

STRM RELEASE NOTES

RELEASE 2008.1

FEBRUARY 2008

Juniper Networks is pleased to introduce Security Threat Response Manager (STRM) 2008.1. This release provides you with several new features and resolved issues. This document includes:

- [STRM 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](#)
- [Documentation Addendum](#)

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

STRM Overview

Juniper Networks STRM is a network security management platform that provides situational awareness and compliance support to organizations that need to tighten security and improve policy monitoring with a modest investment in time and resources. STRM goes beyond traditional security information/event management (SIEM) products and network behavior analysis (NBA) products to create a command-and-control center that delivers:

- **Threat Management:** STRM detects **threats that would otherwise be missed** by product or operational silos.
- **Log Management:** STRM responds to the **right threats at the right time** through effective analysis of log files.
- **Compliance:** STRM implements a **compliance and reporting safety net** with comprehensive event storage and reporting.

New and Updated Functionality

STRM 2008.1 provides you with the following new and updated functionality:

- **New Flow Viewer Tab** - This new tab allows you to monitor and investigate flow data in real-time and perform advanced searches. The new Flow Viewer tab provides enhanced flow search capabilities including an advanced interface for investigating data for forensic or troubleshooting purposes as well as the ability to display and aggregate flow searches for quick reporting. You can also export flow data in XML or CSV format.
- **Offense Manager Enhancements** - The Offense Manager includes the following enhancements:
 - **Export Views** - You can now export attacker and target views within the Offense Manager to XML or CSV format. This allows you to create a report on data within a list.
 - **New Categories** - You can now view offenses related to two new event categories: VIS Host Discover and SIM Audit.
- **Event Viewer Enhancements** - The Event Viewer interface includes the following enhancements:
 - **Enhanced Searching Capabilities** - You can now search logs and events using simple or complex queries. You can also save your event searches, apply them to quick searches for common tasks, and load saved searches as reports.
 - **Displaying Aggregate Events** - You can view events aggregated (grouped) by various attributes. For example, you can view the top devices by event count or top IP addresses involved in a policy violation. By default, the Event viewer displays normalized events. You can use the Display By option to view raw or aggregated logs and events.
- **Dashboard Enhancements** - The Dashboard interface includes the following enhancements:
 - **Events By Severity Item** - A new Dashboard item that monitors the event distribution by severity. This item allows you to view the number of events being received by the assigned severity.
 - **Top Devices Item** - A new Dashboard item that monitors the top 10 devices that sent events to STRM within the last 15 minutes.
 - **My Offenses Item** - A new Dashboard item that monitors offenses assigned to you.
 - **Most Recent Reports** - A new Dashboard item that displays the top recently generated reports.
 - **Time Selection Options** - For some Dashboard items, you can now select the period of time you wish the Dashboard graph to display.
 - **Chart Type Options** - For some Dashboard items, you can now display the data for several Dashboard items using a Time Series (default), Line Chart, or Pie Chart.

- **Groups** - You can now group your Rules, Reports, and Sensor devices into groups, which enables you to easily locate an item. You can use one of the default groups for associating your items or create your own. Also, you can assign an item to one or multiple groups. Sensor device groupings can be used to quickly search for logs and events from groups of devices or for creating rules for groups of devices.
- **Asset Enhancements** - The Assets interface includes the following enhancements:
 - **New Asset Tab** - The asset functionality has been moved from the Offense Manager tab to the new Asset tab. This new tab provides Asset Profile, Server Discovery, and VA scan functionality.
 - **Exporting Assets** - You can now export asset profiles to XML or CSV format. This allows you to create a report on asset profile data.
- **Syslog Forwarding** - You can now forward received log data to other products. The new Syslog Forwarding function allows you to forward syslog data (raw log data) received from devices as well as STRM normalized event data. You can forward data on a per Event Collector/ Event Processor basis and you can configure multiple forwarding destinations.
- **New QoS View** - The Custom View now includes a Quality of Service (QoS) View, which displays the traffic involved in QoS activities.
- **New FlowShape View** - The Custom View now includes FlowShape view, which displays traffic flow activities. This view replaces the Flow Types View.
- **New Report Template Options** - You can now create detailed reports based on saved flow or event searches. Two new chart types within reports are called Event/Logs and Flows, which allow you to import saved searches for creating customized charts and reports for detailed query based reporting.
- **Authenticating Users** - You can configure authentication to validate STRM users and passwords. Authentication options include: STRM authentication, TACACS, RADIUS, or LDAP/Active directory.
- **Logout** - Using the Logout option in the main STRM interface, you can now logout of STRM
- **Clean SIM Model** - Cleaning the SIM Model allows you to remove all offenses, attackers, and target information from the database. This option is useful after tuning your deployment to avoid receiving any additional false positive information.
- **Backup and Recovery** - Using the Administration Console, you can now backup and recover configuration information and data for STRM. You can schedule regular backups of your configuration information and data or initiate a backup on demand.
- **New Administration Console Access** - In STRM, Java is only required to operate the Deployment Editor. Java is no longer required to operate the STRM Administration Console.

- **Updated VA Configuration** - The interface to configure vulnerability assessment (VA) scanners has been updated to simplify integration with VA products. The new interface allows you to configure your scanner in one window.

**Related
Documentation**

For more information on Release 2008.1, refer to the on-line documentation:

- Hardware Installation Guide
- STRM Administration Guide
- STRM User Guide
- Event Category Correlation Reference Guide
- Category Offense Investigation Guide
- STRM Default Application Configuration Guide
- Configuring DSMs Guide
- Adaptive Log Exporter Users Guide
- Managing Sensor Devices Guide
- Managing Vulnerability Assessment
- AQL Flow and Event Query CLI Guide

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 2008.1 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	No	Yes
Firewall/VPN	6.0	Yes	No
Standalone IDP	4.1	No	Yes
J-series	8.5	Yes	No

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 2008.1:

Deleting a User That Created a Custom Rule No Longer Results in an Error

Previously, if a user created a custom rule and then that user account was deleted, the custom rule did not function as expected and an error may have appeared in the log files. This no longer occurs.

Host and Port Counts in Custom View Object No Longer Includes Total Number of Flows

Previously, if your traffic included Type A (one host sending data to many hosts) or Type B (many hosts sending data to one host) superflows, the Flow Processor returned the number of flows instead of the number of hosts or ports. This no longer occurs.

Moving a Flow Source Between Flow Collectors No Longer Causes The Flow Source to Function on Both Flow Collectors

Using the deployment editor, you can move a flow source from one Flow Collector to another Flow Collector in your deployment. Previously, once you deployed the changes, the Flow Source functioned on both Flow Collectors. As a result, the system required additional memory to run both processes. This no longer occurs.

Scanner Configuration Management Now Deploys Changes When Using the Deploy Configuration Changes Option

Previously, when editing the Scanner Configuration Management in the SIM Configuration interface, changes were not deployed when selecting **Configurations > Deploy configuration changes** from the Administration Console. This no longer occurs.

When Performing A Scan nCircle No Longer Scans All Ports Even Though Only a Specific Number Are Requested

Previously, when you requested the nCircle device to scan ports, it scanned all ports, not only the requested ports. This no longer occurs.

Changes Now Appear When Attempting to Re-Order Threats View List

Previously you re-order the Threats View and refresh the page, the list appeared in the original state. This no longer occurs.

Offense Manager Now Displays Correct Offense Number When Limiting Event Search Time

When you attempt to search events and the time selected is greater than the configured search limit, a message appears indicating that you needed to reduce the search time. Previously, the event number that appeared in the message may have been incorrect. This no longer occurs.

Filtering Real Time Events Based on Source or Destination Network Now Returns Results

Previously, when using the Event Viewer to filter your results based on the source or destination network and you selected **all** from the Source or Destination Network drop-down list boxes, no results were returned. This no longer occurs.

Event Viewer Now Able to Filter Events When Source or Destination Port is 0

When using the search function in the Event Viewer, you can filter your results based on ports. Previously, if you entered 0 as the source or destination port, no search results were returned. This no longer occurs.

University Template No Longer Includes Rules with Loops

Previously, the University template included rules that resulted in loops. This caused a memory leak. This no longer occurs.

Entering a Description for Application View No Longer Generates Error

Previously, if you entered a description for an Application View component and deployed the updates, an error appeared in the log files. This no longer occurs.

Changing Templates Now Deployed to Remote Systems

Previously, if you changed the template used in your deployment (for example, change from Enterprise to University template), the Console enforced the template change. However, the update was not enforced by the remote systems. This no longer occurs.

Non-Standard Characters Now Accepted in Password Parameter in JDBC Protocol Configuration

Previously, when configuring the Password parameter in the JDBC protocol configuration, non-standard characters (for example, #, *, @) were not accepted. Only alphanumeric characters and underscores were accepted. In STRM 2008.1, non-standard characters are accepted.

Editing Asset Profile Name Or Description Now Appears in Interface

Previously, if you edited the name or description of an asset profile, the updates did not appear in the interface after you clicked **Save**. No error message appeared but the changes were enforced in the database. This no longer occurs.

Known Issues and Limitations

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

- [General](#)
- [System Configuration](#)
- [Deployment Editor](#)
- [Network Surveillance](#)
- [Offense Manager](#)
- [Event Viewer](#)
- [Flow Viewer](#)
- [Reports](#)

General STRM System May Be Unusable at Startup

On rare occasions, the STRM appliance may be unusable when it is first booted. If this occurs, restart all system process using the STRM GUI: Config > System > System Restart.

Changing Network Settings Causes System Failure

If you change your network settings (for more information, see the *Changing Network Settings Technical Note*), a failure occurs when you attempt to access the system.

Workaround: Reboot your system. If the system failure continues, contact Customer Support.

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.

During a Restart, An Error May Appear 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. If, during this time, you access the STRM interface, a fatal error message appears. Do not attempt to restart the Tomcat server manually. Once the server restarts, STRM will continue to function as expected.

Workaround: Wait several minutes for the server to restart then access the STRM 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 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.

Continuous Use of STRM Over Extended Period of Time May Cause Interface Failure

If you use a session of the STRM 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. To ensure that the browser application frees its allocated memory if left open for a long duration, configure the inactivity timeout in the Admin Console.

System Configuration

Hostname that Includes Underscores and Special Characters Causes Error

If the hostname of your STRM system includes underscores or special characters (except dashes), the Host Context component fails to start. Once this occurs, QRadar fails to collect data. The log files indicate that the Host Context component is attempting to start every few minutes. Note that dashes are supported in the hostname.

Workaround: Edit or create managed host names without special characters. For information on editing your hostname, see the *Changing Network Settings Technical Note*.

Unable to Deploy License Key Once Current Key Expires

If your license key expires and you upload a new license key, STRM does not provide the option to deploy the new license key.

Workaround: Access the Administration Console using the following link: <https://<IP address of STRM system>/console/do/qradar/adminconsole>. Once the Administration Console appears, select **Configurations > Deploy All** to deploy the new license key.

Unable to Retrieve License Key After Restore Operation

If you create a new license key but do not deploy it, and then you attempt to restore configuration information, the previous license key cannot be found.

Workaround: Browse for the previous key, save it, and then perform the restore operation again.

Changing the Authentication to STRM Authentication Requires Edits to Passwords

If you change your authentication from TACACS, RADIUS, or LDAP/ Active Directory to STRM Authentication, you must configure access for users on the system before they are able to login to STRM. No message appears in STRM stating this requirements.

Workaround: None

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 Administration Guide*, however, before you deploy all changes, wait for the STRM interface to become active. Once the interface is active, follow this procedure:

- Step 1** Log in to STRM, 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
```

Configuring a View of 0 in Systems Settings Asset Profile Views Parameter Results in Error

If you configure a view of 0 in the Asset Profile Views parameter located in the System Setting window, an error appears in the log.

Workaround: None.

Performing an Automatic Update Does Not Deploy All Changes

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

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

Updating License Key When Using Internet Explorer 6 May Cause Error

When you are updating your license key using an Internet Explorer 6 browser, a window may appear stating "The page cannot be displayed" when you click **Save**.

Workaround: Click Back to return to the previous window and click Save again. If the issue continues, upgrade your browser to IE 7.

Unable to Disable an Endace DAG Interface Card Using the Web-Based System Administration Interface

If you use the Network Interfaces window of the Web-based System Administration interface to disable an Endace DAG Interface card, a message appears indicating that the card was successfully disabled. However, the Flow Collector continues to receive flows from the disabled Endace DAG Interface card and if you return to the Network Interface window, the card is set to Monitor.

Workaround: None

Deployment Editor New Administrative User Unable to Access Deployment Editor

A STRM administrative (admin) user can create multiple admin accounts for a STRM system. A administrative user should have unrestricted access to all components of your deployment. Currently, when a new administrative user attempts to access the deployment editor, an error message appears and access is denied.

Workaround: None.

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.

Offense Manager **Deleting a False Positive Building Block Value Causes Error**

If you attempt 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 appears: `Invalid category id`.

Workaround: In the User-BB-FalsePositive: User Defined False Positive Tunings Building Block, remove the `CAT:1:1.1.1.1:2.2.2.2` entry. Once removed, you are able to edit values, as desired.

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.

Event Viewer 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.

Flow Viewer Searching For Source or Destination IP Addresses Using CIDR Value Causes Error

If you use a CIDR value when searching for source or destination IP addresses in the Flow Viewer, the search does not return valid data and error messages appear in the log files.

Workaround: If you wish to search for IP addresses using CIDR values, select the **Any IP equals** search function.

Searching Using Aggregate By Destination Port/Protocol with Network View Format Option Selected Does not Filter on Network

When you search for flows using the Aggregate by Destination Port or Destination Protocol option in the Search Parameters fields and select the Network option in the View Format field, the search results do not filter based on network.

Workaround: If you wish the search results to filter based on network, configure the desired filter in the Tests and Filter fields of the search window.

Reports Multiple Reports May Generate From Single Template When Reports are Shared

When you create 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. If the report is shared with other users, both options may result in the generation of multiple reports appearing in the Generated Reports interface with Admin as the listed owner.

Workaround: None

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.

Reports Assigned to Groups May Display Error When Loading Empty Page

When you create a new report and assign it to a group, extra empty pages may be created. Clicking an empty page produces an error message.

Workaround: None

Documentation Addendum

In STRM 2008.1, the following changes are currently not documented in the STRM documentation set:

- [Flow Viewer and Event View Updates](#)
- [Universal DSM Variables](#)
- [Deploying Changes After Scanner Update](#)

Flow Viewer and Event View Updates

In STRM 2008.1, the following changes have been made to the Flow Viewer and Event Viewer interface and are currently not documented in the STRM documentation set:

- **Link to this page Option** - The Link to this page option has been removed.
- **Display drop-down list box** - The options listed in the Display drop-down list box now include several abbreviated terms. For example, the term source now appears as src and destination is dst.

Universal DSM Variables

The Universal DSM now supports additional variables. The new variables do not appear in the genericDSM.xml file, however, the following normalized event fields are now supported: `Host Name`, `Source Mac Address`, `Destination Mac Address`, `Netbios Name`, `Group Name`, `Severity`, `Device Time`, `Source IP Pre NAT`, `Destination IP Pre NAT`, `Source IP Post NAT`, `Destination IP Post NAT`, `Destination Port Post NAT`, `Destination Port Pre NAT`, `Source Port Pre NAT`, and `Source Port Post NAT`.

Deploying Changes After Scanner Update

If you create, edit, or delete a vulnerability assessment scanner, you must select **Configurations > Deploy Configuration Changes** from the Administration Console menu for the changes to take effect.

For more information on Vulnerability Assessment and scanners, see the *Managing Vulnerability Assessment Guide*.

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.