

UPGRADING TO STRM LOG MANAGER 2009.1

RELEASE 2009.1

OCTOBER 2009

This document provides information for upgrading to STRM Log Manager 2009.1 including:

- [Pretesting Your System](#)
- [Before You Begin](#)
- [Upgrading to STRM Log Manager 2009.1](#)
- [Clearing the Cache](#)

You must upgrade the systems in your deployment in the following order:

- 1 Console



Caution: You must complete the upgrade process on your STRM Log Manager Console first and you must be able to access the STRM Log Manager user interface on your desktop system before upgrading other systems in your deployment.

- 2 Remote Event Processors
- 3 Remote Event Collectors

Pretesting Your System

Before you upgrade to STRM Log Manager 2009.1, you must perform a pretest on all systems in your deployment to ensure that your system meets all system requirements for the upgrade. We recommend that you schedule the pretest during non-peak hours.

To pretest your system:

Step 1 Log in as root.

Step 2 Create the **/store/iso** folder:

```
mkdir /store/iso
```

Step 3 Go to the Juniper Customer Support web site to access the STRM Log Manager 2009.1 download:

```
http://www.juniper.net/support
```

Step 4 Copy the file to the **/store/iso** folder on your system.

Step 5 Mount the ISO:

```
mount -o loop /store/iso/<ISO name> /media/cdrom
```

Caution: Make sure there are no CDs in the disk drive before you proceed.

Step 6 Perform the pretest:

```
/media/cdrom/setup -t
```



Caution: When pretesting your system, you will be prompted to run *PRETESTDOWN* script after the initial *PRETEST* script is complete. The *PRETESTDOWN* script requires all services to be stopped, which results in a data outage. The *PRETESTDOWN* script requires all services to be stopped to test the integrity of the database. The prompt resembles the following:

```
Completed all PRETEST scripts successfully.
***** WARNING *****
About to run PRETESTDOWN scripts which will cause tomcat and
hostcontext services to be stopped and cause a data outage.
These test scripts will be run:
check_db_upgrade.sh
check_permissions.sh
***** WARNING *****
Proceed (Y/[N]) (default to N after 55 seconds)? y
Are you absolutely sure? THERE WILL BE A DATA OUTAGE!
Proceed (Y/[N]) (default to N after 55 seconds)?
```

The output of the pretest determines if your system meets the upgrade system requirements, such as:

- Memory requirements
- Partitioning
- Log source limits
- Licensing
- Out of memory notifications
- Disk sentry notifications
- Invalid passwords
- Failed logins
- PostgreSQL issues
- Table constraint/key issues

If the pretest indicates a problem, contact Customer Support.

Before You Begin

Before you upgrade to STRM Log Manager 2009.1, note the following:

- To upgrade to STRM Log Manager 2009.1, you must be running STRM Log Manager 2008.3. If you are not running STRM Log Manager 2008.3, download and install STRM Log Manager 2008.3 from the Juniper Customer Support web site. In the STRM Log Manager user interface, click **Help > About** to view version information.
- The upgrade process validates actual disk space required for your STRM Log Manager 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.
- Close all open STRM Log Manager sessions to avoid access errors in your log file.
- If your system includes a log source (formally sensor device) that uses the JDBC:SiteProtector protocol and you upgrade to STRM Log Manager 2009.1, the JDBC:SiteProtector protocol configuration is no longer available or editable in STRM Log Manager 2009.1. This log source will function normally but you must create a new log source if you wish to edit the log source protocol.
- Make sure that you have Java Runtime Environment installed on your desktop system, not the STRM Log Manager appliance. You can download Java version 1.6.0_13 x86 at the following web site: <http://javasun.com/>
- STRM Log Manager 2009.1 adds new rules and report templates for fresh installations only. The upgrade process does not apply the new rules and report templates to your system. The upgrade process maintains your existing rules and template. After the upgrade process is complete, you can set your rules and report templates by running the `template_setup.pl` script.



Caution: Running the `template_setup.pl` script will delete your customizations.

**Upgrading to STRM
Log Manager
2009.1**

To upgrade to STRM Log Manager 2009.1:



Note: Before you begin the upgrade process, make sure you review the [Before You Begin](#) section. This section outlines requirements that must be satisfied before you begin the upgrade process.

Step 1 Log in as root.

Step 2 Create the `/store/iso` folder:

```
mkdir /store/iso
```

Step 3 Go to the Juniper Customer Support web site to access the STRM Log Manager 2009.1 download:

```
http://www.juniper.net/support/
```

Step 4 Copy the file to the `/store/iso` folder on your system.

Step 5 Mount the ISO:

```
mount -o loop /store/iso/<ISO name> /media/cdrom
```

Step 6 Enter the following command:

```
/media/cdrom/setup
```

The End User License Agreement (EULA) appears.

Step 7 Read the information in the window. Press the Spacebar to advance each window until you have reached the end of the document. Type **yes** to accept the agreement, and then press Enter.

The following prompts appears:

```
About to upgrade your STRM Log Manager from 2008.3-<build> to 2009.1-<build>.
Continue (Y/[N])?
```

Step 8 To continue, enter **y**.

After several minutes, the upgrade pauses and the following message appears:

```
OK: Completed preparation of system.
```

Step 9 Press **Enter** to reboot and proceed with the upgrade.

Your system reboots and the upgrade continues. After a few minutes, log in to your STRM system to verify the upgrade process is complete. To verify the setup process, enter the following command:

```
tail -f /var/log/setup-6.2.0.*/qradar_qsetup.log
```

Wait for the following message to indicate that the upgrade process is complete:

```
OK: Upgraded STRM
```

Clearing the Cache

If you have trouble accessing the STRM Log Manager interface after you upgrade to STRM Log Manager 2009.1, we recommend that you clear your Java cache.

To clear your cache and access the STRM Log Manager interface:



Note: Make sure that you have Java Runtime Environment installed on your desktop system, not the STRM Log Manager appliance. You can download Java version 1.6.0_13 x86 at the following web site: <http://jasun.com/>.

Step 1 Clear your Java cache:

a On your desktop, select **Start > Run**.

The Run window appears.

b In the Open field, enter **javaws - viewer**.

The Java Cache Viewer appears.

c Select all STRM Log Manager Deployment Editor entries.

d Click the delete  icon.

Step 2 Open your web browser.

Step 3 Clear the cache of your web browser:



Note: Before you clear the cache, make sure you only have one instance of your browser open. If you have multiple versions of your browser open, the cache fails to clear.

- a If you are using Internet Explorer 7.0, select **Tools > Internet Options > General > Delete > Delete Files.**
- b If you are using Mozilla Firefox, select **Tools > Options > Advanced > Network > Clear Now.**



Note: If you are using Mozilla Firefox, you **must** clear the cache in Internet Explorer as well as in Mozilla Firefox.

Step 4 Log in to STRM Log Manager.

For more information on accessing and using STRM Log Manager, see the *STRM Log Manager Users Guide* or *STRM Log Manager 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.

Published: 2009-10-12