



Security Threat Response Manager

STRM 5000 Hardware Installation Guide
NEBS Level 3 Compliant

Release 2009.1

Juniper Networks, Inc.

1194 North Mathilda Avenue

Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Part Number: 530-032977

Copyright Notice

Copyright © 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

FCC Statement

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

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

Disclaimer

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

Configuring DSMs
Release 2009.1

Copyright © 2008, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Revision History

November 2009—Revision 1

Published: 2009-11-30

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

CONTENTS

ABOUT THIS GUIDE

Objectives	1
Conventions	1
Technical Documentation	2
Contacting Customer Support	2

STRM OVERVIEW

HARDWARE OVERVIEW

Front Panel Indicators	5
Back Panel Features	7

INSTALLING AND CONNECTING THE STRM HARDWARE

Additional Hardware Requirements	9
Safety Considerations	10
Installing the Hardware	11
LED Behavior	12
Chassis Console Port Pinouts	12
Connecting a Laptop or Keyboard and a Monitor	13

PREPARING YOUR SYSTEM FOR STRM SOFTWARE INSTALATION

STRM Components	15
Browser Support	16
Preparing your network Hierarchy	16
Identifying Network Settings	17
Identifying Security Monitoring Devices and Flow Data Sources	17
Identifying Network Assets	18

SETTING UP STRM SOFTWARE AND CONFIGURING NETWORK SETTINGS

Logging Into STRM for the First Time	21
Accessing STRM	26

HARDWARE SPECIFICATIONS

MAINTAINING AND SERVICING THE HARDWARE

RAID Array	31
Power Supply	31
Cooling Fans	32
Fan Filter	33

LIST OF TABLES

Table 1: Text Conventions	1
Table 2: STRM 5000 NEBS Front Panel LEDs	6
Table 3: STRM 5000 NEBS Front Panel Ports	6
Table 4: STRM 5000 NEBS Back Panel Components	7
Table 5: Required Ports of STRM	9
Table 6: Ethernet Port LEDs	12
Table 7: RJ-45 Console Connector Pinout	12
Table 8: Network Hierarchy	19
Table 9: Devices	20
Table 10: Asset Identification	21
Table 11: STRM 5000 NEBS Hardware Specifications	29

LIST OF FIGURES

Figure 1: STRM 5000 NEBS Front Panel	5
Figure 2: STRM 5000 NEBS Front Panel	6
Figure 3: STRM 5000 NEBS Back Panel	7
Figure 4: Rear Panel of STRM 5000 NEBS	11
Figure 5: Front Panel of STRM 5000 NEBS	12
Figure 6: System Console Window	22
Figure 7: Set the Date and Time Window	22
Figure 8: Time Zone Continent Window	23
Figure 9: Time Zone Region Window	24
Figure 10: Configure STRM Window	24
Figure 11: New Root Password Window	25
Figure 12: Confirm New Root Password Window	25
Figure 13: Unlocking the power supply tab	32
Figure 14: Removing the power supply	32
Figure 15: Rear of chassis	32
Figure 16: Unfasten thumbscrews	33
Figure 17: Removing the Fan Tray Filter	33

ABOUT THIS GUIDE

This preface provides the following guidelines for using the *STRM 5000 NEBS Hardware Installation Guide*:

- [Objectives](#)
- [Conventions](#)
- [Technical Documentation](#)
- [Contacting Customer Support](#)

Objectives

This document describes how to install the Network Equipment-Building System (NEBS) Level 3 compliant STRM 5000 and run the STRM software on the appliance.

NEBS sets a standard for telecommunication devices at three distinct functional levels. Each level has established requirements also known as the NEBS criteria. The NEBS criteria ensures robust, reliable and cost-effective equipment deployment.

The NEBS Level 3 certification guarantees maximum operability of the equipment under normal and abnormal conditions. At this level, the following criteria are met:

- Personnel and equipment safety
- Electromagnetic compatibility and electrical safety
- Operational continuity

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

Technical Documentation

You can access technical documentation, technical notes, and release notes directly from the Juniper Customer Support web site at <https://www.juniper.net/support/>. Once you access the Juniper Customer Support web site, locate the product and software release for which you require documentation. Your comments are important to us. Please send your e-mail comments about this guide or any of the Juniper Networks documentation to:

techpubs-comments@juniper.net.

Include the following information with your comments:

- Document title
- Page number

Contacting Customer Support

To help you resolve any issues that you may encounter when installing or maintaining STRM, you can contact Customer Support as follows:

- Open a support case using the Case Management link at <http://www.juniper.net/support>.
- Call 1-888-314-JTAC (from the United States, Canada, or Mexico) or 1-408-745-9500 (from elsewhere).

1

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.

4 STRM OVERVIEW

2

HARDWARE OVERVIEW

This chapter gives an overview of the STRM 5000 NEBS appliance. It contains the following sections:

- [Front Panel Indicators](#)
- [Back Panel Features](#)

Front Panel Indicators

The STRM 5000 NEBS appliance has a 2U rack-mountable chassis with dual redundant DC supplies and an optional AC power supply, 2U hot-swappable dual redundant RAID10 array, 12 GB of memory, and a Gigabit Ethernet controller.

See [Figure 1](#) and [Figure 2](#) for the front panel features of the system. [Table 2](#) and [Table 3](#) describes the front panel features.

Figure 1 STRM 5000 NEBS Front Panel

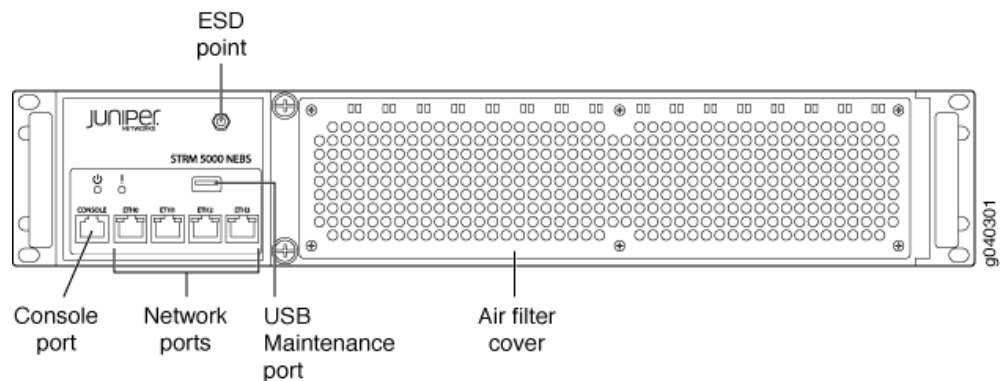


Figure 2 STRM 5000 NEBS Front Panel

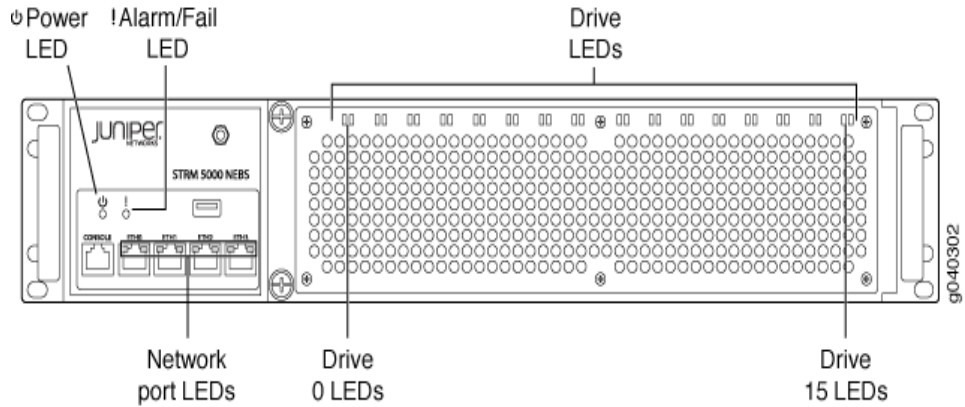


Table 2 STRM 5000 NEBS Front Panel LEDs

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

Table 3 STRM 5000 NEBS Front Panel Ports

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

Back Panel Features

See [Figure 3](#) for the back panel features of the system. [Table 4](#) describes the back panel features.

Figure 3 STRM 5000 NEBS Back Panel

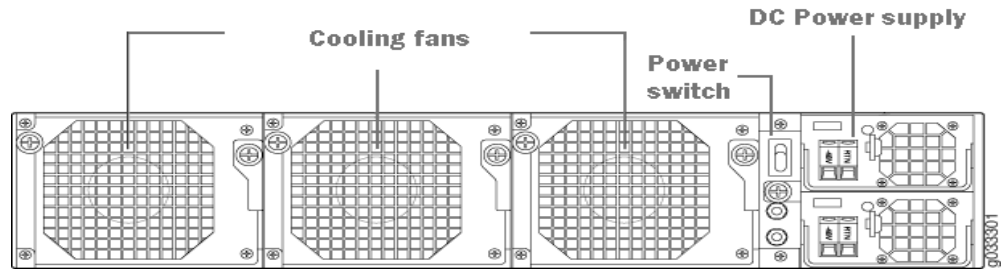


Table 4 STRM 5000 NEBS Back Panel Components

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

3

INSTALLING AND CONNECTING THE STRM HARDWARE

This chapter explains how to install and connect the STRM 5000 NEBS hardware. This chapter contains the following section:

- [Additional Hardware Requirements](#)
- [Safety Considerations](#)
- [Installing the Hardware](#)
- [Connecting a Laptop or Keyboard and a Monitor](#)

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 5](#) shows port information on the STRM appliance.

Table 5 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
	23	Telnet connection to new managed device	Yes	No	Yes

Table 5 Required Ports of STRM

Direction	Port	Description	LAN	Internet	Depends on Configuration
	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

Safety Considerations

The STRM 5000 NEBS appliance is suitable for Common Bonding Network (CBN) and can be installed in a Network telecommunication facilities. Consider the following safety guidelines while installing a STRM 5000 NEBS appliance:

- Install a *star* lock washer between the ground rail and the lug using a #8 self-threading screw.
- Coat bare connectors with an antioxidant before making any crimp connections. Bare conductors must be coated with an appropriate antioxidant compound before crimp connections are made. All un-plated connectors, braided strap, and bus bars must be brought to a bright finish and then coated with an antioxidant before they are connected.
- Connect one end of the grounding cable to the rack and secure it with a rack mount screw using a #3 Philips screwdriver to the recommended torque (35.0 in-lbs).
- Insert a screw into the mounting hole of the bracket and tighten half-way. Check if the bracket dimple is nested properly in the chassis dimple. Insert a Philips-head screwdriver through the outer hole on the bracket to mate with the screw. Torque the screw to 8-10 lbf.in. Do not over-tighten.
- Secure the grounding cable to the rack using a 10mm socket driver, torque the screws to 40 in-lb (4.5 N-m).



Warning: *The intra-building port(s) of the equipment or subassembly is suitable for connection to intra-building or unexposed wiring or cabling only. The intra-building port(s) of the equipment or subassembly MUST NOT be metallically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE, Issue 4) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring.*

Installing the Hardware

The STRM 5000 NEBS is a DC Isolated return (DC-I) installation. The DC Power return conductor will be isolated from the equipment chassis or frame when connected to the power supply. Consider the following guidelines before installing the STRM 5000 NEBS appliance:

- The working voltage range for STRM 5000 NEBS is from -40v to -58v.
- The equipment requires an external Surge Protection Device (SPD) when configured with AC supplies.
- Juniper Networks recommends using a green-colored ground cable to ground the STRM 5000 NEBS appliance.
- Juniper Networks recommends using the following ground lug - *Panduit P/N LCDX8-10A-L, #8 AWG, #10 thread, 1/4 inch-long bolt, 5/8 inch spacing.*
- In order to ensure a reliable ground bond, star washers and thread forming screws with paint piercing washers are required when securing the STRM 5000 NEBS ground wire to the rack frame.

To install the STRM 5000 NEBS appliance:

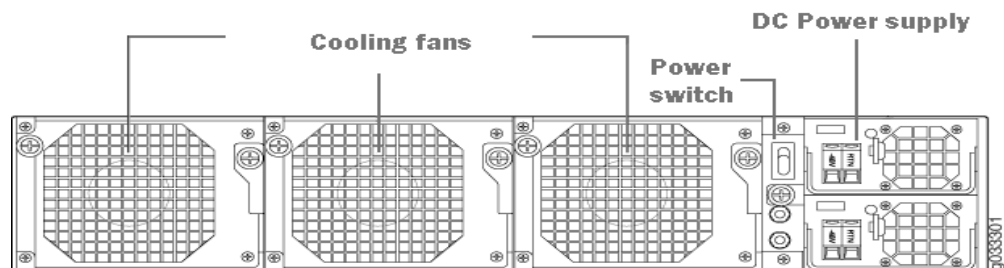
- Step 1** Place the shipping container on a flat surface and remove the hardware components with care.



Warning: Dropping the appliance from a height greater than 3 inches from the ground surface will cause physical irreparable damage to the storage media. Place impact absorbing material under the appliance to prevent loss of hard drive functionality in such cases. The EUT complies with the unpackaged test requirement with the exception of the Hard Disk Storage array.

- Step 2** Mount the STRM appliance in your server rack using the attached mounting brackets.
- Step 3** Connect the -48V and RTN/Ground wires to each power supply module on the rear panel. See [Figure 4](#).

Figure 4 Rear Panel of STRM 5000 NEBS

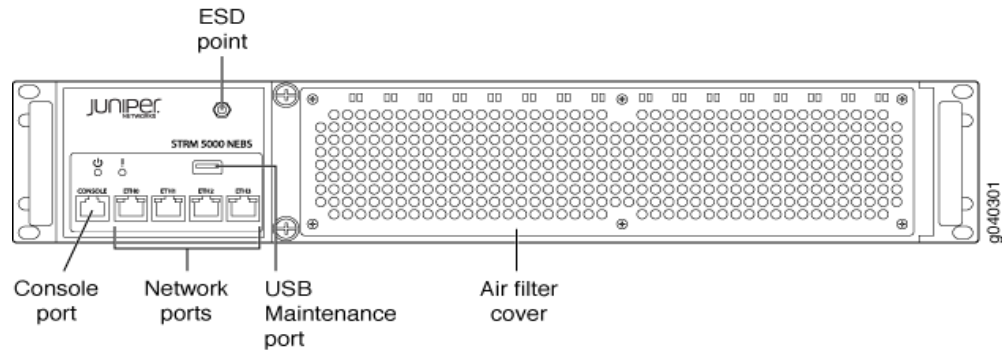


- Step 4** Plug the other end of the power cord into a wall socket.

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.

Step 5 Plug the Ethernet cable into the port labeled ETH0 on the front panel. See [Figure 5](#).

Figure 5 Front Panel of STRM 5000 NEBS



When you turn on the power, the internal port uses two LEDs to indicate the LAN connection status, See [Table 6](#).

Step 6 Plug straight-through or crossover cable into the console port. See [Figure 5](#).

This cable is shipped with your STRM appliance. It is a console cable and DB-9 connector with 1-8 pinouts. See [Table 7](#) for RJ-45 chassis console connector pinout information.

Step 7 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 6 Ethernet Port LEDs

LAN Status	Left LED (Link)	Right LED (Speed)
10 Mbps connection	Solid Green = Link Momentary Blinking = Activity	Off
100 Mbps connection	Solid Green = Link Momentary Blinking = Activity	Green
1000 Mbps connection	Solid Green = Link Momentary Blinking = Activity	Amber
No connection	Off	Off

Chassis Console Port Pinouts

Table 7 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

Table 7 RJ-45 Console Connector Pinout

Pin	Signal	Description
4	GND	Chassis Ground
4	GND	Chassis Ground
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-5 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 2](#) and [Table 3](#) for the location of the ports.

4

PREPARING YOUR SYSTEM FOR STRM SOFTWARE INSTALATION

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

- [STRM Components](#)
- [Browser Support](#)
- [Preparing your network Hierarchy](#)
- [Identifying Network Settings](#)
- [Identifying Security Monitoring Devices and Flow Data Sources](#)
- [Identifying Network Assets](#)

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, mails 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 8](#) 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 8 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 9](#).

Table 9 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 10](#) 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 10 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			

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](#)
- [Accessing STRM](#)

Logging Into STRM for the First Time

To log into STRM for the first time:

- Step 1** Connect your laptop or keyboard and monitor to the STRM 5000 NEBS appliance, 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).

- Step 2** Power on the system and log in to STRM:

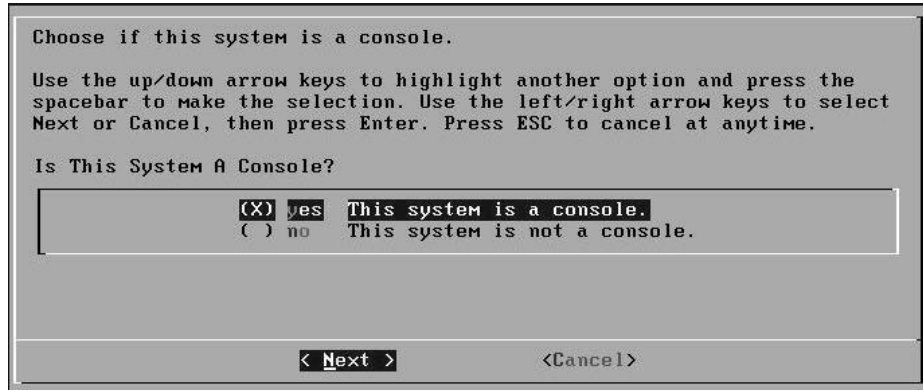
Username: `root`
Password: `password`



Note: The username and password are case sensitive. You can log into STRM either by entering the password or by entering the username only, as the 2009.1 release of STRM does not require a password.

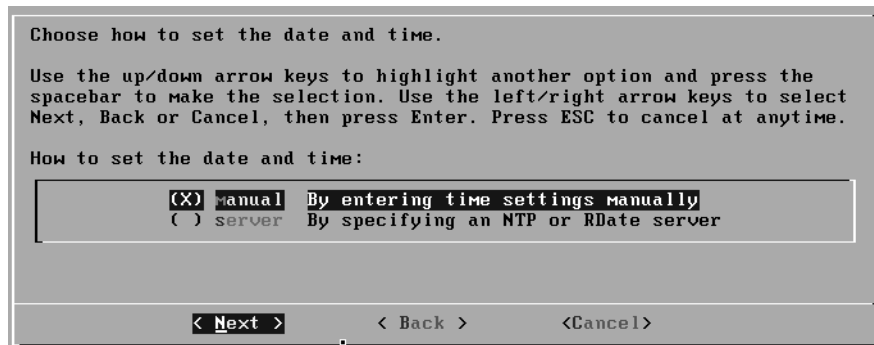
- Step 3** Press Enter. The End User License Agreement (EULA) appears.
- Step 4** Read the information in the window. Press the Spacebar to advance each window until you have reached the end of the document. Type YES to accept the agreement, then press Enter. The System Console window appears. See [Figure 6](#).

Figure 6 System Console Window



- Step 5** Using the up/down arrow keys, highlight one of the following options:
- **Yes** - Select this option only if this system is a Console. If you select this option, the Tuning Template window appears. Go to [Step 6](#).
 - **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 11](#).
- Step 6** 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.
- Step 7** Using the left or right arrow keys, select Set Template. Press the Enter key. The Set the Date and Time window appears. See [Figure 7](#).

Figure 7 Set the Date and Time Window



- Step 8** 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](#).

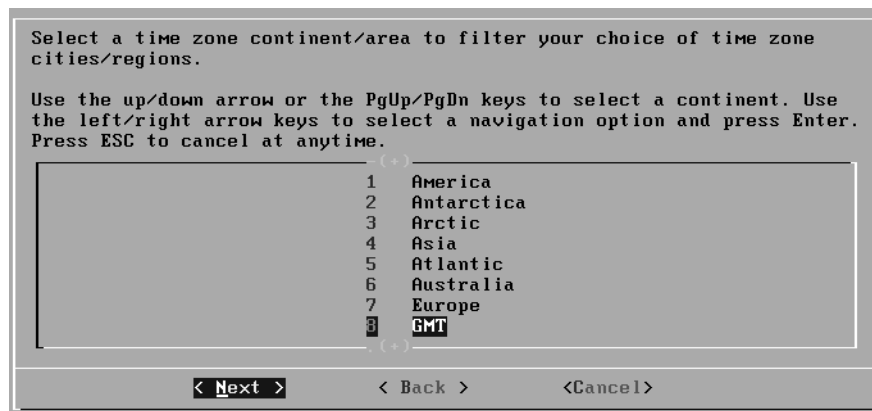
Step 9 To manually enter the time and date:

- a Enter the current date and time.
- b Using the left or right arrow keys, select Next. Press Enter.
- c Go to [Step 10](#).

Step 10 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. See [Figure 8](#).

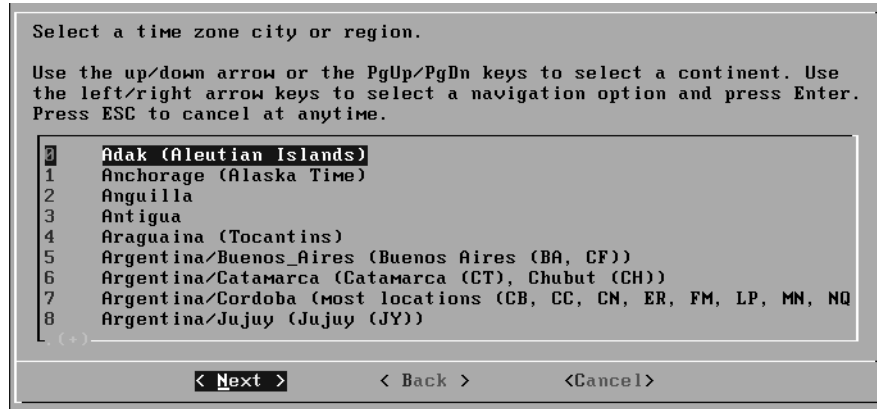
Figure 8 Time Zone Continent Window




Step 11 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. See [Figure 9](#).

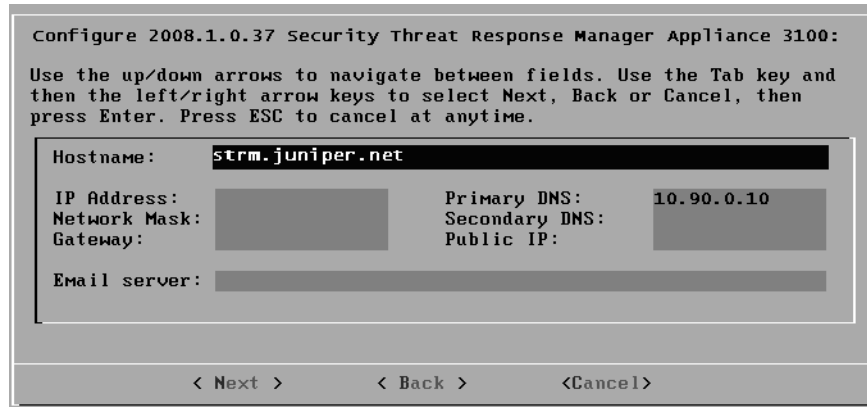
Figure 9 Time Zone Region Window



 **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. See [Figure 10](#).

Figure 10 Configure STRM Window

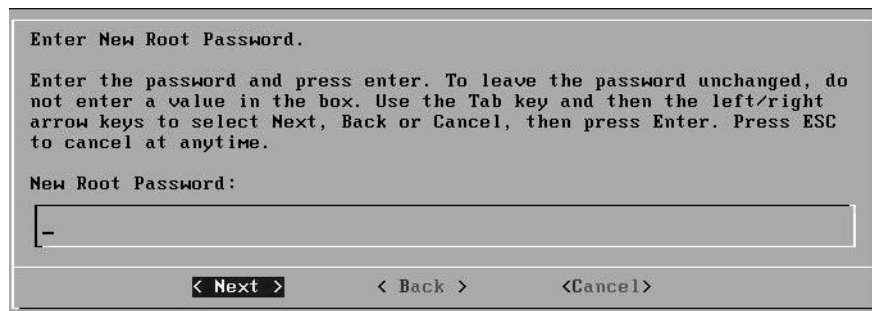


- Step 12** To configure the STRM network settings, enter values for the following parameters. Use the up or down arrow keys to navigate the fields:
- Hostname - Specify a fully qualified domain name as the system hostname.
 - IP Address - Specify the IP address of the system.
 - Netmask - Specify the 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.

Step 13 Use the Tab key to move to the Next option. Press Enter. The New Root Password window appears. See [Figure 11](#).

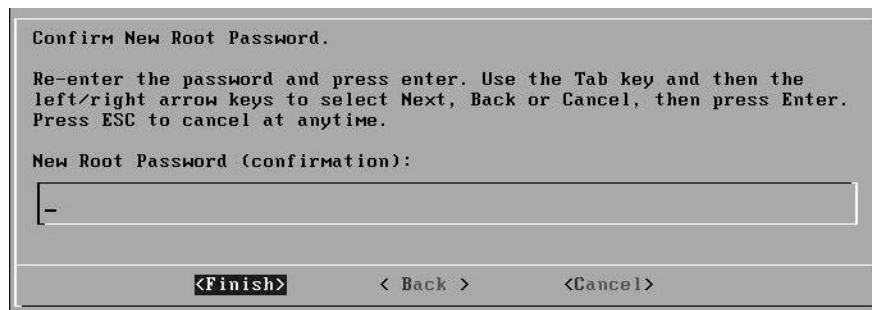
Figure 11 New Root Password Window



Step 14 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. See [Figure 12](#).

Figure 12 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.

Step 15 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:

Step 1 Open your Web browser.

Step 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.

Step 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*.



Note: You will need a permanent license for the STRM appliance to upgrade to a higher version. If you have a temporary license, the upgrade will fail; re-run the installer to upgrade to a higher version.

A

HARDWARE SPECIFICATIONS

See [Table 11](#) for hardware specifications of the STRM 5000 NEBS appliance.

Table 11 STRM 5000 NEBS Hardware Specifications

Physical Specification	STRM 5000 NEBS
Depth	609.5 mm 24 in.
Width	438.4 mm 17.25 in.
Height	88 mm 3.5 in.
Weight	53lbs 11oz
Chassis Material	18 gauge 0.048 in Cold-rolled-steel
Fans	6 x 80mm redundant hot-swap
Rack mountable	Front and rear or mid-mount
Ports	1 console, 2x RJ-45 10/100/1000 Intel 82574 2x RJ45 10/100/1000 Intel 82576
Power	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) Peak inrush: <60A Max efficiency: 80% 700 watt AC, 89% 710 watt DC
Environmental specifications	

Temperature operating	Normal: 5°C – 40°C 41°F – 104°F Short-term: 5°C – 55°C 23°F – 131°F -
Temperature storage	40°C – 70°C -40°F – 158°F
Humidity operating	Normal 8% - 90% non-condensing Short-term relative humidity: 5% - 90%, non-condensing, but not to exceed 0.024 kg water/kg dry air (0.053 lb. water/2.205 lbs. dry air)
Humidity storage	5% - 95% non-condensing
Altitude operating	10000' maximum
Altitude storage	40000' maximum
Thermal Dissipation	Dual power supplies std. 374W, 1276 BTU/hr (typical) 447W, 1525 BTU/hr (max)
 Compliance and safety	
Safety certification	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
NEBS	NEBS Level 3/Verizon NEBS certified by METLABS

B

MAINTAINING AND SERVICING THE HARDWARE

The STRM chassis supports three types of field-replaceable units (FRUs) that you can add or replace. The FRUs include:

- [RAID Array](#)
- [Power Supply](#)
- [Cooling Fans](#)
- [Fan Filter](#)

RAID Array

The STRM appliance ships with hot-swappable hard disks to offer component redundancy. The STRM 5000 NEBS appliance has a RAID10 configuration (16x 146 GB hard disks). 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

The STRM 5000 NEBS RAID10 drives are striped for performance, and all striped drives are mirrored for fault tolerance.

Power Supply

The STRM appliances has dual redundant DC power supply modules. If one power supply fails, the second power supply assumes responsibility for the entire power load. STRM appliances also have a AC power supply option if you need AC power.

To hot swap the power supply module:

- Step 1** Unplug the power cable of the power supply to power it down. Alarm may sound if system is on and running with both power supplies.
- Step 2** Remove the small power supply locking tab by unscrewing the thumb screw located to the left between the two power supply modules. See [Figure 13](#).

Step 3 Press the power supply locking tab and pull the power supply out by grasping the module handle. See [Figure 14](#).

Figure 13 Unlocking the power supply tab

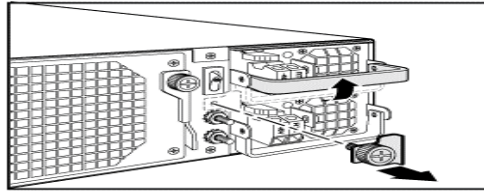
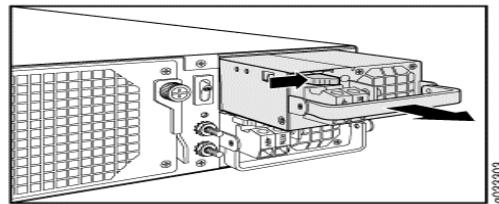


Figure 14 Removing the power supply

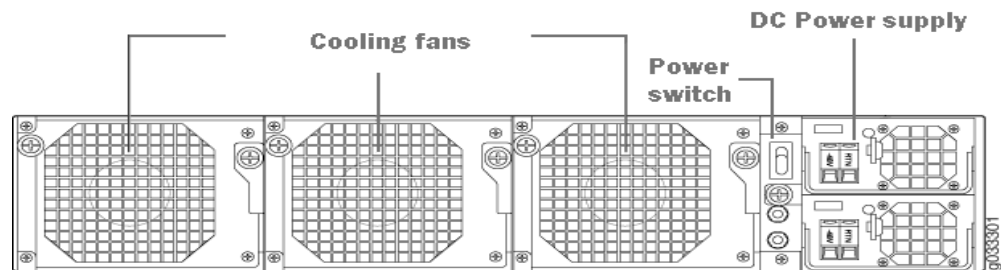


Cooling Fans

The STRM 5000 NEBS appliance has three cooling fans that are hot-swappable. The fan should be replaced in not less than 5 years of accumulated use. To replace the fan:

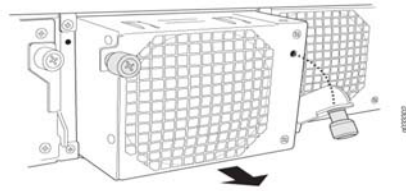
Step 1 Move to the rear of the chassis. Ensure that the fan is not working. See [Figure 15](#).

Figure 15 Rear of chassis



Step 2 Unfasten the 2 thumbscrews on the fan housing of the fan you wish to replace. See [Figure 16](#).

Figure 16 Unfasten thumbscrews



- Step 3** Open the ejector lever downwards to allow extraction of fan assembly.
- Step 4** Pull the front edge of the ejector lever to remove the fan completely.
- Step 5** Insert the new fan assembly in reverse order.
- Step 6** Open the ejector lever upwards to fully seat the new fan assembly.
- Step 7** Refasten the 2 thumbscrews on the fan housing.

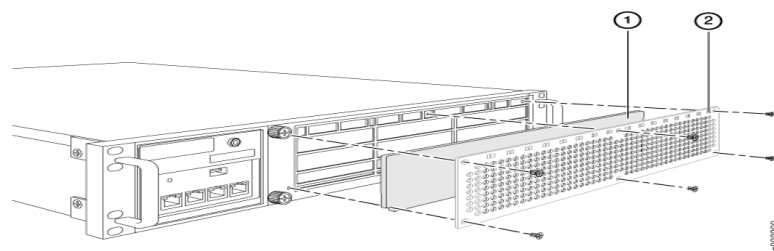
Note: Turn on the fan to check if it is inserted correctly.

Fan Filter

The fan filter should be replaced after 9000 hours of accumulated use. To replace the air inlet filter in STRM 5000 NEBS appliance:

- Step 1** Unfasten the 2 thumbscrews on the left of the front access cover.
- Step 2** Open the access door.
- Step 3** Pull out the front edge of the filter from the Velcro backing.
- Step 4** After you separate the filter from the Velcro backing, use your fingers to pull the filter out of the frame. See [Figure 17](#).

Figure 17 Removing the Fan Tray Filter



- Step 5** Carefully insert a new filter into the chassis front panel as shown in the figure and push the filter carefully to the left.
- Step 6** Push the filter to reach the end of the front door panel.
- Step 7** After you completely insert the filter, ensure that it is secure against the access door wall.

Step 8 Make sure the filter covers up the front panel holes.

Step 9 Close the access door and refasten the 2 thumbscrews.

