

# STRM RELEASE NOTES

## RELEASE 2008.2

OCTOBER 2008--REVISION 2

Juniper Networks is pleased to introduce STRM 2008.2 R2. This release provides you with several resolved issues.

This document includes:

- [Technical Documentation](#)
- [Contacting Customer Support](#)
- [Supported Devices and OS Versions](#)
- [Supported Java and Browser Software](#)
- [Resolved Issues](#)
- [Known Issues and Limitations](#)

---

### 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 Technical 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](mailto:techpubs-comments@juniper.net). <[mailto: techpubs-comments@juniper.net](mailto: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)

---

## Supported Devices and OS Versions

STRM 2008.2 R2 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, 6.1.0r2	No	Yes
Firewall/VPN	6.0, 6.1.0r2	Yes	Yes
Standalone IDP	4.1	Yes	Yes
J-series	8.5, 9.0, 9.1, 9.2r1.10	Yes	No
Secure Access (SA)	6.2	Yes	No
Infranet Controller (IC)	2.2	Yes	No
EX-Series	9.1R2.10	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.

To parse logs from IC devices, the IC device needs to be manually added under Sensor Devices.

---

## Supported Java and Browser Software

STRM 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 2008.2 R2:

### Offense Now Includes Associated Events

Previously, if an event associated with an offense included a destination IP address of 0.0.0.0, the event did not appear in the Offense interface summary or Events list. This no longer occurs.

### STRM Now Reports DDOS Attacks Correctly in the Interface

Previously, after the upgrade process, STRM failed to report DDOS attacks accurately. This resulted in a significant increase in the number of recorded offenses. This no longer occurs and the DDOS attacks are reported appropriately.

**Tomcat Server Now Restarts Properly After Upgrade Process**

Previously, after upgrading your STRM system, the Tomcat server failed to restart. This was due to a missing file for the netVigilance Secure Scout scanner in the upgrade. This no longer occurs and the Tomcat server restarts properly.

**NTP Settings Now Persisted After Upgrade**

Previously, after you upgraded your STRM system, the NTP settings were not persisted. This required you to reset your NTP settings using the web-based system administration interface. This no longer occurs and NTP settings are persisted after the upgrade process.

**Identity Table Now Updated After Upgrade**

Previously, after the upgrade process, the identity table was no longer updated. This may have caused DSMs to no longer function. This no longer occurs and the identity table is updated after the upgrade process.

**Upgrade Process No Longer Fails for Deployments with Encrypted Tunnels**

Previously, if your deployment included encryption tunnels, the upgrade process failed. This no longer occurs.

**STRM No Longer Displays FlowViews Error After Upgrade**

Previously, after the upgrade process, the following error appeared: **Error initializing FlowViews**. This error was caused by an additional line in the application configuration file that resulted in the FlowViews not being initialized. This no longer occurs.

**Applying Multiple Patches No Longer Corrupts Configuration File**

Previously, if you installed multiple patches and enforced the changes (Host Context component should restart automatically), the STRM configuration file was corrupted. This caused a disruption in service. This no longer occurs and installing multiple patches no longer corrupts the system.

**STRM Now Able To Effectively Process Events for Large Number of Sensor Devices.**

Previously, if your deployment consisted of a large number of Sensor Devices, your STRM system experienced reduced performance when events were processed. This no longer occurs.

**During a Restart, an Error No Longer Appears Regarding the Tomcat Server**

Any changes to STRM using the web-based system administration interface requires the Tomcat server to restart. This server may take 1 to 2 minutes to restart. Previously, if you attempted to access the STRM interface during the restart, a fatal error message appeared. This no longer occurs.

### **Continuous Use of STRM Over Extended Period of Time No Longer Causes Interface Failure**

Previously, if you continued to use a session of the STRM interface for an extended period of time, a failure occurred in your browser requiring you to restart your system. This no longer occurs

### **Restoring Configuration Information for Deployment with Encrypted Systems No Longer Fails**

Previously, if you attempted to restore configuration information in a deployment that included encrypted systems and then deployed all changes, the restore process failed for the encrypted systems. This no longer occurs.

### **Accessing Right-Click Menu in Event Viewer No Longer Causes Java Error**

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

### **Reports No Longer Stops Generating Multiple Reports When One Report Times Out**

Using the Reports interface, you can schedule multiple reports to generate within the same time frame. All reports that are scheduled to be generated within the same time frame are generated sequentially. Previously, when generating multiple reports and a report in the queue required an extensive amount of time to generate, the report generator timed out. This caused the current report and all subsequent reports in the queue to fail the report generation process. In STRM 2008.2 R2, when generating multiple reports and the time to generate a report exceeds the maximum time limit, the report generator skips the current report and starts to process the next report in the list. Then, a red exclamation mark appears beside the report in the Report interface to indicate that an issue occurred with the generation of the report.

### **The end <time> Option Now Functions Properly When Checking Log Integrity**

The `check_ariel_integrity.sh` command allows you to check the integrity of event and flow logs to determine if the logs have been modified. Previously, if you attempted to use the end <time> option, no results were returned and no errors appeared. This no longer occurs.

### **DSMs Installed Prior to Upgrading Now Appear in User Interface**

Previously, any DSMs that were installed prior to upgrading did not appear in the Sensor Device Type drop-down list box in the STRM interface after the upgrade process was complete. This no longer occurs. Any DSMs that you install prior to upgrading now appear in the STRM interface after the upgrade process is complete.

### **Error No Longer Occurs When Viewing Flows for Application View**

Previously, in the Network Surveillance interface, when using the View Flows function to obtain additional information on the Application view, an error appeared indicating that no data was found. This no longer occurs.

### **Event Graphs In Dashboard No Longer Stop Plotting Data After Performing a Soft Clean SEM**

In the Administration Console, you can clean the SIM model using the Soft Clean option, which closes all offenses in the database. Previously, this action resulted in the event graphs in the Dashboard to stop plotting data. This no longer occurs.

### **Accessing the Right-Click Menu Options in Offense Manager No Longer Causes Error**

Previously, in the Offense Manager, if you attempted to access the menu options available using the right mouse button (right-click), a Java script error may have appeared. This no longer occurs.

### **Reports Now Distributed Properly to Users**

Previously, if an administrative user created a report and configured the report to be distributed to another user, the designated user did not receive the report. No error appeared and no e-mail was received. This no longer occurs and reports are distributed properly.

## **Known Issues and Limitations**

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

- [General](#)
- [Deployment Editor](#)
- [Network Surveillance](#)
- [Dashboard](#)
- [Offense Manager](#)
- [Reports](#)

### **General An auto-discovered EX-Series Ethernet Switch may appear incorrectly as a “Juniper Networks Routing Platform” device.**

*Workaround:* Add the EX-Series Ethernet Switch manually.

### **Objects Menu Tree May Not Appear in Equation Editor After Adding a New Custom View**

If you create a new Custom View and then open the Equation Editor, the menu tree displaying network objects may not appear the first time you attempt to access the menu tree. However, if you choose a new object using the drop-down list box, the menu tree appears.

*Workaround:* Close the Equation Editor window and re-open.

### **Configuring an Asset Profile View of 0 Causes Errors**

In the STRM System Settings, you can configure the Asset Profile View parameter to specify the views you wish the system to use when accumulating asset profile data. By default, the list includes the following views: 1, 2, 15, and 16. If you set a view to 0, an error appears in the log files. Also, if you upgrade to STRM 2008.2, any Asset Profile View set to 0 is automatically changed to a value of 16.

*Workaround:* None.

### **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 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 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.

### **Deployment Editor Able to Configure Scanner Assignments for Last Entered IP Address**

When configuring scanner assignments, you are able to enter multiple IP addresses; however, scanner assignment configurations are applied *only* to the IP address that was entered last.

*Workaround:* Create scanner assignments for one CIDR address at a time.

### **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 interprets the data as one, displaying each component with the same color.

*Workaround:* None

### **Sentry Wizard Sensitivity Slider Is Reading From Lowest To Highest**

When setting the alert sensitivity in the Sentry Wizard, the slider has a reading of 0 to 100. Increasing the slider to a higher number results in a lower sensitivity reading.

*Workaround:* Position the slider to zero to increase the sensitivity rating.

### **Dashboard Time Series Charts Displays 6 Hours as Days**

In the Network Surveillance interface, you can create a view and configure the new view to display data in the Dashboard. However, if you wish to view the data for the

new view for a 6 hour time period in a Time Series chart, the Dashboard displays the 6 hours as a day value.

*Workaround:* Change the Time Series chart to display 8 hours and then back to 6 hours to refresh the Dashboard.

## **Offense Manager    Sorting Columns in Offense Search Results Causes Interface to Display Inaccurate Search Results**

If you search for offense and then sort a column in the search results, the display reverts to a list of offenses that is not valid for the defined search.

*Workaround:* When defining your search parameters, choose your desired sort option from Sort by drop-down list box.

### **An IP Address Previously Identified as a Remote Attacker Can Not Be Created as an Offense When Creating a New Network**

Even if your network hierarchy is not defined, STRM can start generating offenses. However, STRM records all generated offenses as remote offenses since no local systems are defined in your network hierarchy. If this occurs, any IP address that has been previously defined as a remote attacker can not be created as an offense when defining your network.

*Workaround:* You must restart the Event Correlation System (ECS). From the command prompt, type `service ecs restart`. Also, make sure your network hierarchy is defined.

### **Overlapping CIDR(s) in Network Hierarchy Configuration Allows Users to View Assets to Which They Have No Access**

If your network hierarchy configuration includes overlapping CIDR ranges, a STRM non-administrative user is able to view assets for which they have no access. They can view a list of the restricted assets by clicking **Search** or **Show All** in the Asset Profile window of the Offense Manager. However, an error appears if the user attempts the edit the asset or view detailed information.

*Workaround:* None.

### **Viewing a List of Attackers May Display Blank Pages**

The Offense Manager 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.

### **Exported Attacker List to XML or CSV Does Not Include Target Count**

The Offense Manager allows you to export an Attacker list in XML or CSV formats. Currently, the exported list includes a target count of zero.

*Workaround:* None.

**Reports A No Response E-mail May be Received When Attempting to E-mail Generated Report**

When you generate a report and attempt to send a generated report to an e-mail address, the e-mail containing the report is received from the no-reply.report@qradar.com e-mail address instead of the address specified in your system settings.

*Workaround:*

**Step 1** Locate the following files:

- /opt/qradar/conf/templates/reporting.properties
- /opt/qradar/conf/reporting.properties

**Step 2** In the files, change the reporting address.

**From:** reporting.report.from=no\_reply.reporting@qradar.com  
<mailto:reporting.report.from=no\_reply.reporting@qradar.com>

**To:** the address specified in your system settings.

**Step 3** From the STRM Web user interface, do a “Deploy All”.

**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.

Part Number 530-027292-01

530-027292-01