

STRM LOG MANAGER RELEASE NOTES

RELEASE 2009.1

NOVEMBER 2009 - REVISION 2

Juniper Networks is pleased to introduce STRM Log Manager 2009.1. This release provides you with several resolved issues.

This document includes:

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

New and Updated Functionality

STRM Log Manager 2009.1 provides you with the following new and updated functionality:

- **License Limits** - Your STRM Log Manager 2009.1 license key now enforces limits to the number of active log sources allowed. If you exceed the limit, an error message appears. When upgrading to STRM Log Manager 2009.1, the upgrade will abort if you exceed the limit. You can pre-test your system prior to performing the upgrade to verify that your active log sources does not exceed your license. For more information about pre-testing your system, see *Upgrading to STRM Log Manager 2009.1*. Contact Customer Support for assistance.
- **User Interface Update** - The STRM Log Manager user interface provides the following name changes:

Table 1 Name Changes

Previous Name	STRM Log Manager 2009.1 Name
Event Viewer	Events
Administration Console	Admin

Note: This tab replaces the STRM Log Manager Administration Console.

Table 1 Name Changes (continued)

Previous Name	STRM Log Manager 2009.1 Name
Sensor Devices	Log Sources
Device Extensions	Log Source Extensions
Tools menu	Preferences

- **Events Interface Enhancements** - The Events interface provides the following enhancements:
 - **New Real-Time (Streaming) Mode** - You can now view events or flows in real-time (streaming) mode, which supports full filtering capabilities. This mode provides you a real-time view of your current event and flow activity by displaying the last 40 events.
 - **Improved Views for Grouped Events** - When viewing grouped events, you can now double-click a group (row) to view the events that comprise the selected group. You can also click a field that indicates Multiple (*n*) to view the dataset with the data grouped on the selected field and filtered on the original group(s).
 - **Adding Filters** - The new Add Filter button allows you to filter your current view of events without requiring you to go to the edit search window.
 - **Filtering on Event Processor** - In the Events interface, you can now filter on the Event Processor parameter, allowing you to perform searches based only on selected Event Processors.
 - **Improvements to IP Right-Click Functionality** - In previous releases, there were two right-click menus, depending on where you clicked within a field (white space or text). These menus are now combined into one menu, which is launched regardless of where you click within the field.
You can also right-click on any username to access additional menus, which allow you to further investigate that username.
 - **Search Groups** - You can now create and manage search groups. These groups allow you to easily locate a saved search that you want to perform or base a report on a saved search.
 - **Search Results Management** - You can now perform multiple event searches while navigating to other interfaces. You can configure the search feature to send you an e-mail notification when a search is complete.
 - **Viewing Partial Search Results** - You can now view search results before the search is complete. When you generate a search in the Events interface, you can view partial results before the search has collected all results. If the search is not complete, a progress indicator appears in the top right corner.
While viewing the partial search results, the search engine works in the background to complete the search and refreshes the partial results to update your view.
 - **Sub-Searches** - You can now perform sub-searches of event data. Each time you perform a search, STRM Log Manager searches the entire

database for events that match your criteria. This process may take an extended period of time depending on the size of your database. The sub-search feature allows you to perform searches within a set of completed search results. The sub-search function allows you to refine your search results without requiring you to search the database again.

- **Administration and Management Functionality Enhancement** - The administration and management functionality provides the following functional and usability enhancements:
 - **Admin Tab** - In previous releases, the administration functionality was located in the Administration Console. This functionality is now located in the Admin tab in the main STRM Log Manager interface.
 - **Improved System Management** - You can now remotely shutdown and restart systems. You can also view and manage the status of your systems and licenses.
 - **Log Source Configuration Improvements** - In previous releases, you were required to configure a log source and the associated protocol in separate windows. In STRM Log Manager 2009.1, you can now configure the log source (formally known as sensor device) and protocol within the same window.
 - **Improved Log Source Management** - The Log Sources window now includes a Status column, which displays the current status of the log source. The status will indicate Error, Warning, or Success. STRM Log Manager monitors the status of the log sources to provide up-to-date information.
 - **Improved Backup and Recovery Functionality** - When restoring a backup, a progress window now appears providing the status of the restore process. This window provides any errors for each host. This window also provides instructions for resolving errors that have occurred.

STRM Log Manager 2009.1 also introduces the ability to restore backup archive on system with a different IP address than the backup archive.
 - **SNMP Configuration Improvements** - The System Settings window now provides improved SNMP configuration options. After you select your SNMP version, the window automatically updates to provide the appropriate fields for your selected version.
- **SNMP Agent Functionality No Longer Available** - The SNMP Agent functionality is not available in STRM Log Manager 2009.1. If you are upgrading to STRM Log Manager 2009.1 and require this functionality, contact Customer Support
- **Juniper Networks NSM Plug-In** - STRM Log Manager 2009.1 introduces a plug-in that allows you to view the policy details from the Juniper Networks NSM server directly from the Events interface.
- **Automatic Updates Improvements** - The automatic update service has been improved to support delivery of minor updates (such as on-line Help or updated scripts) and major updates (such as updated JAR files), and DSM updates.

- **Management Interface Selection** - Previously, ETH0 was the default management interface. When installing STRM Log Manager 2009.1, you can specify your management interface. The upgrade or installation script prompts you to select from a list of interfaces and indicate which interfaces have detected links.



Note: *Third-party RPMs are not supported on STRM Log Manager systems. Before you upgrade to STRM Log Manager 6.3, pretest your systems to determine if your deployment includes any third-party RPMs. For more information, see the [Upgrading to STRM Log Manager 6.3 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 2009.1:

Error No Longer Appear in Log File If Deployment Includes RPM Installed Scanners and DSMs Prior to Upgrade

Previously, if your deployment included DSMs or scanners installed using an .rpm file, an error appeared in the log files after you upgraded your system. This error did not affect the upgrade process or system functionality. This no longer occurs.

Exported Flow Data Now Contains Payload

Previously, if you exported flow data in the Flows interface that included payload content, the payload information did not appear in the exported data. This no longer occurs and the exported flow data includes payload content.

Vulnerability No Longer Exists in Apache Web Server

In previous releases, STRM Log Manager used a version of the Apache Web Server that included a vulnerability, which was exposed if a flawed HTTP client was forced to send an HTTP request with an invalid method name. STRM Log Manager 2009.1 uses an upgraded version of Apache Web Server that is no longer vulnerable to this activity.

Default-Rule-System: Device Stop Sending Events Rule Now Indicates Specific Event Source

The Default-Rule-System: Device Stopped Sending Events rule reports when an event source has not sent an event to the system in over 1 hour. Previously, when this rule generated a response, the specific event source was not specified. In STRM Log Manager 2009.1, the rule now generates a response detailing the specific event source involved in the activity.

Asset Names Now Appear in the Events, Flows, and Offenses Interfaces

Previously, asset names may have appeared instead of the IP address in the STRM Log Manager interface. In STRM Log Manager 2009.1, assets names now appear in separate fields in the Events, Flows, and Offenses interfaces. In the Offenses interface, asset names appear in the All Offenses, Offense Summary, and Attacker Summary windows. In the Events and Flows interfaces, two new columns (Source Asset Name and Destination Asset Name) display the asset names. Also, you can filter and sort on the asset name.

Offense Count in Dashboard and Offense Interfaces Now Accurate

Previously, the System Summary item in the Dashboard displayed an offense count that did not match the offense count displayed in the Offenses interface. This no longer occurs and the offense counts are accurate for both interfaces.

List of Event Categories Now Displays All Categories

Previously, the List of Event Categories window did not display all event categories. This was as a result of a page size issue in the browser. This issue no longer occurs in STRM Log Manager 2009.1 and all the event categories appear.

Enabling an Additional Interface Using Web-Based System Administration Interface No Longer Results in Error

Previously, if you attempted to enable another interface using the web-based system administration interface, an error appeared indicating the IP address was invalid. This no longer occurs and a valid IP address is now validated properly.

Passwords Longer than 16 Characters No Longer Causes Error

Previously, if your STRM Log Manager system included a password that was longer than 16 characters, error messages appeared in the log files. In STRM Log Manager 2009.1, this no longer occurs. If you update your global configuration password in the web-based system administration interface, the password may be longer than 16 characters.

Reports Interface Now Has Increased Memory Capabilities

Previously, when generating a large report, the Reports interface may have experienced memory issues resulting in an error message. The report did not generate. In STRM Log Manager 2009.1, the Reports interface has been optimized to provide increased performance enabling large reports to be generated.

Improved Notifications for Dropped Events

Previously, the dropped event notifications only provided minimal information to investigate the cause of the dropped events. Notifications have been improved to provide additional information, such as the reason for the dropped events, where in the event pipeline the events were dropped, and statistics for all event sources. Also, the frequency for notifications has increased to every 60 seconds.

Searches Now Produce Results That Include Log Source Sub-Groups

Previously, event searches that included log source groups that contained sub-groups did not produce results for log sources in the sub-groups. This no longer occurs.

Search Time Out Functionality No Longer Exists

Previously, event searches that extended over 10 minutes generated a time-out message that allowed you to bypass the restriction. If you selected to bypass the time-out restriction, the search did not restart as expected. The time-out functionality no longer exists.

Wildcard Searches Now Functional in the Log Sources Window

Previously, you could not perform a wildcard search to locate a log source(s) in the Log Sources window. STRM Log Manager 2009.1 now supports the following wildcard characters when searching the Name or Log Source Identifier fields:

- % - Matches any string.
- _ - Matches any single character.

Restored Systems That Include Scanners No Longer Causes Tomcat Server Failure

Previously, if you restored a system that included scanners or DSMs installed as plug-ins, the Tomcat server failed to restart. This no longer occurs.

Time Setting on Quick Searches No Longer Incorrect

Previously, the incorrect time showed on a quick search if you saved the search with the **Include with time** and **Include in quick searches** options selected. This only occurred when you saved the search directly from the results screen, and not from Saved Searches screen. This no longer occurs.

An IP Address Previously Identified as a Remote Attacker Can Now Be Created as an Offense When Creating a New Network

Previously, STRM Log Manager could start generating offenses even if your network hierarchy was not defined. STRM Log Manager recorded all generated offenses as remote offenses since no local systems were defined in your network hierarchy. When this occurred, any IP address that had been previously defined as a remote attacker could not be created as an offense when defining your network. This no longer occurs.

Double-Clicking on Unioned Flow to Access Additional Information Now Functions Properly

Previously, if you wanted to access additional information on a unioned flow in the Flows interface, the option to double-click on a flow was disabled. This no longer occurs.

Search for (SrcIP = x or SrcIP = Y) and (DstIP = x or DstIP = y) Now Returns Correct Results

Previously, if you performed a search with the parameters (SrcIP = x or SrcIP = Y) and (DstIP = x or DstIP = y), invalid results were returned. This search should have looked for all traffic between the specified source IP address and destination IP address, but it returned results for all traffic for either IP address. This no longer occurs.

Reports Based on Specific Flow Columns and Groupings No Longer Stops Collecting Data After Upgrade

Previously, reports collecting data based on flow-based searches involving the following flow columns and groupings stopped collecting data:

- ICMP Type
- Flow Source
- Flow Source/Interface
- Source QoS
- Destination QoS
- Application/Source QoS/Destination QoS

This no longer occurs.

Known Issues and Limitations

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

- [General](#)

- [System Configuration](#)
- [Deployment Editor](#)
- [Network Surveillance](#)
- [Offenses Interface](#)
- [Events Interface](#)
- [Flows Interface](#)
- [Reports Interface](#)
- [Dashboard](#)
- [Assets Interface](#)
- [Log Source Management](#)
- [Vulnerability Assessment](#)

General **SNMP Source Payloads Displaying as HEX Instead of ASCII Plain Text**

SNMP-based event sources with long messages may display as HEX instead of ASCII plain text. This occurs when messages are long and contain non-ASCII printable characters, such as carriage returns or line feeds.

Workaround: None

NSM cannot be contacted from the STRM dashboard or the Event page.

If you set NSM as the preference in the STRM dashboard, or view the NSM Policy details from the STRM Event page, an error message appears: "NSM cannot be contacted at https://10.205.75.2:8443. Please verify the URL."

Since the SSH certificate connects NSM to STRM, the error could appear either because the SSH certificate on the NSM box has expired or is invalid.

Workaround: Accept the invalid SSH key and continue with the SSH connection. To do this:

Step 1 Copy the following file from the NSM box:

```
/usr/netscreen/GuiSvr/lib/webproxy/conf/client.truststore
```

Step 2 Go to the following file on the STRM box:

```
/opt/gradar/conf/webplugins/117/client.truststore
```

Step 3 Replace this file on the STRM box with the file from the NSM box.

Step 4 Restart tomcat using the following command:

```
# service tomcat restart
```

Pretest Failing Because of Undeployed Changes

When you add a flow source and disable the flow source before you deploy your changes, the status is not updated in the database. When you perform the upgrade pre-test, the test fails because of undeployed changes.

Workaround: In STRM Log Manager 2008.3, access the Administration Console and click **Deploy Configuration Changes**. Perform the pretest again. If the pretest fails again:

- Step 1** Access the Administration Console.
- Step 2** Click **Flow Configuration > Manage Flow Sources**.
- Step 3** Enable the Flow Sources that show a status of False.
- Step 4** Click **Deploy Configuration Changes**.
- Step 5** Disable the flows sources again, if required.
- Step 6** Click **Deploy Configuration Changes**.

You can now perform the pretest successfully.

Failed Upgrade Message May Appear in the Login Banner If You Log Out and Log In After Successfully Pretesting Your System

If you log out and log back in to your system after successfully pretesting your system prior to upgrading, the following failure message appears the login banner:

```
FAILED to upgrade this server to QRadar 6.2.0.<build> patch
<patch>!
```

Workaround: None. Ignore this error message. After you perform the upgrade, the correct message appears.

The Term “Notification” in More than One Default-Rule-System Rule May Cause Your Upgrade to Fail

STRM Log Manager provides the following default rule: `Default-Rule-System: Notification`. If the term “Notification” is included in an additional Default-Rule-System rule, your upgrade may fail during the pretest.

The following error message appears:

```
ERROR: Cannot unambiguously identify default system notification
custom rule for update.
ERROR: Failed to run 'check_notification_rule.sh' script!
Please contact customer support for assistance with this error.
Your system has not been upgraded so that this can be resolved.
No services have been shutdown yet.
```

Workaround: Review your Default-Rule-System rules in the Offense Manager interface and remove the term “Notification” from the description field of any rule other than `Default-Rule-System: Notifications`.

Changing Network Settings on Your STRM Log Manager 2008.3 Console Encrypts Password, Causing the STRM Log Manager 2009.1 Upgrade Pre-Test to Fail

If you run the `qchange_netsetup` command on a STRM Log Manager 2008.3 Console to change your network settings, the configuration services password becomes encrypted. Then during the setup process, the password is re-encrypted. Therefore, when upgrading to STRM Log Manager 2009.1, the upgrade pretest

script fails because of internal configuration authentication issues. The following error message appears:

```
PRETEST: Running check_double_encrypted_pass.pl...
ERROR: configuration.services.password is encrypted value.
qchange_netsetup was run on Mon Apr 27 11:34:32 MDT 2009.
ERROR: Failed to run 'check_double_encrypted_pass.pl' script!
```

Workaround: Update the configuration services password on all managed hosts in your deployment:

Step 1 Log in to STRM Log Manager.

Step 2 Click the **Admin** tab.

Step 3 In the navigation menu, click **System Configuration > System and License Management**.

The System and License Management window appears.

Step 4 Select the host for which you want to update the configuration services password.

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

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

Username: **root**

Password: **<your root password>**



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

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

The STRM Log Manager Setup window appears.

Step 8 In the **Enter the global configuration password**, enter the password you want to use to access the host. Confirm the entered password. The password must be the same for all hosts in your deployment

Step 9 Click **Apply Configuration**.

Repeat for all managed hosts in your deployment.

Unable to configure IPv6 through webmin as the webmin code does not set "NETWORKING_IPV6=yes" in "/etc/sysconfig/network".

Workaround: Manually add "NETWORKING_IPV6=yes" to "/etc/sysconfig/network" and reinitialize the interface by ifdown/ifup on eth1.

Modification time of Log Sources shows as "unknown".

When you view the modification time for Log Source Group in the Date modified column under the Other Group option, it shows as "unknown". This issue will be fixed for the 2009.1 R1 release.

If you use `https://<ip address>/console` to launch the STRM GUI, the link redirects you to "`https://<box console name>.juniper.net/console/`" and prompts an error as "Address not found".

Workaround: Use only "`https://<ip address>`" without the console to launch the STRM GUI.

Unable to resize column headings in the Event Viewer page using Internet Explorer 7.

This issue will be fixed in the STRM 2009.2 release.

In the Manage License option, from Admin > System Configuration > System and License Management > Action, the License details displays "Offense Manager".

This will be changed to only "Offenses" in the 2009.2 release.

Devices sending logs through NSM will get AutoDetected as "NetscreenNSM".

Workaround: NSM can still be used as a central management tool however have all devices send their Syslog to STRM directly.

STRM does not support Structured Syslog sent by IDP.

Workaround: None. Need to be fixed in future release.

JunOS devices get autodetected as "Juniper Router".

Workaround: Add the M, MX, T-Series routers manually.

StandaloneIDP gets autodetected as "NetscreenFirewall".

Workaround: Manually Add Device as "JuniperIDP".

An auto-discovered Infranet Controller may appear incorrectly as a "JuniperSA", "Juniper Networks Secure Access (SA) SSL VPN" device.

Workaround: Add this device manually in Sensor Devices.

An auto-discovered EX-Series Ethernet Switch may appear incorrectly as a "JuniperRouter", "Juniper Networks Routing Platform" device.

Workaround: Add the EX-Series Ethernet Switch manually.

Read Timeout Error May Occur for Searches With a Duration Over 1 Hour

When performing a search on a system that receives events or flows from multiple sources, a read timeout error may occur if the search duration for any source exceeds 1 hour. The read timeout message displays in the search results banner. The search continues and returns results for the other sources. After the search completes, the Error status displays in the top right corner of the interface.

Workaround: None

Items Assigned to a User May Not Be Removed After Deleting the User

After you delete a user, items such as saved searches, reports, sentries, and assigned offenses, will remain associated with the deleted user. This does not affect functionality, but messages may appear in the log files.

Workaround: None

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

If you want to export data (such as events, assets, or flows), using the STRM Log Manager 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 Manager 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.

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

If you are viewing events or flows 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 Flows or 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.

User Account Name Containing a Less Than Sign (<) Does Not Appear Properly in the Interface

If you create a user account with a name that contains a less than sign (<), any characters after the less than sign do not appear in the interface. For example, if you create a user account with a name of **NS<Admin**, only **NS** appears in the interface as the user account name.

Workaround: Create a user account name without a less than sign (<).

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 or flow search, an error message may appear to indicate a sorting problem when no sort is in progress.

Workaround: None

System Configuration

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

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. STRM Log Manager does not support JDK 6 or any JRE version higher than RE 1.6.0_13 X86.

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.

SSH Keys Not Restored When Restoring a Backup on a System with a Different IP address than the Backup Archive

When restoring a backup on a system with a different IP address than the backup archive, the SSH keys are not restored if you do not select the option to restore all items. The Console will no longer communicate with the managed hosts.

Workaround: When restoring a backup to a different Console, select the **All items** check box in the Restore a Backup window.

TACACS Authentication Creating Offenses for False Failed Login Attempts

If you enable TACACS as your authentication type, STRM Log Manager will attempt to access the active directory for login credentials. The attempts will fail and result in offenses being generated. These offenses are false positive.

Workaround: None

Installation With a Potentially Corrupt Zip File

When you deploy configuration changes in STRM Log Manager, the following error may appear in the log file: Failed to unpack new configuration files. This error condition may be the result of a corrupted zip file.

Workaround: In the Admin interface, click **Deploy Changes**.

Editing Administrative Email Address in System Settings Causes Error

If you edit the Administrative Email Address parameter in the System Settings Window, an error message may appear in the log files. This error does not affect system performance and the updated e-mail address is enforced.

Workaround: None.

Scanner Description Field Only Allows Maximum of 50 Characters

When configuring a scanner, you can enter a description for that scanner. The description field only allows a maximum of 50 characters. If you enter a description longer than 50 characters, no error message appears and you are able to save the scanner. However, if you view the scanner information, the description is truncated to 50 characters.

Workaround: None.

License is Invalid if the Serial Number in a Backup Archive Does Not Match the Serial Number on the Current Console

After restoring a backup archive, the license is invalid if the serial number of the backup archive does not match the serial number of the current Console.

Workaround: Before you restore the backup archive, save the current license. The license is located at `/opt/qradar/conf/license.key`. After restoring the backup archive, apply the saved license. You can also find the license in the `config-pre_restore` archive.

Server Status Appears As Unknown On System and License Management Window

If you remove a host from your deployment and then re-add the host with different IP address prior to upgrading to STRM Log Manager 2009.1, the system status for the host may display as unknown on the System and License Management window after the upgrade.

Workaround: None

Deployment Editor Unable to Launch Deployment Editor After Changing Management Interface

You can change the management interface using the `qchange_netsetup` command (for more information, see the *STRM Log Manager Installation Guide*). However, if you change the management interface, the deployment editor fails to launch and an error appears.

Workaround: None

Network Surveillance Graph By Lines Option May Display Multiple Lines with Same Color

When you are viewing a graph that includes multiple network view objects, the graph may display multiple view objects using the same color since the colors are based on the network. For example, if you are viewing the Chat, Mail, and web components in an Application View, each data set is different, however, since they

are based on the same network, STRM Log Manager interprets the data as one, displaying each component with the same color.

Workaround: None

Offenses Interface Attackers/Src Column May Show Incorrect Values

When viewing attackers in the Offenses interface, the Attackers/Src column may display a numeric value rather than an IP address.

Workaround: None

Offense Counts in the By Category View May be Incorrect

When viewing the By Category view in the Offenses interface, the offense count may be inaccurate. The offense count should only include active and dormant offenses; however, inactive offenses may be included in the count.

Workaround: None.

Sorting on Specific Search in Offenses Interface Displays All Searches

In the Offenses interface, you can search offenses based on closed or hidden offenses. If you search closed or hidden offenses, then sort the search results (click on the column heading), the Offenses interface displays all active, hidden, and closed offenses.

Workaround: None.

Viewing a List of Attackers May Display Blank Pages

The Offenses interface allows you to view a list of attackers for a network. If your system includes closed offenses that have been removed from the database, the list of attackers may not return the same number of results as the attacker count. If the list of attacker results are returned over multiple pages, there may be several blank pages at the end of the results. All results are included in the output.

Workaround: Click on the previous page to view information.

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.

Flows Interface ASN Values Inaccurate When Searching Grouped Flows

If you search grouped flows using a time range other than real-time streaming and include the Source ASN and the Destination ASN columns in the search results, the ASN values are inaccurate.

Workaround: None.

Reports Interface TopN Reports Unable to Graph Flow Data from a Lower Leaf Level Geographic

When creating TopN Reports that includes lower leaf level geographic flow data, the report graphs are blank, because the flow data is not captured.

Workaround: None

Reports With Event or Flow Data in Table Format Displays Incorrect Output for Single Values

When creating reports that contain tables, any field that should contain a single value displays Multiple (1) instead of the actual value.

Workaround: None

Dashboard Unable to Add New Offenses Over Time Item to the Dashboard

In the Dashboard interface, the New Offenses Over Time item does not successfully add. The Offenses - New Offense Count item displayed in the default dashboard is the same item as the New Offenses Over Time item, but with a different name.

Workaround: None

Assets Interface Unable to Delete Assets That Have a Value of Never in the Last Seen Column

In the Assets interface, you are unable to delete assets that have a value of Never in the Last Seen column.

Workaround: None

Unable to Save Approved Servers When More Than 1000 Results are Returned

The Server Discovery function does not save approvals when more than 1000 results are returned for Windows Server and Web Server. This may also occur when selecting a sub-network group that shows less than 1000 results.

Workaround: None.

Log Source Management Events Not Being Received After Changing the Log Source Identifier for a Log Source Using the OPSEC/LEA Protocol

If you change the log source identifier for a log source using the OPSEC/LEA protocol, events are no longer received because the certificate is no longer associated. For example, if you want to configure a Check Point Firewall-1 to send logs to a secondary device, you need to change the log source identifier to the secondary device and pull the certificate from the primary device.

Workaround: To change the log source identifier for a log source using the OPSEC/LEA protocol:

- Step 1** Log in to the STRM Log Manager interface.
- Step 2** Click the **Admin** tab.
The Admin interface appears.
- Step 3** Click the **Log Sources** icon.
- Step 4** Select the log source you want to edit.
- Step 5** In the **Log Source Identifier** field, enter the new IP address.
- Step 6** Clear the **Use Server IP for Log Source** check box.

1000 Log Source Limit in Event Searches Based on 'Other' Log Source Group

When searching events associated with the 'Other' log source group, the results are limited to 1,000 log sources. This limitation maximizes user interface performance.

Workaround: If you have more than 1,000 log sources in the Other log source group, we recommend that categorize your log sources into groups, allowing you to efficiently view and track your log sources.

Log Source Using a JDBC Protocol May Display Incorrect Status

If you are using a log source with the JDBC protocol, STRM Log Manager receives events from the log source; however, the Log Sources window may display an incorrect status.

Workaround: None

Vulnerability Assessment **Unable to Advance to Next Page in VA Scan and Scan Scheduling Windows**

In the VA Scan and Scan Scheduling windows, you are unable to advance to the Page 2 if there are more than 40 listed items.

Workaround: None

Successful Scan Showing Incorrect Status

If a scanner performs a successful scan after a failed scan has occurred, the Scan Scheduling window displays a status of failed for the scanner. It appears that the actual scan has failed, when in fact the status refers to the scanner and not the scan.

Workaround: None

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.

Published: 2009-11-30