



Security Threat Response Manager

STRM Installation Guide

Release 2008.2 R2

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 530-027290-01, Revision 1

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 2008.2 R2

Copyright © 2008, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Revision History

September 2008—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 4
- Additional Hardware Requirements 6
- Additional Software Requirements 6
- Browser Support 6
- Preparing Your Network Hierarchy 6
- Identifying Network Settings 7
- Identifying Security Monitoring Devices and Flow Data Sources 8
- Identifying Network Assets 9

2 INSTALLING STRM

- Setting Up Appliances 11
- Installing STRM Using Red Hat Enterprise 4.6 16
- Installing Japanese Support 21
- Accessing STRM 22

A SETTING UP RED HAT ENTERPRISE

- Before You Begin 23
- Configuring Network Parameters 24
- Configuring Firewall Configuration 24
- Configuring Disk Partitions 24
- Installing Red Hat Enterprise 4
Update 6 25
- Customizing Red Hat Upgrades 26

B CHANGING NETWORK SETTINGS

- Changing Network Settings in an All-in-One Console 27
- Changing the Network Settings of a Console in a Multi-System Deployment 28
- Changing the Network Settings of a Non-Console in a Multi-System Deployment 31

INDEX




ABOUT THIS GUIDE

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

Conventions

[Table 1](#) 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 Qmmunity web site at <https://support@juniper.net/>. Once you access the Qmmunity 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:

documentation@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:

- Log a support request 24/7: <https://support@juniper.net>
For access to the Qmmunity web site, please contact Customer Support.

2 ABOUT THIS GUIDE

- Access Qmmunity and Self-Service support using e-mail: support@juniper.net
- Telephone assistance: 1.866.377.7000.

1

PREPARING FOR YOUR INSTALLATION

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

- [Deploying STRM](#)
- [Additional Hardware Requirements](#)
- [Additional Software Requirements](#)
- [Browser Support](#)
- [Preparing Your Network Hierarchy](#)
- [Identifying Network Settings](#)
- [Identifying Security Monitoring Devices and Flow Data Sources](#)
- [Identifying Network Assets](#)

Your STRM deployment may consist of STRM installed on one or multiple systems. You can use the STRM three-tier architecture to install any or all components on a single server for small enterprises or distributed across multiple servers for maximum performance and scalability in large enterprise environments.

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

Deploying STRM

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

- [STRM Components](#)

A STRM appliance includes STRM software and a CentOS-4 operating system. For further information on STRM appliances, see the *Hardware Installation Guide*.

STRM Components

STRM components that may 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 appliances.
- **Flow Processor** - Normalizes flows sent from one or more QFlow Collector(s) by consolidating, aggregating, and removing duplicate flows. The QFlow Collector can also create *superflows* (aggregate 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 interface for STRM. The Console provides real time views, reports, alerts, and in-depth flow views of network traffic and security threats. This Console is also used to manage distributed STRM deployments.
The Console is accessed from a standard web browser. When you access the system, a prompt appears for a user name and password, which must be configured during the installation process. You must also have Java installed. For information on software requirements, see [Additional Software Requirements](#).
- **Update Daemon** - Stores the database and TopN data. Typically, the Update Daemon is installed on the Console.
- **Flow Writer** - Stores the flow and asset profile data.
- **Offense Resolution** - Offense Resolution is a module that 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 sends the information to the Event Processor. Before being sent 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 creates the bundles.

- **Event Processor** - Processes events collected from one or more Event Collector(s). Once received, the Event Processor correlates the information from STRM and distributes to the appropriate area, depending on the type of event. The Event Processor also includes information gathered by STRM to indicate any behavioral changes or policy violations for the event. Rules are applied to the events that allow the Event Processor to process 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 no custom rules exist, the Magistrate uses the 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.

Additional Hardware Requirements

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

- Monitor and keyboard or a serial console
- 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 storing 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 1.5.0_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 interface. STRM supports the following web browsers:

- Microsoft Internet Explorer 6.0/7.0
- Firefox 2.0

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.

Once you define the components you wish to add to your network hierarchy and install STRM, you can then configure the network hierarchy using the STRM interface. For each component you wish to add to your network hierarchy, use the following table to indicate each component in your network map.

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

- Internal/external Demilitarized zone (DMZ)
- 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

Table 1-1 Network Hierarchy

Description	Name	IP/CIDR Value	Weight

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

Identifying Network Settings

Before you install STRM, you must have the following information for each system you wish to install:

- Hostname
- IP address
- Network Mask address
- Subnet Mask
- Default Gateway
- Primary DNS Server
- Secondary DNS Server (Optional)
- Public IP address for networks using Network Address Translation (NAT)

- E-mail Server
- NTP Server (Console only) or Time server

Identifying Security Monitoring Devices and Flow Data Sources

STRM can collect and correlate events received from external sources such as security equipment (for example, firewalls, VPNs, or IDSs) and host or application security logs, such as, window logs. Device Support Modules (DSMs) and QFlow Collectors allows you to integrate STRM with this external data.

STRM automatically discovers sensor devices that are sending syslog messages to an Event Collector. Any sensor devices that are automatically discovered by STRM appear in the Sensor Devices window within the STRM Administration Console. For more information, see Chapter 4 Using the Deployment Editor of the *STRM Administration Guide*.

Non-syslog based information sources must be added to your deployment manually. For more information, see the *Managing Sensor Devices Guide*. For each device you wish to add to your deployment, record the device in [Table 1-2](#).

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:

- **Link Speed & Type** indicates the maximum network link (in Kbps) for firewall, router, and VPN devices. Record the primary application of the host system, for example, e-mail, anti-virus, domain controller, or a workstation.
- **Msg Level** indicates the message level you wish to log. For example, critical, informational, debug.
- **No. of Users** indicates the maximum number of hosts/users using or being served by this device.
- **Network Location** indicates whether this device is located on the Internet DMZ, Intranet, or Extranet DMZ.
- **Geographic Location** indicates if the device is located on the same LAN as STRM or sending logs over the WAN identified in the Link Speed & Type column.

- **Credibility** indicates the integrity of an event or offense as determined by the credibility rating from source devices. Credibility increases as multiple sources report the same event.

Identifying Network Assets

STRM can learn about your network and server infrastructure based on flow data. The Server Discovery function uses STRM's Asset Profile database to discover many types of servers.

Defining certain additional server and IP address types also improves tuning results. [Table 1-3](#) provides a list of possible servers. When identified, see the *STRM Users Guide* for information on defining servers within STRM. If your network includes a large number of servers, you can use CIDR or IP subnet addresses within the server networks category.

Table 1-3 Asset Identification

Server	IP Address(es)	QTY	Name
NAT Address Range			
Vulnerability Scanners			
Network Management Servers			
Proxy Servers			
Virus Definition and Other Update Servers			
Windows Server Networks, such as, domain controllers or exchange servers			

2

INSTALLING STRM

This chapter provides information on installing your STRM system using one of the following options:

- [Setting Up Appliances](#)
- [Installing Japanese Support](#)
- [Installing STRM Using Red Hat Enterprise 4.6](#)
- [Accessing STRM](#)

Setting Up Appliances

A STRM appliance includes STRM software and a CentOS-4 operating system. This section provides information on setting up your appliance. For more information on appliances see the *Hardware Installation Guide*.

To set-up your appliance:

Step 1 Install all necessary hardware.

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

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:

Username: **root**

Password: **password**



Note: The username and password are case sensitive.

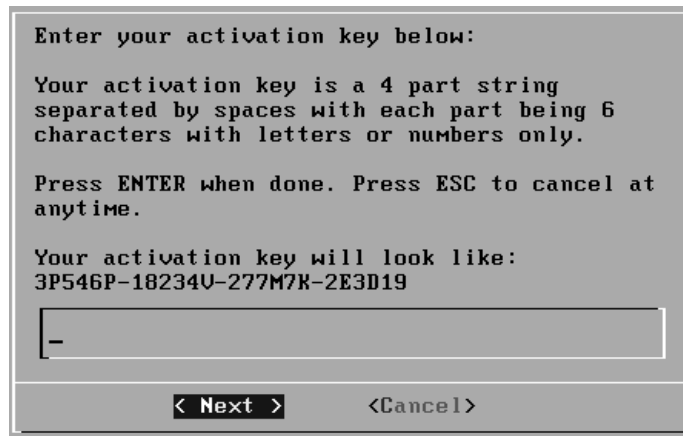
Step 4 Press **Enter**.

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, 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. The letter l and the number 1 (one) are treated the same, as are the letter O and the number 0 (zero). You can find the 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.

If you are setting up a STRM appliance, such as a STRM 2100, the Tuning Template window appears. Go to [Step 7](#).

If you are setting up a QFlow appliance, such as a QFlow 1101, the Time Zone Continent window appears. Go to [Step 11](#).

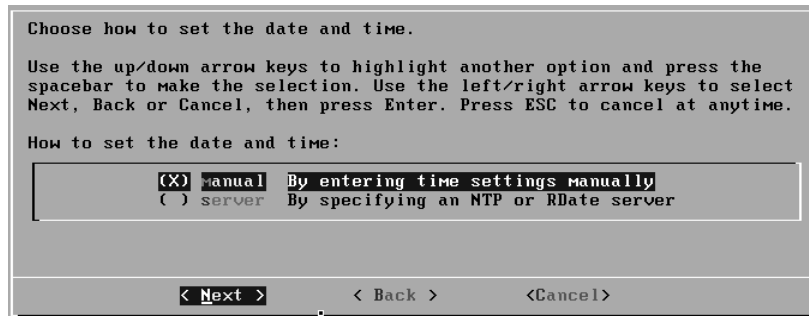
- Step 7** To select a tuning template:

- 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.
 - **ISP** - Tunes properties for Internet Service Provider (ISP) concerns.



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

- Using the left/right arrow keys, select Set Template. Press **Enter**.
The Set the Date and Time window appears.



Step 8 Using the up/down arrow keys, highlight the method you wish to use to set the date and time, 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 9](#).
- **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 10](#).

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 11](#).

Step 10 To specify a time server:

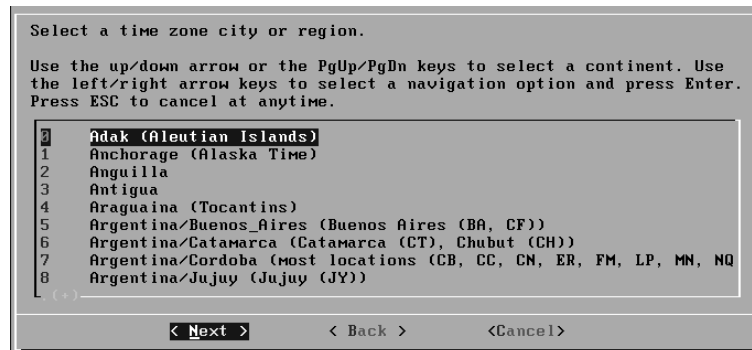
- a In the text field, enter the time server name or IP address.
- b Using the left/right arrow keys, select Next. Press **Enter**.
The Time Zone Continent window appears.



Step 11 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 Configure STRM window appears.

Step 12 To configure the STRM 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 email server. If you do not have an email 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 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 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. For more information, see [Accessing STRM](#).

Installing STRM Using Red Hat Enterprise 4.6

To install STRM when using Red Hat Enterprise 4 Update 6 on your own hardware:



Note: For information on setting up Red Hat Enterprise for use with STRM, see [Appendix A Setting Up Red Hat Enterprise](#).

- Step 1** Install all necessary hardware.
- Step 2** Install Red Hat Enterprise. See [Setting Up Red Hat Enterprise](#).
- Step 3** Obtain the STRM software and copy to a CD.



Note: To download the software from the Qmmunity web site, see <https://support@juniper.net/>. For access to the Qmmunity web site, please contact Customer Support.

Step 4 Place the STRM CD in the CD drive.

Step 5 Login as root.

Step 6 Mount the CD drive and change the CD content location:

```
mount /media/cdrom  
cd /media/cdrom
```

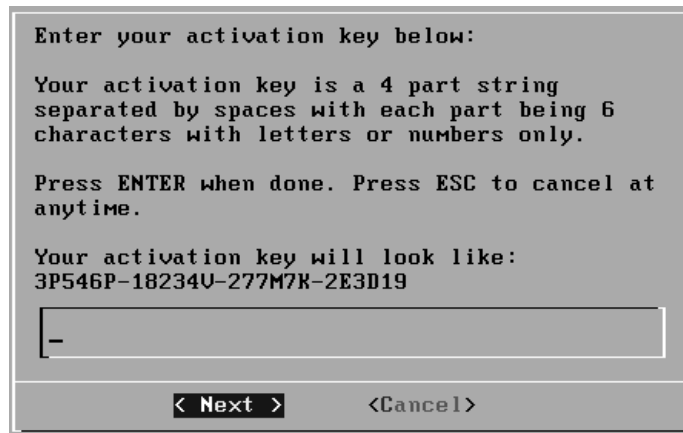
Step 7 Begin the installation:

```
./setup
```

The End User License Agreement (EULA) appears.

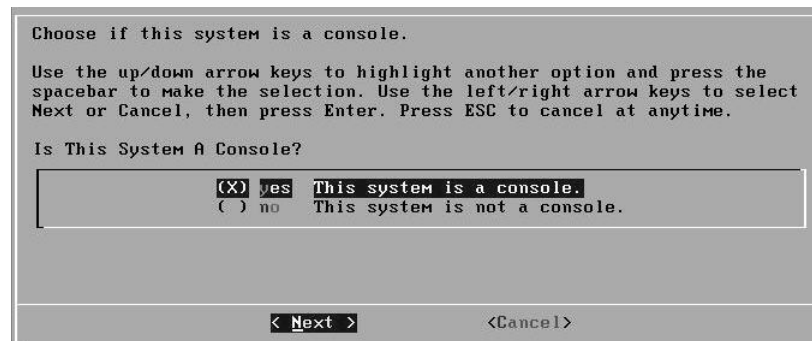
Step 8 Read the information in the window. Press the **Spacebar** to advance each window until you have reached the end of the document. Type **yes** to accept the agreement, then press **Enter**.

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. The letter l and the number 1 (one) are treated the same, as are the letter O and the number 0 (zero). You can find the activation key included with the packing slip.



Step 9 Enter your activation key.

A series of messages appear as STRM continues with the installation. This process typically takes several minutes. The System Console window appears.



Step 10 Using the up/down arrow keys, highlight one of the following options and use the spacebar to select that option:

- **Yes** - Select this option only if this system is a Console. If you select this option, the Tuning Template window appears. Go to [Step 11](#).
- **No** - Select this option only if this system is not a Console. If you select this option the Time Zone Continent window appears. Go to [Step 16](#).



Note: To select the desired option, make sure you highlight the option and press the spacebar to place an X in the parentheses.

Step 11 To select a tuning template:

- a Using the up/down arrow keys, select one of the following:
 - **Enterprise** - Tunes properties for internal network activity.
 - **ISP** - Tunes properties for Internet Service Provider (ISP) concerns.
 - **University** - Tunes properties for education specific concerns.



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

- b Using the left/right arrow keys, select Set Template. Press **Enter**.
The Set Time and Date window appears.



Step 12 Using the up/down arrow keys, highlight the method you wish to use to set the time and date, 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 14](#).

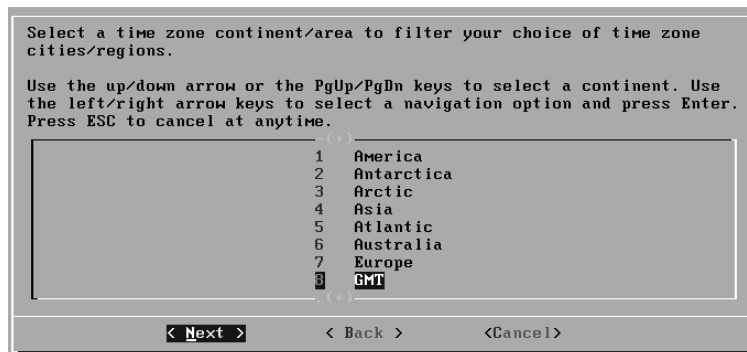
- **Server** - Allows you to specify your time server. Use the Tab key to select the Next option. Press **Enter**. The Enter Time Server window appears. Go to [Step 15](#).

Step 13 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 16](#).

Step 14 To specify a time server:

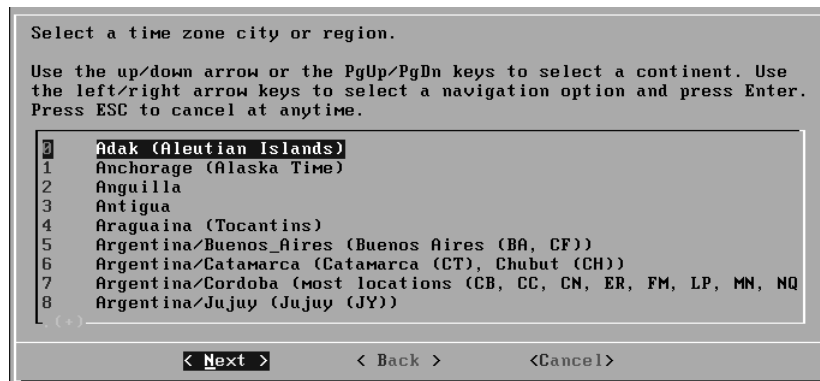
- a In the text field, enter the time server name or IP address.
- b Using the left/right arrow keys, select Next. Press **Enter**.
The Time Zone Continent window appears.



Step 15 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 relevant to 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 Configure STRM window appears.

Step 16 To configure the STRM 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 email server. If you do not have an email 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 17 To configure your STRM 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 continues with the installation. This process typically takes several minutes. The Configuration is Complete window appears.

Step 18 Press **Enter**.

The shell prompt appears.

Step 19 Unmount the CD:

```
cd /opt/qradar/conf
umount /media/cdrom
eject
```

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

Installing Japanese Support

You can install a separate plug-in to provide Japanese character support in the STRM Reports interface. Once you install the plug-in located on the Qmmunity

web site, your Report templates will be replaced to ensure that the appropriate font and characters appear in the Reports interface.



Note: To display reports in PDF format, Adobe Acrobat may require the installation of a Japanese plug-in to view your reports. For more information, see your Adobe documentation.

This section provides information on installing the plug-in for your STRM system including:

- [Installing Plug-In on an Appliance](#)
- [Installing Plug-In on a System Running Red Hat Enterprise](#)

Installing Plug-In on an Appliance

To install the Japanese plug-in on a STRM appliance:

- Step 1** Set-up STRM.
- Step 2** Go to the Qmmunity web site to download the plug-in:
`https://support@juniper.net`
- Step 3** Install the plug-in:
`rpm -Uvh <path to RPM>/japanese-support-6.1.3-<build>_ctrh.i386.rpm`

Installing Plug-In on a System Running Red Hat Enterprise

To install the Japanese plug-in on a STRM system running Red Hat Enterprise:

- Step 1** Install STRM.
- Step 2** Insert your STRM CD.
- Step 3** Mount the CD:
`mount /media/cdrom`
- Step 4** Install the plug-in:
`rpm -Uvh /media/cdrom/qradar/japanese-support-6.1.3-<build>_ctrh.i386.rpm`

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.

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

SETTING UP RED HAT ENTERPRISE

STRM supports the 32-bit version of Red Hat Enterprise 4 Update 6. This appendix provides information on setting up Red Hat Enterprise including:

- [Before You Begin](#)
- [Configuring Network Parameters](#)
- [Configuring Firewall Configuration](#)
- [Configuring Disk Partitions](#)



Note: For further information on hardware requirements for your STRM installation, see the *Hardware Installation Guide*. We recommend that your system hardware used for a Red Hat Enterprise 4 Update 6 installation correspond to the requirements outlined in the *Hardware Installation Guide* for appliances.

Before You Begin

Before you install Red Hat Enterprise 4 Update 6, note the following:

- You must use the 32-bit version of Red Hat Enterprise 4 Update 6. Using another version causes the installation process to fail.
- When installing Red Hat Enterprise, you must use the **Minimal** install option and set the SELinux option to **Disabled**.



Note: To access the **Minimal** install option, select the **Customize Software Packages to be Installed** option and scroll to the bottom of the menu.

- STRM does not support KickStart disks, using these disks may cause the application to install improperly.
- If you wish to use NTP as your time server, make sure you install the NTP package. For more information, see your Red Hat documentation.
- For non-Console systems, make sure all systems include a minimum of 100 GB drives.
- For Console systems, make sure the primary drive includes a minimum of 500 GB drive with RAID for storage.

For more information on Red Hat Enterprise installation, see your Red Hat documentation.



CAUTION: *If the hardware on which you wish to install STRM includes Red Hat Enterprise 4 Update 6, you must re-install Red Hat Enterprise from the CD using the minimal package option. The default Red Hat Enterprise 4 Update 6 installation does not have the appropriate options selected.*

Configuring Network Parameters

The access (management) interface must be eth0. You must configure this interface with the access information for the network. You must use a static IP address for your STRM systems.

Configuring Firewall Configuration

The firewall configuration must allow WWW (http, https) and SSH traffic. Prior to configuring the firewall, disable the SELinux option.

During the STRM installation, a default firewall template is installed, which you can update using the web-based system administration interface.

Configuring Disk Partitions

During the installation process, you must configure several disk partitions, typically Disk 1.

You must configure your deployment partitions before installing the STRM application. For all deployments, configure the following partitions:



Note: *Make sure all EXT3 file systems are mounted as noatime.*

- **/boot** - System boot files should typically be 1G. Select a file system type of **EXT3** and the **forced to be primary** option.
- **swap** - Must be 8 GB. Choose **swap** as your file system type and leave the mount point empty. Also, select the **forced to be primary** option.
- **/** - Enter "/" as the partition to indicate root. This is the install area for STRM, the operating system, and associated files. In a typical system this should be 30 GB. However, if you have a single disk in the system, you may choose the option to expand the disk to maximum allowable size. Select the file system type as **EXT3**.

We recommend that you configure the following partitions:

- **/store/tmp** - This partition, which stores STRM temporary files, should be 10 GB, depending on the size of your primary disk. Select the file system type as **EXT3**.
- **/var/log** - This partition, which stores STRM and system log files, should be 20 GB, depending on the size of your primary disk. Select the file system type as **EXT3**.
- **/store** - This partition should contain the remaining disk space.



Note: *For assistance creating disk partitions, contact your system administrator. If an error appears during the creation of software RAID partitions, contact Juniper Networks Customer Support.*

For multi-disk deployments only, configure the following partitions for the Console:

- **/store** as **RAID5** - Stores STRM data. Choose **EXT3** as the file system type.
- **FLOWLOGS** and **DB** are located in the **Store** partition. In a system with five drives, a suggested configuration includes:
 - **disk 1** - boot, swap, OS, STRM temporary files, and log files
 - **remaining disks** - RAID 5, mounted as /store



Note: Other STRM components do not require the storage partitions mentioned above.



Note: Make sure that your system includes at least Red Hat 4 Update 6. You must run `Up2Date` if your system is running a version earlier than Red Hat 4 Update 6 to ensure that you have the latest Red Hat Enterprise version. Also, make sure you configure your `Up2Date` to exclude the boost library and the kernel from the update process (see [Customizing Red Hat Upgrades](#)). For information on configuring `Up2Date`, see your Red Hat Enterprise documentation or for on-line help, enter `up2date --help`.

If you wish to install Red Hat 4 Update 6 on an appliance with a disk larger than 2 TB, see [Installing Red Hat Enterprise 4 Update 6](#).

You are now ready to install STRM.

Installing Red Hat Enterprise 4 Update 6

Red Hat Enterprise 4 Update 6 is not compatible with a disk larger than 2 TB. If you attempt to install Red Hat Enterprise 4 Update 6 on a system with a disk larger than 2 TB, Red Hat will not boot.

On some hardware systems, such as a Dell 2950, RAID 10 may cause the system to detect only one disk greater than 2 TB. If the boot drive (array) is over 2 TB, at the end of the installation process, when grub is installed, an error message appears and no boot loader is installed. You can install Red Hat 4 Update 6 on a disk larger than 2 TB by modifying grub before the system is rebooted.

To install Red Hat 4 Update 6 on a disk larger than 2 TB:

Step 1 Install Red Hat Enterprise 4 Update 6.

Step 2 When the Red Hat Installation is complete, press **Control-Alt-F2**.



Note: Do not click the Reboot button.

Step 3 Enter the following command:

```
fdisk -l /dev/sda
```

Values for the disk appear.

Step 4 Write down the values from the following line:

```
<x-value> heads, <y-value> sectors/track, <z-value> cylinders
```

Step 5 Enter the following command:

```
grub
```

The grub command line prompt appears.

Step 6 Enter the following command using the values recorded in [Step 4](#):

```
geometry (hd0) <x-value> heads, <y-value> sectors/track,
<z-value> cylinders
```

Step 7 Enter the following command:

```
root (hd0,0)
```

Step 8 Enter the following command:

```
setup (hd0)
```

Step 9 Enter the following command:

```
quit
```

Step 10 Press **Alt-F7**.

The Installation is complete screen appears.

Step 11 From the Installation is complete screen, click **Reboot**.

The installation completes.

Customizing Red Hat Upgrades

STRM installs both a customized version of boost and modules to support the Endace cards that are tied to a particular version of the kernel. If you upgrade Red Hat Enterprise, the wrong versions of boost and the kernel will be installed. To ensure that boost and the kernel function properly you must exclude them from upgrades and installations by configuring Up2Date.

To exclude kernel and boost from upgrades and installations:

Step 1 Enter the following command:

```
up2date --configure
```

A list of items that you can edit appears.

Step 2 Enter the pkgSkipList number, for example:

```
20
```

A prompt appears to enter values for the pkgSkipList.

Step 3 Enter the following command:

```
kernel*;boost*
```

Step 4 Enter the following command:

```
up2date -u
```

B

CHANGING NETWORK SETTINGS

This appendix provides information on changing network settings for the Console and non-Console systems when using Trustix or CentOS-4 operating systems in your deployment 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 components, including the Administration Console, 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
```

The Configure STRM window appears.

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.



Note: If you change the hostname and you are using Offense Resolution, we recommend you also update the Resolver Agent name, if a Resolver Agent is assigned to the host.

- **IP Address** - Specify the IP address of the system.
- **Netmask** - 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. 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 email server. If you do not have an email 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 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: `<root password>`

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

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

Step 3 Click the deployment editor icon.

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

Step 5 Select the managed host you wish 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**.

Step 8 Exit from the Administration Console.



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**.*

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.



Note: *If you change the hostname and you are using Offense Resolution, we recommend you also update the Resolver Agent name, if a Resolver Agent is assigned to the host.*


- **IP Address** - Specify the IP address of the system.
- **Netmask** - 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. 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 email server. If you do not have an email 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 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 and access the System View in the Deployment Editor, as defined in [Step 1, Removing Non-Console Managed Hosts](#).
Re-add managed host(s) to your deployment.
- Step 2** From the menu, select **Actions > Add a managed host**.
The Add a new host wizard appears.
- Step 3** Click **Next**.
The Enter the host's IP window appears.
- Step 4** Enter values for the parameters:
- **Enter the IP of the server or appliance to add** — Specify the IP address of the host you wish 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.
- Step 5** Click **Next**.
- Step 6** Click **Finish**.
- Step 7** Re-assign all components to your non-Console managed host.
- a In the STRM Deployment Editor, click the **Flow View** or **Event View** tab.
 - b Select the component you wish 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 wish to re-assign to this component. Click **Next**.
 - e Click **Finish**.
- Step 8** Repeat for each non-Console managed host until all hosts are re-added and re-assigned.
- Step 9** From the Administrative Console menu, select **Configurations > Deploy Configuration Changes**.
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: <root password>

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

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

Step 3 In the main STRM Interface, click **Config**.

Step 4 Click the deployment editor icon.

Step 5 Click the **System View** tab.

Step 6 Select the managed host you wish to delete.

Step 7 Use the right mouse button (right-click) to access the menu, select **Remove host**.

Step 8 From the Administrative Console menu, select **Configurations > Deploy Configuration Changes**.

Step 9 Exit from the Administration Console.



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**.

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.



Note: *If you change the hostname and you are using Offense Resolution, we recommend you also update the Resolver Agent name, if a Resolver Agent is assigned to the host.*

- **IP Address** - Specify the IP address of the system.
- **Netmask** - 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. 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 email server. If you do not have an email 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 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 and access the System View in the Deployment Editor, as defined in [Step 1, Removing the Non-Console Managed Host](#).

Re-add managed host to your deployment.

Step 2 From the menu, select **Actions > Add a managed host**.

The Add a new host wizard appears.

Step 3 Click **Next**.

The Enter the host's IP window appears.

Step 4 Enter values for the parameters:

- **Enter the IP of the server or appliance to add** — Specify the IP address of the host you wish 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.

Step 5 Click **Next**.

Step 6 Click **Finish**.

Step 7 Re-assign all components to your non-Console managed host.

- a In the STRM Deployment Editor, click the **Flow View** or **Event View** tab.
- b Select the component you wish 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 wish to re-assign to this component. Click **Next**.
- e Click **Finish**.

Step 8 From the Administrative Console menu, select **Configurations > Deploy Configuration Changes**.

Changes are deployed.

INDEX

A

about this guide 1
appliances
 setting-up 11

B

browser support 6

C

Classification Engine
 definition 4
configuring disk partitions 24
configuring firewall configuration 24
configuring network parameters 24
Console
 definition 4
conventions 1
customizing Up2Date 26

D

disk partitions
 configuring 24

E

Event Collector
 definition 4
Event Processor
 definition 5

F

firewall 24
flow data sources
 identifying 8
Flow Processor
 definition 4
Flow Writer
 definition 4

I

installing
 Japanese support 21
 preparing 3
 Red Hat Enterprise 4 update 6 25

J

Japanese support 21

M

Magistrate
 definition 5

N

network assets
 identifying 9
network hierarchy
 preparing 6
network settings
 identifying 7

O

Offense Resolution
 definition 4

P

preparing 3

Q

QFlow Collector
 definition 4
STRM
 using Red Hat Enterprise 4 update 6 16

R

Red Hat Enterprise 4 update 6
 setting up 23
 upgrading 26
requirements
 hardware 6

S

Secure Shell 24
security monitoring devices
 identifying 8
software
 requirements 6

U

- Up2Date
 - customizing 26
- Update Daemon
 - definition 4