

STRM RELEASE NOTES

RELEASE 2008.3 - REVISION 2

FEBRUARY 2009

Juniper Networks is pleased to introduce STRM 2008.3. This release provides you with several resolved issues and enhanced functionality.

This document includes:

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

New and Updated Functionality

STRM 2008.3 provides you with the following new and updated functionality:

- **Event Viewer and Flow Viewer Enhancements** - The Event Viewer and Flow Viewer provides the following enhancements:
 - **New Right Click Filtering Options** - You can now use the right mouse button (right-click) to access additional event filter information.
 - **Resizable columns** - You can now resize any column by pointing your mouse over the column divider and dragging the column to the desired size. You can also double-click the column divider to automatically resize the column to the width of the largest field.
 - **Improved Flow and Event Viewer Charts** - The Event Viewer and Flow Viewer details window now displays a pie chart in addition to the bar chart. Also, chart colors are enhanced to make the charts more meaningful.
 - **Default Searches** - You can now choose any saved event or flow search to run and display search results in the default view when you launch the Event Viewer or Flow Viewer.
 - **Custom Columns and Groupings** - You can now choose which columns you want to display in saved search results. You can also choose how you want to group the columns.

- **Custom Event Properties** - You can now create Custom Event Properties, which you can use to extract unnormalized data from event payloads. Custom Event Properties allow you to search, view, and report on information within logs that STRM does not typically normalize and display.
- **Reports Enhancements** - The Reports interface provides the following enhancements:
 - **Default report templates** - Provides new default report templates that you can use to create high-level and device-specific reports.
 - **Reports Leverage Event and Flow Searches** - Due to enhancements to the event and flow search functionality, you can now choose which columns you want to display in your reports and define how the column are grouped with the reports.
 - **Time Series Chart Enhancements** - The time series reports provide the following enhancements:
 - Event and Flow Search Data** - Time series charts can derive data from saved event and flow searches.
 - Configurable Axis** - You can now configure the X and Y axis for Event/Logs and Flow report charts.
 - Graph Total** - You can now display the graph value of an object plotted in a chart.
 - New Graphing Options** - Two new graphing options are introduced for time series charts: Line and Stacked Line.
 - **Report Template Generation Status** - When you manually generate a report, you can now view the generation status in the Next Run Time column. The status specifies when the report is generating and, if queued, the position in the queue. The status also specifies the estimated time to generate the report.
- **Dashboard Enhancements** - The Dashboard interface provides the following enhancements:
 - **Search-Based Dashboard Items** - You can now add Dashboard items that are based on saved event and flow searches. After you add an search-based Dashboard item, you can further customize the item by choosing whether the data will be displayed in a bar, table, or pie chart.
 - **Default Dashboard for New Users** - When a new user accesses STRM 2008.3, a default Dashboard is displayed. In earlier versions of STRM, a new user had to built their own Dashboard.
- **User Role Permissions** - The user role functionality provides the following enhancements:
 - **Device Permissions** - If a user role has Event Viewer permissions, Administrators can now specify which devices the user role has access to.
 - **Event Permissions Precedence** - Administrators can now specify which permissions take precedence for all users.

- **Offense Manager Enhancements** - The Offense Manager interface provides the following enhancements:
 - **Rules Contributing to Offenses** - The Offense Summary now displays a list of rules contributing to the offense. From the list, you can access the Rules Wizard to edit a selected rule.
 - **New Offense Property Tests for Custom Rules** - You can configure notifications by creating custom rules that include new offense property tests: **when a new offense has been created** and **when the offense property has increased by at least this percent**. These rule tests can be combined with other tests.
 - **More Information Included in Alerts or Response Notifications** - Additional fields are now included in alerts or response notifications. To support this enhancement, a new SNMP trap ensures that parameters are separate fields within the trap.
 - **On Demand Offense Alert or Response Notification** - In previous releases, the Email option allowed you to configure notification settings. This functionality has been migrated to the custom rule engine. Now, the Email option allows you to immediately send an e-mail containing all displayed information about the offense in text format.
- **Device Parsing Order** - You can now configure the order that you want each Event Collector in your deployment to parse events from external devices, called Device Support Modules (DSMs). Defining the parsing order for DSMs ensures that the required DSMs are parsed in a specific order, regardless of changes to the DSM configuration. This ensures system performance is not affected by changes to DSM configuration by preventing unnecessary parsing.
- **Authorized Services** - You can now configure authorized services in the Administration Console to pre-authenticate a customer support service for your STRM deployment. By authenticating a customer support service, you allow the service to connect to your STRM interface to dismiss or close offenses, and update offense notes. You can add or revoke an authorized service at any time.
- **QID Map Utility** - STRM 2008.3 introduces a new utility to manage the STRM Identifier (QID) map. The QID map provides the association or mapping of an event of an external device to a QID. You can use the QID map utility to create, export, import, or modify user-defined QID map entries.
- **ISP Template** - The ISP template has been removed.
- **IPv6 Management and Monitoring Support** - STRM 2008.3 now supports deployment in both IPv4, IPv6, or mixed environments. IPv4 and IPv6 addressing is supported for network connectivity and management of STRM software and appliances.

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).

Supported Devices and OS Versions

STRM 2008.3 supports platforms from multiple vendors. [Table 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 Supported Juniper Networks Devices and OS Versions

Device Family	OS	Logs Sent Directly to STRM from Device	Logs Sent Through NSM to STRM
ISG-IDP	6.0, 6.1.0r4	No	Yes
FW/VPN	6.0, 6.1.0r4	Yes	Yes
Standalone IDP	4.1R3	Yes	Yes
J-series	8.5, 9.0, 9.1,9.2r1.10	Yes	No
Secure Access (SA)	6.3R1	Yes	No
Infranet Controller (IC)	2.2R3	Yes	No
EX-series	9.1R2.10,9.2	Yes	No
M-Series	9.2	Yes	No

Table 1 Supported Juniper Networks Devices and OS Versions

Device Family	OS	Logs Sent Directly to STRM from Device	Logs Sent Through NSM to STRM
MX-Series	9.2	Yes	No
T-Series	9.2	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 and above.

Resolved Issues

This section describes the resolved issues in STRM 2008.3:

Configuring an Asset Profile View of 0 No Longer 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. Previously, if you set a view to 0, an error would appear in the log files. Also, if you upgraded to STRM 2008.2R1, any Asset Profile View set to 0 was automatically changed to a value of 16.

This no longer occurs. If you set a view to 0 in STRM 2008.3, a message appears to advise you that the asset profile views list contains an invalid view ID.

Offense Manager Now Displays 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.

Exported Flow Data Now Contains Payload

Using the Flow Viewer, you can export flow data in CSV or XML format. If you exported flow data that includes payload information, the exported file did not include the payload information. This no longer occurs.

DoS Rules No Longer Detecting Attacks Without Contributing to the Offense

Previously, DoS rules were generating offenses, but it was not easy to identify which rules were generating the offenses. This no longer occurs. In all templates,

the rules have been modified to create event names that are easier to correlate to the rules that generated them.

Sorting Columns in Offense Search Results No Longer Causes Interface to Display Inaccurate Search Results

Previously, if you searched for an offense and then sorted a column in the search results, the display reverted to a list of offenses that is not valid for the defined search. This no longer occurs.

Tomcat No Longer Requires an Extended Time to Restart When Parsing Report Templates

Previously, a report template parsing problem may have caused the Tomcat server to take an extended period of time to restart.

Network Hierarchy Now Saves Properly

When defining your network hierarchy, you can use the Re-Order button to arrange your network objects. Previously, once saved, the new order reverted to the previous order. This no longer occurs.

Port 0 Now Valid in a Rule or Building Block

Previously, the valid range for port values in rules or building blocks was 1 to 65535. Therefore, port 0 was an invalid port. The valid range for source, destination, local, and report ports in rules or building blocks is now 0 to 65535.

Large Data Backups No Longer Fail

Previously, when a large number of files were included in the data backup process, the backup may have failed. This no longer occurs.

Unknown Traffic Now Mapping Between Network Surveillance and Flow Viewer Interfaces

Previously, when you clicked the **View Flows** button for unknown traffic displayed in the Network Surveillance interface, no flows were displayed. This was because the corresponding data in the Flow Viewer was marked as *other*, while the Network Surveillance interface was looking for *unknown*. This no longer occurs. Now, unknown items are marked as *other* in the Network Surveillance interface.

Backup Archive Now Only Includes Necessary Files

Previously, the backup process included files that did not need to be included in the backup. This resulted in backup archive files that were larger than necessary. This no longer occurs.

STRM User Interface Ceases to Function When Locks Occur in Postgres Database

Previously, if Postgres database locked up, the STRM user interface would cease functioning in a tunneled deployment. This problem no longer occurs, due to the Transaction Sentry. The Transaction Sentry functions by detecting stalled or locked applications. If erroneous processes are found, the Transaction Sentry

returns the process to a usable state. Now, you can configure the Transaction Sentry to resolve erroneous or locked transactions on a tunneled deployment (encrypted host). For more information, see *STRM Administration Guide, Configuring System Settings*.

AQL Now Respecting Search Time Limit

Previously, AQL searches extended for a longer period than configured in the `exec_time <time limit>` parameter. This parameter specifies the maximum period of time, in seconds, a single query may continue processing; however,

Asset Profile History No Longer Searches Over 2000 Results Causing Tomcat Failure

Previously, when you performed an Asset Profile search using the History option, the search would try to return all results in history causing the tomcat server to fail. This no longer occurs. The search will now return only the last 2000 records.

AQL No Longer Requires Root User Login

Previously, you had to log into AQL as root. This no longer applies. You can log into AQL as any user that has access privileges.

DiskMaintd No Longer Generating Unnecessary E-mails

Previously, the nightly cron job (diskmaintd) was generating unnecessary e-mails, based on directory errors. This no longer occurs.

Device Extensions Enhancement Now Displays Proper Time

Previously, enhancement-based extensions (extensions that parse null events from scratch) did not display the correct time in the corresponding event records. This no longer occurs.

Users Can Now Include Shared Searches in Their Quick Search List

Previously, the Include in my Quick Searches feature was not working properly. If the owner of a search selected to share the search with everyone, other users could access and use the search, but could not Include the search in their quick search list. This no longer occurs.

Truncated sFlow Packets Now Generating IP Addresses in the Flow Viewer

Previously, sFlow data appears in the Flow Viewer with a source and destination IP address of 0.0.0.0. The problem occurred with sFlow records with packet headers that are truncated at layer 4. The truncated packet headers result in flows with IP addresses, but no port information. This no longer occurs. The Flow Collector has been modified to capture the IP address, even if the packet is truncated.

NSF Backups No Longer Generating Extra Flow Traffic

Previously, Network File System (NFS) traffic was increasing flow rates on the Flow Collector during the NFS backup. This no longer occurs.

Restore Process Not Checking Version/Patch Level of Backup Files

Previously, restoring a backup to a newer version of STRM was unsuccessful, but no error message appeared. Now when you restore a backup to a newer version of STRM, the version and patch level of the backup files are checked. If the version/patch level is older than the version you are restoring to, a message will appear to indicate that the backup cannot be restored. We recommend that you upgrade to the latest build indicated in the message.

Hostcontext No Longer Fails on Monitored STRM Processes

Previously, hostcontext would suspend monitoring on core component processes that were required to run STRM, such as encrypted connections back to the Console when the Console was unavailable for extended periods of time, or startup errors on processes, such as flow classification. This is no longer the case. Hostcontext no longer stops attempting to restart required processes.

Period character “.” in Network Hierarchy Group Names Now Supported

Previously, problems were encountered when adding a group that contained the period character “.” in the Network Hierarchy. This no longer occurs and periods are supported.

Special Characters Now Permitted in Passwords For Checkpoint Firewall

Previously, if an operation security (OPSEC) password for a CheckPoint Firewall certificate had a special character, such as "|", the characters after the special character were interpreted as a command, which caused the certificate to fail. This no longer occurs.

JDBC Siteprotector Drop Down List Box Option No Longer Causes an Error

Previously, an error occurred when selecting the JDBC:SiteProtector option from the Protocol drop down-list box when configuring protocols. This no longer occurs.

Offense rules Now Sending E-mail and Syslog Notifications Correctly

Previously, offense rules with notification set to email or syslog did not work properly. The offense rule did not generate e-mails or syslog entries. 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](#)
- [Offense Manager](#)
- [Event Viewer](#)
- [Flow Viewer](#)

- [Reports](#)
- [Asset Manager](#)

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 then re-open it.

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.

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. There are no warnings or errors resulting from this issue.

Workaround: None

Restored System That Includes Scanner May Cause Tomcat Server Failure

If you restore a system that includes scanners or DSMs installed as plug-ins, the Tomcat server may fail to restart.

Workaround: Before restoring STRM, re-install any DSM or scanner plug-ins. For more information on scanners and DSMs, see the Juniper Customer Support web site.

Potential File System Corruption After a Power Outage or Hard Reboot

After a power outage or hard reboot of a STRM appliance, the file system could potentially be corrupted.

Workaround: Use Uninterrupted Power Supply (UPS) on all STRM appliances and avoid hard reboots.

Time Setting on Quick Searches Incorrect

The incorrect time shows on a quick search if you saved the search with the **Include with time** and **Include in quick searches** options selected. This only

occurs when you save the search directly from the results screen, and not from Saved Searches screen.

Workaround: If you want to configure a search as a quick search and include with time, click **Saved Searches** and configure the necessary parameters.

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 gets 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.

New Reporting structure

This is only available on Fresh install of 2008.3.

Recovery partition

This is only available on Fresh Install of 2008.3. Refer to "Add-Recovery-ReinstallingSTRM" for recovery partition on devices upgraded from 2008.2r2 to 2008.3.

Juniper Networks Net-Screen Security Manager(NSM) is renamed as JuniperNetworks Network & Security Manager(NSM). STRM still uses the old naming convention for NSM.

Workaround: None.

Often, the event viewer gives an error message as "There is a problem connecting to the query server, please try again later".

Workaround: Multiple refreshes or select another search pattern for the Events.

Custom Event properties

This is only available on Fresh Install of 2008.3.

System Configuration

Installation With a Potentially Corrupt Zip File

When you deploy configuration changes in STRM, 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 STRM Administration Console, select **Configurations > Deploy All**.

Error Appears in Log File If Deployments Includes RPM Installed Scanners and DSMs Prior to Upgrade

If your deployment includes DSMs or scanners installed using an .rpm file, the following error appears in the log files after you upgrade your system to STRM 2008.3:

```
ErrorStream ExecuteAutoUpdate-Deploy: Can't load '/opt/strm/
perl5libs/lib/site_perl/5.6.1/i686-linux-thread-multi/auto/XML/
Parser/Expat/Expat.so' for module XML::Parser::Expat: /opt/
strm/perl5libs/lib/site_perl/5.6.1/i686-linux-thread-multi/auto
/XML/Parser/Expat/Expat.so: wrong ELF class: ELFCLASS32 at
/usr/lib64/perl5/5.8.8/x86_64-linux-thread-multi/DynaLoader.pm
line 230
```

This error does not affect the upgrade process or system functionality and can be ignored.

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 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.

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 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

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.

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.

Search for (SrcIP = x or SrcIP = Y) and (DstIP = x or DstIP = y) Returns Too Many Results

If you perform a search with the parameters (SrcIP = x or SrcIP = Y) and (DstIP = x or DstIP = y), invalid results are returned. This search should look for all traffic between the specified source IP address and destination IP address, but it returns results for all traffic for either IP address.

Workaround: None

Reports Reports Based on Specific Flow Columns and Groupings Stops Collecting Data After Upgrade

Due to improvements made in STRM 2008.3 to support customizable column definitions, reports collecting data based on flow-based searches involving the following flow columns and groupings, will stop collecting data:

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

To begin collecting data for these reports again, you will need to create a new report using the previously saved flow search.

Workaround: None

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

The Server Discovery function does not save approvals when the 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.

Upgrade Considerations

Before you upgrade to 2008.3 version of STRM, make sure you are running 2008.2r2 version. If you are running versions earlier than 2008.2r2, first upgrade to 2008.2r2 before upgrading to 2008.3 version. STRM can be upgraded to 2008.3 version only from 2008.2r2 version.

Documentation Addendum

This section includes documentation updates including:

- [Free Space Requirement for Upgrades](#)
- [Flow Viewer Parameters](#)
- [Resizing Columns](#)
- [System Summary Permissions](#)
- [Default Building Blocks](#)
- [Updating Your Host Set-up](#)
- [Integration of New QIDs into QID Map](#)
- [Accessing STRM Using Mozilla Firefox 3.0](#)

Free Space Requirement for Upgrades

The STRM 2008.3 upgrade requires a minimum of 2 GB of free disk space. The upgrade process validates actual disk space required for your STRM configuration and determines if enough disk space is available. If your system does not have enough free disk space, the upgrade process stops and a message appears warning you that additional disk space is required to perform the upgrade.

Flow Viewer Parameters

The following parameters have been added to the Flow Viewer Parameters table in the *STRM Users Guide - Using the Flow Viewer* chapter:

Table 2 Flow Viewer Parameters

Parameter	Description
Bytes In	Specifies the number of bytes sent to the local network.
Bytes Out	Specifies the number of bytes sent from the local network.

Table 2 Flow Viewer Parameters (continued)

Packets In	Specifies the number of packets sent to the local network.
Packets Out	Specifies the number of packets sent from the local network.

The following parameter has been modified in the Flow Viewer Parameters table in the *STRM Users Guide - Using the Flow Viewer* chapter:

Table 3 Flow Viewer Parameters

Parameter	Description
ICMP Type	Specifies the ICMP type and code, if applicable. If the flow has ICMP type and code information that is not in a known format, the field displays as Type <A>, Code , where A and B are the numeric values of the type and code.

The ICMP Code column has been removed from the Flow Viewer Parameters table.

Resizing Columns

The *STRM Users Guide* details how to resize the columns of the Flow Viewer and Event Viewer display. You can also resize columns by double-clicking the line that separates the columns to automatically resize the column to the width of the largest field.

System Summary Permissions

The following row was modified in Flow Viewer Parameters table in

Table 4 Flow Viewer Parameters

Dashboard Item	Role
System Summary	<ul style="list-style-type: none"> All Networks At least one of the following: <ul style="list-style-type: none"> Network Surveillance Event Viewer Offense Management <p>Note: The user must also have permission to view all networks in the deployment.</p>

Default Building Blocks

The following default building blocks have been added to the Enterprise Template:

Table 5 Default Building Blocks

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
Default-BB-Category Definition: Post DMZ Jump	Category Definitions	Event	Edit this BB to define actions that may be seen within a Remote-to-Local (R2L) and a DMZ host jumping scenario.	
Default-BB-Category Definition: Pre DMZ Jump	Category Definitions	Event	Edit this BB to define actions that may be seen within a Local-to-Local (L2L) and a DMZ host jumping scenario.	

Table 5 Default Building Blocks (continued)

Building Block	Group	Block Type	Description	Associated Building Blocks, if applicable
Default-BB-Category Definition: Pre Reverse DMZ Jump	Category Definitions	Event	Edit this BB to define actions that may be seen within a Pre DMZ jump followed by a reverse DMZ jump.	
Default-BB-Category Definition: Reverse DMZ Jump	Category Definitions	Event	Edit this BB to define actions that may be seen within a Remote-to-Local (R2L) and a DMZ host reverse jumping scenario.	

Updating Your Host Set-up

The Console Information and Web Address settings have been removed from the STRM Setup window in the Web Based System Administration interface. The following procedure was modified in the *STRM Administration Guide - Configuring Access Settings* chapter:

To configure your host set-up:

- Step 1** In the Administration Console, click the **System Configuration** tab.
The System Configuration panel appears.
- Step 2** Click the **System Management** icon.
The System Management window appears.
- Step 3** For the host you want to update your host set-up, click **Manage System**.
- Step 4** 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 5** From the menu, select **Managed Host Config > STRM Setup**.

The STRM Setup window appears.

STRM Setup

Enter the address of the mail server STRM should use.

Mail server:

Global STRM Configuration Password

Enter the global configuration password:

Confirm the global configuration password:

Step 6 In the **Mail Server** field, specify the address for the mail server you want STRM to use. STRM uses this mail server to distribute alerts and event messages. To use the mail server provided with STRM, enter **localhost**.

Step 7 In the **Enter the global configuration password**, enter the password you want to use to access the host. Confirm the entered password.



Note: *The global configuration password must be the same throughout your deployment. If you edit this password, you must also edit the global configuration password on all systems in your deployment.*

Step 8 Click **Apply Configuration**.

Integration of New QIDs into QID Map

To ensure that rules and searches continue to function after an upgrade to STRM 2008.3 or applying the QID map flattening patch on 6.1.x systems, new QIDs will be implemented and the old QIDs will be maintained temporarily.

Note the following:

- Event mappings will be updated automatically to point to the new QIDs.
- Custom rules will be updated automatically to point to the new QIDs.
- Pre-upgrade/patch saved searches will work as normal.
- When you create a search that requires you to choose Event Names or QIDs, the Event Browser window will appear. By default, the Event Browser displays only new QIDs. However, you will have the option to show OLD QIDs. When creating new saved searches that include searching for:
 - Events that span pre- and post-upgrade/patch, use both the old QID and new QID.
 - Events from before the upgrade/patch, use the old QID.
 - Events from after the upgrade/patch, use the new QID.
- The option to show old QIDs will be removed automatically after the Device Log Data Retention Period parameter setting in the System Settings has elapsed. For more information, see the *STRM Administration Guide*.

When using saved search results that span a time period that includes both pre- and post-upgrade/patch data, filtering on event name in the Event Viewer may not seem to filter correctly because the results table will show both the old QIDs and the new QIDs.

Accessing STRM Using Mozilla Firefox 3.0

To access STRM using Mozilla Firefox 3.0, you must add an exception to Mozilla Firefox. To add an exception:

Step 1 Open your Mozilla Firefox 3.0 browser.

Step 2 In the address bar, enter the IP address of your STRM system:

`https://<IP Address>`

Where **<IP Address>** is the IP address of the STRM system.

The Secure Connection Failed window appears.

Step 3 Click **Add Exception**.

The Add Security Exception window appears.

Step 4 Click **Get Certificate**.

The Certificate Status information appears.

Step 5 Click **Confirm Security Exception**.

The STRM login window appears. The default values are:

Username: **admin**

Password: **<root password>**

Where **<root password>** is the password assigned to STRM during the installation process.

Step 6 Click **Login To STRM**.

For your STRM Console, a default license key provides you access to STRM for five weeks. For more information about the license key, see the *STRM Administration Guide*.

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 530-028582-01