

STRM RELEASE NOTES

RELEASE 2008.2

JUNE 2008

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

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](#)

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 2008.2 provides you with the following new and updated functionality:

- **Activation and License Key Enhancement** - STRM 2008.2 includes several enhancements to activation and license keys including:
 - **Activation Keys** - During installation of STRM, you must now enter an activation key to complete the installation. This activation key is available on

the license CD. See the instructions that came with the license CD to install the activation key.

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

Related Documentation

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

- Hardware Installation Guide
- STRM Software Installation Guide
- STRM Administration Guide
- STRM Users Guide
- Getting Started with STRM Appliances
- Event Category Correlation Reference Guide
- Category Offense Investigation Guide
- STRM 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](#)
- [SNMP Agent](#)
- [Upgrading to STRM 2008.2](#)

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

Table 1-1 Supported Juniper Networks Devices and OS Versions

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

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

Supported Java and Browser Software

STRM 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:

Changing Network Settings No Longer Causes System Failure

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

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

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

Hostname that Includes Underscores and Special Characters No Longer Causes Error

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

Now Able to Deploy License Key Once Current Key Expires

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

Changing the Authentication to STRM Authentication No Longer Requires Edits to Passwords

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

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

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

New Administrative User Now Able to Access Deployment Editor

An 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. Previously, when a new administrative user attempted to access the deployment editor, an error message appeared and access was denied.

Deleting a False Positive Building Block Value No Longer Causes Error

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

Searching For Source or Destination IP Addresses Using CIDR Value No Longer Causes Error

Previously, if you used a CIDR value when searching for source or destination IP addresses in the Flow Viewer, the search did not return valid data and an error message appeared in the log files. This no longer occurs.

Searching Using Aggregate By Destination Port/Protocol with Network View Format Option Selected Now Filters on Network

Previously, when you searched for flows using the Aggregate by Destination Port or Destination Protocol option in the Search Parameters fields and selected the Network option in the View Format field, the search results did not filter based on network. This no longer occurs.

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

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

Now Able to Add 200 CIDRS for a Network Object

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

Now Able to Apply Any IP Filter When Searching for Flows and Events

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

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

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

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

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

Accessing Right-Click Menu In Offense Manager No Longer Results in Error

Previously, when using the right mouse button (right-click) on an IP address in the Offense Manager, an error message may have appeared. This no longer occurs.

Trusted SSL Key Now Enforced Through Deployment During Upgrade

When upgrading from STRM 2008.1 to STRM 2008.1r2, the trusted SSL key may not have been properly enforced through your deployment. This caused an error indicating that the SSL key was not able to be validated. This no longer occurs when you upgrade from STRM 2008.1 to STRM 2008.2.

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

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

Restoring Configuration Now Create Proper Directory Structure

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

Unioned Flow Details Now Retrieving Correct Flow Information

Using the Display drop-down list box in the Flow Viewer, you are able to view flows using one of the available aggregate options. Previously, when the Flow Viewer encountered several flows that occurred in the same collection interval, which also had the same source and destination information, the incorrect flow details may have been returned when you double-clicked the flow. This no longer occurs.

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

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

Known Issues and Limitations

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

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

General 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.

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.

Upgrade May Fail with Custom SSL Certificate

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

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

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

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

- Step 1** Open the configuration file on the machine that uses the custom SSL key (normally the Web Server console).
- Step 1** Add the directory path to your custom SSL key.
- Step 2** Restart the hostcontext service using the following command:

```
service hostcontext restart
```

Infranet Controller Device Appears as Enterasys Device

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

Workaround: Add the Infranet Controller device manually.

Infranet Controller Device Appears as Secure Access Device

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

Workaround: Add the Infranet Controller device manually.

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 continue to 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.

System Configuration Restoring Configuration Information for Deployment with Encrypted Systems Fails

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

Workaround: Follow the *Restoring Your Configuration* procedure outlined in the *STRM 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/STRM/bin/push_ssh_auth_keys.sh
```
- Step 3** On the Console, enter the following command:

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

```
ssh <IP address/hostname of the Console>
```
- Step 5** For all systems in your deployment, use SSH to connect from the Console to non-Console systems and enter the following command:

```
service hostcontext restart
```

Performing an Automatic Update Does Not Deploy All Changes

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

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

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

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

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

Event Viewer Does not Respond to Searches

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

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

Accessing Right-Click Menu in Event Viewer Causes Java Error

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

Workaround: Enable pop-ups in your web browser.

Unable to Remove Custom Event Mapping

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

Workaround: None.

Flow Viewer Unable to Double-Click on Unioned Flow to Access Additional Information

If you wish to access additional information on a unioned flow in the Flow Viewer, the option to double-click on a flow is disabled.

Workaround: Using the search function in the Flow Viewer, search flows based on the union flows that you wish to isolate by using the right-mouse button (right-click) on the source/ destination IP address, ports, and protocols. Once the details of the flows appears, select the None option from the Display drop-down list box.

Reports Size of Pie Charts in Reports is Dynamic

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

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

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

Part Number 530-025618-01

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

Copyright © 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.