

# STRM LOG MANAGEMENT RELEASE NOTES

## RELEASE 2008.2

### JUNE 2008

Juniper Networks is pleased to introduce STRM Log Management 2008.2. This release provides you with several resolved issues and enhanced functionality.

This document includes:

- [STRM Log Management Overview](#)
- [New and Updated Functionality](#)
- [Related Documentation](#)
- [Contacting Customer Support](#)
- [Supported Devices and OS Versions](#)
- [Supported Java and Browser Software](#)
- [Resolved Issues](#)
- [Known Issues and Limitations](#)

**Note:** *If your current deployment includes ISS SiteProtector, contact Juniper Networks Customer Support before you install STRM Log Management.*

---

## STRM Log Management Overview

Juniper Networks Security Threat Response Manager Log Management Only (STRM LM) provides a comprehensive log management solution for organizations that want to implement a distributed log management solution to collect, archive, and analyze network and security event logs. Log management has emerged as a required part of an organization's ability to deliver security best practices and meet specific auditing and reporting requirements of government regulations, including PCI, Sarbanes-Oxley, HIPAA, and FISMA.

STRM LM provides numerous advantages over other log management solutions including:

- Easy-to-deploy turnkey log management solution—Architecture provides a simple and easy-to-use solution for secure and efficient log management.
- Scalable distributed log collection and archival—Appliance architecture scales to support any size enterprise network.
- Simple policy-driven event correlation—Hundreds of useful out-of-the box correlation rules provide immediate value.

- Effective reporting and compliance auditing—Compliance-driven report templates meet specific regulatory reporting and auditing requirements.
- Reliable and tamper-proof log storage—Support of extensive log file integrity checks, including NIST Log Management Standard SHA-x (1-256) hashing for tamper-proof log archives.
- Simple upgrade to full STRM—Provides investment protection for organizations with expanding requirements in the areas of threat and compliance management.

---

## New and Updated Functionality

STRM Log Management 2008.2 provides you with the following new and updated functionality:

- **Activation and License Key Enhancement** - STRM Log Management 2008.2 includes several enhancements to activation and license keys including:
  - **Activation Keys** - During installation of STRM Log Management, you must now enter an activation key to complete the installation. This activation key is available on the license CD. See the instructions that came with the license CD to install the activation key.
  - **License Keys** - The License key functionality is now enhanced in the STRM Log Management interface to include individual license keys for each system in your deployment.
- **New Device Extensions Functionality** - You can now modify how a DSM parses logs. For example, you can use a device extension to detect an event that has missing or incorrect fields. A device extension can also parse an event when the DSM to which it is attached fails to produce a result.
- **Universal DSM Enhancement** - With STRM Log Management 2008.2, the Universal DSM includes the following enhancements:
  - **Device Extensions** - Allows you to use the new device extensions functionality to enhance the DSM parsing of your logs.
  - **Multiple Universal DSMs** - Allows you to support multiple Universal DSMs.
  - **Integration with Asset Profiles** - Using STRM Log Management 2008.2, the Universal DSM is associated with an asset profile allowing you to track user identity data and associate that information to an asset profile.
- **User Roles Enhancement** - Administrative users can now be assigned additional controls including:
  - **Administrator Management** - Allows Administrative users to create and edit other administrative accounts.
  - **System Administrator** - Allows Administrative users to access all areas of STRM Log Management. Also, users with this access are not able to edit other administrator accounts.
- **User Account Enhancement** - You can now disable a user account without deleting the account. A user with a disabled account is no longer able to access the STRM Log Management interface.

---

**Related  
Documentation**

For more information on Release 2008.2, refer to the on-line documentation:

- STRM Log Management Installation Guide
- STRM Log Management Administration Guide
- STRM Log Management Users Guide
- STRM Log Management Sensor Devices
- Getting Started with STRM Log Management Appliances

---

**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:

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

---

**Supported Devices  
and OS Versions**

STRM Log Management 2008.2 supports platforms from multiple vendors. [Table 1-1](#) lists Juniper Networks device families and operating systems that support NSM. The table shows whether a device requires STRM to forward logs through NSM.

**Table 1-1** Supported Juniper Networks Devices and OS Versions

Device Family	OS	Logs Sent Directly to STRM from Device	Logs Sent Through NSM to STRM
ISG with IDP	6.0, 6.1.0r1b	No	Yes
Firewall/VPN	6.0, 6.1.0r1	Yes	Yes
Standalone IDP	4.1	Yes	Yes
J-series	8.5, 9.0, 9.1	Yes	No
Secure Access (SA)	6.1	Yes	No
Infranet Controller (IC)	2.1	Yes	No

**Note:** For STRM to correctly process logs from SA and IC, the logs should be sent from the devices in WELF format. To enable WELF format on the device: Under System > Logs > Events > Settings, select the WELF filter for the syslog (STRM) server entry in this table.

---

**Supported Java  
and Browser  
Software**

STRM Log Management supports the following versions of Java and browsers:

- Java version 1.5 and later
- Internet Explorer version 7
- Firefox version 2.0

---

**Resolved Issues**

This section describes the resolved issues in STRM Log Management 2008.2:

**Changing Network Settings No Longer Causes System Failure**

Previously, if you changed your network settings (for more information, see the *Changing Network Settings Technical Note*), a failure occurred when you attempted to access the system. This no longer occurs.

**During Installation Process, Error No Longer Occurs When Root Password is Not Changed**

During the installation process, a message appears indicating that you are able to use the default root password. However, if you attempted to use the default password, a message appeared indicating that you must enter a new password. This no longer occurs.

**Hostname that Includes Underscores and Special Characters No Longer Causes Error**

Previously, if the hostname of your STRM Log Management system included underscores and/or special characters (except dashes), the Host Context component failed to start. Once this occurred, STRM Log Management failed to collect data. This no longer occurs.

**Now Able to Deploy License Key Once Current Key Expires**

Previously, if your license key expired and you uploaded a new license key, STRM Log Management did not provide the option to deploy the new license key.

**Changing the Authentication to STRM Log Management Authentication No Longer Requires Edits to Passwords**

Previously, if you changed your authentication from TACACS, RADIUS, or LDAP/Active Directory to STRM Log Management Authentication, you were required to configure access for users on the system before they are able to login to STRM Log Management. No message appeared in STRM Log Management stating these requirements. In STRM Log Management 2008.2, you must define passwords for all users that do not have a password defined.

**Updating License Key When Using Internet Explorer 6 No Longer Causes Error**

Previously, when you updated your license key using an Internet Explorer 6 browser, a window appeared stating "The page cannot be displayed" when you click **Save**. This no longer occurs.

**New Administrative User Now Able to Access Deployment Editor**

A STRM Log Management administrative (admin) user can create multiple admin accounts for a STRM Log Management system. An administrative user should have unrestricted access to all components of your deployment. Previously, when a new administrative user attempted to access the deployment editor, an error message appeared and access was denied.

### **Deleting a False Positive Building Block Value No Longer Causes Error**

Previously, if you attempted to edit the User-BB-FalsePositive: User Defined False Positive Tunings Building Block to edit any of the configured values within the Building Block, the following error message appeared `Invalid category id`. This no longer occurs.

### **Multiple Reports No Longer Generate From Single Template When Reports are Shared**

When you created a new report using the Report Wizard, you can generate the report by selecting the **Would you like to run the report now?** check box in the report wizard or request the completed report template to generate using the Reports Template interface. Previously, if the report was shared with other users, both options may have resulted in the generation of multiple reports appearing in the Generated Reports interface with Admin as the listed owner. This no longer occurs.

### **Now Able to Add 200 CIDRS for a Network Object**

Previously, the limit of CIDR range(s) you could add to the network object was 70. If you attempted to add more than 70 CIDR range(s), an error appeared. In STRM Log Management 2008.2, the limit of CIDR ranges you can add is approximately 200, depending on the data on your system.

### **Now Able to Apply Any IP Filter When Searching for Events**

Previously, when you attempted to filter in the Event Viewer using the Any IP filter option, invalid results appears. Now, in STRM Log Management 2008.2, this no longer occurs and valid search results appear.

### **Now Able to Filter on Device Type Using Right-Click Option in Aggregate Display**

Using the Display drop-down list box in the Event Viewer, you are able to view events using one of the available aggregate options. Previously, if you selected the Device Type option in the Display drop-down list box, you were not able to access the Filter menu using the right mouse button (right-click) for the Device Type column. This no longer occurs and the Filter menu is available.

### **Now Able to Use Exclamation Point (!) In LDAP Authentication Passwords**

Previously, when defining a password for your LDAP authentication, if you entered an exclamation point (!) as part of your password, the password was rejected. Exclamation points (!) are now supported.

### **Now Able to Use Same IP Address for Off-Site Source and Target**

Previously, when configuring off-site source and target in the deployment editor, an error appeared if you attempted to use the same IP address for the source and target. This no longer occurs.

### **Restoring Configuration Now Create Proper Directory Structure**

Previously, when restoring configuration information on a new Console system, the /store/db directory was not properly created. In STRM Log Management 2008.2, this directory structure is properly created.

### **Events Appear in Event Viewer and Flows in Flow Viewer After June 30, 2008**

The Event Correlation Engine license expires on 30 June 2008. This license is needed for the events and flows to be processed. STRM version 2008.2 extends the Event Correlation Engine license until December 2009. In the future, there will be a software upgrade that will eliminate the requirement for this license.

## Known Issues and Limitations

This section describes the known issues and limitations for the following areas:

- [General](#)
- [System Configuration](#)
- [Event Viewer](#)
- [Reports](#)

### General Upgrade May Fail with Custom SSL Certificate

The upgrade of STRM may fail if your deployment meets both of the following conditions:

- You use a custom SSL (trusted) certificate, rather than the default certificate shipped with STRM, somewhere in your deployment.
- The custom certificate has an Intermediate key.

Not all trusted certificates have an Intermediate key. Verisign certificates are one example that uses an Intermediate key. The overall impact of this problem depends on your particular deployment. The upgrade may fail because the configuration file is missing a line that provides the directory path to your custom certificate key on the server.

*Workaround:* Follow these steps to update the configuration file and restart services:

**Step 1** Open the configuration file on the machine that uses the custom SSL key (normally the Web Server console).

**Step 1** Add the directory path to your custom SSL key.

**Step 2** Restart the hostcontext service using the following command:

```
service hostcontext restart
```

### During a Restart, an Error May Appear Regarding the Tomcat Server

Any changes to STRM Log Management using the web-based system administration interface requires the Tomcat server to restart. This server may take 1 to 2 minutes to restart. If, during this time, you access the STRM Log Management interface, a fatal error message appears. Do not attempt to restart the Tomcat server manually. Once the server restarts, STRM Log Management will continue to function as expected.

*Workaround:* Wait several minutes for the server to restart then access the STRM Log Management interface.

### Exporting Information Using CSV/XML Export may be Blocked Using Internet Explorer 7

If you wish to download information (such as events, assets, or flows), using the STRM Log Management Export function, you can select the **Notify When Done**

option that enables the browser to notify you when the download is complete. However, if you are using Internet Explorer 7, a warning appears requiring you to select an option menu to download the file. When you select the option menu, the browser refreshes to the STRM Log Management Dashboard and the exported file is not downloaded.

*Workaround:* In Internet Explorer 7, change the Security Settings > Downloads > Automatic Prompting for file downloads option to Enable.

### **Continuous Use of STRM Log Management Over Extended Period of Time May Cause Interface Failure**

If you continue to use a session of the STRM Log Management interface for an extended period of time, a failure may occur in your browser requiring you to restart your system. This failure is a result of a memory loss due to a limitation in the web browser architecture.

*Workaround:* Restart your browser if your browser performance degrades.

### **Infranet Controller Device Appears as Enterasys Device**

An auto-discovered Infranet Controller (IC) device may appear incorrectly as an Enterasys device.

*Workaround:* Add the Infranet Controller device manually.

### **Infranet Controller Device Appears as Secure Access Device**

An auto-discovered Infranet Controller (IC) device may appear incorrectly as a Secure Access (SA) device.

*Workaround:* Add the Infranet Controller device manually.

## **System Configuration**

### **Restoring Configuration Information for Deployment with Encrypted Systems Fails**

If you attempt to restore configuration information in a deployment that includes encrypted systems and then deploy all changes, the restore process fails for the encrypted systems.

*Workaround:* Follow the *Restoring Your Configuration* procedure outlined in the *STRM Log Management Administration Guide*, however, before you deploy all changes, wait for the STRM Log Management interface to become active. Once the interface is active, follow this procedure:

- Step 1** Log in to STRM Log Management, as root.
- Step 2** Enter the following command and any non-Console passwords, as prompted:  

```
/opt/qradar/bin/push_ssh_auth_keys.sh
```
- Step 3** On the Console, enter the following command:  

```
ssh <IP address/hostname of the non-Console>
```
- Step 4** On the non-Console, enter the following command:  

```
ssh <IP address/hostname of the Console>
```

- Step 5** For all systems in your deployment, use SSH to connect from the Console to non-Console systems and enter the following command:

```
service hostcontext restart
```

### **Performing an Automatic Update Does Not Deploy All Changes**

When you update your system using the Auto-Update Configuration window in the STRM Log Management Administration Console, the changes are not enforced throughout your deployment. This results in updated contents do not appearing in the deployment.

*Workaround:* From the Administration Console Menu, select **Configurations > Deploy All** to enforce the changes.

### **Event Viewer Events Are Marked "Unknown" in Event Viewer**

Events that arrive from a device that has not yet been auto-discovered are marked "Unknown." This is normal behavior.

*Workaround:* Wait for auto-discovery to detect the device.

### **Event Viewer Does not Respond to Searches**

After a configuration change, the event query service process restarts and may be temporarily unable to process event searches.

*Workaround:* Wait between 2 and 3 minutes for the Event Viewer to finish restarting. Then try your search again.

### **Accessing Right-Click Menu in Event Viewer Causes Java Error**

Using the right mouse button (right click) in the Event Viewer allows you to access additional menu options. If pop-ups are disabled in your web browser, a Java error occurs.

*Workaround:* Enable pop-ups in your web browser.

### **Unable to Remove Custom Event Mapping**

Once you create a custom event mapping using the event mapping tool in the Event Viewer, you are able to edit the mapping, however, you are unable to remove the event mapping or restore default settings.

*Workaround:* None.

### **Reports Size of Pie Charts in Reports is Dynamic**

When creating a report that includes pie charts, the chart size depends on the area consumed by the legend. Pie charts with only a single item in the legend are much larger than pie charts with many items in the legend.

*Workaround:* Reduce the number of items you wish to display in the pie chart.

Revision History  
June 2008—Revision 1.  
July 2008—Updated.

Part Number 530-025628-01

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089  
USA

Copyright © 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of 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.