

STRM LOG MANAGER RELEASE NOTES

RELEASE 2009.2

APRIL 2010

Juniper Networks is pleased to introduce STRM Log Manager 2009.2. This release provides you with several resolved issues and enhanced functionality.

This document includes:

- [New and Updated Functionality](#)
- [Technical Documentation](#)
- [Contacting Customer Support](#)
- [Resolved Issues](#)
- [Known Issues and Limitations](#)
- [Document Addendum](#)

New and Updated Functionality

STRM Log Manager 2009.2 provides you with the following new and updated functionality:

- **Product Name Change** - STRM SLIM is now referred to as STRM Log Manager.
- **High Availability** - STRM Log Manager 2009.2 introduces High Availability (HA) functionality. HA provides automatic failover and full disk replication between a primary and secondary host. To deploy HA in your environment, you can purchase HA appliances or HA software licenses for your existing STRM Log Manager systems. Contact your sales representative for more information.

HA functionality provides the following capabilities:

- Heartbeat monitoring between the primary and secondary host. When the heartbeat monitoring detects that the primary host has failed, STRM Log Manager services automatically failover to the secondary host.
- Disk replication and shared storage solutions ensure availability of all data in the event of a failover. Disk replication synchronizes all data, such as configuration, logs, and reports from the primary host to the secondary host. In a shared storage solution, the primary and secondary host are configured to send data to the same external storage solution.

- A Cluster Virtual IP address is shared between the primary and the secondary host. The Cluster Virtual IP address allows data sources to continue sending logs to STRM Log Manager during a failover without needing to be reconfigured with a new IP address. This feature significantly reduces downtime in the event of a failover.
- System notifications in the STRM Log Manager user interface alerts you to failover conditions in your HA deployment.
- **Dashboard Enhancements** - The System Notification Dashboard item provides the following enhancements:
 - You can now specify the number of notifications that you want to appear in the Dashboard and dismiss any system notifications.
 - System notifications also appear as pop-up notifications in the STRM Log Manager interface. These pop-up notifications appear in the lower right corner of the interface, regardless of the selected tab.



Note: *Third-party RPMs are not supported on STRM Log Manager systems. Before you upgrade to STRM Log Manager 2009.2, pretest your systems to determine if your deployment includes any third-party RPMs. For more information, see the [Upgrading to STRM Log Manager 2009.2 Guide](#).*

Caution: *If you want to maintain your current configuration, you must first upgrade to STRM 2009.2 and then back up your configuration and data prior to performing a fresh installation on this system. For information on backing up your system, see the [STRM Administration Guide](#). For more information on installing STRM 2009.2, see the [STRM Installation Guide](#).*

Technical Documentation

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

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

techpubs-comments@juniper.net.

Include the following information with your comments:

- Document title
- Page number

Contacting Customer Support

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

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

Resolved Issues

This section describes the resolved issues in STRM Log Manager 2009.2:

TopN Reports No Longer Fail to Generate

Previously, TopN reports may have failed to generate due to out of memory conditions. This no longer occurs.

Rule Settings Are Now Maintained Properly After Editing Rules

Previously, when editing a rule in the Rules Wizard, some rule settings were cleared in error. This no longer occurs.

Source IP Test No Longer Removed When Editing the Default-Rule-Authentication:Repeated Login Failures, Single Host Rule

Previously, when editing the Source IP test in the Default-Rule-Authentication:Repeated Login Failures, Single Host rule, the test was removed from the rule. This no longer occurs.

Error No Longer Occurs in the Manage Search Window After Deleting a Saved Search

Previously, if you performed a saved search from the event search window and then deleted that saved search, an error occurred the next time you clicked Manage Search Results to access the search results window. This no longer occurs.

SSH Keys Are Now Restored When Restoring a Backup on a System with a Different IP address than the Backup Archive

Previously, when restoring a backup on a system with a different IP address than the backup archive, the SSH keys were not restored if you did not select the option to restore all items. This no longer occurs.

License No Longer Invalid if the Serial Number in a Backup Archive Does Not Match the Serial Number on the Current Console

Previously, after restoring a backup archive, the license was invalid if the serial number of the backup archive did not match the serial number of the current Console. This no longer occurs.

Server Status No Longer Appears As Unknown On System and License Management Window After Upgrade

Previously, if you removed a host from your deployment and then re-added the host with different IP address prior to upgrading to STRM Log Manager 2009.2, the system status for the host displayed as unknown on the System and License Management window after the upgrade. This no longer occurs.

Events Are Now Received Properly After Changing the Log Source Identifier for a Log Source Using the OPSEC/LEA Protocol

Previously, if you changed the log source identifier for a log source using the OPSEC/LEA protocol, events were no longer received because the certificate was no longer associated. This no longer occurs.

Log Source Using a JDBC Protocol No Longer Displays Incorrect Status

Previously, if you were using a log source with the JDBC protocol, STRM Log Manager received events from the log source; however, the Log Sources window displayed an incorrect status. This no longer occurs.

Known Issues and Limitations

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

- [General](#)
- [System Configuration](#)
- [Events Interface](#)
- [Reports Interface](#)
- [Dashboard](#)

General Upgrading from STRM Log Manager 2009.1 to STRM Log manager 2009.2 might give a warning

During Upgrade from STRM Log Manager 2009.1 to STRM Log Manager 2009.2 a Warning message might appear:

```
OK: Running kernel 2.6.18-128.1.10.el5 is a valid pre-upgrade kernel.
```

```
PRETEST: Running check_installed_rpms.pl...
Found changes to default RPMs installation.
```

```
The following RPMs are new and will cause conflicts:
```

```
---
compat-libstdc++-33-3.2.3-61 x86_64
StorMan-6.40-18530 x86_64
---
```

```
The following required RPMs have been removed:
```

```
---
StorMan-5.50-17523 x86_64
---
```

```
WARNING: The changes reported above may cause the upgrade to fail.
Do you want to continue (Y/[N])?
```

Workaround: Type Y to continue and press enter, the upgrade will continue as normal.

Deploying a license on an active HA unit might give an error

Error might occur when deploying a license, when the HA has synced between Primary and Secondary and the appliances are in Active and Standby states respectively.

Workaround: Deploy the required licenses by primary appliance on Primary HA appliance before adding the secondary HA appliance to the system. Add the Secondary HA appliance. After the initial start, there will be a prompt for secondary HA appliance license “Needs License”, apply the appropriate HA license on the secondary appliance.

Primary HA appliance will take longer time to initiate the restart process

Primary HA appliance will restart once the “Add HA Host” wizard is finished and It takes 15 - 20 minutes to initiate the restart.

The restart is necessary for Secondary HA appliance to start synchronization with the Primary HA appliance.

Workaround: None



Note: The Primary HA appliance should **not** be restarted manually during this wait time.

Set System Online” manually to failover to primary unit

When the primary unit is recovered from a failure, the system has to be set online manually for the primary unit to resume function as the Active unit.

Workaround: None

View NSM Policy Details” for a device in NSM sub domain will give error

If you are trying to view the NSM policy details for a device in the NSM sub domain then there would be an error.

Workaround: None

Unable to use non-management interface for initial HA Sync

STRM does not support HA sync on a non-management interface.

Workaround: None

Secondary HA appliance needs to be fresh installed

Workaround: Refer to the “For Secondary HA Appliance” section in the STRM Log Management Installation Guide.

STRM services might not be ON after upgrading from 2009.1 to 2009.2

After Upgrading the STRM unit from 2009.1 to 2009.2, none of the services might be running as the “reboot” prompt has not shown up at the end of the upgrade.

Workaround: Manually type “reboot” from the console.

Technical contact on manage license page does not open in a browser

Clicking on the technical contact link under “System and License Management”à “Manage License”, opens the page in an Email client.

Workaround: None

Excessive System Notifications For ECS Memory Cache Causing Performance Issues

When the ECS memory cache is being written to disk, the following error message appears in the logs and system notifications:

```
dao_cache.com.qllabs.core.dao.sem.TargetProperties is  
experiencing heavy COLLISIONS exceeding configured threshold  
(this may have negative performance impact) threshold = 5.0  
average collisions = 13.0
```

This error message is not an accurate indication that the system is having issues or experiencing performance issues. This error message will be changed in a future release to better represent the memory to disk utilization of ECS

Workaround: None

Unable to Resize Columns in Real-Time (Streaming) Mode in Internet Explorer

If you are viewing events in Real-Time (streaming) mode and you are using IE 7.0, you will be unable to resize columns. This feature works with Firefox 3.0.

Workaround: To resize columns in Real-Time (streaming) mode, pause streaming.

Sorting Request is Not Maintained Once a Filter is Cleared

In the Events interface, when viewing data in a time range other than Real-Time (streaming), you can sort the displayed information by clicking a column heading. If you clear an existing filter after you sort the data, the sort request is also cleared. The interface displays the data as it appeared before the data was sorted.

Workaround: None.

Deploying Changes Causes In-Progress Searches to Disappear

If there are searches in progress when you deploy changes in the Admin interface, the searches will no longer be available in the Manage Search Results window.

Workaround: None

Unsaved Searches May Show a Hyphen (-) in the Expires On Column

The Expires On column shows a hyphen (-) if you perform a new unsaved search using the same criteria and time span as another cached search result that has been saved. The hyphen value has the same meaning as a value of Never. This has no impact on your search functionality.

Workaround: None

Sorting Error May Display When No Sort is in Progress

When you perform an event search, an error message may appear to indicate a sorting problem when no sort is in progress.

Workaround: None

Excessive Web Browser Memory Consumption

When you are using Internet Explorer to access STRM Log Manager over an extended period of time, excessive amounts of memory are consumed and may eventually cause the browser to cease functioning.

Workaround: Periodically minimizing your browser window releases memory consumption and significantly increases the amount of time it takes before a browser crash.

Passwords Over 13 Characters Causing Database Maintenance to Fail

If your root password is over 13 characters, the database maintenance script fails to log in to your database and no error message is logged. Database maintenance includes procedures to discard older data according to specified retention periods. If your database management procedures fail to perform, the database will grow too large and may significantly impact performance.

Workaround: None

Main STRM Log Manager Interface May Time Out While a Separate Configuration Window is Active

When a separate configuration window is active, the main STRM Log Manager user interface may time out due to inactivity and you may need to log back in to continue. Examples of configuration windows include the Rules Wizard and Reports Wizard.

Workaround: You can configure the **Inactivity Timeout (in minutes)** parameter for the STRM Log Manager Console. For more information, see the *STRM Log Manager Administration Guide*.

Export Function Not Displaying Status Window When Displaying a Subset of Events in a Separate Window

If you perform an event or flow search and then select a Multiple (N) link, a new window appears displaying the subset of events or flows. From this window, if you select Actions > Export to XML or Actions > Export to CSV, the export status window does not appear. When the export is complete, you may be prompted to save results, depending on the size of the results.

Workaround: None

System Configuration**Unable to Restore an HA Backup Onto an HA Cluster With Different IP Address**

If you restore an HA backup onto an HA cluster that has different IP addresses than the backup archive, the backup will not complete.

Workaround: None

Log Sources are Unassigned After Re-Adding an Event Collector

If you delete an Event Collector in the deployment editor and then re-add the Event Collector with the same IP address, the log sources that were previously assigned to the original Event Collector show a status of Unassigned in the Log Sources window.

Workaround: Assign the unassigned log sources in the STRM Log Manager user interface to the new Event Collector. If you have multiple log sources from multiple unassigned collectors, contact Customer Support.

Unable to Open Deployment Editor If You Have JDK 6 or JRE 1.6.0_14 X86 or Higher Installed

STRM Log Manager does not support JDK 6 or any JRE version higher than JRE 1.6.0_13 X86. If you have JDK 6 or JRE 1.6.0_14 X86 (or higher) installed on your desktop, an error appears when you attempt to access the deployment editor.

Workaround: If you have JDK 6 installed on your desktop system, uninstall it. If you have JRE 1.6.0_14 X86 or higher installed, uninstall it and then install JRE 1.5.0_13. For further assistance, contact Customer Support.

Users with System Configuration Role Cannot Change Their Own Password

Users that are assigned the System Configuration role but not the Administrator Manager role are unable to change their own password. Only users with the Administrator Manager role can create or edit other administrators.

Workaround: None

Spaces in Root Password Blocking Access to the STRM Log Manager User Interface

When installing STRM Log Manager, the Root Password window allows for spaces in your password. However, if you include a space in your root password, you would not be able to access the STRM Log Manager user interface.

Workaround: Avoid using spaces in your root password.

Unable to Edit Automatically Discovered Juniper NSM Log Source

After STRM Log Manager automatically discovers a Juniper NSM log source, the log source functions properly, however, you cannot edit the log source because the Log Source Identifier parameter and the IP address in the protocol do not match.

Workaround: None

Delay in Managed Host Appliances Processing Events After HA Failover

After a primary managed host fails over, the HA configuration does not immediately synchronize the time on the secondary system. While the time is unsynchronized, events are not processed, therefore, no events appear on the Console. After several minutes, the time synchronizes and event processing restarts.

Workaround: Perform a full deployment to immediately restart event processing. In the Admin tab, select **Advanced > Deploy Full Configuration**.

Events Interface Unable to Remove Custom Event Mapping

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

Workaround: None.

Overlapping Text May Appear in the Events Interface

If your screen resolution is set to 1024x768 and you view data in the Events interface for the most recent interval, the Next Refresh text may overlap the Display drop-down list box.

Workaround: None.

Mapping Events to the Unknown/Stored Events Category

Using the Map Event button available in the Event Details window, you can map events to the Unknown/Stored category. Please note that after you map an event to the Unknown/Stored category, you cannot change the mapping. STRM Log Manager does not allow events in the Unknown / Stored category to be remapped to a new category.

Workaround: Avoid mapping events to the unknown/stored category.

Using Certain Offense Property Tests and Device Tests in Same Rule May Cause the Rule to Not Function

If you use the following tests in the same rule, the rule may not generate offenses, as expected:

- Offense Property Tests: when a new offense is created
- Device Tests: when the device type(s) that detected the offense is one of the following types

An error may appear and the rule does not generate offenses.

Workaround: None.

Deleted Custom Event Properties May Still Appear in the Existing Property List

If you delete a custom event property, the property may still appear in the Existing Property drop-down list box in the Event Property Definition window.

Workaround: None

Events Interface is Not Displaying Events Mapped to a User-Defined QID

Using the event mapping tool, you can map a normalized or raw event to a STRM Log Manager Identifier (QID) from the QID map. The QID map contains default