



**Security Threat Response Manager**

# **STRM Installation Guide**

***Release 2009.2***

**Juniper Networks, Inc.**

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

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

Published: 2010-04-01

## 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.

*STRM Installation Guide*  
Release 2009.2

Copyright © 2008, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Revision History

April 2010—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	3
Additional Hardware Requirements	6
Additional Software Requirements	6
Browser Support	6
Identifying Network Settings	7
Preparing Your Network Hierarchy	7
Identifying Security Monitoring Log Sources	8
Preparing For HA	10

---

## 2 INSTALLING STRM

Using This Document	11
Installing STRM Appliances	11
Installation Procedures	13
Accessing STRM	24

---

## A CHANGING NETWORK SETTINGS

Changing Network Settings in an All-in-One Console	25
Changing the Network Settings of a Console in a Multi-System Deployment	26
Changing the Network Settings of a Non-Console in a Multi-System Deployment	28

---

## 3 RE-INSTALLING STRM

About the Recovery Partition	31
Re-installing STRM	32

---

## INDEX



# ABOUT THIS GUIDE




The *STRM Installation Guide* provides you with information on setting up STRM. STRM appliances are pre-installed with CentOS operating system. This guide assumes a working knowledge of networking 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

Your STRM deployment can consist of STRM installed on one or multiple systems. You can use the STRM three-tier architecture to install components on a single server for small enterprises or distributed across multiple servers for maximum performance and scalability in large enterprise environments. STRM also provides High Availability (HA) functionality, which requires you to install redundant appliances for each system you want to provide HA protection.

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

This chapter provides information about planning your STRM deployment including:

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

---

### Deploying STRM

You can deploy STRM using STRM appliances or STRM software installed on your own hardware. This section provides information about deploying STRM including:

- [STRM Components](#)
- [Examples of STRM Deployments](#)

A STRM appliance includes STRM software and a CentOS operating system. For further information about STRM appliances, see the *Hardware Installation Guide*.

**STRM Components** STRM components that can exist in your deployment include:



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

- **QFlow Collector** - Passively collects traffic flows from your network through span ports or network taps. The QFlow Collector also supports the collection of external flow-based data sources, such as NetFlow. You can install a QFlow Collector on your own hardware or use one of the QFlow Collector appliances.
- **Flow Processor** - Normalizes flows sent from one or more QFlow Collector by consolidating, aggregating, and removing duplicate flows. The QFlow Collector can also create *superflows* (grouped flows) before the flows reach the Classification Engine.
- **Classification Engine** - Analyzes flows to classify and identify all traffic in the enterprise network into multiple objects.
- **Console** - Provides the user interface for STRM. The Console provides real time views, reports, alerts, and in-depth flow views of network traffic and security threats. Using the Console, you can also manage distributed STRM deployments.

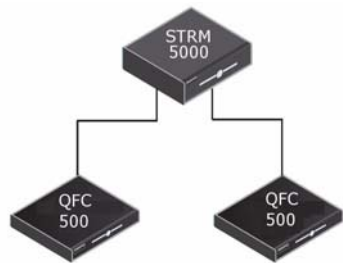
You access the Console from a standard web browser. When you access the system, a prompt appears for a user name and password, which you configure during the installation process. You must also have Java installed on your desktop system. For information about software requirements, see [Additional Software Requirements](#).

- **Update Daemon** - Writes to the database and TopN data. Typically, the Update Daemon is installed on the Console.
- **Flow Writer** - Writes the flow and asset profile data.
- **Resolution** - The Resolution module provides enterprise-wide intrusion prevention for your network and includes Resolvers, Resolutions, and Resolver Agents.
- **Event Collector** - The Event Collector gathers events from local and remote device sources. The Event Collector normalizes events, and then sends the information to the Event Processor. Before sending information to the Event Processor, the Event Collector bundles identical events to conserve system usage. During this process, Magistrate risk factors map the events to the STRM Identification System, and then creates the bundles.
- **Event Processor** - Processes events collected from one or more Event Collector. Once received, the Event Processor correlates the information from STRM and distributes the information to the appropriate area, depending on the type of event. The Event Processor also includes information gathered by STRM to indicate behavioral changes or policy violations for the event. Rules are applied to the events that allow the Event Processor to process events according to the configured rules. Once complete, the Event Processor sends the events to the Magistrate.

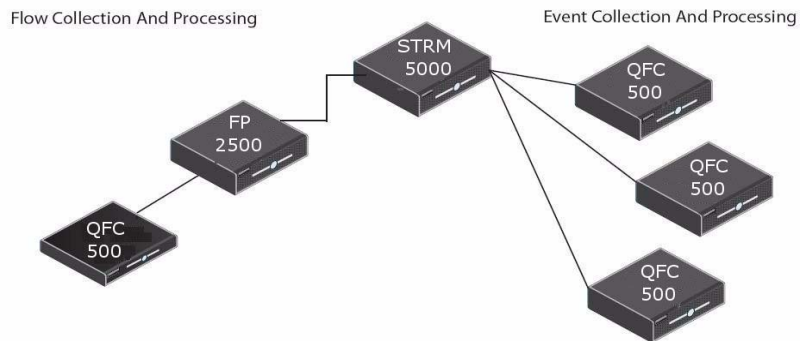
- Magistrate** - Provides the core processing components. You can add one Magistrate component for each deployment. The Magistrate provides views, reports, alerts, and analysis of network traffic and security events. The Magistrate processes the event against the defined custom rules to create an offense. If there is no match to a custom rule, the Magistrate uses default rules to process the event. An offense is an event that has been processed through STRM using multiple inputs, individual events, and events combined with analyzed behavior and vulnerabilities. Magistrate prioritizes the offenses and assigns a magnitude value based on several factors, including number of events, severity, relevance, and credibility.

**Examples of STRM Deployments**

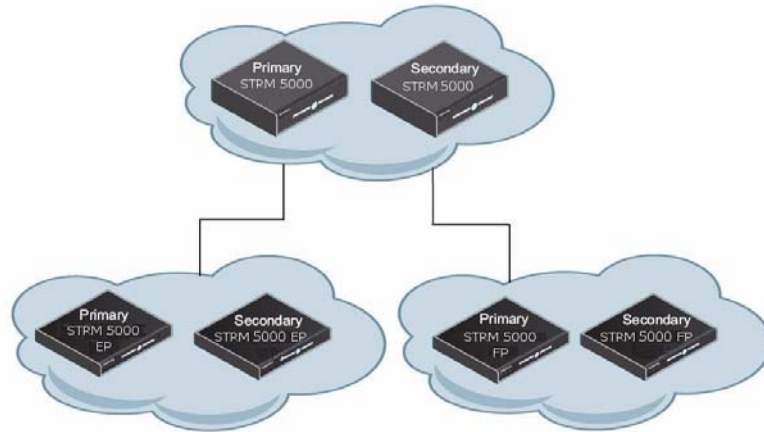
The following figure shows an example of a small deployment using STRM and QFlow Collector appliances.



The following figure shows an example of a multisystem deployment using a mixture of QFlow Collector and STRM appliances.



The following figure shows an example of a small HA deployment using STRM and QFlow Collector appliances.



---

**Additional Hardware Requirements**

Before installing your STRM systems, make sure you have access to an Uninterrupted Power Supply (UPS).



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

---

**Additional Software Requirements**

Before installing STRM, make sure you have Java Runtime Environment installed on your system. You can download Java version 1.6.0\_17 x86 at the following web site: <http://java.sun.com/>.



**Note:** Make sure that you install Java Runtime Environment on your desktop system, not the appliance.

---

**Browser Support**

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

- Microsoft Internet Explorer 7.0
- Firefox 3.0

---

## Identifying Network Settings

Before you install STRM, 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 Domain Name System (DNS) server address
- Secondary DNS server (optional) address
- Public IP address for networks using NAT
- E-mail server name
- Network Time Protocol (NTP) server (Console only) or time server name

If you have already installed STRM 2009.2 and are recovering a failed primary HA host, you must gather the following information from the STRM user interface:

- Cluster Virtual IP Address
- Primary IP Address



**Note:** You can find these IP addresses in the System and License Management window by pointing your mouse over the row for the HA cluster. For more information, see the STRM Installation Guide.

---

## Preparing Your Network Hierarchy

STRM uses the network hierarchy to understand your network traffic and provide you with the ability to view network activity for your entire deployment. STRM 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 components you want to add to your network hierarchy and install STRM, you can then configure the network hierarchy using the STRM Console. For each STRM 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, 10.0.0.0/8)
- Proxy servers
- Network Address Translation (NAT) IP address range
- Server Network subnets
- Voice over IP (VoIP) subnets

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

---

**Identifying Security Monitoring Log Sources**

STRM 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) and QFlow Collectors allow you to integrate STRM with this external data.

STRM automatically discovers log sources that send syslog messages to an Event Collector. Automatically discovered log sources appear in the Log Sources window within the STRM Admin interface. For more information, see the *STRM Administration Guide*.

You must add non-syslog based information sources to your deployment manually. For more information, see the *Managing Log Sources Guide*. For each log source

you want to add to your deployment, record log source information in the following table.

**Table 1-2** Log Sources

Log Source 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:

- **Log Source Type** - Specifies the type of log source, such as firewall, router, or VPN log sources.
- **QTY** - Specifies how many log sources you have of each log source type.
- **Product Name/Version** - Specifies the log source product name and version number.
- **Link Speed & Type** - Specifies the maximum network link speed (in Kbps) for firewall, router, and VPN log sources. 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 log source.
- **Network Location** - Specifies whether this log source is located on the DMZ, Internet, Intranet, or Extranet.
- **Geographic Location** - Specifies if the log sources are located on the same LAN as STRM or if they are sending logs over the WAN identified in the Link Speed & Type column.
- **Credibility** - Specifies the integrity of an event or offense as determined by the credibility rating from log sources. Credibility increases as multiple sources report the same event.

## Preparing For HA

Before deploying HA in your environment, ensure your HA hosts adhere to the following requirements:

- The secondary host must have a valid High Availability (HA) activation key.
- The secondary host must have the same STRM software version installed as the primary host in the HA cluster.
- The secondary host's memory must be equal to or greater than the primary host's memory.
- The secondary host must be located on the same subnet as the primary host.
- The secondary host must have the same STRM HW model as the primary host in the HA cluster.
- If you plan to enable disk synchronization, we recommend that there is at least a 1 GB connection between the primary host and secondary host.
- If you plan for your HA hosts to share external storage, we recommend that there is at least a 1 GB connection between each HA host and your external storage solution.

# 2

## INSTALLING STRM

This chapter provides information on installing your STRM system including:

- [Using This Document](#)
- [Installing STRM Appliances](#)
- [Installation Procedures](#)
- [Accessing STRM](#)

---

### Using This Document

See the below section to identify the necessary steps to install STRM and deployment requirements. Throughout the document, navigation links at the end of each procedure guide you to the next step in your installation process.

---

### Installing STRM Appliances

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

Choose which type of installation you want to perform:

- [Installing an Appliance](#)
- [Installing or Recovering a Secondary HA Appliance](#)
- [Recovering a Failed Primary HA Host](#)

### Installing an Appliance

To install an appliance:

- Step 1** Prepare your appliance. See [Preparing Your STRM Appliance](#).
- Step 2** To set up your STRM appliance:
  - [Choosing Your Type of Setup](#)
  - [Selecting a Tuning Template](#)
  - [Setting the Time and Date](#)
  - [Configuring Your Internet Protocol](#)
  - [Configuring STRM Network Settings](#)
  - [Configuring the STRM Root Password](#)

- Step 3** To set up your QFlow appliance:
- a [Choosing Your Type of Setup](#)
  - b [Setting the Time and Date](#) (only perform [Step 4](#))
  - c [Configuring Your Internet Protocol](#)
  - d [Configuring STRM Network Settings](#)
  - e [Configuring the STRM Root Password](#)

You can now access STRM. See [Accessing STRM](#).

### Installing or Recovering a Secondary HA Appliance

Before installing or recovering your secondary HA appliance, confirm that the appliance adheres to the requirements identified in [Preparing For HA](#).

To install or recover your secondary HA appliance for STRM appliance:

- Step 1** Prepare your appliance. See [Preparing Your STRM Appliance](#).
- Step 2** To set up your secondary STRM appliance:
- a [Specifying Your Secondary Device Type](#)
  - b [Setting the Time and Date](#)
  - c [Configuring Your Internet Protocol](#)
  - d [Configuring STRM Network Settings](#)
  - e [Configuring the STRM Root Password](#)
- Step 3** To set up your secondary QFlow appliance:
- a [Specifying Your Secondary Device Type](#)
  - b [Setting the Time and Date](#) (only perform [Step 4](#))
  - c [Configuring Your Internet Protocol](#)
  - d [Configuring STRM Network Settings](#)
  - e [Configuring the STRM Root Password](#)

**Step 4** Log in to the STRM interface. See [Accessing STRM](#).

**Step 5** Configure your HA cluster.

For more information on managing HA, see the *STRM Administration Guide - Managing High Availability*.

### Recovering a Failed Primary HA Host

Before you recover a failed primary HA host, you must gather the following information from the STRM user interface:

- Cluster Virtual IP Address
- Primary IP Address



**Note:** You can find these IP addresses in the *System and License Management* window by pointing your mouse over the row for the HA cluster. For more information, see the *STRM Administration Guide - Managing High Availability*.

To recover a failed primary HA host:

**Step 1** Prepare your appliance. See [Preparing Your STRM Appliance](#).

**Step 2** To recover your failed primary STRM host:

- a [Choosing Your Type of Setup](#)
- b [Setting the Time and Date](#)
- c [Configuring Your Internet Protocol](#)
- d [Configuring Your Cluster Virtual IP Address](#)
- e [Configuring STRM Network Settings](#)
- f [Configuring the STRM Root Password](#)

**Step 3** To recover your failed primary QFlow host:

- a [Choosing Your Type of Setup](#)
- b [Setting the Time and Date](#) (only perform [Step 4](#))
- c [Configuring Your Internet Protocol](#)
- d [Configuring Your Cluster Virtual IP Address](#)
- e [Configuring STRM Network Settings](#)
- f [Configuring the STRM Root Password](#)



**Caution:** *If your HA cluster uses shared storage, you must manually configure iSCSI. For more information about configuring iSCSI, see the [Configuring iSCSI technical note](#).*

**Step 4** Log in to the STRM interface. See [Accessing STRM](#).

**Step 5** Restore the failed primary HA system.

For more information on restoring a failed primary HA system, see the *STRM Administration Guide - Managing High Availability*.

---

## Installation Procedures

This section includes:

- [For Primary HA Appliance](#)
- [For Secondary HA Appliance](#)
- [Preparing Your STRM Appliance](#)
- [Choosing Your Type of Setup](#)
- [Specifying Your Secondary Device Type](#)
- [Selecting a Tuning Template](#)
- [Setting the Time and Date](#)
- [Configuring Your Internet Protocol](#)
- [Configuring IPv6](#)
- [Configuring Your Cluster Virtual IP Address](#)

- [Configuring STRM Network Settings](#)
- [Configuring the STRM Root Password](#)

- For Primary HA Appliance** For more information on upgrading from STRM 2009.1 to STRM 2009.2, see the *Upgrading STRM Guide*.
- For Secondary HA Appliance** The STRM 2009.2 ISO needs to be installed fresh on the Secondary HA Appliance.
- The partition script is used to allow a user to run installs of different versions of STRM on an appliance that has a previously installed version of STRM. For example, from STRM 2009.1 to STRM 2009.2 as fresh install, instead of an upgrade.
- To install the Secondary HA appliance:
- Step 1** Copy the new 2009.2 ISO to the Secondary HA STRM Appliance using the following command:
- ```
scp <iso file name> root@<strm ip>:/root
```
- Note:** The script can be extracted directly from the 2009.2 ISO.
- Step 2** Mount the ISO using the following command:
- ```
mount -o loop <iso_file_name> /media/cdrom/
```
- Step 3** Extract the script by running the following command:
- ```
rpm2cpio /media/cdrom/post/*branding*.rpm | cpio -idv
./opt/oem/branding/recovery.py
```
- Step 4** Move file into root directory:
- ```
mv opt/oem/branding/recovery.py .
```
- Step 5** Unmount the ISO using the following command:
- ```
umount /media/cdrom/
```
- Note:** If the STRM appliance has been previously managed then IPTables will need to be stopped in order to allow SCP. Run the following command: **service tables stop**.
- Step 6** Run the extracted script using the following command:
- ```
./recovery.py -r --default --reboot <STRM2009.2.iso_file_name>
```
- The following is an example output that will be displayed within the command line:
- ```
[root@vmb63 ~]# ./recovery.py -r --default --reboot
CentOS564STRM2009_2_0_1480xx.iso
INFO :copying CentOS564STRM2009_2_0_148034.iso to /recovery/iso
INFO :Found iso /recovery/iso/CentOS564STRM2009_2_0_1480xx.iso
as Security Threat Response Manager 2009.2.0.1480xx
INFO :Wrote new grub.cfg
INFO :About to reboot
INFO :Press enter when ready
```

**Step 7** Press Enter to reboot the appliance. The following message appears:

```
Welcome to factory reset option.
You have selected the option to re-install your system. This
option returns all system settings to the factory defaults and
removes all existing data and configuration. This process is not
reversible.
If you do not wish to continue, type REBOOT at the prompt.
If you wish to continue, type FLATTEN at the prompt.
```

**Step 8** Enter `flatten` and press Enter to continue.

The installer repartitions and reformats the hard disk, installs the OS, and then re-installs STRM. Wait for the flatten process to complete. This process can take up to several minutes, depending on your system.

When this process is complete, the normal fresh install process proceeds.

**Step 9** When the installation completes, enter `setup` and login to the system with the username `root`.

To configure the Secondary HA appliance, refer to [Preparing Your STRM Appliance](#).

## Preparing Your STRM Appliance

To set up your STRM appliance:

**Step 1** Install all necessary hardware.

For information on your STRM appliance, see the *Hardware Installation Guide*.

**Step 2** Connect a laptop to the console port on the front 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).

**Step 3** Using the keyboard with monitor or laptop, log in using the default username and password.



**Note:** The username is case sensitive.

Username: `root`

Password: `password`

Press Enter.

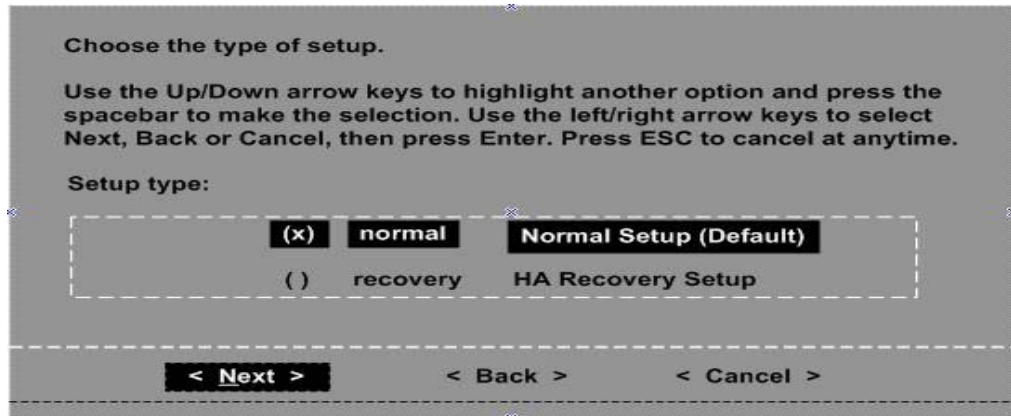
The End User License Agreement (EULA) appears.

**Step 4** 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.

You are now ready to choose your setup type. See [Choosing Your Type of Setup](#).

### Choosing Your Type of Setup

To choose your type of setup:



**Step 1** Choose one of the following options:

- If you are installing an appliance, using the up/down arrow keys, highlight **normal**, and then use the spacebar to select it.
- If you are recovering a failed primary HA system, using the up/down arrow keys, highlight **recovery**, and then use the spacebar to select it.

**Step 2** Press Enter to select **Next**.

Choose one of the following options:

- If you are recovering a failed primary HA QFlow host, see [Setting the Time and Date](#) (only perform [Step 4](#)).
- If you are recovering a primary STRM appliance, see [Setting the Time and Date](#).

## Specifying Your Secondary Device Type

To specify your secondary device type:

```

Choose if this system is a stand-by for console.

Use the Up/Down arrow keys to highlight another option and press the
spacebar to make the selection. Use the left/right arrow keys to
select Next, Back or Cancel, then press Enter. Press ESC to cancel at
anytime.

Is This System A Stand-By For Console?

(*)  yes  This system is a stand-by for console.
( )   no  This system is a stand-by for non-console.

< Next >      < Back >      < Cancel >

```



*This step is only required if you are installing a secondary appliance.*

**Step 1** Choose one of the following options:

- If you are installing a secondary device for a Console, using the up/down arrow keys, highlight **This system is a stand-by for a console**, and then use the spacebar to select the option.
- If you are not installing a secondary device for a Console, using the up/down arrow keys, highlight **This system is a stand-by for a non-console**, and then use the spacebar to select the option.

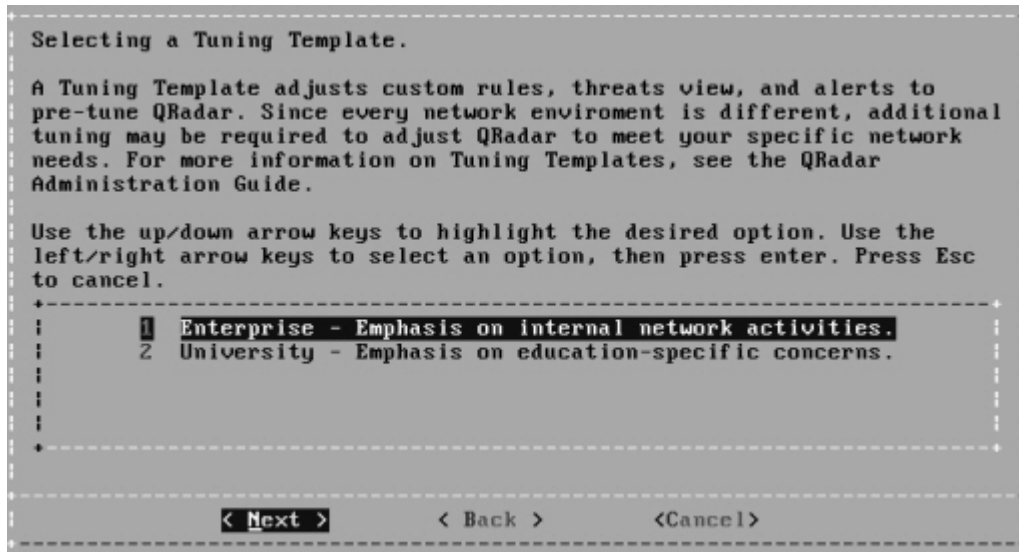
**Step 2** Press Enter to select **Next**.

Choose one of the following options:

- If you are installing or recovering a secondary device for a Console, see [Setting the Time and Date](#).
- If you are installing or recovering a secondary device for a non-Console, see [Setting the Time and Date](#) (only perform [Step 4](#)).

### Selecting a Tuning Template

To select a tuning template:



**Step 1** Using the up/down arrow keys, select one of the following tuning templates:

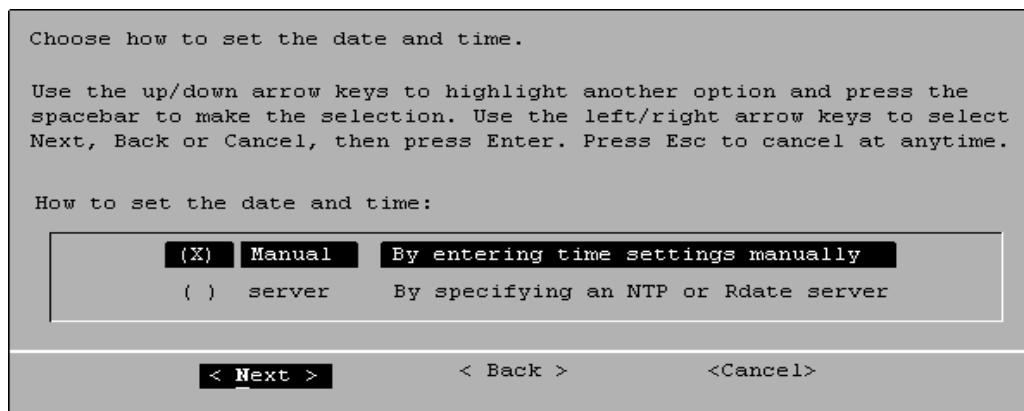
- **Enterprise** - Tunes properties for internal network activity.
- **University** - Tunes properties for education-specific concerns.

**Step 2** Press Enter to select **Next**.

Now you are ready to set the time and date. See [Setting the Time and Date](#).

### Setting the Time and Date

To set the time and date:



**Step 1** 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 [Step 2](#).

- **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 3](#).

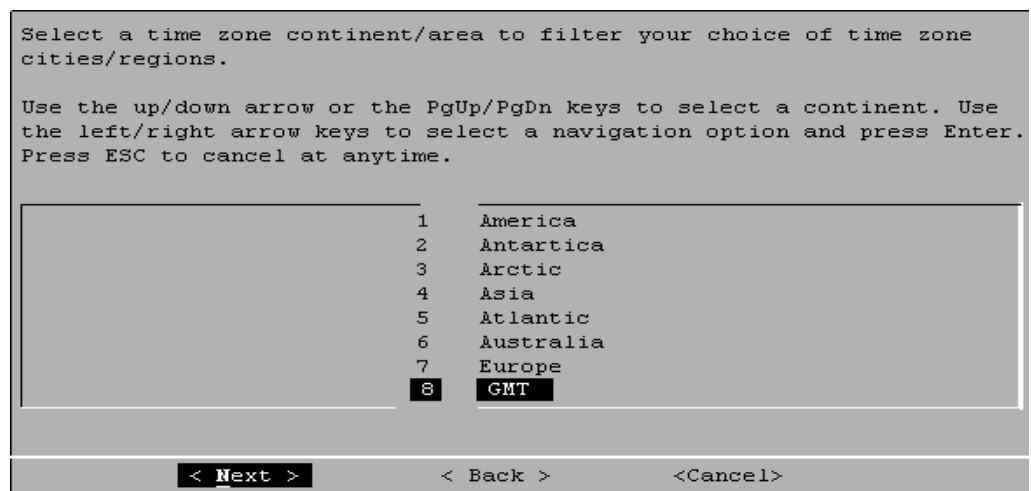
**Step 2** To manually enter the time and date:

- Enter the current date and time.
- Using the Tab key, select **Next**. Press Enter.
- Go to [Step 4](#).

**Step 3** To specify a time server:

- In the text field, enter the time server name or IP address.
- Using the Tab key, select **Next**. Press Enter.

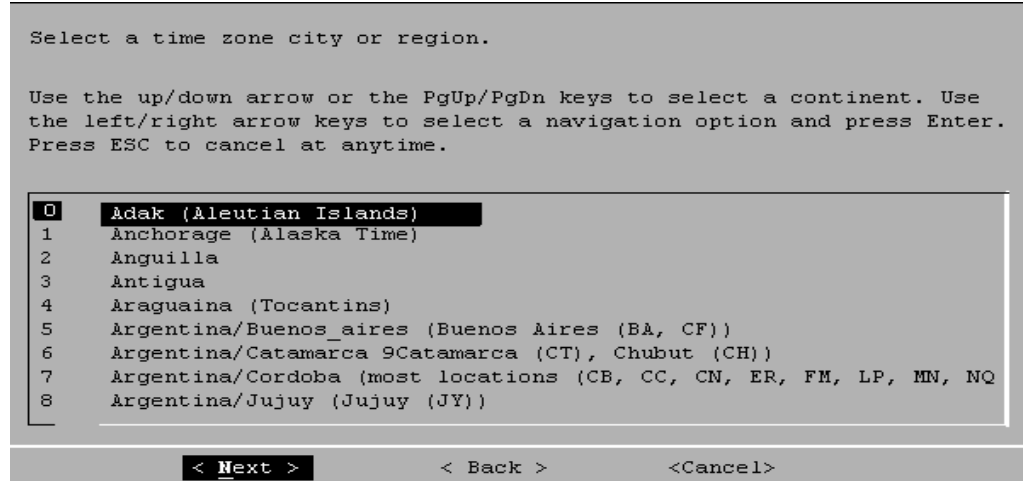
The Time Zone Continent window appears:



**Step 4** To select the time zone continent:

- Using the up/down arrow keys, or the page up/page down keys, select your time zone continent or area.
- Press Enter to select **Next**.

The Time Zone Region window appears.



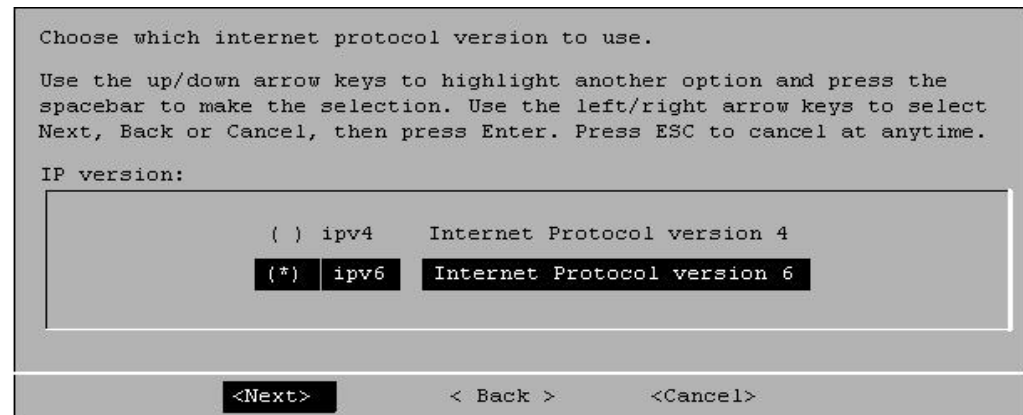
**Note:** The options that appear in this window are regions that are associated with the continent or area previously selected.

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

You are now ready to choose your Internet protocol. See [Configuring Your Internet Protocol](#).

## Configuring Your Internet Protocol

To configure your Internet protocol:



**Step 1** To select the Internet protocol:

- a Using the up/down arrow keys, and then the spacebar, select one of the following options:
  - IPv4
  - IPv6



**Note:** IPv6 is not supported in an HA environment. If you are installing software or an appliance with an HA activation key and you select the IPv6 option, an error

message appears. In this case, select **Back** and then select **IPv4**. You can then proceed to next procedure in your installation.

b Press Enter to select **Next**.

The Management Interface window appears:

```
Specify which is the management interface. If the interface has a link
(cable connected), a plus (+) is displayed before the description.
Use the Up/Down arrow keys to highlight another option and press the
spacebar to make the selection. Use the left/right arrow keys to
select Next, Back or Cancel, then press Enter. Press ESC to cancel at
anytime.
Select management interface:

(*) eth0 +Ethernet Hwaddr 00:30:48:DO:14:02
( ) eth1 Ethernet Hwaddr 00:30:48:DO:14:03
( ) eth0 IPv6-in-IPv4

< Next >      < Back >      < Cancel >
```

**Step 2** Using the up/down arrow keys, highlight the interface you want to specify as the management interface and press the spacebar to select it.

The plus (+) symbol indicates which interfaces have physical links.



**Note:** If you are installing a secondary system, you must specify the same management interface specified as the primary host. For example, if the primary host uses `ETH0` as the management interface, the secondary host must also use `ETH0`.

**Step 3** Press Enter to select **Next**.

**Step 4** Choose one of the following options:

- If you are recovering an Primary HA host, see [Configuring Your Cluster Virtual IP Address](#).
- If you are using IPv6 as your Internet protocol, see [Configuring IPv6](#).
- If you are using IPv4 as your Internet protocol, see [Configuring STRM Network Settings](#).

**Configuring IPv6** To configure IPv6:

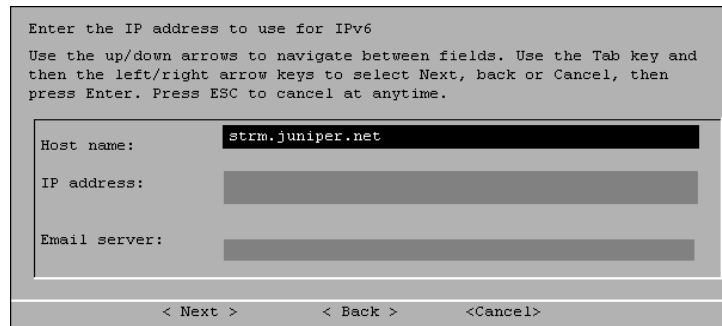
```
System can now try to use autoconfigure to
obtain an IP Address.

Do you want to use autoconfigure for IPv6?

< Yes >      < No >
```

**Step 1** Choose one of the following options:

- a To automatically configure for IPv6, select **Yes**. Press Enter. The automatic configuration can take an extended period of time. When the automatic configuration is complete, the Specify a management interface window appears. Go to [Configuring STRM Network Settings](#).
- b To manually configure for IPv6, select **No**. Press Enter. Go to [Step 2](#).  
The Enter the IP address to use for IPv6 window appears.



**Step 2** To enter the IP address to use for IPv6:

- a Enter the values for the **Hostname**, **IP Address**, and **Email server**.
- b Using the Tab key, select **Next**. Press Enter.

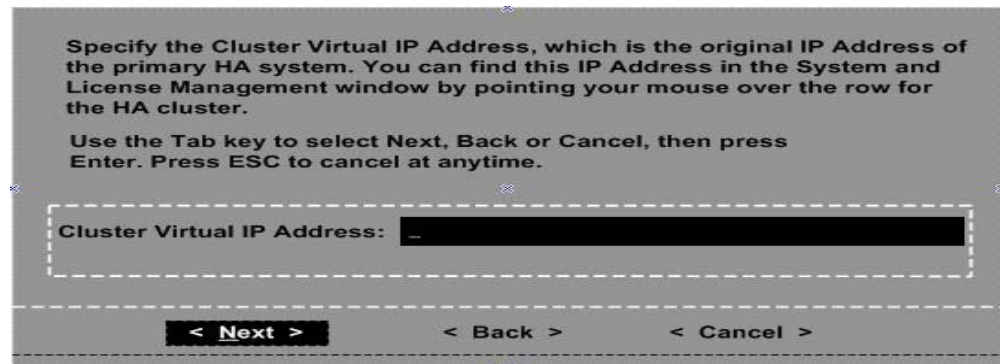
You are now ready to configure your network settings. See [Configuring STRM Network Settings](#).

### Configuring Your Cluster Virtual IP Address

To configure your Cluster Virtual IP address:



**Note:** This step is only required if you are recovering a failed HA host.



**Step 1** Enter the Cluster Virtual IP address.

The Cluster Virtual IP address is the original IP address of the primary HA system. You can find this IP address in the System and License Management window by pointing your mouse over the row for the HA cluster.

**Step 2** Press Enter to select **Next**.

Choose one of the following options:

- If you are using IPv4 as your Internet protocol, see [Configuring STRM Network Settings](#).
- If you are using IPv6 as your Internet protocol, see [Configuring IPv6](#).

## Configuring STRM Network Settings

To configure the STRM network settings:

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>

To configure the STRM network settings:

**Step 1** 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.



**Note:** If you are recovering an HA appliance, the IP address is the Primary HA IP address, which you can identify in the System and License Management window by pointing your mouse over the row for the HA cluster. For more information on managing HA, see the STRM Administration Guide - Managing High Availability.

- **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 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. 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.

**Step 2** Use the Tab key to move to the **Next** option. Press Enter.



**Note:** If you are changing network settings using *qchange\_netsetup*, use the Tab key to move the Finish option and press Enter. See [Appendix A Changing Network Settings](#).

You are now ready to configure your root password and finish the installation. See [Configuring the STRM Root Password](#).

### Configuring the STRM Root Password

To configure the STRM root password:

```

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> ]
    
```

To configure the STRM root password:

**Step 1** Enter your password.

**Step 2** Use the Tab key to move to the **Next** option. Press Enter.

The Confirm New Root Password window appears.

```

Confirm New Root Password.

Re-register 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> ]
    
```

**Step 3** Re-enter your new password to confirm.

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

A series of messages appear as STRM continues with the installation. This process typically takes several minutes.

The Configuration is Complete window appears.

**Step 5** Press Enter to select **OK**.

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

---

## Accessing STRM

To access the STRM interface:

**Step 1** Open your web browser.

**Step 2** Log in to STRM:

`https://<IP Address>`

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

Username: **admin**

Password: **<root password>**

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

For your STRM Console, a default key provides you access to STRM for five weeks. For more information on the license key, see the *STRM 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](#)



**Caution:** Changing the network settings of a host in an HA cluster causes HA to cease functioning on the cluster. If you want to change the network settings of a host in an HA cluster, you must first remove the host from the cluster, make your changes, and then re-add the host to the cluster.

---

### 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 components, including the Admin interface, installed on one system.

To change the settings on the STRM 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
```
- Step 3** Configure your Internet protocol. See [Configuring Your Internet Protocol](#).
- Step 4** Configure the STRM network settings. See [Configuring STRM Network Settings](#).
- Step 5** Use the Tab key to navigate to the **Finish** option. Press Enter.

A series of messages appear as STRM processes the requested changes. After the requested changes are processed, the STRM system is automatically shutdown 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 Administration Guide.

## Removing Non-Console Managed Hosts

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

**Step 1** Log in to STRM:

`https://<IP Address>`

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

Username: **admin**

Password: **<admin password>**

**Step 2** In the main STRM interface, click the **Admin** tab.

The Admin interface appears.

**Step 3** Click the **Deployment Editor** 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** Click **Save**.

**Step 8** Close the deployment editor.

**Step 9** From the Admin interface, click **Deploy Changes**.

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
```

- Step 3** Configure your Internet protocol. See [Configuring Your Internet Protocol](#).
- Step 4** Configure the STRM network settings. See [Configuring STRM Network Settings](#).
- Step 5** Use the Tab key to move to the **Finish** option. Press Enter.

A series of messages appear as STRM processes the requested changes. After the requested changes are processed, the STRM system is automatically shutdown 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:
  - `https://<IP Address>`
  - Where `<IP Address>` is the IP address of the STRM system.
  - Username: **admin**
  - Password: **<admin password>**
- Step 2** In the main STRM Interface, click the **Admin** tab.
  - The Admin interface appears.
- Step 3** Click the **Deployment Edit** icon.
  - The deployment editor appears.
- Step 4** Click the **System View** tab.
- Step 5** From the menu, select **Actions > Add a managed host**.
  - The Add a new host wizard appears.
- Step 6** Click **Next**.
  - The Enter the host's IP window appears.
- Step 7** 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 8** Click **Next**.
- Step 9** Click **Finish**.
- Step 10** Re-assign all components to your non-Console managed host.
  - a In the STRM 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 the **Select a host** drop-down list box, select the host you want to re-assign to this component. Click **Next**.
- e Click **Finish**.

**Step 11** Repeat for each non-Console managed host until all hosts are re-added and re-assigned.

**Step 12** Close the deployment editor.

**Step 13** From the Admin interface, click **Deploy 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 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:

`https://<IP Address>`

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

Username: **admin**

Password: **<admin password>**

**Step 2** In the main STRM Interface, click the **Admin** tab.

The Admin interface appears.

**Step 3** Click the **Deployment Editor** 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** Close the deployment editor.
- Step 8** From the Admin interface, click **Deploy Changes**.  
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`
- Step 3** Configure your Internet protocol. See [Configuring Your Internet Protocol](#).
- Step 4** Configure the STRM network settings. See [Configuring STRM Network Settings](#).
- Step 5** Use the Tab key to move to the **Finish** option. Press Enter.  
A series of messages appear as STRM processes the requested changes. After the requested changes are processed, the STRM 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:  
`https://<IP Address>`  
Where `<IP Address>` is the IP address of the STRM system.  
Username: **admin**  
Password: **<admin password>**
- Step 2** In the main STRM Interface, click the **Admin tab**.  
The Admin interface appears.
- Step 3** Click the **Deployment Editor** icon.  
The deployment editor appears.
- Step 4** Click the **System View** tab.
- Step 5** From the menu, select **Actions > Add a managed host**.  
The Add a new host wizard appears.
- Step 6** Click **Next**.  
The Enter the host's IP window appears.

**Step 7** 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 8** Click **Next**.

**Step 9** Click **Finish**.

**Step 10** Re-assign all components to your non-Console managed host.

- a In the STRM 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 11** Close the deployment editor.

**Step 12** From the Admin interface, click **Deploy Changes**.

The changes are deployed.

# 3

## RE-INSTALLING STRM

This appendix provides information about re-installing STRM software from the recovery partition. When you re-install STRM, your system will be restored back to factory default configuration, meaning that your current configuration and data files will be overwritten.



**Note:** *This appendix only applies to fresh STRM 2009.1 installations or upgrades from fresh STRM 2008.3 installations. This appendix includes:*

- [About the Recovery Partition](#)
- [Re-installing STRM](#)

---

### About the Recovery Partition

When you install STRM 2009.2, the installer (ISO) is copied into the recovery partition. From this partition, you can re-install STRM, which restores STRM to factory defaults.



**Note:** *Any software upgrades you perform after you install STRM 2009.1 will replace the ISO file with newer version.*

Whenever you reboot your STRM appliance, you will be presented with the option to re-install the software. If you do not respond to the prompt after 5 seconds, the system will reboot as normal, thus maintaining your configuration and data files. If you choose the re-install STRM, a warning message appears and you must confirm that you want to re-install STRM. After confirmation, the installer is run and you can follow the prompts through the installation process.



**Note:** *After a hard disk failure, you will be unable to re-install from the recovery partition, because it will no longer be available. If you experience a hard disk failure, contact Customer Support for assistance.*

---

**Re-installing STRM**

This section includes:

- [Preparing for Re-installation](#)
- [Re-installing on a STRM Appliance](#)
- [Re-installing on a QFlow Appliance](#)

**Preparing for Re-installation**

To prepare for re-installation:

**Step 1** Reboot your STRM appliance.

A menu appears with the following options:

- Normal System - Starts STRM as normal.
- Factory re-install - Runs the installer.

**Step 2** Select **Factory re-install**.

The installer runs and detects that there is already an installation present.

**Step 3** Enter `flatten` to continue.

The installer repartitions and reformats the hard disk, installs the OS, and then re-installs STRM. Wait for the flatten process to complete. This process can take up to several minutes, depending on your system. When the process is complete, the following appears:

```
OK: qsetup is completed.
```

```
Type HALT to shutdown or SETUP to login and configure system
```

**Step 4** Enter `SETUP`.

**Step 5** Log in to STRM as root.

**Step 6** Press Enter.

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 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 key:

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



**Note:** If you do not have your activation key, contact the Welcome Center at [welcomecenter@q1labs.com](mailto:welcomecenter@q1labs.com) with the serial number of the STRM appliance. Software activation keys do not require serial numbers.

**Step 8** Enter your activation key and press Enter.



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

If you are setting up a STRM appliance, such as a STRM 2100, the Tuning Template window appears. Go to [Re-installing on a STRM Appliance](#).

If you are setting up a QFlow Collector appliance, such as a QFlow 1101, the Time Zone Continent window appears. Go to [Re-installing on a QFlow Appliance](#).

### Re-installing on a STRM Appliance

To re-install on a STRM appliance:

- Step 1** Select a tuning template. See [Selecting a Tuning Template](#).
- Step 2** Set the time and date. See [Setting the Time and Date](#).
- Step 3** Configure your Internet protocol. See [Configuring Your Internet Protocol](#).
- Step 4** Configure your network settings. See [Configuring STRM Network Settings](#).
- Step 5** Configure the root password. See [Configuring the STRM Root Password](#).
- Step 6** Use the Tab key to move to the **Finish** option. Press Enter.

A series of messages appear as STRM continues with the installation. This process typically takes several minutes.

The Configuration is Complete window appears.



- Step 7** Press Enter to select **OK**.  
You are now ready to access STRM.

### Re-installing on a QFlow Appliance

To re-install on a QFlow appliance:

- Step 1** Set the time and date. [Setting the Time and Date](#) ( [Step 4](#) )
- Step 2** Select a tuning template. See [Selecting a Tuning Template](#).
- Step 3** Set the time and date. See [Setting the Time and Date](#).
- Step 4** Configure your Internet protocol. See [Configuring Your Internet Protocol](#).
- Step 5** Configure your network settings. See [Configuring STRM Network Settings](#).
- Step 6** Configure the root password. See [Configuring the STRM Root Password](#).
- Step 7** Use the Tab key to navigate to the **Finish** option. Press Enter.

A series of messages appear as STRM continues with the installation. This process typically takes several minutes.

The Configuration is Complete window appears.



**Step 8** Press Enter to select **OK**.

You are now ready to access STRM.

# INDEX

---

## A

about this guide 1  
appliances  
    setting-up 14

---

## B

browser support 6

---

## C

Classification Engine  
    definition 4  
Console  
    definition 4  
conventions 1

---

## E

Event Collector  
    definition 4  
Event Processor  
    definition 4

---

## F

Flow Processor  
    definition 4  
Flow Writer  
    definition 4

---

## H

hardware requirements 6  
high availability  
    example of deployment 6

---

## I

installation procedures 13  
    choosing your type of setup 14  
    configuring IPv6 20  
    configuring STRM network settings 22  
    configuring the STRM root password 23  
    configuring your cluster virtual IP address 21  
    configuring your internet protocol 19  
    preparing your STRM appliance 14  
    selecting a template 17  
    setting the time and date 17  
    specifying your secondary device type 16  
installing

    preparing 3  
installing STRM 11

---

## M

Magistrate  
    definition 5

---

## N

network hierarchy  
    preparing 7  
network settings  
    all-in-one Console 25  
    changing 25  
    Console in a multi-system deployment 26  
    identifying 7  
    non-Console in a multi-system deployment 28

---

## P

preparing  
    installation 3  
preparing your network hierarchy 7

---

## R

recovery partition 31  
re-installing STRM 31  
requirements  
    hardware 6  
    software 6  
Resolution module  
    definition 4

---

## S

security monitoring devices  
    identifying 8  
software requirements 6

---

## U

Update Daemon  
    definition 4  
using this document 11

