



**Security Threat Response Manager**

# **STRM Installation Guide**

***Release 2009.1***

**Juniper Networks, Inc.**

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

**[www.juniper.net](http://www.juniper.net)**

Published: 2009-10-12

## 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.

*Configuring DSMs*  
Release 2009.1

Copyright © 2008, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Revision History

October 2009—Revision 1

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

# CONTENTS

---

## ABOUT THIS GUIDE

Conventions	1
Technical Documentation	1
Contacting Customer Support	2

---

## 1 PREPARING FOR YOUR INSTALLATION

Deploying STRM Log Manager	3
Additional Hardware Requirements	4
Additional Software Requirements	4
Browser Support	4
Preparing Your Network Hierarchy	5
Identifying Network Settings	5
Identifying Security Monitoring Devices	6

---

## 2 INSTALLING STRM LOG MANAGER

Setting Up Appliances	9
Accessing STRM Log Manager	14

---

## A CHANGING NETWORK SETTINGS

Changing Network Settings in an All-in-One Console	19
Changing the Network Settings of a Console in a Multi-System Deployment	20
Changing the Network Settings of a Non-Console in a Multi-System Deployment	23

---

## INDEX



# ABOUT THIS GUIDE




The *STRM Log Manager Installation Guide* provides you with information on setting up STRM Log Manager. This guide assumes a working knowledge of networking and Linux systems.

---

## Conventions

The following table lists conventions that are used throughout this guide.

**Table 1** Icons

Icon	Type	Description
	Information note	Information that describes important features or instructions.
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, device, or network.
	Warning	Information that alerts you to potential personal injury.

---

## 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](mailto: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).

# 1

## PREPARING FOR YOUR INSTALLATION

This chapter provides information for when planning your STRM Log Manager deployment including:

- [Deploying STRM Log Manager](#)
- [Additional Hardware Requirements](#)
- [Additional Software Requirements](#)
- [Browser Support](#)
- [Preparing Your Network Hierarchy](#)
- [Identifying Network Settings](#)
- [Identifying Security Monitoring Devices](#)

Your STRM Log Manager deployment may consist of STRM Log Manager installed on one or multiple systems. You can also connect one or multiple STRMLM EP systems to your STRM Log Manager system. For more information on appliances, see the *Hardware Installation Guide*.

To ensure a successful STRM Log Manager deployment, adhere to the recommendations in this document.

---

### Deploying STRM Log Manager

You can deploy STRM Log Manager using appliances or STRM Log Manager software installed on your own hardware. A STRM Log Manager appliance includes STRM Log Manager software and a CentOS-5.2 operating system. For further information on STRM appliances, see the *Hardware Installation Guide*.

STRM Log Manager components that may exist in your deployment include:

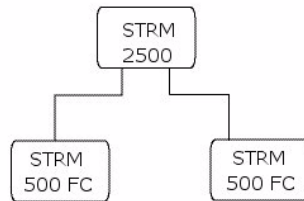


**Note:** For more information on each STRM Log Manager component, see the *STRM Log Manager Administration Guide*.

- **Console** - Provides the interface for STRM Log Manager. The Console is accessed from a standard web browser. When you access the system, a prompt appears for a user name and password, which you configure during the installation process. You must also have Java installed. For information on software requirements, see [Additional Software Requirements](#).

- **Event Collector** - The Event Collector gathers events from local and remote device sources. The Event Collector normalizes events and sends the information to the Event Processor. Before being sent to the Event Processor, the Event Collector bundles identical events to conserve system usage.
- **Event Processor** - Processes events collected from one or more Event Collector. Once received, the Event Processor correlates the information from STRM Log Manager and distributes the information to the appropriate area, depending on the type of event. Rules are applied to the events that allow the Event Processor to process according to configured rules.

The following figure shows an example of a small deployment using STRM Log Manager.




---

**Additional Hardware Requirements**

Before installing your STRM Log Manager systems, make sure you have access to the additional hardware components:

- Monitor and keyboard or a serial console
- Uninterrupted Power Supply (UPS)



**Note:** To make sure that your STRM Log Manager data is preserved during a power failure, we highly recommend that all STRM Log Manager appliances or systems running STRM Log Manager software that store data, such as, Consoles or Event Processors be equipped with a Uninterrupted Power Supply (UPS).

---

**Additional Software Requirements**

Before installing STRM Log Manager, make sure you have Java Runtime Environment installed on your system. You can download Java version 1.5.0\_15 at the following web site: <http://java.com/>

---

**Browser Support**

You must have a browser installed on your client system to access the STRM Log Manager interface. STRM Log Manager supports the following web browsers:

- Microsoft Internet Explorer 6.0/7.0
- Firefox 3.0

**Preparing Your Network Hierarchy**

STRM Log Manager uses the network hierarchy to understand your network traffic and provide you with the ability to view network activity for your entire deployment. STRM Log Manager supports any network hierarchy that can be defined by a range of IP addresses. You can create your network based on many different variables, including geographical or business units. For example, your network hierarchy may include corporate IP address ranges (internal or external), physical departments or areas, mails servers, and web servers.

After you define the STRM Log Manager components you want to add to your network hierarchy and install STRM Log Manager, you can then configure the network hierarchy using the STRM Log Manager Console. For each STRM Log Manager component you want to add to your network hierarchy, use the following table as a job aid to indicate each network component (object) in your network map.

**Table 1-1** Network Hierarchy

Description	Name	IP/CIDR Value	Weight

At a minimum, we recommend that you define objects in the network hierarchy for:

- Internal/external Demilitarized zone (DMZ)
- Virtual Private Network (VPN)
- All internal IP address space (for example, 0.0.0.0/8)
- Proxy servers
- Network Address Translation (NAT) IP address range
- Server Network subnets
- Voice over IP (VoIP) subnets

For more information, see the *STRM Log Manager Administration Guide - Setting Up STRM Log Manager, Creating Your Network Hierarchy*.

**Identifying Network Settings**

Before you install STRM Log Manager, you must have the following information for each system you want to install:

- Hostname
- IP address
- Network mask address

- Subnet mask
- Default gateway address
- Primary DNS server address
- Secondary DNS server address (optional)
- Public IP address for networks using Network Address Translation (NAT)
- E-mail server name
- NTP Server (Console only) or Time server name

**Identifying Security Monitoring Devices**

STRM Log Manager collects and correlates events received from external sources including:

- Security equipment, such as firewalls, VPNs, and Intrusion Detection Systems (IDSs)
- Host or application security logs such as window logs

Device Support Modules (DSMs) allow you to integrate STRM Log Manager with this external data.

STRM Log Manager automatically discovers sensor devices that send syslog messages to an Event Collector. Automatically discovered sensor devices appear in the Sensor Devices window within the STRM Log Manager Administration Console. Once auto discovery is complete, you should disable the Auto Detection Enabled option in the Event Collector configuration. For more information, see the *STRM Log Manager Administration Guide*.

You must add non-syslog based information sources to your deployment manually. For more information, see the *Managing Sensor Devices Guide*. For each device you want to add to your deployment, record device information in the following table.

**Table 1-2** Devices

Device Type	QTY	Product Name/Version	Link Speed & Type	Msg Level	Avg Log Rate (Event/Sec)	No. of Users	Network Location	Geographic Location	Credibility (0 to 10)

Where:

- **Device Type** - Specifies the type of device, such as firewall, router, or VPN devices.
- **QTY** - Specifies how many devices you have of each device type.
- **Product Name/Version** - Specifies the device product name and version number.
- **Link Speed & Type** - Specifies the maximum network link speed (in Kbps) for firewall, router, and VPN devices. For the type, record the primary application of the host system, for example, e-mail, anti-virus, domain controller, or a workstation.
- **Msg Level** - Specifies the message level you want to log. For example, critical, informational, or debug.
- **Avg Log Rate (Event/Sec)** - Specifies the average event rate per second.
- **No. of Users** - Specifies the maximum number of hosts/users using or being served by this device.
- **Network Location** - Specifies whether this device is located on the Internet DMZ, Intranet, or Extranet DMZ.
- **Geographic Location** - Specifies if the devices are located on the same LAN as STRM Log Manager or if they are sending logs over the WAN identified in the Link Speed & Type column.
- **Credibility** - Specifies the integrity of an event as determined by the credibility rating from source devices. Credibility increases as the multiple sources report the same event.



# 2

## INSTALLING STRM LOG MANAGER

This chapter provides information on installing your STRM Log Manager system including:

- [Setting Up Appliances](#)
- [Accessing STRM Log Manager](#)

---

### Setting Up Appliances

A STRM Log Manager appliance includes STRM Log Manager software and a CentOS-5.2 operating system. This section provides information for how to set up your appliance. For more information about appliances, see the *Hardware Installation Guide*.

To set-up your appliance:

**Step 1** Install all necessary hardware.

For information on rack mounting your STRM Log Manager appliance, see the *Hardware Installation Guide*.

**Step 2** Choose one of the following options:

a Connect a laptop to the serial port on the rear of the appliance.



**Note:** If you use a laptop to connect to the system, you must use a terminal program, such as *HyperTerminal*, to connect to the system. Make sure you 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).

b Connect a keyboard and monitor to their respective ports.

For more information on appliance ports, see the *Hardware Installation Guide*.

**Step 3** Power on the system and log in to STRM Log Manager:

Username: **root**

Password: **password**



**Note:** The username and password are case sensitive.

**Step 4** Press Enter.

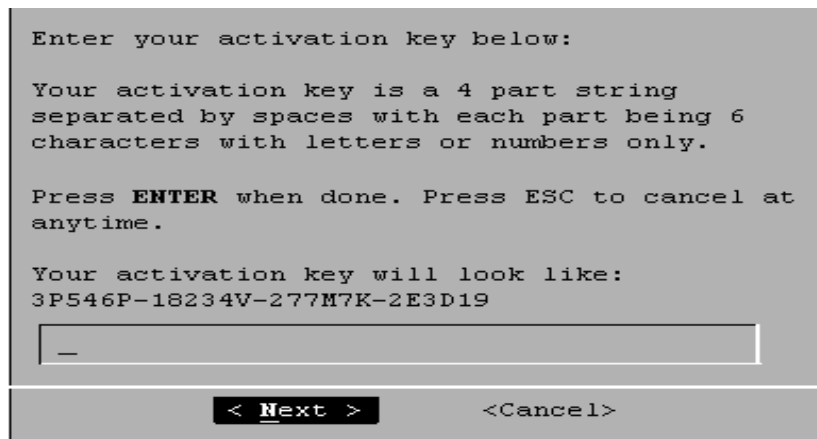
The End User License Agreement (EULA) appears.

**Step 5** 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 activation key window appears. The activation key is a 24-digit, four-part (separated by hyphens), alphanumeric string that you receive from Juniper Networks.

You can find the activation key:

- Printed on a sticker and physically placed on your appliance.
- Included with the packing slip; all appliances are listed along with their associated keys.

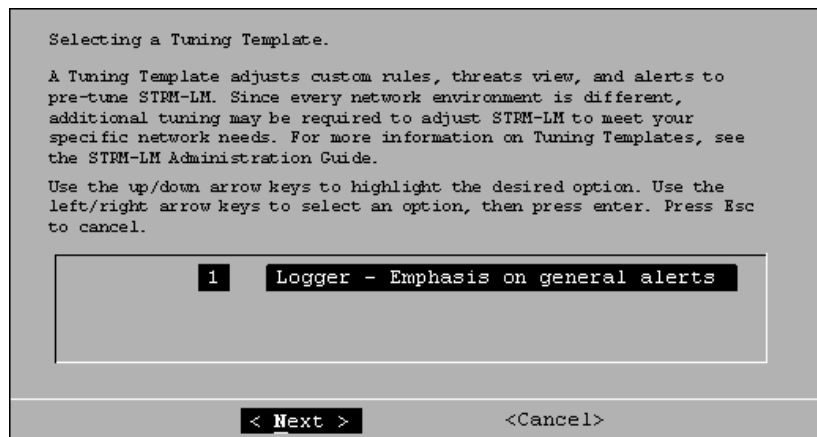


**Step 6** Enter your activation key.



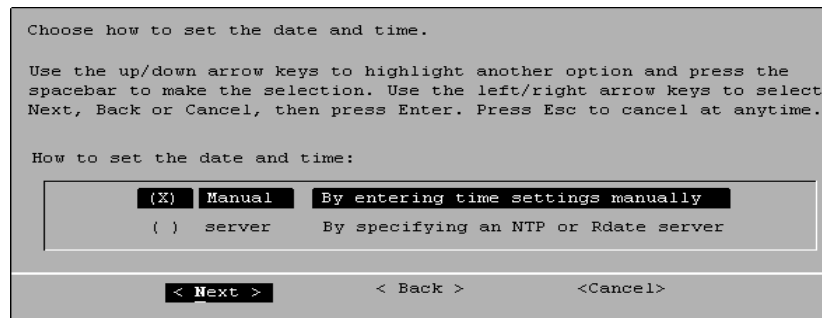
**Note:** The letter *l* and the number 1 (one) are treated the same, as are the letter *O* and the number 0 (zero).

The Tuning Template window appears.



**Step 7** Press Enter.

The Set Time and Date window appears.



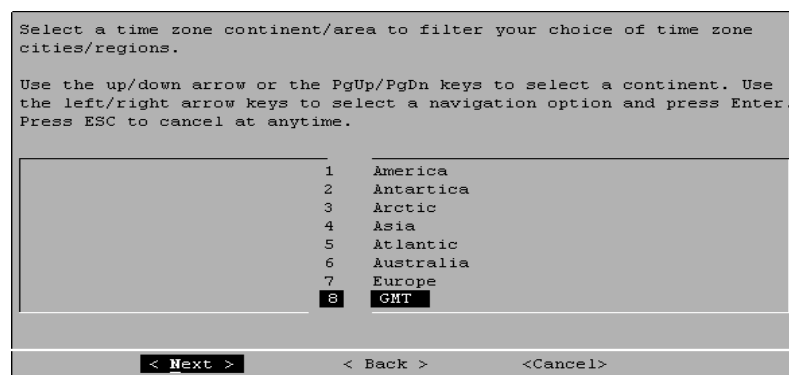
**Step 8** Using the up/down arrow keys, highlight the method you want to use to set the date and time, and then use the spacebar to select that option:

- **Manual** - Allows you to manually input the time and date. Use the Tab key to select the **Next** option. Press Enter. The Current Date and Time window appears. Go to •.
- **Server** - Allows you to specify your time server. Use the Tab key to select the **Next** option. Press Enter. The Enter Time Server window appears. Go to [Step 9](#).
- To manually enter the time and date:
  - a Enter the current date and time.
  - b Using the left/right arrow keys, select **Next**. Press Enter.
  - c Go to [Step 10](#).

**Step 9** To specify a time server:

- a In the text field, enter the time server name or IP address.
- b Using the left/right arrow keys, select **Next**. Press Enter.

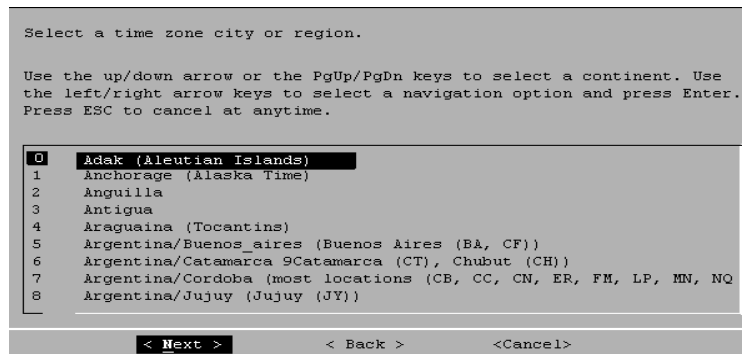
The Time Zone Continent window appears.



**Step 10** To select the time zone continent:

- a Using the up/down arrow keys, or the page up/page down keys, select your time zone continent or area.
- b Using the left/right arrow keys, select **Next**, then press Enter.

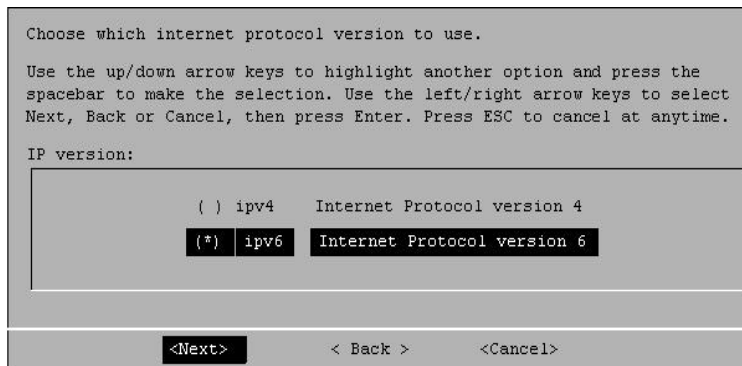
The Time Zone Region window appears.



**Note:** The options that appear in this window are regions that are associated with the continent or area previously selected.

- c Using the up/down arrow keys, or the page up/page down keys, select your time zone region.
- d Using the left/right arrow keys, select **Next**. Press Enter.

The Choose which Internet protocol to use window appears.



**Step 11** To choose which Internet protocol version to use:

- a If you want to select IPv6:
    - Using the up/down arrow keys, or the page up/page down keys, select **IPv6**.
    - Using the left/right arrow keys, select **Next**. Press Enter.
- The Enter the IP address to use for IPv6 window appears.

```

Enter the IP address to use for IPv6
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.

```

Host name:	strm.juniper.net		
IP address:			
Email server:			

< Next >      < Back >      <Cancel>

- Enter the IP address or name for the **Hostname**, **IP Address**, and **Email server**.
  - Using the left/right arrow keys, select **Next**. Press Enter.
- b** If you want to select IPv4:
- Using the up/down arrow keys, or the page up/page down keys, select **IPv4**.
  - Using the left/right arrow keys, select **Next**. Press Enter.

The Configure STRM Log Manager 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.

```

Host name:	strm.juniper.net		
IP address:		Primary DNS:	
Network mask:		Secondary DNS:	
Gateway:		Public IP:	
Email server:			

< Next >      < Back >      <Cancel>

**Step 12** To configure the STRM Log Manager network settings:

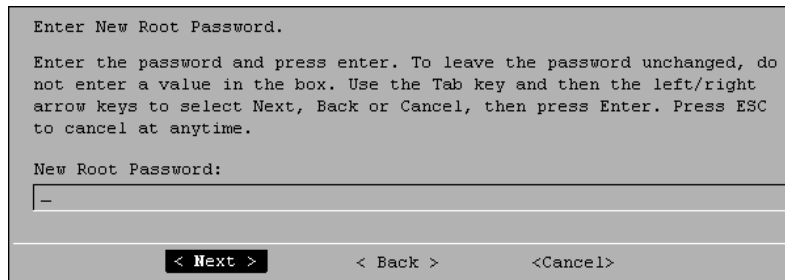
- a** You must change the displayed default values. Using the up/down arrow keys to navigate the fields, enter values for the following parameters:
- **Hostname** - Specify a fully qualified domain name as the system hostname.
  - **IP Address** - Specify the IP address of the system.
  - **Network Mask** - Specify the network mask address for the system.
  - **Gateway** - Specify the default gateway of the system.
  - **Primary DNS** - Specify the primary DNS server.
  - **Secondary DNS** - Optional. Specify the secondary DNS server.
  - **Public IP** - Optional. Specify the Public IP address of the server. This is a secondary IP address that is used to access the server, usually from a different network or the Internet, and is managed by your network administrator. The Public IP address is often configured using Network Address Translation (NAT) services on your network or firewall settings on

your network. NAT translates an IP address in one network to a different IP address in another network.

- **Email Server** - Specify the e-mail server. If you do not have an e-mail server, specify **localhost** in this field.

b Use the TAB key to move to the **Next** option. Press Enter.

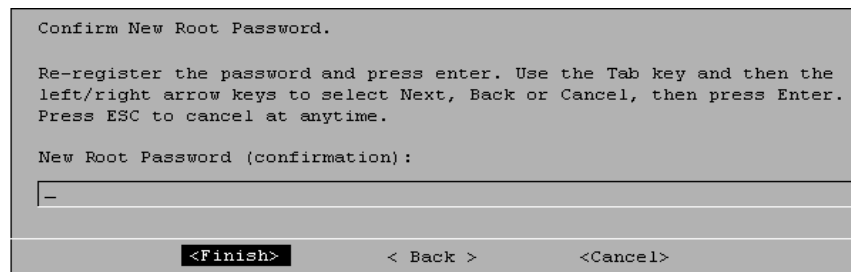
The New Root Password window appears.



**Step 13** To configure the STRM Log Manager root password:

- a Enter your password.
- b Use the TAB key to move to the **Next** option. Press Enter.

The Confirm New Root Password window appears.



- c Re-enter your new password to confirm.
- d Use the TAB key to move to the **Finish** option. Press Enter.

A series of messages appear as STRM Log Manager continues with the installation. This process typically takes several minutes. The Configuration is Complete window appears.

**Step 14** Press Enter to select **OK**.

You are now ready to access STRM Log Manager. For more information, see [Accessing STRM Log Manager](#).

## Accessing STRM Log Manager

To access the STRM Log Manager interface:

- Step 1** Open your web browser.
- Step 2** Log in to STRM Log Manager:

**https://<IP Address>**

Where **<IP Address>** is the IP address of the STRM Log Manager system. The default values are:

Username: **admin**

Password: **<root password>**

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



**Note:** *If you are using Mozilla Firefox 3.0, you must add an exception to Mozilla Firefox to log in to STRM. For more information, see your Mozilla documentation.*

**Step 3** Click **Login To STRM Log Manager**.

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







# A

## CHANGING NETWORK SETTINGS

This appendix provides information on changing network settings for the Console and non-Console systems including:

- [Changing Network Settings in an All-in-One Console](#)
- [Changing the Network Settings of a Console in a Multi-System Deployment](#)
- [Changing the Network Settings of a Non-Console in a Multi-System Deployment](#)

---

### Changing Network Settings in an All-in-One Console

You can change the network settings in your All-In-One system. An All-In-One system has all STRM Log Manager components, including the Administration Console, installed on one system.

To change the settings on the STRM Log Manager Console:



**Note:** You must have a local connection to your Console before executing the script.

**Step 1** Log in to the Console, as root.

**Step 2** Enter the following command:

```
qchange_netsetup
```

The Configure STRM Log Manager 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.

Host name:	strm.juniper.net		
IP address:		Primary DNS:	
Network mask:		Secondary DNS:	
Gateway:		Public IP:	
Email server:			

< Next >      < Back >      <Cancel>

**Step 3** Using the up/down arrow keys to navigate the fields, change the necessary parameters:

- **Hostname** - Specify a fully qualified domain name as the system hostname.

- **IP Address** - Specify the IP address of the system.
- **Netmask** - Specify the network mask address for the system.
- **Gateway** - Specify the default gateway address of the system.
- **Primary DNS** - Specify the primary DNS server address.
- **Secondary DNS** - Optional. Specify the secondary DNS server address.
- **Public IP** - Optional. Specify the Public IP address of the server. This is a secondary IP address that is used to access the server, usually from a different network or the Internet, and is managed by your network administrator. This Public IP address is often configured using Network Address Translation (NAT) services on your network or firewall settings on your network. NAT translates an IP address in one network to a different IP address in another network.
- **Email Server** - Specify the e-mail server. If you do not have an e-mail server, specify **localhost** in this field.

**Step 4** Use the TAB key to navigate to the **Finish** option. Press Enter.

A series of messages appear as STRM Log Manager processes the requested changes. After the requested changes are processed, the STRM Log Manager system is automatically shut down and rebooted.

---

## Changing the Network Settings of a Console in a Multi-System Deployment

To change the network settings in a multi-system deployment, you must remove all non-Console managed hosts from the deployment, change the network settings, re-add the managed host(s), and then re-assign the component(s).

You must perform this procedure in the following order:

- [Removing Non-Console Managed Hosts](#)
- [Changing the Network Settings](#)
- [Re-Adding Managed Host\(s\) and Re-Assigning the Components](#)



**Note:** This procedure requires you to use the Deployment Editor. For more information on using the Deployment Editor, see the STRM Log Manager Administration Guide.

### Removing Non-Console Managed Hosts

To remove non-Console managed hosts from your deployment, you must:

**Step 1** Log in to STRM Log Manager:

`https://<IP Address>`

Where `<IP Address>` is the IP address of the STRM Log Manager system.

Username: `admin`

Password: `<admin password>`

**Step 2** In the main STRM Log Manager Interface, click **Config**.

The Administration Console appears.

**Step 3** Click the **Edit** icon.

The Deployment Editor appears.

**Step 4** Click the **System View** tab.

**Step 5** Select the managed host you want to delete.

**Step 6** Use the right mouse button (right-click) to access the menu, select **Remove host**. Repeat for each non-Console managed host until all hosts are deleted.

**Step 7** From the Administrative Console menu, select **Configurations > Deploy Configuration Changes**.



**Note:** If the Administration Console is still active on your system tray, use the right-mouse button (right-click) to access the menu and select **Exit**.

The changes are deployed.

### Changing the Network Settings

To change the network settings, you must:

**Step 1** Log in to the Console as root.

**Step 2** Enter the following command:

```
qchange_netsetup
```

The Network Settings window appears.

**Step 3** Using the up/down arrow keys to navigate the fields, make the necessary changes to the following parameters:

- **Hostname** - Specify a fully qualified domain name as the system hostname.
- **IP Address** - Specify the IP address of the system.
- **Netmask** - Specify the network mask address for the system.
- **Gateway** - Specify the default gateway address of the system.
- **Primary DNS** - Specify the primary DNS server address.
- **Secondary DNS** - Optional. Specify the secondary DNS server address.
- **Public IP** - Optional. Specify the Public IP address of the server. This is a secondary IP address that is used to access the server, usually from a different network or the Internet, and is managed by your network administrator. This Public IP address is often configured using Network Address Translation (NAT) services on your network or firewall settings on your network. NAT translates an IP address in one network to a different IP address in another network.
- **Email Server** - Specify the e-mail server. If you do not have an e-mail server, specify **localhost** in this field.

**Step 4** Use the TAB key to move to the **Finish** option. Press Enter.

A series of messages appear as STRM Log Manager processes the requested changes. After the requested changes are processed, the STRM Log Manager system is automatically shut down and rebooted.

### Re-Adding Managed Host(s) and Re-Assigning the Components

To re-add the managed host(s) and re-assign component(s), you must:

**Step 1** Log in to STRM Log Manager:

`https://<IP Address>`

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

Username: **admin**

Password: **<admin password>**

**Step 2** In the main STRM Log Manager Interface, click **Config**.

The Administration Console appears.

**Step 3** Click the **Edit** icon.

The Deployment Editor appears.

**Step 4** From the menu, select **Actions > Add a managed host**.

The Add a new host wizard appears.

**Step 5** Click **Next**.

The Enter the host's IP window appears.

**Step 6** Enter values for the parameters:

- **Enter the IP of the server or appliance to add** - Specify the IP address of the host you want to add to your System View.
- **Enter the root password of the host** - Specify the root password for the host.
- **Confirm the root password of the host** - Specify the password again, for confirmation.
- **Host is NATed** - Select if you want to specify NAT values if necessary.
- **Enable Encryption** - Select if you want to enable encryption.

**Step 7** Click **Next**.

**Step 8** Click **Finish**.

**Step 9** Re-assign all components to your non-Console managed host.

- a In the STRM Log Manager Deployment Editor, click the **Event View** tab.
- b Select the component you want to re-assign to the managed host.
- c From the menu, select **Actions > Assign**



**Note:** You can also use the right mouse button (right-click) to access the Actions menu items.

The Assign Component wizard appears.

- d From a **Select a host** drop-down list box, select the host you want to re-assign to this component. Click **Next**.
  - e Click **Finish**.
- Step 10** Repeat for each non-Console managed host until all hosts are re-added and re-assigned.
- Step 11** From the Administrative Console menu, select **Configurations > Deploy Configuration Changes**.  
The changes are deployed.

### Changing the Network Settings of a Non-Console in a Multi-System Deployment

To change the network settings of a non-Console in a multi-system deployment, you must remove all non-Console managed host from the deployment, change the network settings, re-add the managed host, and then re-assign the component(s).

You must perform this procedure in the following order:

- [Removing the Non-Console Managed Host](#)
- [Changing the Network Settings](#)
- [Re-Adding the Managed Host and Re-Assigning the Components](#)



**Note:** This procedure requires you to use the Deployment Editor. For more information on using the Deployment Editor, see the STRM Log Manager Administration Guide.

### Removing the Non-Console Managed Host

To remove non-Console managed host from your deployment, you must:

- Step 1** Log in to STRM Log Manager:  
`https://<IP Address>`  
 Where **<IP Address>** is the IP address of the STRM Log Manager system.  
 Username: **admin**  
 Password: **<admin password>**
- Step 2** In the main STRM Log Manager Interface, click **Config**.  
 The Administration Console appears.
- Step 3** Click the **Edit** icon.  
 The Deployment Editor appears.
- Step 4** Click the **System View** tab.
- Step 5** Select the managed host you want to delete.
- Step 6** Use the right mouse button (right-click) to access the menu, select **Remove host**.

- Step 7** From the Administrative Console menu, select **Configurations > Deploy Configuration Changes**.



**Note:** If the Administration Console is still active on your system tray, use the right-mouse button (right-click) to access the menu and select **Exit**.

The changes are deployed.

### Changing the Network Settings

To change the network settings, you must:

- Step 1** Log in to the non-Console as root.

- Step 2** Enter the following command:

```
qchange_netsetup
```

The Network Settings window appears.

- Step 3** Using the up/down arrow keys to navigate the fields, make the necessary changes to the following parameters:

- **Hostname** - Specify a fully qualified domain name as the system hostname.
- **IP Address** - Specify the IP address of the system.
- **Netmask** - Specify the network mask address for the system.
- **Gateway** - Specify the default gateway address of the system.
- **Primary DNS** - Specify the primary DNS server address.
- **Secondary DNS** - Optional. Specify the secondary DNS server address.
- **Public IP** - Optional. Specify the Public IP address of the server. This is a secondary IP address that is used to access the server, usually from a different network or the Internet, and is managed by your network administrator. This Public IP address is often configured using Network Address Translation (NAT) services on your network or firewall settings on your network. NAT translates an IP address in one network to a different IP address in another network.
- **Email Server** - Specify the e-mail server. If you do not have an e-mail server, specify **localhost** in this field.

- Step 4** Use the TAB key to move to the **Finish** option. Press Enter.

A series of messages appear as STRM Log Manager processes the requested changes. After the requested changes are processed, the STRM Log Manager system is automatically shutdown and rebooted.

### Re-Adding the Managed Host and Re-Assigning the Components

To re-add the managed host and re-assign component(s), you must:

- Step 1** Log in to STRM Log Manager:

```
https://<IP Address>
```

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

Username: **admin**

Password: **<admin password>**

**Step 2** In the main STRM Log Manager Interface, click **Config**.

The Administration Console appears.

**Step 3** Click the **Edit** icon.

The Deployment Editor appears.

**Step 4** From the menu, select **Actions > Add a managed host**.

The Add a new host wizard appears.

**Step 5** Click **Next**.

The Enter the host's IP window appears.

**Step 6** Enter values for the parameters:

- **Enter the IP of the server or appliance to add** - Specify the IP address of the host you want to add to your System View.
- **Enter the root password of the host** - Specify the root password for the host.
- **Confirm the root password of the host** - Specify the password again, for confirmation.
- **Host is NATed** - Select if you want to specify NAT values if necessary.
- **Enable Encryption** - Select if you want to enable encryption.

**Step 7** Click **Next**.

**Step 8** Click **Finish**.

**Step 9** Re-assign all components to your non-Console managed host.

- a In the STRM Log Manager Deployment Editor, click the **Flow View** or **Event View** tab.
- b Select the component you want to re-assign to the managed host.
- c From the menu, select **Actions > Assign**



**Note:** You can also use the right mouse button (right-click) to access the Actions menu items.

The Assign Component wizard appears.

d From a **Select a host** drop-down list box, select the host you want to re-assign to this component. Click **Next**.

e Click **Finish**.

**Step 10** From the Administrative Console menu, select **Configurations > Deploy Configuration Changes**.

The changes are deployed.



# INDEX

---

## A

about this guide 1  
appliances  
    setting-up 9

---

## B

browser support 4

---

## C

Console  
    definition 3  
conventions 1

---

## E

Event Collector  
    definition 4  
Event Processor  
    definition 4

---

## I

installing  
    preparing 3

---

## N

network hierarchy  
    preparing 5  
network settings  
    identifying 5

---

## P

preparing 3

---

## R

requirements  
    hardware 4

---

## S

security monitoring devices  
    identifying 6  
software  
    requirements 4

