Intel Corp.) (rev 5) IP Address: 10.100.100.25 Netmask: 255.255.255.0 Gateway: 10.100.100.1	Management
eth1	PCI device 8086:1076 (Intel Corp.) (rev 5)	Disabled ▾

- Step 6** For each interface listed, select the role you wish to assign to the interface using the Role list box.
- Step 7** Click **Save Configuration**.
- Step 8** Wait for the interface to refresh before continuing.

Changing Passwords To change the passwords:

- Step 1** In the Administration Console, click the **System Configuration** tab. The System Configuration panel appears.
- Step 2** Click the **System Management** icon. The System Management window appears.
- Step 3** For the host you wish to change passwords, click **Manage System**.
- Step 4** 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 5** From the menu, select **Managed Host Config > Root Password**. The Root Passwords window appears.

Root Password

Enter new root password below:

New Root Password:

Confirm New Root Password:

Step 6 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 7 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: 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 In the Administration Console, click the **System Configuration** tab.

The System Configuration panel appears.

Step 2 Click the **System Management** icon.

The System Management window appears.

Step 3 For the host on which you wish to configure time, click **Manage System**.

Step 4 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 5 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.

System Time																																																																																																																																																	
Day	Date	Month	Year	Hour																																																																																																																																													
Friday	7	March	2008	11:33:11																																																																																																																																													
<input type="button" value="Apply"/> <input type="button" value="Set system time to hardware time"/>																																																																																																																																																	
Hardware Time																																																																																																																																																	
Day	Date	Month	Year	Hour																																																																																																																																													
Friday	7	March	2008	11:33:11																																																																																																																																													
<input type="button" value="Save"/> <input type="button" value="Set hardware time to system time"/>																																																																																																																																																	
Time Zone																																																																																																																																																	
Change timezone to: America/Halifax (Atlantic Time - Nova Scotia (most places), PEI)																																																																																																																																																	
<input type="button" value="Save"/>																																																																																																																																																	
Time Server																																																																																																																																																	
Timeserver hostnames or addresses: boxster																																																																																																																																																	
<input checked="" type="checkbox"/> Set hardware time too																																																																																																																																																	
Synchronize on schedule? <input type="radio"/> No <input type="radio"/> Yes, at times below ..																																																																																																																																																	
<input type="radio"/> Simple schedule .. Hourly <input type="radio"/> Times and dates selected below ..																																																																																																																																																	
Minutes	Hours	Days	Months	Weekdays																																																																																																																																													
<input type="radio"/> All <input type="radio"/> Selected ..	<input type="radio"/> All <input type="radio"/> Selected ..	<input type="radio"/> All <input type="radio"/> Selected ..	<input type="radio"/> All <input type="radio"/> Selected ..	<input type="radio"/> All <input type="radio"/> Selected ..																																																																																																																																													
<table border="1"> <tr><td>0</td><td>12</td><td>24</td><td>36</td><td>48</td></tr> <tr><td>1</td><td>13</td><td>25</td><td>37</td><td>49</td></tr> <tr><td>2</td><td>14</td><td>26</td><td>38</td><td>50</td></tr> <tr><td>3</td><td>15</td><td>27</td><td>39</td><td>51</td></tr> <tr><td>4</td><td>16</td><td>28</td><td>40</td><td>52</td></tr> <tr><td>5</td><td>17</td><td>29</td><td>41</td><td>53</td></tr> <tr><td>6</td><td>18</td><td>30</td><td>42</td><td>54</td></tr> <tr><td>7</td><td>19</td><td>31</td><td>43</td><td>55</td></tr> <tr><td>8</td><td>20</td><td>32</td><td>44</td><td>56</td></tr> <tr><td>9</td><td>21</td><td>33</td><td>45</td><td>57</td></tr> <tr><td>10</td><td>22</td><td>34</td><td>46</td><td>58</td></tr> <tr><td>11</td><td>23</td><td>35</td><td>47</td><td>59</td></tr> </table>	0	12	24	36	48	1	13	25	37	49	2	14	26	38	50	3	15	27	39	51	4	16	28	40	52	5	17	29	41	53	6	18	30	42	54	7	19	31	43	55	8	20	32	44	56	9	21	33	45	57	10	22	34	46	58	11	23	35	47	59	<table border="1"> <tr><td>0</td><td>12</td></tr> <tr><td>1</td><td>13</td></tr> <tr><td>2</td><td>14</td></tr> <tr><td>3</td><td>15</td></tr> <tr><td>4</td><td>16</td></tr> <tr><td>5</td><td>17</td></tr> <tr><td>6</td><td>18</td></tr> <tr><td>7</td><td>19</td></tr> <tr><td>8</td><td>20</td></tr> <tr><td>9</td><td>21</td></tr> <tr><td>10</td><td>22</td></tr> <tr><td>11</td><td>23</td></tr> <tr><td>12</td><td>24</td></tr> </table>	0	12	1	13	2	14	3	15	4	16	5	17	6	18	7	19	8	20	9	21	10	22	11	23	12	24	<table border="1"> <tr><td>1</td><td>13</td><td>25</td></tr> <tr><td>2</td><td>14</td><td>26</td></tr> <tr><td>3</td><td>15</td><td>27</td></tr> <tr><td>4</td><td>16</td><td>28</td></tr> <tr><td>5</td><td>17</td><td>29</td></tr> <tr><td>6</td><td>18</td><td>30</td></tr> <tr><td>7</td><td>19</td><td>31</td></tr> <tr><td>8</td><td>20</td><td></td></tr> <tr><td>9</td><td>21</td><td></td></tr> <tr><td>10</td><td>22</td><td></td></tr> <tr><td>11</td><td>23</td><td></td></tr> <tr><td>12</td><td>24</td><td></td></tr> </table>	1	13	25	2	14	26	3	15	27	4	16	28	5	17	29	6	18	30	7	19	31	8	20		9	21		10	22		11	23		12	24		<table border="1"> <tr><td>January</td></tr> <tr><td>February</td></tr> <tr><td>March</td></tr> <tr><td>April</td></tr> <tr><td>May</td></tr> <tr><td>June</td></tr> <tr><td>July</td></tr> <tr><td>August</td></tr> <tr><td>September</td></tr> <tr><td>October</td></tr> <tr><td>November</td></tr> <tr><td>December</td></tr> </table>	January	February	March	April	May	June	July	August	September	October	November	December	<table border="1"> <tr><td>Sunday</td></tr> <tr><td>Monday</td></tr> <tr><td>Tuesday</td></tr> <tr><td>Wednesday</td></tr> <tr><td>Thursday</td></tr> <tr><td>Friday</td></tr> <tr><td>Saturday</td></tr> </table>	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
0	12	24	36	48																																																																																																																																													
1	13	25	37	49																																																																																																																																													
2	14	26	38	50																																																																																																																																													
3	15	27	39	51																																																																																																																																													
4	16	28	40	52																																																																																																																																													
5	17	29	41	53																																																																																																																																													
6	18	30	42	54																																																																																																																																													
7	19	31	43	55																																																																																																																																													
8	20	32	44	56																																																																																																																																													
9	21	33	45	57																																																																																																																																													
10	22	34	46	58																																																																																																																																													
11	23	35	47	59																																																																																																																																													
0	12																																																																																																																																																
1	13																																																																																																																																																
2	14																																																																																																																																																
3	15																																																																																																																																																
4	16																																																																																																																																																
5	17																																																																																																																																																
6	18																																																																																																																																																
7	19																																																																																																																																																
8	20																																																																																																																																																
9	21																																																																																																																																																
10	22																																																																																																																																																
11	23																																																																																																																																																
12	24																																																																																																																																																
1	13	25																																																																																																																																															
2	14	26																																																																																																																																															
3	15	27																																																																																																																																															
4	16	28																																																																																																																																															
5	17	29																																																																																																																																															
6	18	30																																																																																																																																															
7	19	31																																																																																																																																															
8	20																																																																																																																																																
9	21																																																																																																																																																
10	22																																																																																																																																																
11	23																																																																																																																																																
12	24																																																																																																																																																
January																																																																																																																																																	
February																																																																																																																																																	
March																																																																																																																																																	
April																																																																																																																																																	
May																																																																																																																																																	
June																																																																																																																																																	
July																																																																																																																																																	
August																																																																																																																																																	
September																																																																																																																																																	
October																																																																																																																																																	
November																																																																																																																																																	
December																																																																																																																																																	
Sunday																																																																																																																																																	
Monday																																																																																																																																																	
Tuesday																																																																																																																																																	
Wednesday																																																																																																																																																	
Thursday																																																																																																																																																	
Friday																																																																																																																																																	
Saturday																																																																																																																																																	
<small>Note: Ctrl-click (or command-click on the Mac) to select and de-select minutes, hours, days and months.</small>																																																																																																																																																	
<input type="button" value="Sync and Apply"/>																																																																																																																																																	

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**.

Step 7 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 wish to set the hardware time as well.
- **Synchronize on schedule?** - Specify one of the following options:
 - **No** - Select the option if you do not wish to synchronize the time specified in the Run at selected time below options. Go to [Step 8](#).
 - **Yes** - Select the option if you wish to synchronize the time. See options below.
- **Simple Schedule** - Specify if you wish 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 wish the time update to occur.

Step 8 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 wish 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.

System Time

Day	Date	Month	Year	Hour
Friday	7	March	2008	11 : 33 : 11

Apply Set system time to hardware time

Hardware Time

Day	Date	Month	Year	Hour
Friday	7	March	2008	11 : 33 : 11

Save Set hardware time to system time

Time Zone

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

Save

Time Server

Timeserver hostnames or addresses: boxster

Set hardware time too

Synchronize on schedule? No Yes, at times below ..

Simple schedule .. Hourly Times and dates selected below ..

Minutes	Hours	Days	Months	Weekdays
<input type="radio"/> All <input checked="" type="radio"/> Selected .. 0 12 24 36 48 1 13 25 37 49 2 14 26 38 50 3 15 27 39 51 4 16 28 40 52 5 17 29 41 53 6 18 30 42 54 7 19 31 43 55 8 20 32 44 56 9 21 33 45 57 10 22 34 46 58 11 23 35 47 59	<input type="radio"/> All <input checked="" type="radio"/> Selected .. 0 12 1 13 2 14 3 15 4 16 5 17 6 18 7 19 8 20 9 21 10 22 11 23	<input type="radio"/> All <input checked="" type="radio"/> Selected .. 1 13 25 2 14 26 3 15 27 4 16 28 5 17 29 6 18 30 7 19 31 8 20 9 21 10 22 11 23 12 24	<input type="radio"/> All <input checked="" type="radio"/> Selected .. January February March April May June July August September October November December	<input type="radio"/> All <input checked="" type="radio"/> Selected .. Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Note: Ctrl-click (or command-click on the Mac) to select and de-select minutes, hours, days and months.

Sync and Apply

- Step 4** 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 5** In the System Time box, you must specify the current date and time you wish to assign to the managed host. Click **Apply**.
- If you wish to set the System Time to the same as the Hardware time, click **Set system time to hardware time**.
- Step 6** In the Hardware Time box, you must specify the current date and time you wish to assign to the managed host. Click **Save**.
- If you wish to set the System Time to the same as the Hardware time, click **Set hardware time to system time**.

4

MANAGING BACKUP AND RECOVERY

Using the Administration Console, you can backup and recover configuration information and data for STRM Log Management. You can backup and recover the following information for your system:

- License key information
- Configuration database information
- User profile information

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

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

Managing Backup Archives

Using the Administration Console, 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** In the Administration Console, click the **System Configuration** tab.
The System Configuration panel appears.
- Step 2** Click the **Backup Recovery** icon.
The Backup Archives window appears.



The list of archives includes backup files that exist in the database. 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.

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.

Each archive file includes the data from the previous day.

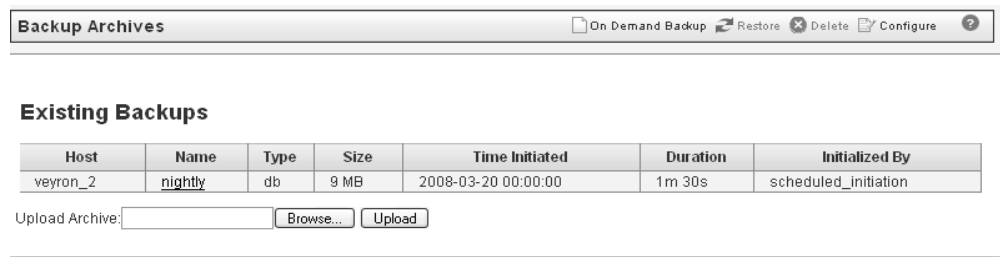
The Backup Archives window provides the following information for each backup archive.

Table 4-6 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.
Type	Specifies the type of backup. The options are: <ul style="list-style-type: none"> • db (database) • config (configuration data) • data (events information)
Size	Specifies the size of the archive file.
Time Initiated	Specifies the time that the backup file was created.
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 Management backup archive file:

- Step 1** In the Administration Console, click the **System Configuration** tab.
The System Configuration panel appears.
- Step 2** Click the **Backup Recovery** icon.
The Backup Archives window appears.



- Step 3** In the Upload Archive field, click **Browse**.
The File Upload window appears.
- Step 4** Select the archive file you wish to upload. Click **Open**.
- Step 5** 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.

- Step 1** In the Administration Console, click the **System Configuration** tab.
The System Configuration panel appears.
- Step 2** Click the **Backup Recovery** icon.
The Backup Archives window appears.



- Step 3** Select the archive you wish to delete.
- Step 4** Click **Delete**.
- Step 5** A confirmation window appears.
- Step 6** Click **Ok**.

Backing Up Your Information

You can backup your configuration information and data using the Backup Recovery Configuration window. You can backup your configuration information using a manual process. Also, you can also backup your configuration information and data using a scheduled process. By default, STRM Log Management creates a backup archive of your configuration information every night at midnight. This section provides information both methods of backing up your data including:

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

Scheduling Your Backup

To schedule your backup process:

To configure your backup settings:

- Step 1** In the Administration Console, click the **System Configuration** tab.
The System Configuration panel appears.
- Step 2** Click the **Backup Recovery** icon.
The Backup Archives window appears.
- Step 3** Click **Configure**.
The Backup Recovery Configuration window appears.

General Backup Configuration	
Backup Repository Path	/store/backup
Backup Retention Period (days)	2
Nightly Backup Schedule	
<input type="radio"/> No Nightly Backups <input checked="" type="radio"/> Configuration Backup Only <input type="radio"/> Configuration and Data Backups	
Configuration Only Backup	
Backup Time Limit (min)	20
Backup Priority	HIGH
Medium and high priorities will have a greater negative effect on the performance of the server running the backup	
Data Backup	
Backup Time Limit (min)	1200
Backup Priority	LOW

Save Cancel

- Step 4** Enter values for the parameters:

Table 4-7 Backup Recovery Configuration Parameters

Parameter	Description
General Backup Configuration	

Table 4-7 Backup Recovery Configuration Parameters (continued)

Parameter	Description
Backup Repository Path	Specifies the location you wish 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 wish to maintain backup files. The default is 2 days. <i>Note: This period of time only affects backup files generated as a result of a scheduled process. Manually initiated backup processes are not affected by this value.</i>
Nightly Backup Schedule	Select one of the following options: <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 wish to backup. This option backs up all database table information including your event data and reports.
Configuration Only Backup	
Backup Time Limit	Specify the length of time, in minutes, that you wish to allow the backup to process.
Backup Priority	Specify the level of importance (low, medium, high) you wish the system to place on the configuration information backup process compared to other processes.
Data Backup	
Backup Time Limit (min)	Specify the length of time, in minutes, that you wish to allow the backup to process.
Backup Priority	Specify the level of importance (low, medium, high) you wish the system to place on the data backup process compared to other processes.

Step 5 Click **Save**.

Step 6 From the Administration Console menu, select **Configurations > Deploy All**.

Initiating a Backup To manually initiate a backup:

Step 1 In the Administration Console, click the **System Configuration** tab.

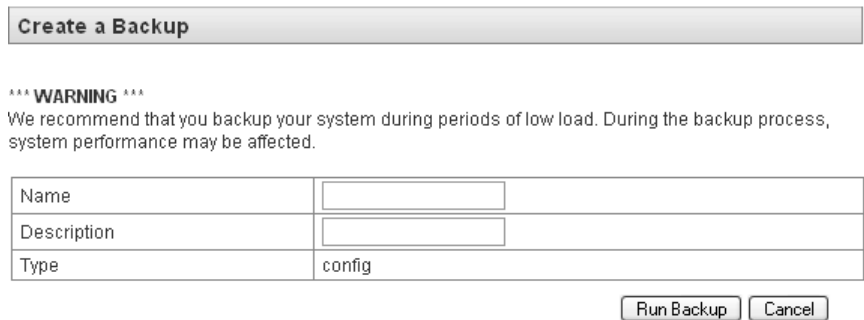
The System Configuration panel appears.

Step 2 Click the **Backup Recovery** icon.

The Backup Archives window appears.



Step 3 Click On Demand Backup.
The Create a Backup window appears.



Step 4 Enter values for the following parameters:

- **Name** - Specify a unique name you wish 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 5 Click Run Backup.
A confirmation window appears.

Step 6 Click OK.

Restoring Your Configuration Information

You can restore configuration information from existing backup archives using the Restore Backup window. Note the following requirements when you are restoring configuration information:

- You can only restore a backup archive created within the same release of software. For example, if you are running STRM Log Management 6.1.2, the backup archive must of been created in STRM Log Management 6.1.2. You can not restore configuration information archived in a previous release.
- Each backup archive includes IP address information of the system from which the backup archive was created. The IP address of the system on which you wish to restore the information must match the IP address of the backup archive. If the IP addresses do not match, the restore process will fail.

To restore your configuration information using a backup archive:



Note: The restore process only restores your configuration information. For assistance in restoring your data, contact Q1 Labs Customer Support.

Step 1 In the Administration Console, click the **System Configuration** tab.

The System Configuration panel appears.

Step 2 Click the **Backup Recovery** icon.

The Backup Archives window appears.

Step 3 Select the archive you wish to restore.

Step 4 Click **Restore**.

The Restore a Backup window appears.

Name	Description	Type
9-12-backup	Configuration backup for today	config

All Items

Restore Cancel

Step 5 To restore specific items in the archive:

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

Step 6 Click **Restore**.

A confirmation window appears.

Step 7 Click **Ok**.

The restore process begins. This process may take several minutes.

Step 8 From the Administration Console menu, select **Configurations > Deploy All**.



Note: The restore process only restores your configuration information. For assistance in restoring your data, contact Q1 Labs Customer Support.

5

USING THE DEPLOYMENT EDITOR

The deployment editor allows you to manage the individual components of your STRM Log Management 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 Management Administration Console. You must disable any third-party web browsers installed on your system. For further assistance, please contact customer support.*

If you wish to access the STRM Log Management Administration Console 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 Management Components](#)

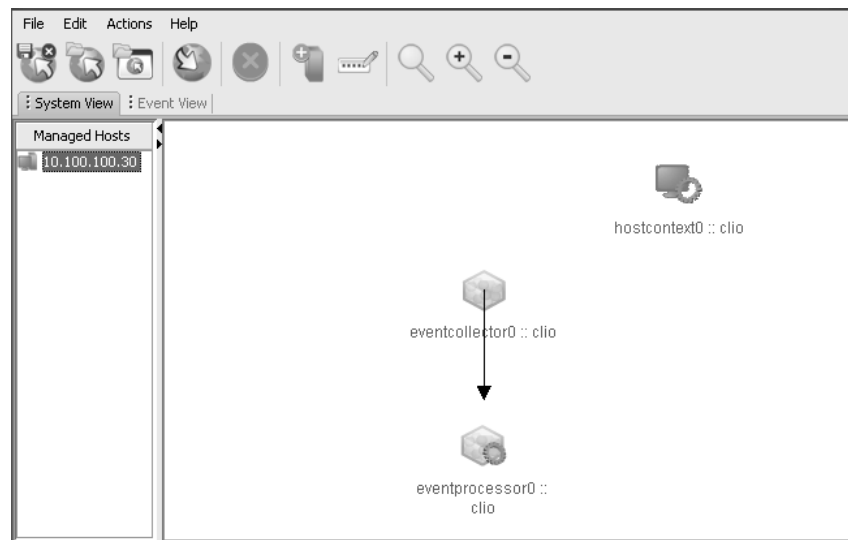
About the Deployment Editor

You can access the deployment editor using the STRM Log Management Administration Console. 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 Management 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 Administration Console, click the deployment editor  icon. 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 Administration Console Deploy menu option or, upon exiting the Administration Console, a window appears prompting you to deploy changes before you exit. 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 5-1](#) provides a list of the menu options and the component for which they appear.

Table 5-1 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	Delete	Deletes a component, host, or connection.
	Close editor	Closes the deployment editor.
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.

Table 5-1 Deployment Editor Menu Options (continued)

Menu Option	Sub Menu Option	Description
	Configure	Configure a STRM Log Management components. This option is only available when Event Collector or Event Processor is selected.
	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 Management software. This option is only available when Event Collector or Event Processor is selected.

Toolbar Options

The toolbar options include:

Table 5-2 Toolbar Options











Icon	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 Management 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.

Table 5-2 Toolbar Options (continued)

Icon	Description
	Zoom in.
	Zoom 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 Management 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 Administration Console menu, select **Configurations > Deploy All**.

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

Before you Begin

Before you begin, you must:

- Install all necessary hardware and STRM Log Management software.
- Install Java Runtime Environment. You can download Java version 1.5.0_12 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 Management deployment including the IP addresses and login information for all devices in your STRM Log Management deployment.

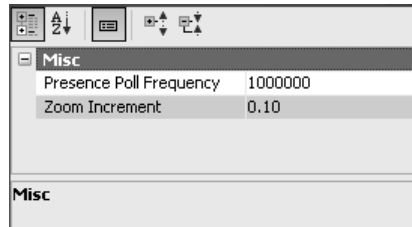


Note: *If you require assistance with the above, please contact Juniper Customer Support.*

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 flows collected from one or more Event Collector(s). The events are bundled once again to conserve network usage. Once received, the Event Processor correlates the information from STRM Log Management and distributes to the appropriate area, depending on the type of event. The Event Processor also includes information gathered by STRM Log Management 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 wish to add to your deployment.

The Adding a New Component Wizard appears.

Step 3 Enter a unique name for the component you wish 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 wish to assign the new component. Click **Next**.
- Step 5** Click **Finish**.
- Step 6** Repeat for each component you wish 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 wish 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 wish 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 wish 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 wish to connect.
- **Encrypt traffic from off-site source** - Select the check box if you wish 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 wish 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 wish to send data.

For example, if you wish to forward normalized events between two deployments (A and B), where deployment B wishes 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 wish 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 wish to enable encryption between deployments, you must enable encryption on both off-site source and target. Also, you must ensure both the off-site source and target include the public keys to ensure appropriate access. For example, in the example below, if you wish 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 Event Collector to the off-site source (copy the file to `/root/.ssh/authorized_keys`).

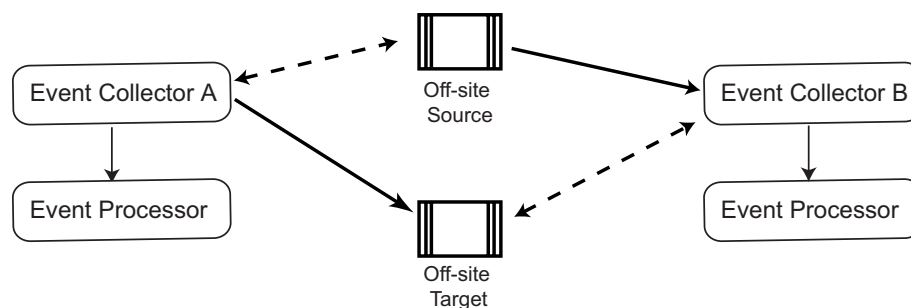


Figure 5-1 Example of Connecting Deployments

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 wish to connect.

- **Encrypt traffic from off-site source** - Select the check box if you wish 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 wish to rename a component in your view to uniquely identify components through your deployment.

To rename a component:

Step 1 Select the component you wish 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 Management software. If you are using a STRM Log Management appliance, the components for that appliance model appear. If your STRM Log Management 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 wish 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 Management with NATed networks in your deployment. See [Using NAT with STRM Log Management](#).

- 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 Management 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 Management traffic between managed hosts. To provide enhanced security, STRM Log Management 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 Management, Reflection SSH provides secure communication between STRM Log Management components. For information on Reflection SSH, see the following web site:

www.wrq.com/products/reflection/ssh



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

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.



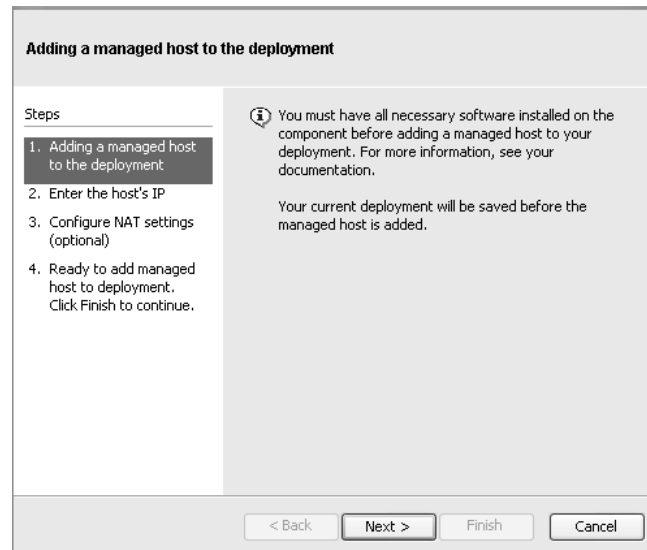
Note: Enabling encryption reduces the performance of a managed host by at least 50%.

Adding a Managed Host

To add a managed host:

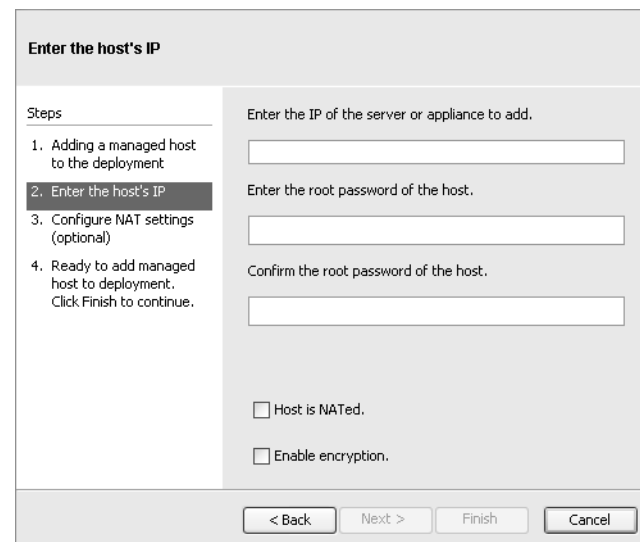
Step 1 From the menu, select **Actions > Add a managed host**.

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 wish 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 wish to use an existing Network Address Translation (NAT) on this managed host. For more information on NAT, see [Using NAT with STRM Log Management](#).


 **Note:** *If you wish 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 Management](#).*

- **Enable Encryption** - Select the check box if you wish 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](#).


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 network you wish this managed host to use.

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

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

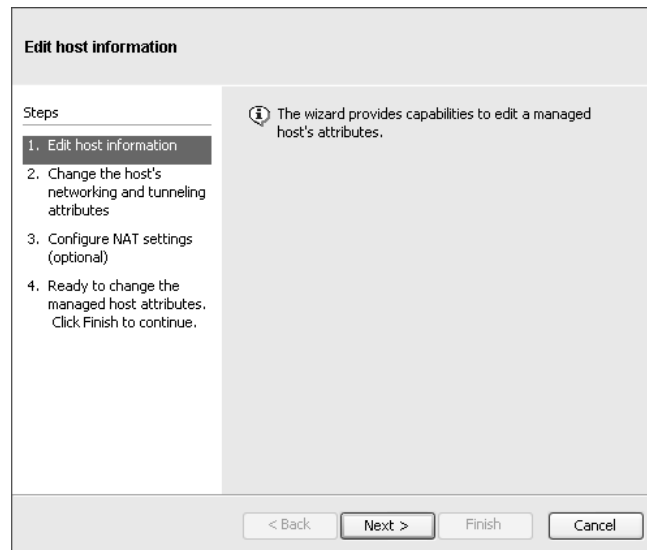
To edit an existing managed host:

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

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

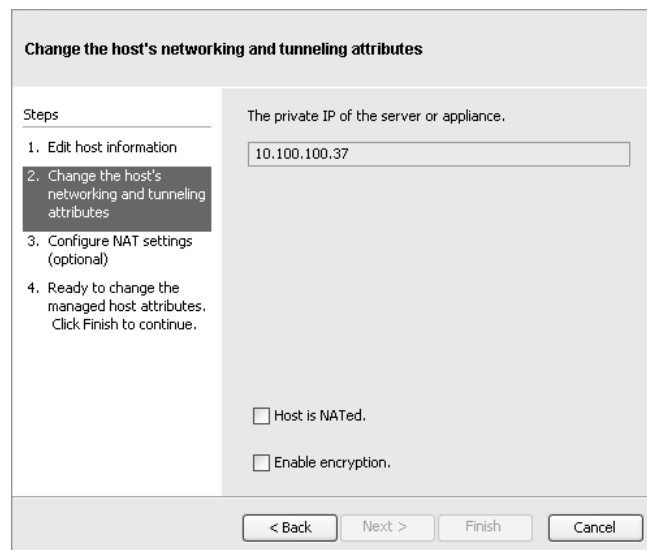
The Edit a managed host wizard appears.

 **Note:** *This option is only available when the selected component has a managed host running a compatible version of STRM Log Management 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 wish to use existing Network Address Translation (NAT) on this managed host. For more information on NAT, see [Using NAT with STRM Log Management](#).



Note: If you wish 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 Management](#).

- **Enable Encryption** - Select the check box if you wish 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 network you wish this managed host to use.



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

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 Management 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 wish 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 Management software.

A confirmation window appears.

Step 3 Click **Ok**.

Step 4 From the Administration Console menu, select **Configurations > Deploy All**.

Using NAT with STRM Log Management

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 address.

Before you enable NAT for a STRM Log Management 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 set-up and configured on your network before you enable NAT using STRM Log Management. For more information, see your network administrator.


You can add a non-NATed managed host using inbound NAT for the public IP address and dynamic for outbound NAT but are located on the same switch as the Console or managed host. However, 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 Management](#)
- [Editing a NATed Network](#)
- [Deleting a NATed Network From STRM Log Management](#)
- [Changing the NAT Status for a Managed Host](#)

Adding a NATed Network to STRM Log Management

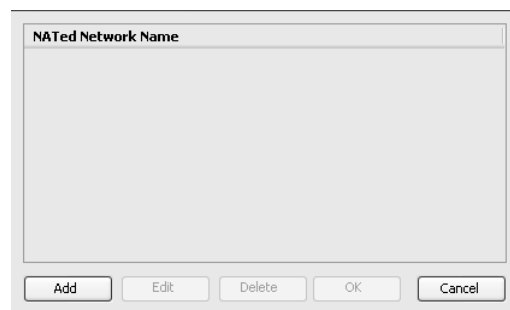
To add a NATed network to your STRM Log Management deployment:

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



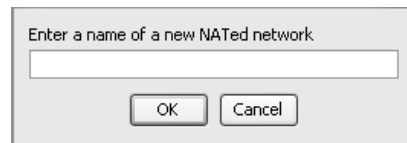
Note: You can also use the **Actions > Managed NATed Networks** menu option to access the *Managed NATed Networks* window.

The Manage NATed Networks window appears.



Step 2 Click **Add**.

The Add New Nated Network window appears.



Step 3 Enter a name of a network you wish 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

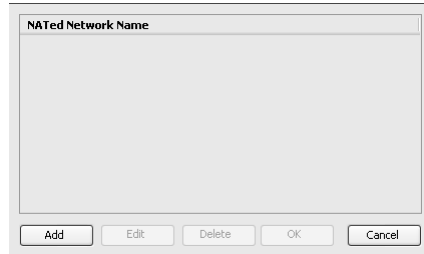
To edit a NATed network:

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



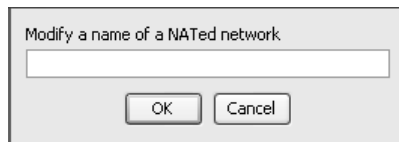
Note: You can also use the **Actions > Managed NATed Networks** menu option to access the Managed NATed Networks window.

The Manage NATed Networks window appears.



Step 2 Select the NATed network you wish to edit and click **Edit**.

The Edit NATed Network window appears.



Step 3 Update the name of the network you wish 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 Management

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 wish 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 Management 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 wish 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 wish to enable NAT for the managed host, select the check box. Go to [Step 5](#)



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

b If you wish 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 wish this managed host to use.
- **Manage NATs List** - Update the NATd network configuration. For more information see, [Using NAT with STRM Log Management](#).

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.

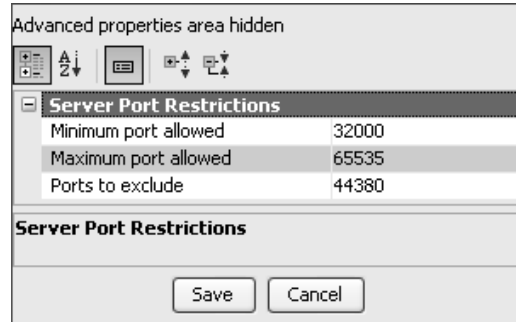
Step 9 From the STRM Log Management Administration Console menu, select **Configurations > Deploy All**.

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 wish 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 wish to establish communications.
- **Maximum port allowed** - Specify the maximum port for which you wish to establish communications.
- **Ports to exclude** - Specify the port you wish to exclude from communications. You can enter multiple ports you wish to exclude. Separate multiple ports using a comma.

- Step 3** Click **Save**.

Assigning a Component to a Host

You can assign the STRM Log Management 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 wish to assign a STRM Log Management component.

The System View of the host appears.

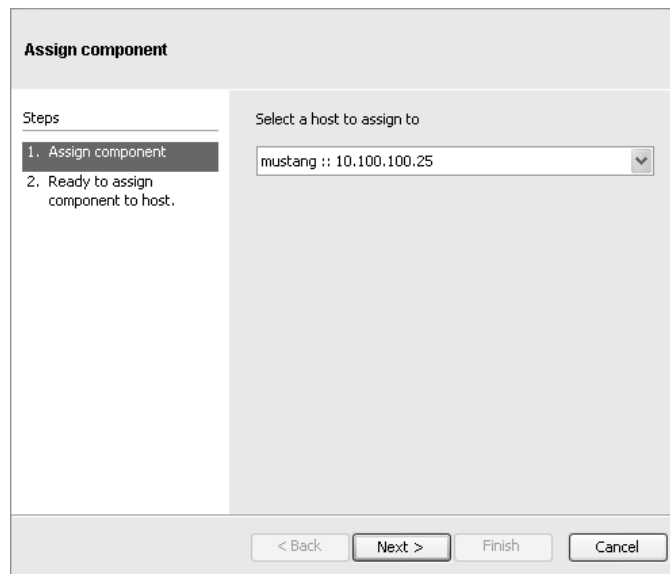
- Step 3** Select the component you wish to assign to a managed host.

- 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 drop-down list box, select the host that you wish 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 Management software.

Step 6 Click **Finish**.

Configuring Host Context The Host Context component monitors all STRM Log Management 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 wish to configure.

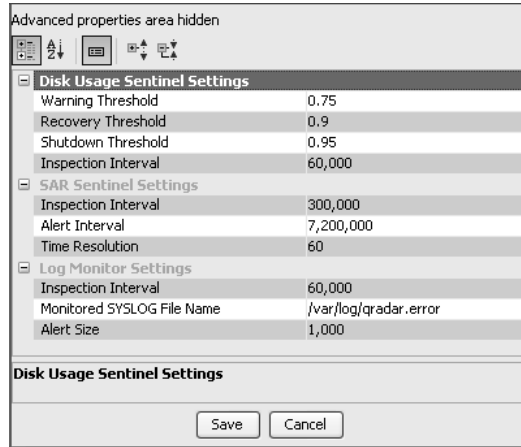
Step 3 Select the Host Context component.

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 5-3 Host Context Parameters

Parameter	Description
Disk Usage Sentinel Settings	
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 3 Setting Up STRM Log Management.</p>

Table 5-3 Host Context Parameters (continued)

Parameter	Description
Recovery Threshold	<p>Once the system has exceeded the shutdown threshold, disk usage must fall below the recovery threshold before STRM Log Management 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 3 Setting Up STRM Log Management.</p>
Shutdown Threshold	<p>When the system exceeds the shutdown threshold, all STRM Log Management 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 Management 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 3 Setting Up STRM Log Management.</p>
Inspection Interval	Specify the frequency, in milliseconds, that you wish to determine disk usage.
SAR Sentinel Settings	
Inspection Interval	Specify the frequency, in milliseconds, that you wish to inspect SAR output. The default is 300,000 ms.
Alert Interval	Specify the frequency, in milliseconds, that you wish 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 wish the SAR inspection to be engaged. The default is 60 seconds.
Log Monitor Settings	
Inspection Interval	Specify the frequency, in milliseconds, that you wish 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 wish to monitor from the log file. The default is 1000.

Step 6 Click **Save**.

The System View appears.

Configuring STRM Log Management Components

This section provides information on configuring STRM Log Management 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:

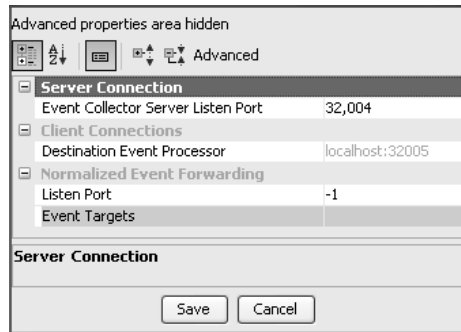
Step 1 From either the Event View or System View, select the Event Collector you wish to configure.

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.

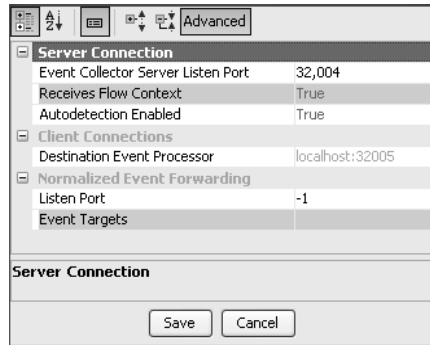


Step 3 Enter values for the parameters:

Table 5-4 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 5-5 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 wish the Event Collector to auto analyze and accept traffic from previously unknown sensor devices. The default is true, which means that the Event Collector detects sensor devices 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 sensor devices, see the <i>Managing Sensor Devices Guide</i> .

Step 6 Click **Save**.
 The deployment editor appears.

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

Configuring an Event Processor

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

To configure an Event Processor:

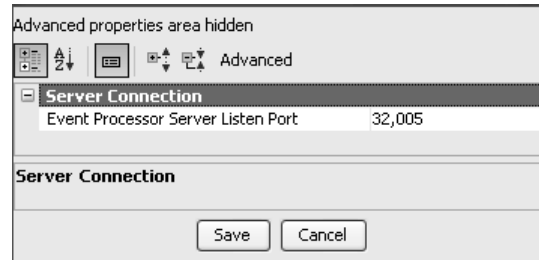
Step 1 From either the Event View or System View, select the Event Processor you wish to configure.

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.



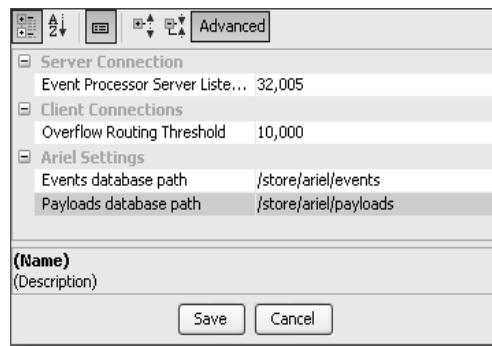
Step 3 Enter values for the parameters:

Table 5-6 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 32000 to 65535.

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 5-7 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 wish to store events. The default is <code>/store/ariel/events</code> .
Payloads database path	Specify the location you wish 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 wish to configure.

6

FORWARDING SYSLOG DATA

STRM Log Management 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 Management 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 Management ensures that all data that is forwarded is unaltered.

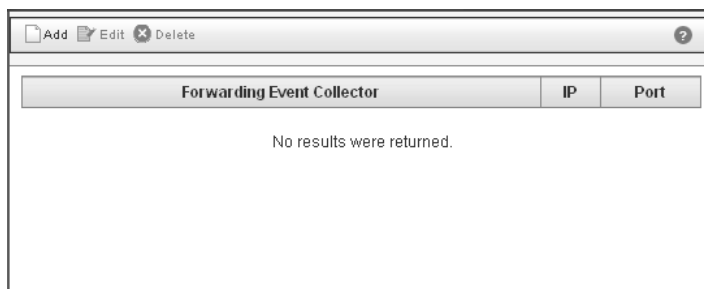
This chapter includes:

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

Adding a Syslog Destination

To add a syslog forwarding destination:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.
The SIM Configuration panel appears.
- Step 2** Click the **Syslog Forwarding Destinations** icon.
The Syslog Forwarding Destinations window appears.



- Step 3** Click **Add**.
The Syslog Forwarding Destinations window appears.

Step 4 Enter values for the parameters:

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

Step 5 Click **Save**.

Editing a Syslog Destination

To edit a syslog forwarding destination:

Step 1 In the Administration Console, click the **SIM Configuration** tab.

The SIM Configuration panel appears.

Step 2 Click the **Syslog Forwarding Destinations** icon.

The Syslog Forwarding Destinations window appears.

Step 3 Select the entry you wish to edit.

Step 4 Click **Edit**.

The Syslog Forwarding Destinations window appears.

Step 5 Update values, as necessary:

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

Step 6 Click **Save**.

Delete a Syslog Destination

To delete a syslog forwarding destination:

- Step 1** In the Administration Console, click the **SIM Configuration** tab.
The SIM Configuration panel appears.
- Step 2** Click the **Syslog Forwarding Destinations** icon.
The Syslog Forwarding Destinations window appears.
- Step 3** Select the entry you wish to delete.
- Step 4** Click **Delete**.
A confirmation window appears.
- Step 5** Click **Ok**.

A

Q1 LABS MIB

This appendix provides information on the Q1 Labs Management Information Base (MIB). The Q1 Labs MIB allows you to send SNMP traps to other network management systems. The Q1 Labs OID is 1.3.6.1.4.1.20212.



Note: For assistance with the Q1 Labs MIB, please contact Q1 Labs Customer Support.

The Q1 Labs MIB includes:

```
Q1LABS-MIB DEFINITIONS ::= BEGIN
IMPORTS
OBJECT-TYPE, NOTIFICATION-TYPE, MODULE-IDENTITY, Integer32,
Opaque, enterprises, Counter32 FROM SNMPv2-SMI
DisplayString FROM SNMPv2-TC;
q1Labs MODULE-IDENTITY
    LAST-UPDATED "200508120000Z"
    ORGANIZATION "Q1 Labs Inc"
    CONTACT-INFO
        "
        890 Winter Street
        Suite 230
        Waltham, MA 02451 USA
        Phone: 781-250-5800
        email:    info@q1labs.com
        "
    DESCRIPTION
        "Q1 Labs MIB Definition"
        ::= { enterprises 20212 }

q1NotificationData OBJECT-TYPE
```

```
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION "Notification Data"
 ::= { q1Labs 100 }

q1Notifications OBJECT IDENTIFIER
 ::= { q1Labs 200 }

q1CRENotification NOTIFICATION-TYPE
STATUS current
DESCRIPTION "QRADAR Custom Rule Engine Notification"
 ::= { q1Notifications 0 }

q1EventRuleNotification NOTIFICATION-TYPE
STATUS current
DESCRIPTION "Notification Triggered by an Custom Event
Rule"
 ::= { q1Notifications 1 }

q1OffenseRuleNotification NOTIFICATION-TYPE
STATUS current
DESCRIPTION "Notification Triggered by an Custom Offense
Rule"
 ::= { q1Notifications 2 }

q1SentryNotification NOTIFICATION-TYPE
STATUS current
DESCRIPTION "Notification Triggered by a QRadar Sentry"
 ::= { q1Notifications 3 }

END
```

INDEX

A

- administration console
 - about 3
 - accessing 4
 - using 4
- administrator role 10
- Ariel database 78
- audience 1
- audit log
 - viewing 7
- audit logs 5
- authentication
 - configuring 15
 - LDAP 15
 - RADIUS 15
 - system 15
 - TACACS 15
 - user 15
- auto detection 77
- automatic update
 - about 26
 - scheduling 26

B

- backup and recovery 45

C

- changes
 - deploying 5
- command line max matched results 28
- components 76
- console
 - settings 33
- conventions 1
- customer support
 - contacting 2

D

- database settings 28
- deploying changes 5
- deployment editor 53
 - about 53
 - accessing 55
 - creating your deployment 57
 - event view 58
 - preferences 58
 - STRM Log Management components 76
 - requirements 57
 - system view 63
 - toolbar 56

- using 55
- device access 36
- device management 39

E

- encryption 60, 61, 63
- Event Collector
 - about 58
 - configuring 76
- Event Processor
 - about 58
 - configuring 77
- event view
 - about 54
 - adding components 59
 - building 58
 - connecting components 60
 - renaming components 63

F

- firewall access 36
- flow view
 - components 61

H

- hashing
 - algorithm 29
- host
 - adding 65
- host context 54, 73

I

- interface roles 39

L

- LDAP/Active directory 15
- license key
 - exporting 21
 - managing 19
- logs 5

M

- managed host
 - adding 65
 - assigning components 72
 - editing 66

- removing 68
- set-up 38
- maximum real-time results 28
- MIB 83

N

- NAT
 - editing 70
 - enabling 68
 - removing 70
 - using with STRM Log Management 68
- Network Address Translation. See NAT
- network hierarchy
 - creating 22
- NTP 43

O

- off-site source 62
- off-site target 62

P

- passwords
 - changing 40

Q

- STRM Log Management components 76
- STRM Log Management user 12

R

- RADIUS authentication 15
- RDATE 41
- recovery 45
- restarting STRM Log Management 35
- role 9
 - administrator 10
 - creating 9
 - editing 11
 - managing 9

S

- SNMP agent
 - accessing 35
- SNMP Settings 29
- source
 - off-site 61, 62
- starting STRM Log Management 35
- stopping STRM Log Management 35
- syslog
 - forwarding 79
 - adding 79
 - deleting 81
 - editing 80
- system authentication 15

- system settings 27
 - configuring 27, 33
- system thresholds 31
- system time 41
- system view
 - about 54
 - assigning components 72
 - Host Context 73
 - managed host 72
 - managing 63

T

- TACACS authentication 15
- target
 - off-site 61, 62
- thresholds 31
- time 41
- time limit
 - command like execution 29
 - reporting execution 29
 - web execution 28

U

- user
 - creating account 12
 - editing account 13, 14
 - managing 9
 - roles 9
- users
 - authentication 15