



## **Security Threat Response Manager**

# **Hardware Installation Guide**

### **Juniper Networks, Inc.**

1194 North Mathilda Avenue  
Sunnyvale, CA 94089

USA

408-745-2000

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

Part Number: 530-023510-01, 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 Hardware Installation Guide

Copyright © 2008, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Revision History

14 February 2008—Revision 1

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

# Table of Contents

	<b>About This Guide</b>	<b>vii</b>
	Conventions.....	vii
	Related Documentation .....	vii
	Requesting Support.....	viii
	Documentation Feedback .....	viii
<b>Chapter 1</b>	<b>STRM Overview</b>	<b>1</b>
<b>Chapter 2</b>	<b>Hardware Overview</b>	<b>3</b>
	STRM 500 Front Panel and Back Panel Indicators and Features.....	3
	Front Panel Indicators .....	3
	Back Panel Features .....	4
	STRM 2500 Front Panel and Back Panel Indicators and Features.....	5
	Front Panel Indicators .....	5
	Back Panel Features .....	6
<b>Chapter 3</b>	<b>Installing And Connecting The STRM Hardware</b>	<b>9</b>
	Additional Hardware Requirements .....	9
	Installing the Hardware.....	10
	LED Behavior.....	11
	Chassis Console Port Pinouts .....	11
	Connecting a Laptop or Keyboard and a Monitor.....	12
<b>Chapter 4</b>	<b>Preparing Your System for STRM Software Installation</b>	<b>13</b>
	STRM Components .....	13
	Browser Support .....	14
	Preparing Your Network Hierarchy .....	14
	Identifying Network Settings.....	15
	Identifying Security Monitoring Devices and Flow Data Sources .....	16
	Identifying Network Assets .....	17
<b>Chapter 5</b>	<b>Setting Up STRM Software and Configuring Network Settings</b>	<b>19</b>
	Logging Into STRM for the First Time.....	19
	Accessing STRM .....	23
<b>Appendix A</b>	<b>Hardware Specifications</b>	<b>25</b>
<b>Appendix B</b>	<b>Maintaining and Servicing the Hardware</b>	<b>27</b>
	STRM Appliance Field-Replaceable Units.....	27
	RAID Array .....	27

Power Supply .....	27
Cooling Fans.....	28

# List of Figures

- Figure 1: STRM 500 Front Panel ..... 4
- Figure 2: STRM 500 Back Panel ..... 5
- Figure 3: STRM 2500 Front Panel ..... 5
- Figure 4: STRM 2500 Front Panel ..... 6
- Figure 5: STRM 2500 Back Panel ..... 7
- Figure 6: STRM 2500 Back Panel ..... 7
- Figure 7: Rear Panel of STRM 500 ..... 10
- Figure 8: Front Panel of STRM 500 ..... 11
- Figure 9: Set the Date and Time window ..... 20
- Figure 10: Time Zone Continent window ..... 21
- Figure 11: Time Zone Region window ..... 21
- Figure 12: Configure STRM window ..... 22
- Figure 13: New Root Password window ..... 22
- Figure 14: Confirm New Root Password window ..... 23



# List of Tables

- Table 1: Text Conventions..... vii
- Table 2: STRM 500 Front Panel LEDs ..... 4
- Table 3: STRM 500 Front Panel Ports ..... 4
- Table 4: STRM 500 Rear View Components ..... 5
- Table 5: STRM 2500 Front Panel LEDs ..... 6
- Table 6: STRM 2500 Front Panel Ports ..... 6
- Table 7: STRM 2500 Back Panel Components ..... 7
- Table 8: Required Ports of STRM ..... 9
- Table 9: Ethernet Port LEDs ..... 11
- Table 10: RJ-45 Console Connector Pinout ..... 11
- Table 11: Network Hierarchy..... 15
- Table 12: Devices ..... 16
- Table 13: Asset Identification ..... 17
- Table 14: STRM 500 and 2500 Hardware Specifications ..... 25



# About This Guide

This preface provides the following guidelines for using the *STRM Hardware Installation Guide*:

- Conventions on page vii
- Related Documentation on page vii
- Requesting Support on page viii
- Documentation Feedback on page viii

## Conventions

---

The sample screens used throughout this guide are representations of the screens that appear when you install and configure the STRM appliances. The actual screens may differ.

Table 1 shows the text conventions used in this guide.

**Table 1: Text Conventions**

Conventions	Description	Examples
Bold typeface	Represents commands and key strokes in text	Click <b>Next</b>
<i>Italics</i>	Identify book names	<i>Security Threat Response Manager Administrator's Guide</i>

## Related Documentation

---

The Security Threat Response Manager documentation includes the following guides:

- *STRM Adaptive Log Exporter*
- *Event Category Correlation Reference Guide*
- *Configuring DSMs*
- *Category Offense Investigation Guide*
- *STRM Application Configuration Guide*

- *STRM Users Guide*
- *STRM Administration Guide*
- *Managing Sensor Devices*
- *Managing Vulnerability Assessment*
- *AQL Flow and Event Query CLI Guide*

## **Requesting Support**

---

For technical support, open a support case with the Case Manager link at <http://www.juniper.net/support> or call 1-888-314-JTAC (from the United States, Canada, or Mexico) or 1-408-745-9500 (from elsewhere).

## **Documentation Feedback**

---

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net), or fill out the documentation feedback form at <http://www.juniper.net/techpubs/docbug/docbugreport.html>. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version

## Chapter 1

# STRM Overview

STRM appliances are designed to respond to the right threats at the right time through effective analysis of networks, events, and audit log files. STRM has the ability to identify environmental anomalies in the network, an attack path, and the source of a threat. STRM provides network remediation for threat responses across all security products.

The STRM appliances use two drivers, Security Information Management (SIM) and Security Event Management (SEM), for security analysis of external and internal threats. SIM provides reporting and analysis of data from host systems, applications, and security devices to support security policy compliance management, internal threat management, and regulatory compliance initiatives. SEM improves security incident response capabilities by processing data from security devices and network devices. It helps network administrators to provide effective responses to external and internal threats.



## Chapter 2

# Hardware Overview

This chapter gives an overview of the STRM appliances. It contains the following sections:

- STRM 500 Front Panel and Back Panel Indicators and Features on page 3
- STRM 2500 Front Panel and Back Panel Indicators and Features on page 5

### **STRM 500 Front Panel and Back Panel Indicators and Features**

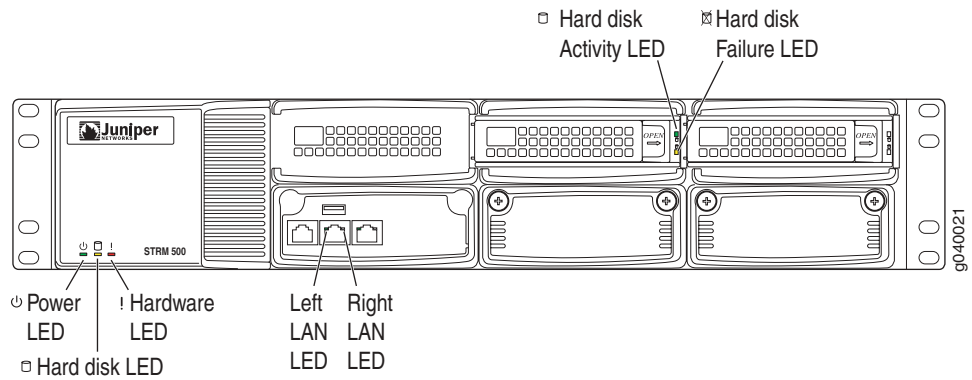
---

The STRM 500 appliance has a 2U rack-mountable chassis with optional redundant AC and DC power supplies, a 2U hot-swappable dual redundant RAID1 array, 8 GB of memory, and a Gigabit Ethernet controller.

#### ***Front Panel Indicators***

See Figure 1 for the front panel features of the system. Table 2 and Table 3 describes the front panel features.

**Figure 1: STRM 500 Front Panel**



**Table 2: STRM 500 Front Panel LEDs**

LEDs	Description
LED	<p><b>Chassis LEDs</b></p> <ul style="list-style-type: none"> <li>■ Power (green) - Indicates that the appliance is powered on</li> <li>■ Hard disk (yellow) - Indicates the hard disk is in use (writing or reading data)</li> <li>■ Hardware (red) - Indicates that a fan, power supply, or temperature alarm has occurred</li> </ul> <p><b>LAN LEDs</b></p> <ul style="list-style-type: none"> <li>■ Left LED (green) - Indicates that the link is active</li> <li>■ Right LED - Indicates the link speed                             <ul style="list-style-type: none"> <li>■ off - 10 Mbps</li> <li>■ green - 100 Mbps</li> <li>■ yellow - 1 Gbps</li> </ul> </li> </ul> <p><b>Hard disk tray LEDs</b></p> <ul style="list-style-type: none"> <li>■ Top (green) - For disk activity</li> <li>■ Bottom (yellow) - For disk failure</li> </ul>

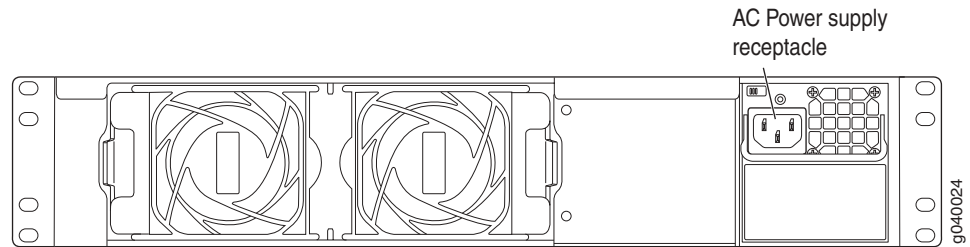
**Table 3: STRM 500 Front Panel Ports**

Ports	Description
Console port	One RJ-45 console port
Traffic port	Two RJ-45 Ethernet 10/100/1000

## Back Panel Features

See Figure 2 for the back panel features of the system. Table 4 describes the back panel features.

**Figure 2: STRM 500 Back Panel**



**Table 4: STRM 500 Rear View Components**

Components	Description
Cooling fans	Draws air through vents of the chassis and exhaust it through vents on the other side of the chassis
Power supply	Provides power to all components

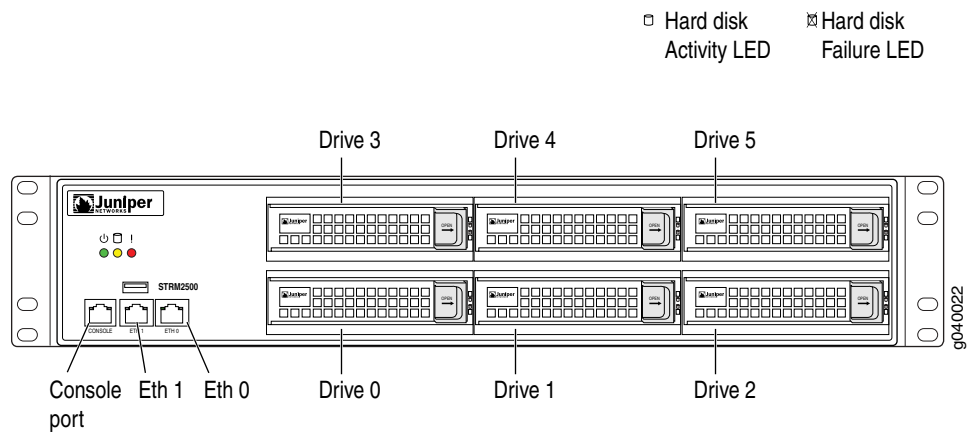
## STRM 2500 Front Panel and Back Panel Indicators and Features

The STRM 2500 appliance has a 2U rack-mountable chassis with optional redundant AC and DC power supplies, 2U hot-swappable dual redundant RAID5 array, 8 GB of memory, and a Gigabit Ethernet controller.

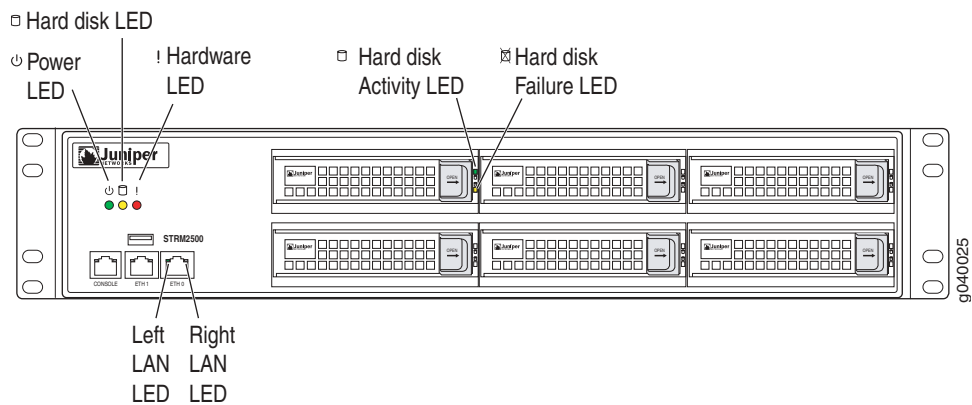
### Front Panel Indicators

See Figure 3 and Figure 4 for the front panel features of the system. Table 5 and Table 6 describes the front panel features.

**Figure 3: STRM 2500 Front Panel**



**Figure 4: STRM 2500 Front Panel**



**Table 5: STRM 2500 Front Panel LEDs**

LEDs	Description
LED	<p><b>Chassis LEDs</b></p> <ul style="list-style-type: none"> <li>■ Power (green) - Indicates that the appliance is powered on</li> <li>■ Hardware (red) - Indicates that a fan, power supply, or temperature alarm has occurred</li> </ul> <p><b>LAN LEDs</b></p> <ul style="list-style-type: none"> <li>■ Left LED (green) - Indicates that the link is active</li> <li>■ Right LED - Indicates the link speed <ul style="list-style-type: none"> <li>■ off -10 Mbps</li> <li>■ green - 100 Mbps</li> <li>■ yellow - 1Gbps</li> </ul> </li> </ul> <p><b>Hard disk module LEDs</b></p> <ul style="list-style-type: none"> <li>■ Top (green) - For disk activity</li> <li>■ Bottom (yellow) -For disk failure</li> </ul>

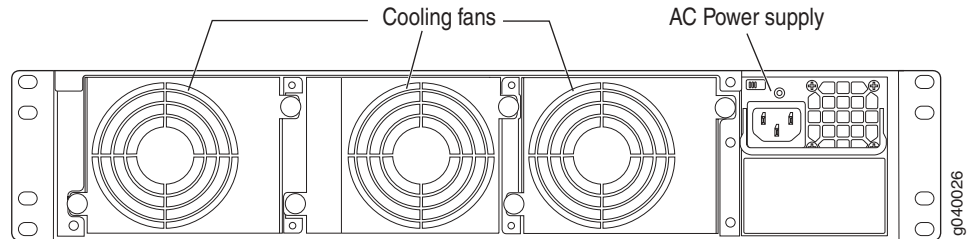
**Table 6: STRM 2500 Front Panel Ports**

Ports	Description
Console port	One RJ-45 console port
Traffic port	Two RJ-45 Ethernet 10/100/1000

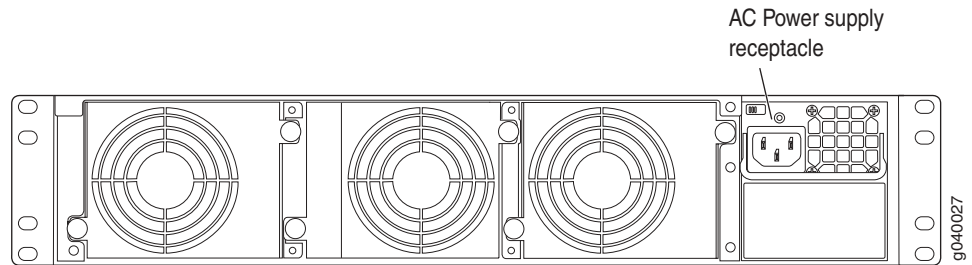
## Back Panel Features

See Figure 5 and Figure 6 for the back panel features of the system. Table 7 describes the back panel features.

**Figure 5: STRM 2500 Back Panel**



**Figure 6: STRM 2500 Back Panel**



**Table 7: STRM 2500 Back Panel Components**

Components	Description
Cooling fans	Draws air through vents of the chassis and exhaust it through vents on the other side of the chassis
Power supply	Provides power to all components

## Chapter 3

# Installing And Connecting The STRM Hardware

This chapter explains how to install and connect the STRM hardware. This chapter contains the following section:

- Additional Hardware Requirements on page 9
- Installing the Hardware on page 10
- Connecting a Laptop or Keyboard and a Monitor on page 12

## Additional Hardware Requirements

---

Before installing your STRM systems, ensure that you have access to the following additional hardware components:

- A serial console.
- To make sure that your STRM data is preserved during a power failure, we recommend that all STRM appliances or systems running STRM software storing data (such as, Consoles, Event Processors, or Flow Processors) be equipped with an Uninterrupted Power Supply (UPS).

We recommend that you install STRM on your LAN to ensure that it can communicate with your applicable resources, such as authentication servers, DNS servers, internal Web servers through HTTP/HTTPS, external Web sites through HTTP/HTTPS (optional), the Juniper Networks update server via HTTP, Network File System (NFS) file servers (optional), and client/server applications (optional). Table 8 shows port information on the STRM appliance.

**Table 8: Required Ports of STRM**

Direction	Port	Description	LAN	Internet	Depends on Configuration
In	22	SSH command-line management	Yes	No	No
	443	Web interface	Yes	No	No
Out	22	SSH connection to new managed device	Yes	Yes	No

Direction	Port	Description	LAN	Internet	Depends on Configuration
	23	Telnet connection to new managed device	Yes	No	Yes
	53	DNS lookups	Yes	No	No
	80	System Security Updates from Juniper Networks	Yes	Yes	Yes
	123	Network Time Protocol (NTP) time synchronization	Yes	Yes	Yes

## Installing the Hardware

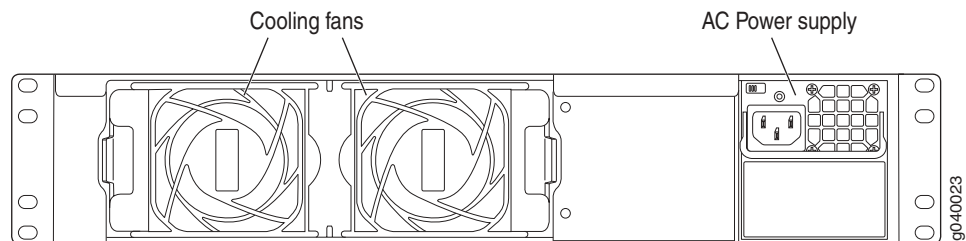
Place the shipping container on a flat surface and remove the hardware components with care.

To install the STRM appliance:

1. Mount the STRM appliance in your server rack using the attached mounting brackets.
2. Plug the power cord into the AC receptacle on the rear panel. See Figure 7.

If your STRM contains two power supplies, plug a power cord into each of the AC receptacles.

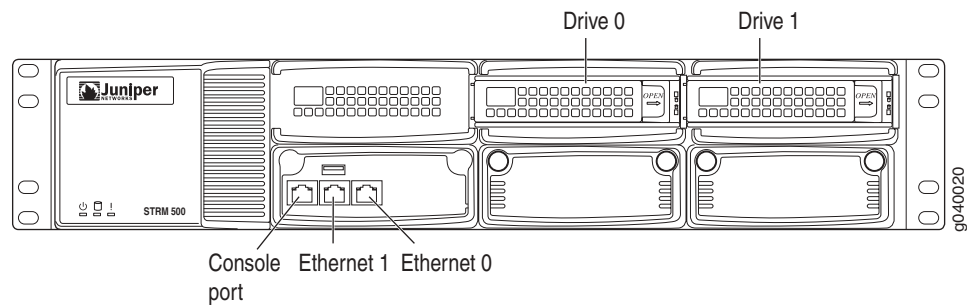
**Figure 7: Rear Panel of STRM 500**



3. Plug the other end of the power cord into a wall socket.

If your STRM appliance contains two power supplies, plug each power cord into a separate power circuit to ensure that the device continues to receive power if one of the power circuits fails.

4. Plug the Ethernet cable into the port labeled ETH0 on the front panel. See Figure 8.

**Figure 8: Front Panel of STRM 500**

When you turn on the power, the internal port uses two LEDs to indicate the LAN connection status, See Table 9.

5. Plug straight-through or crossover cable into the console port. See Figure 8.

This cable is shipped with your STRM appliance. It is a console cable and DB-9 connector with 1-8 pinouts. See Table 10 for RJ-45 chassis console connector pinout information.

6. Push the power button on the front panel.

The green LED below the power button turns on. The STRM hard disk LED turns on whenever the appliance reads data from or writes data to the STRM hard disk.

## LED Behavior

**Table 9: Ethernet Port LEDs**

LAN Status	LED 1	LED 2
10 Mbps connection	Off	N/A
100 Mbps connection	Green	N/A
1000 Mbps connection	Orange	N/A
Data is being transferred	Orange, green, or off	Blinking
No connection	Off	Off

## Chassis Console Port Pinouts

**Table 10: RJ-45 Console Connector Pinout**

Pin	Signal	Description
1	RTS Output	Request to Send
2	DTR Output	Data Terminal Ready
3	TxD Output	Transmit Data
4	GND	Chassis Ground
4	GND	Chassis Ground

Pin	Signal	Description
6	RxD Input	Receive Data
7	DSR Input	Data Set Ready
8	CTS Input	Clear to Send

## Connecting a Laptop or Keyboard and a Monitor

---

A STRM appliance includes STRM software and a CentOS-4 operating system. You control the appliance through a connected laptop or keyboard and monitor.

Follow the appropriate step:

- Connect a laptop to the RJ-45 serial port on the front panel of the appliance.
- Connect a keyboard and monitor to their respective ports on the front panel.

See Table 3 and Table 4 for the location of the ports.

## Chapter 4

# Preparing Your System for STRM Software Installation

This chapter explains how to prepare your system and network before you install the STRM software. It contains the following sections:

- STRM Components on page 13
- Browser Support on page 14
- Preparing Your Network Hierarchy on page 14
- Identifying Network Settings on page 15
- Identifying Security Monitoring Devices and Flow Data Sources on page 16
- Identifying Network Assets on page 17

STRM deployment may consist of STRM installed on one or multiple systems. You can 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.

## STRM Components

---

STRM components that may exist in your deployment include:

- **Flow Processor** - The Flow Processor creates 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, it prompts you to enter the user name and password, which must be configured during the installation process.

- **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.
- **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 create the bundles.
- **Event Processor** - Processes events collected from one or more Event Collectors. When events are received, the Event Processor correlates the information from STRM and distributes it 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. The Magistrate prioritizes the offenses and assigns a magnitude value based on several factors, including number of events, severity, relevance, and credibility.

## Browser Support

---

To access the STRM interface, you must have a browser installed on your client system. STRM supports the following Web browsers:

- Microsoft Internet Explorer 7.0
- Firefox 2.0

## Preparing Your Network Hierarchy

---

STRM uses the network hierarchy to understand your network traffic and provides 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, mail servers, and Web servers.

Once you define the components you wish to add to your network hierarchy, install STRM, and then configure the network hierarchy using the STRM interface. For each component you wish to add to the network hierarchy, use Table 11 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 11: Network Hierarchy**

Description	Name	IP/CIDR Value	Weight

For more information, see the *STRM Administration Guide*.

## 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 Flow Collectors allow you to integrate STRM with this external data. STRM automatically discovers sensor devices that are sending system log (syslog) messages to an Event Collector. The sensor devices that are automatically discovered by STRM appear in the Sensor Devices window within the STRM Administration Console. Once auto discovery is completed, you should disable the Auto Detection Enabled option in the Event Collector configuration. For more information, see 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 12.

**Table 12: 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)

In this table:

- 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 workstation.
- Msg Level indicates the message level you wish to log - for example, critical, informational, or debug.
- No. of Users indicates the maximum number of hosts and users using or being served by this device.

- Network Location indicates whether this device is located on the Internet demilitarized zone (DMZ), Intranet, or Extranet DMZ.
- Geographic Location indicates whether the devices are 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 the STRM Asset Profile database to discover many types of servers.

Defining certain additional server and IP address types also improves tuning results. Table 13 provides a list of possible servers. 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 13: 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			



## Chapter 5

# Setting Up STRM Software and Configuring Network Settings

This chapter provides information on setting up your STRM software and configuring network settings:

- Logging Into STRM for the First Time on page 19
- Accessing STRM on page 23

### Logging Into STRM for the First Time

---

1. Connect your laptop or keyboard and monitor to the STRM device, as described in Chapter 2.

---

**NOTE:** When using a laptop to connect to the system, you must use a terminal program, such as HyperTerminal. 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).

---

2. Power on the system and log in to STRM:

Username: **root**

Password: **password**

---

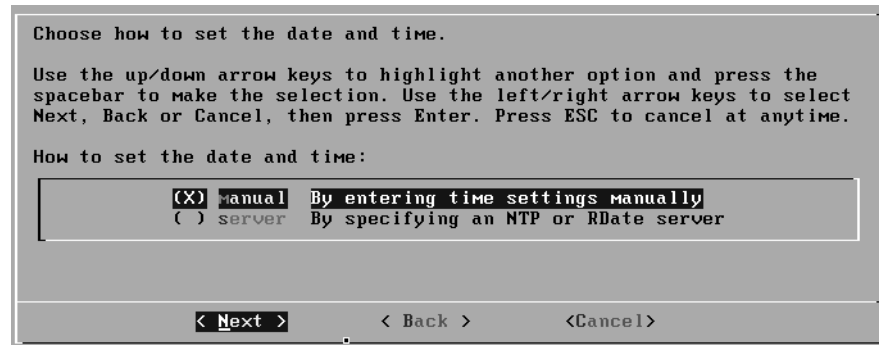
**NOTE:** The username and password are case sensitive.

---

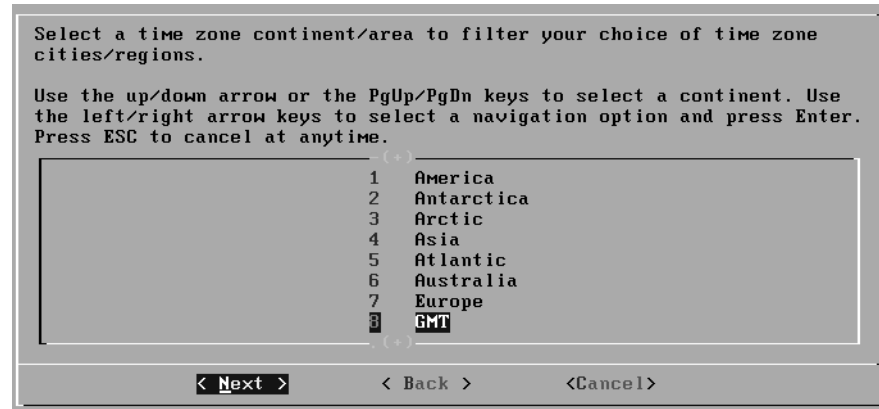
3. Press Enter. The End User License Agreement (EULA) appears.
4. Read the information in the window. Press the Spacebar to advance each window until you have reached the end of the document. Type YES to accept the agreement, then press Enter. The Tuning Template window appears.
5. Using the up or down 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.
6. Using the left or right arrow keys, select Set Template. Press the Enter key. The Set the Date and Time window appears.

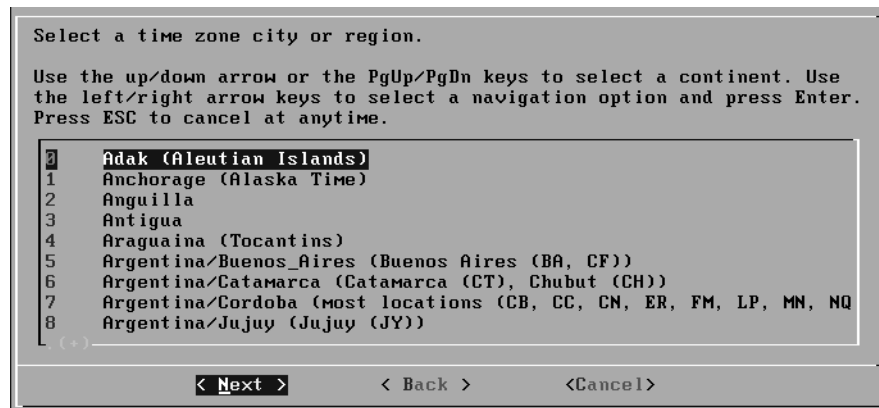
**Figure 9: Set the Date and Time window**



7. Using the up or down arrow keys, select the method you wish to use to set the date and time:
  - Manual - Allows you to manually input the time and date. Use the Spacebar to select the option and then use the Tab key to select the Next option. Press Enter. The Current Date and Time window appears. Go to Step 8.
  - Server - Allows you to specify your time server. Use the Spacebar to select the option and then use the Tab key to select the Next option. Press Enter. The Enter Time Server window appears. Go to Step 9.
8. To manually enter the time and date:
  - a. Enter the current date and time.
  - b. Using the left or right arrow keys, select Next. Press Enter.
  - c. Go to Step 10.
9. To specify a time server:
  - a. In the text field, enter the time server name or IP address.
  - b. Using the left or right arrow keys, select Next. Press Enter. The Time Zone Continent window appears.

**Figure 10: Time Zone Continent window**

10. To select the time zone continent:
  - a. Using the up or down arrow keys, or the PageUp or PageDown keys, select your time zone continent or area.
  - b. Using the left or right arrow keys, select Next, then press Enter. The Time Zone Region window appears.

**Figure 11: Time Zone Region window**


---

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

---

- c. Using the up or down arrow keys, or the page up/page down keys, select your time zone region.
- d. Using the left or right arrow keys, select Next. Press the Enter key. The Configure STRM window appears.

**Figure 12: Configure STRM window**

Configure 2008.1.0.37 Security Threat Response Manager Appliance 3100:

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

Hostname:	strm.juniper.net		
IP Address:		Primary DNS:	10.90.0.10
Network Mask:		Secondary DNS:	
Gateway:		Public IP:	
Email server:			

< Next >      < Back >      <Cancel>

11. To configure the STRM network settings, enter values for the following parameters. Use the up or down arrow keys to navigate the fields:
  - Hostname - Specify a fully qualified domain name as the system hostname.
  - IP Address - Specify the IP address of the system.
  - Netmask - Specify the network mask address for the system.
  - Gateway - Specify the default gateway 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. The server uses this IP address to communicate with another server that belongs to a different network using Network Address Translation (NAT). 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.
  
12. Use the Tab key to move to the Next option. Press Enter. The New Root Password window appears.

**Figure 13: New Root Password window**

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:

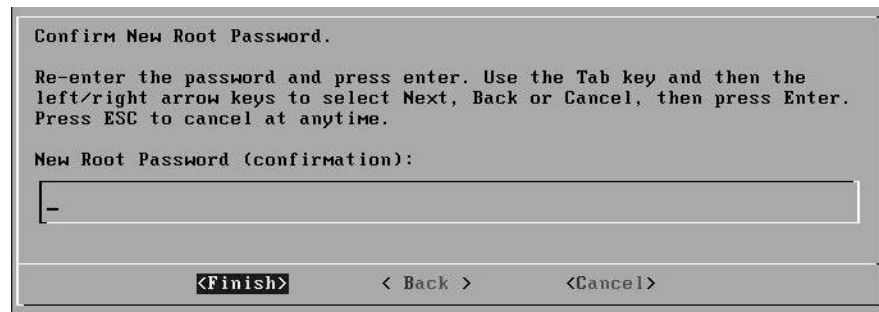
\_\_\_\_\_

< Next >      < Back >      <Cancel>

13. To configure the STRM root password:

- a. Type a new password.
- b. Use the Tab key to move to the Next option. Press Enter. The Confirm New Root Password window appears.

**Figure 14: Confirm New Root Password window**



- c. Retype your new password to confirm it.
- 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 is typically a three to five minute process. The Configuration is Complete window appears.

14. Press Enter to select OK.

You are now ready to access STRM. For more information, see the section “Accessing STRM”.

## Accessing STRM

---

To access the STRM interface:

1. Open your Web browser.
2. Log in to STRM:

`https://<IP Address>`

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

Username: **admin**

Password: **< root password >**

**< root password >** is the new root password you set during the installation process.

3. Click Login To STRM.

STRM includes a default license key that allows you to access the interface for five weeks. A window shows the expiry date of the temporary license key. For information on installing a permanent license key, see the *STRM Administration Guide*.



## Appendix A

# Hardware Specifications

See Table 14 for hardware specifications of STRM 500 and STRM 2500.

**Table 14: STRM 500 and 2500 Hardware Specifications**

	<b>STRM 500</b>	<b>STRM 2500</b>
<b>Physical Specification</b>		
Depth	450 mm 17.72 in.	597.5 mm 23.52 in.
Width	438.4 mm 17.26 in.	438.4 mm 17.26 in.
Height	88 mm 3.5 in.	88 mm 3.5 in.
Weight	26 lbs 2 oz	39 lbs 5 oz
Warranty	1 year HW, 90 days SW	1 year HW, 90 days SW
Peak inrush	< 25 A 400w AC, < 60A 710 watt DC	< 60 A for both AC and DC modules
Fans	2x80 mm redundant hot-swap	3 x 80mm redundant hot-swap
Rack mountable	Front and rear or mid-mount	Front and rear or mid-mount
Ports	1 console, 2x RJ-45 10/100/1000	1 console, 2x RJ-45 10/100/1000
Power	90 V to 264 V hot-swap dual redundant 400 watt AC power module, 90 V to 264 V hot-swap dual redundant 710 watt DC power module -48V DC power supply (optional) Max efficiency: 90 % 400 watt AC, 89 % 710 watt DC	90 V to 264 V hot-swap dual redundant 700 watt AC power module, 90 V to 264 V hot-swap dual redundant 710 watt DC power module -48 V DC power supply (optional) Max efficiency: 80 % 700 watt AC, 89 % 710 watt DC
Thermal dissipation	<ul style="list-style-type: none"> <li>■ Single power supply 323 BTU/hr (typical) 413 BTU/hr (max)</li> <li>■ Dual power supplies 413 BTU/hr (typical) 499 BTU/hr (max)</li> </ul>	<ul style="list-style-type: none"> <li>■ Single power supply 601 BTU/hr (typical) 800 BTU/hr (max)</li> <li>■ Dual power supplies 676 BTU/hr (typical) 887 BTU/hr (max)</li> </ul>

### Environmental specifications

	<b>STRM 500</b>	<b>STRM 2500</b>
Temperature operating	5°C – 40°C 41°F – 104°F	5°C – 40°C 41°F – 104°F
Temperature storage	-40°C – 70°C -40°F – 158°F	-40°C – 70°C -40°F – 158°F
Humidity operating	8% - 90% non-condensing	8% - 90% non-condensing
Humidity storage	5% - 95% non-condensing	5% - 95% non-condensing
Altitude operating	10000' maximum	10000' maximum
Altitude storage	40000' maximum	40000' maximum
<b>Compliance and safety</b>		
Safety certification	CAN/CSA-C22.2 No. 60950-1-03 UL60950-1:2003 EN60950-1:2001 + A11 IEC 60950-1:2001	CAN/CSA-C22.2 No. 60950-1-03 UL60950-1:2003 EN60950-1:2001 + A11 IEC 60950-1:2001
Emissions certification (FCC Class A with -6dB margin is a minimum requirement)	FCC Class A, EN 55022 Class A, EN 55024 Immunity, EN 61000-3-2, VCCI Class A	FCC Class A, EN 55022 Class A, EN 55024 Immunity, EN 61000-3-2, VCCI Class A

## Appendix B

# Maintaining and Servicing the Hardware

## STRM Appliance Field-Replaceable Units

---

The STRM chassis supports three types of field-replaceable units (FRUs) that you can add or replace. The FRUs include redundant hot swappable hard disks, power supplies, and fans.

### **RAID Array**

The STRM appliance ships with hot-swappable hard disks to offer component redundancy. The STRM 500 appliance has a RAID1 hard disk. The second (redundant) disk maintains a copy of the software image and configuration information on the working hard disk. If the working hard disk fails, the redundant hard disk immediately assumes responsibility for STRM operations. STRM 2500 has six disks with RAID5 configuration. You can hot-swap the disk if any one of the disks fails.

Redundant array of independent disk (RAID) is an organization of multiple disks of fault tolerance and performance. It is used in the servers for data storage and to replicate data among multiple hard disk drives. There are different RAID levels designed to increase data reliability and increased I/O performance.

The key concepts in RAID are:

- Mirroring - copy data to more than one disk
- Striping - split data across more than one disk
- Error correction - redundant data storage to detect and resolve problems

STRM 500 and STRM 2500 use RAID1 and RAID5 respectively. RAID1 uses mirroring and duplexing techniques to copy data to the redundant disk. RAID5 uses block interleaved distributed parity technique to provide data striping at the byte level.

### **Power Supply**

The STRM appliances has a single AC power supply module. But the STRM appliances can support dual redundant power supply modules. If one power supply fails, the optional second power supply assumes responsibility for the entire power load. STRM appliances also have a DC power supply option if you need DC power. You can have both AC and DC power supplies in the same chassis.

## **Cooling Fans**

The STRM 500 appliance has two cooling fans and the STRM 2500 appliance has three cooling fans. The fans are hot-swappable.

# Index

## **B**

Browser Support 14

## **C**

Classification Engine 13

Console 13

## **E**

Event Collector 14

Event Processor 14

## **F**

Flow Data Sources 16

Flow Processor 13

Flow Writer 14

## **H**

Hardware Requirements 9

## **L**

Link Speed 16

## **M**

Magistrate 14

## **N**

Network Assets 17

Network Hierarchy 14

Network Settings 15

## **S**

Security Monitoring Devices 16

STRM 2500 5

STRM 500 3

syslog messages 16

## **U**

Update Daemon 14

