



Security Threat Response Manager

Getting Started with STRM Log Management Appliances

Release 2008.2

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

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.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense. The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: Reorient or relocate the receiving antenna. Increase the separation between the equipment and receiver. Consult the dealer or an experienced radio/TV technician for help. Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

Getting Started With STRM Log Management Appliances
Release 2008.2

Copyright © 2008, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Revision History

June 2008—Revision 1

The information in this document is current as of the date listed in the revision history.

CONTENTS

Before You Begin 1

STRM Log Management Appliance Installation and Configuration 3

Before You Begin

Before performing these procedures, you must have access to the following:

- **Hardware Requirements** — You must have access to a hard drive, monitor, keyboard, and mouse to log in to the application.
- **Java Requirements** — You must install Java version 1.5.0_12. For more information see <http://java.com/>.
- **Browser Requirements** — You must have Internet Explorer 6.0/7.0 or Firefox 2.0.



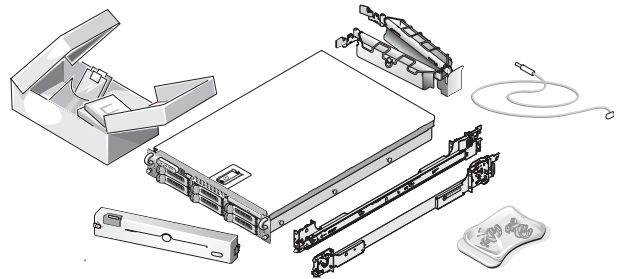
Warning: *Before performing these procedures, see the safety instructions and important regulatory information in your QRadar SLIM Installation Guide and the Hardware Installation Guide.*



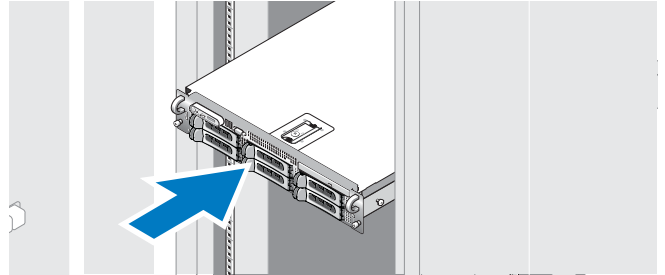
Note: *When using a laptop to connect to the appliance you must use a terminal program, such as HyperTerminal, to connect to the appliance. Be sure to set **Connect Using** to the appropriate COM port of the serial connector and **Bits per second** to 9600. You must also set **Stop Bits** (1), **Data bits** (8), and **Parity** (None).*

STRM Log Management Appliance Installation and Configuration

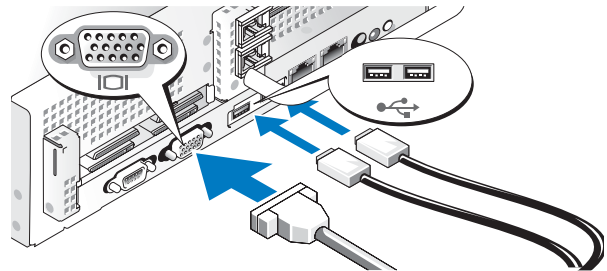
1 **Unpack Your Appliance**
Save all shipping materials in case you need them later. (Your appliance may not include all accessories shown.)



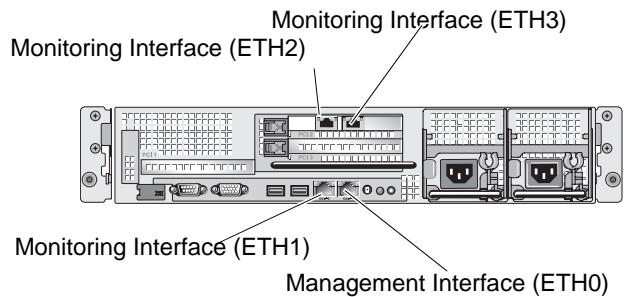
2 **Install the Appliance in a Rack**
See the *Hardware Installation Guide* for instructions on installing your appliance in a rack.



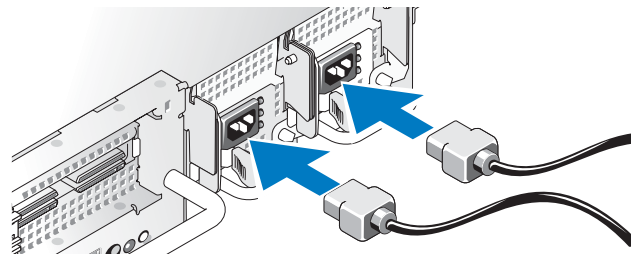
3 **Connect to External Devices**
Connect external devices using the ports on the rear of the appliance. If you are using a monitor with a keyboard, tighten the screws on the monitor's cable connector. You must use a USB keyboard or a PS2 to USB adapter. If you use a laptop, connect the laptop to the serial connector on the rear of the appliance.



4 **Connect to the Network**
Connect the appliance to your network using the ports on the rear of the appliance. The Management Interface is the communications port for your appliance; the Monitoring Interfaces allow you to connect to span ports or taps.
If you wish to connect to a tap, see your tap vendor documentation.

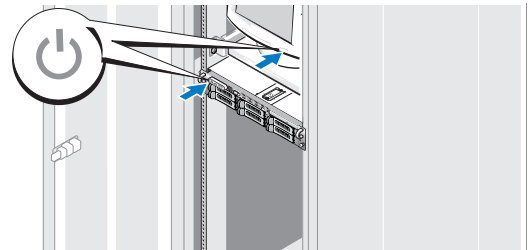


5 **Connect to Power Source**
Connect the power cable(s) to the appliance. Next, plug the other end of the cable into a grounded outlet on a separate power source, such as an Uninterruptible Power Supply (UPS) or a Power Distribution Unit (PDU). Connect the monitor's (or laptop) power cable to a grounded electrical outlet.



- 6 Turn on the Appliance**
Press the power button on the appliance and the monitor or laptop. The power indicators should light. Install the bezel after turning on the appliance.

When the prompt appears, you are ready to log in.



- 7 Log in as Root**
Using the keyboard with monitor or laptop, log in using the default username and password.

Note: Username and password are case sensitive.

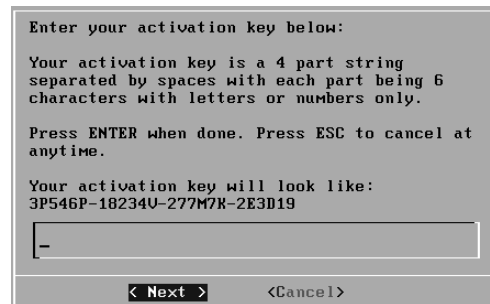
Username: `root`

Password: `password`

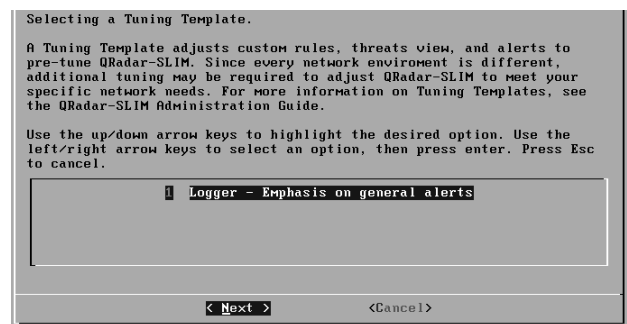
Press **Enter**. The End User Licensing Agreement window appears.

- 8 Read the End User Licensing Agreement**
Read the End User Licensing Agreement (EULA) information. Press the **Spacebar** to advance to each window until you have reached the end of the document. Type **yes** to accept the agreement. Press **Enter**. The Activation Key window appears.

- 9 Enter Your Activation Key**
The activation key is a 24-digit four-part (separated by hyphens) alphanumeric string that you receive from Juniper Networks. Press **Next**. The Tuning Template window appears.



- 10 Select a Tuning Template**
Using the left/right arrow keys, select **Next**. Press **Enter**. The Set the Date and Time window appears. For more information on templates, see the *STRM Log Management Administration Guide*.



- 11 Choose How to Set Date and Time**
Using the up/down arrow keys, select the method you wish to use to set the date and time.

- **Manual** - Allows you to manually input the date and time. Press the spacebar to select and then press **Enter** to select **Next**. Go to Step 12.
- **Server** - Allows you to specify your time server. Press the spacebar to select and then press **Enter** to select **Next**. Go to Step 13.



12 Enter the Date and Time

Enter the current date and time. Using the left/right arrow keys, select **Next**. Press **Enter**. The Time Zone window appears.

Go to Step 14.

Select the current date and time

Enter the date, as specified, then use the down arrow key to go to the next section. Enter the time, as specified then press enter. Use the Tab key and then the left/right arrow key to select Next, Back, or Cancel, then press Enter. Press ESC to cancel at anytime.

Current Date (YYYY/MM/DD): 2006/02/10

24h Clock Time (HH:MM:SS):

< Next > < Back > <Cancel>

13 Enter Time Server Name

In the text field, enter the time server name or IP address. Using the left/right arrow keys, select **Next**. Press **Enter**. The Time Zone Continent window appears.

Enter Time Server name or IP address.

Use the Tab key and then the left/right arrow keys to select Next, Back or Cancel, then press Enter. Press ESC to cancel at anytime.

Time server:

< Next > < Back > <Cancel>

14 Configure Time Zone

a Using the up/down arrow keys, or the page up/page down keys, select your time zone continent or area.

Using the left/right arrow keys, select **Next**, then press **Enter**. The Time Zone Region window appears.

Select a time zone continent/area to filter your choice of time zone cities/regions.

Use the up/down arrow or the PgUp/PgDn keys to select a continent. Use the left/right arrow keys to select a navigation option and press Enter. Press ESC to cancel at anytime.

1	America
2	Antarctica
3	Arctic
4	Asia
5	Atlantic
6	Australia
7	Europe
8	GMT

< Next > < Back > <Cancel>

b The options appearing in this window are regions associated with the continent or area previously selected.

Using the up/down arrow keys, or the page up/page down keys, select your time zone region. Using the left/right arrow keys, select **Next**. Press **Enter**. The Configure STRM Log Management window appears.

Select a time zone city or region.

Use the up/down arrow or the PgUp/PgDn keys to select a continent. Use the left/right arrow keys to select a navigation option and press Enter. Press ESC to cancel at anytime.

0	Adak (Aleutian Islands)
1	Anchorage (Alaska Time)
2	Anguilla
3	Antigua
4	Araguaina (Tocantins)
5	Argentina/Buenos Aires (Buenos Aires (BA, CF))
6	Argentina/Catamarca (Catamarca (CT), Chubut (CH))
7	Argentina/Cordoba (most locations (CB, CC, CN, ER, FM, LP, MN, NQ))
8	Argentina/Jujuy (Jujuy (JY))

< Next > < Back > <Cancel>

15 Configure STRM Log Management Settings

Using the up/down arrow keys to navigate the fields, update the following parameters:

- **Hostname** - Domain name as hostname.
- **IP Address** - IP address of the appliance.
- **Netmask** - Network mask address.
- **Gateway** - Default gateway.
- **Primary DNS** - Primary DNS server.
- **Secondary DNS*** - Secondary DNS server.
- **Public IP*** - Public IP address of the server.
- **E-mail Server** - E-mail server. If you do not have an e-mail server, enter **localhost**.

** All fields are mandatory with the exception of the **Secondary DNS** and **Public IP**.*

Press **Tab** and then use the left/right arrow keys, select **Next**. Press **Enter**. The New Root Password window appears.

Use the up/down arrows to navigate between fields. Use the Tab key and then the left/right arrow keys to select Next, Back or Cancel, then press Enter. Press ESC to cancel at anytime.

Hostname:	qgradar.q1labs.inc		
IP Address:		Primary DNS:	
Network Mask:		Secondary DNS:	
Gateway:		Public IP:	
Email server:			

< Next > < Back > <Cancel>

16 Configure Passwords

a Enter your root password. Use the TAB key to navigate to the Next option. Press **Enter**. The Confirm Password window appears.

b Re-enter your password to confirm. Use the TAB key to navigate to the Finish option and press **Enter**. When STRM Log Management completes the installation process, the Configuration is Complete window appears.

Enter New Root Password.

Enter the password and press enter. To leave the password unchanged, do not enter a value in the box. Use the Tab key and then the left/right arrow keys to select Next, Back or Cancel, then press Enter. Press ESC to cancel at anytime.

New Root Password:

—

< Next > < Back > <Cancel>

Confirm New Root Password.

Re-enter the password and press enter. Use the Tab key and then the left/right arrow keys to select Next, Back or Cancel, then press Enter. Press ESC to cancel at anytime.

New Root Password (confirmation):

—

< Finish > < Back > <Cancel>

17 Finish Installation

Press **Enter** to select OK. Type **exit** and press **Enter**.

Initial configuration of QRadar is now complete.

You are now ready to connect to the QRadar interface.

< OK >

18

Access STRM Log Management

a Open your web browser.

b Log in to STRM Log Management:

https://<IP Address>

Where <IP Address> is the IP address of the STRM Log Management Console. The default values are:

Username: **admin**

Password: <your root password>

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

c Click **OK**.

The STRM Log Management interface appears. You are now ready to start tuning STRM Log Management. For more information, see the *STRM Log Management Administration Guide*.

