SRC-PE Software

Monitoring and Troubleshooting Guide

Release 1.0.x

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
www.juniper.net

Part Number: 530-020346-01, Revision A00

SRC-PE Software Monitoring and Troubleshooting Guide, Release 1.0.x
Writing: Linda Creed, Justine Kangas, Betty Lew, Helen Shaw, Brian Wesley Simmons, Sarah Lesway-Ball
Editing: Fran Mues
Illustration: Nathaniel Woodward
Cover Design: Edmonds Design

Revision History
6 April 2007—Revision 1

Software License

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions.

Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details.

For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.

END USER LICENSE AGREEMENT

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. The Parties. The parties to this Agreement are Juniper Networks, Inc. and its subsidiaries (collectively "Juniper"), and the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. The Software. In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, and updates and releases of such software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller. "Embedded Software" means Software which Juniper has embedded in the Juniper equipment.

3. License Grant. Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

a. Customer shall use the Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.

b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius software on multiple computers requires multiple licenses, regardless of whether such computers are physically contained on a single chassis.

c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface,

processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.

e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. Use Prohibitions. Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use the Embedded Software on non-Juniper equipment; (j) use the Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. Audit. Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. Confidentiality. The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. Ownership. Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. Warranty, Limitation of Liability, Disclaimer of Warranty. The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. Termination. Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. Taxes. All license fees for the Software are exclusive of taxes, withholdings, duties, or levies (collectively "Taxes"). Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software.

11. Export. Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. Commercial Computer Software. The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

13. Interface Information. To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. Third Party Software. Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at http://www.gnu.org/licenses/gpl.html, and a copy of the LGPL at http://www.gnu.org/licenses/lgpl.html.

15. Miscellaneous. This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentés confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattaché, soient redigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Table of Contents

About This Guide

This preface provides the following guidelines for using the *SRC-PE Software Monitoring and Troubleshooting Guide.*

Objectives

This guide provides information about how to monitor and troubleshoot the Session and Resource Control (SRC) software and a C-series platform. It describes how to configure logging and SNMP traps, and how to use the SRC CLI and C-Web interface for monitoring.

NOTE: If the information in the latest *SRC Release Notes* differs from the information in this guide, follow the *SRC Release Notes*.

Audience

This guide is intended for experienced system and network specialists working with JUNOSe routers and JUNOS routing platforms in an Internet access environment. We assume that readers know how to use the routing platforms, directories, and RADIUS servers that they will deploy in their SRC networks. For users who deploy the SRC software on a Solaris platform, we also assume that readers are familiar with the Lightweight Directory Access Protocol (LDAP) and the UNIX operating system.

If you are using the SRC software in a cable network environment, we assume that you are familiar with the *PacketCable Multimedia Specification* (PCMM) as defined by Cable Television Laboratories, Inc. (CableLabs) and with the Data-over-Cable Service Interface Specifications (DOCSIS) 1.1 protocol. We also assume that you are familiar with operating a multiple service operator (MSO) multimedia-managed IP network.

Documentation Conventions

The sample screens used throughout this guide are representations of the screens that are displayed when you install and configure the SRC software. The actual screens may differ.

For convenience and clarity, the installation and configuration examples show default file paths. If you do not accept the installation defaults, your paths will vary from the examples.

Table 1 defines notice icons used in this guide. Table 2 defines text conventions used throughout the documentation.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury.

Table 2: Text Conventions

Convention	Description	Examples
Bold typeface	■ Represents keywords, scripts, and tools in text. ■ Represents a GUI element that the user selects, clicks, checks, or clears.	■ Specify the keyword **exp-msg**. ■ Run the **install.sh** script. ■ Use the **pkgadd** tool. ■ To cancel the configuration, click **Cancel**.
Bold sans serif typeface	Represents text that the user must type.	user@host# **set cache-entry-age** *cache-entry-age*

`Monospace sans serif typeface`	Represents information as displayed on your terminal's screen, such as CLI commands in output displays.	`nic-locators {`
		`  login {`
		`  resolution {`
		`  resolver-name /realms/login/A1;`
		`  key-type LoginName;`
		`  value-type SaeId;`
		`  }`

Table 2: Text Conventions (continued)

Convention	Description	Examples
Regular sans serif typeface	■ Represents configuration statements. ■ Indicates SRC CLI commands and options in text. ■ Represents examples in procedures. ■ Represents URLs.	■ system ldap server { stand-alone; ■ Use the request sae modify device failover command with the force option. ■ user@host# . . . ■ http://www.juniper.net/techpubs/software/management/sdx/api-index.html
Italic sans serif typeface	Represents variables in SRC CLI commands.	user@host# **set local-address** *local-address*
Angle brackets	In text descriptions, indicate optional keywords or variables.	Another runtime variable is < gfwif > .
Key name	Indicates the name of a key on the keyboard.	Press Enter.
Key names linked with a plus sign (+) .	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
Italic typeface	■ Emphasizes words. ■ Identifies chapter, appendix, and book names. ■ Identifies distinguished names. ■ Identifies files, directories, and paths in text but not in command examples.	■ There are two levels of access: *user* and *privileged.* ■ *Chapter 2, Services.* ■ *o = Users, o = UMC* ■ The */etc/default.properties* file.
Backslash	At the end of a line, indicates that the text wraps to the next line.	Plugin.radiusAcct-1.class = \ net.juniper.smgt.sae.plugin\ RadiusTrackingPluginEvent
Words separated by the | symbol	Represent a choice to select one keyword or variable to the left or right of this symbol. (The keyword or variable may be either optional or required.)	diagnostic | line

Related Juniper Networks Documentation

With each SRC software release, we provide the *SRC Documentation CD,* which contains the documentation described in Table 3.

With each SRC Application Library release, we provide the *SRC Application Library CD*. This CD contains both the software applications and the *SRC Application Library Guide*.

The C-Web interface, which is based on the J-Web interface, is available for monitoring C-series platforms and the SRC software. For general information about the J-Web interface, see the *J-Web Interface User Guide*.

A complete list of abbreviations used in this document set, along with their spelled-out terms, is provided in the *SRC Getting Started Guide*.

Table 3: Juniper Networks C-series and SRC Technical Publications

Document	Description
Core Documentation Set	
C-series Hardware Guide	Describes the hardware platforms and how to install, maintain, replace, and troubleshoot them. The guide also includes specifications.
SRC-PE Getting Started Guide	Describes the SRC software and explains how to set up an initial configuration and manage a C-series platform. The guide describes how to set up and start the SRC CLI and C-Web, as well as other SRC configurations. It provides information about setting up an initial SRC configuration on a Solaris platform. The guide also describes how to upgrade the SRC software and how to use the SRC configuration tools. It includes reference material for the SRC documentation.
SRC-PE CLI User Guide	Describes how to use the SRC CLI, configure and monitor the platform with the CLI, and control the CLI environment. The guide also describes how to manage SRC components with the CLI.
SRC-PE Network Guide: SAE, Juniper Networks Routers, and NIC	Describes how to use and configure the SAE and the NIC. This guide also provides detailed information for using JUNOSe routers and JUNOS routing platforms in the SRC network.
SRC-PE Integration Guide: Network Devices, Directories, and RADIUS Servers	Describes how to integrate external components—network devices, directories, and RADIUS servers—into the SRC network. The guide provides detailed information about integrating specific models of the external components.
SRC-PE Services and Policies Guide	Describes how to work with services and policies. The guide provides an overview, configuration procedures, and management information. The guide also provides information about the SRC tools for configuring policies.
SRC-PE Subscribers and Subscriptions Guide	Describes how to work with residential and enterprise subscribers and subscriptions. The guide provides an overview, configuration procedures, and management information. This guide also provides information about the sample residential portals and enterprise service portals, including the Enterprise Manager Portal.
SRC-PE Monitoring and Troubleshooting Guide	Describes how to use logging, the SNMP agent, the SRC CLI, and the C-Web interface to monitor and troubleshoot SRC components. This guide also describes the SNMP traps.
SRC-PE Solutions Guide	Provides high-level instructions for SRC implementations. The guide documents the following scenarios: managing QoS services on JUNOSe routers; managing subscribers in a wireless roaming environment; providing voice over IP (VoIP) services; integrating the SRC software in a PCMM environment, including the use of the Juniper Policy Server (JPS); mirroring subscriber traffic on JUNOSe routers; demonstrating network resource management features in a sample IP television (IPTV) application; and demonstrating the integration of prepaid services in a sample application.
SRC-PE CLI Command Reference, Volume 1 *SRC-PE CLI Command Reference, Volume 2*	Together constitute information about command and statement syntax; descriptions of commands, configuration statements, and options; editing level of statement options; and a history of when a command was added to the documentation.
SRC-PE Comprehensive Index	Provides a complete index of the SRC guides, excluding the *C-series Hardware Guide* and the *SRC-PE CLI Command Reference*.
J-Web User Interface Guide	Provides general information about the J-Web interface.

Table 3: Juniper Networks C-series and SRC Technical Publications (continued)

Document	Description
Application Library	
SRC Application Library Guide	Describes how to install and work with applications that you can use to extend the capabilities of the SRC software. The guide documents the following applications: SRC-SG (SOAP Gateway) Web applications, applications to integrate the Juniper Networks Intrusion Detection and Protection (IDP) software into an SRC-managed environment, an application to provide endpoint security by integrating Juniper Networks Instant Virtual Extranet (IVE) Host Checker, a traffic-mirroring Web application, an application to integrate IP address managers with the SAE, an application to provide tracking and QoS control at the application level by integrating the SRC software with the Ellacoya deep packet inspection (DPI) platform, an application to control volume usage,and the SRC-ACP (Admission Control Plug-In) application.
Release Notes	
SRC-PE Release Notes *SRC Application Library Release Notes*	In the *Release Notes*, you will find the latest information about features, changes, known problems, resolved problems, supported platforms and network devices (such as Juniper Networks routers and CMTS devices), and third-party software. If the information in the *Release Notes* differs from the information found in the documentation set, follow the *Release Notes*. Release notes are included in the corresponding software distribution and are available on the Web.

Obtaining Documentation

To obtain the most current version of all Juniper Networks technical documentation, see the products documentation page on the Juniper Networks Web site at

http://www.juniper.net/

To order printed copies of this manual and other Juniper Networks technical documents or to order a documentation CD, which contains this manual, contact your sales representative.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation to better meet your needs. Send your comments to 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

Requesting Support

For technical support, open a support case using 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).

Part 1

Monitoring and Troubleshooting the SRC Software and C-series Platforms

Chapter 1

Overview of Monitoring and Troubleshooting Tools

The SRC software provides the following tools to help you monitor and troubleshoot your SRC environment:

- Logging support for SRC components
- System log server on C-series platforms
- NIC test commands to troubleshoot NIC configuration
- Router simulation to facilitate application testing
- Subscriber simulation to facilitate application testing
- SNMP agent to monitor SRC components as well as system performance. The agent can send data to SNMP network management systems.
- SNMP trap notification to SNMP management systems
- SRC CLI to monitor specified SRC components and C-series platforms
- C-Web interface to monitor specified SRC components and C-series platforms

In addition, the SRC Volume Tracking Application (SRC-VTA) in the SRC application library includes a Web-based application to test events.

The SRC software also includes various sample and test clients for the dynamic service activator, the SAE remote interface, and the SAE plug-in interface.

Part 2

Using Logging for the SRC Software and C-series Platforms

Chapter 2

Configuring Logging for SRC Components

This chapter describes logging for SRC components and applications. Topics include:

Overview of Logging

SRC components and applications generate event messages that you can save in logs—either by writing the messages to text files or by using the system log (syslog) facilities. You can use these logs to monitor the SRC components and troubleshoot problems. By default, log files are stored in the */var/log* directory.

Each SRC component has its own logging configuration. For example, the license server, the NIC, the SAE, and SNMP each have logging configuration. The C-series platform includes a system log server that you can configure to manage messages generated on that platform.

You can use the CLI to configure logging on a C-series platform or on a Solaris platform and to configure the system log server on a C-series platform. You can also use SRC configuration applications to configure component logging on a Solaris platform. For the SNMP agent, you can also configure logging through the agent's local configuration tool.

Related Information

For additional information, see the following sources:

- *SRC-PE Getting Started Guide, Chapter 14, Configuring System Logging for a C-series Platform*
- The syslog Protocol—draft-ietf-syslog-protocol-16.txt (July 2006 expiration)

- *SRC-PE Getting Started Guide, Chapter 23, Configuring and Starting the SNMP Agent with the SRC CLI*
- *SRC-PE Getting Started Guide, Chapter 31, Configuring and Starting the SDX SNMP Agent on a Solaris Platform*

Categories and Severity Levels for Event Messages

In the logging configuration, you can specify a filter for each type of log. This filter can include an expression that defines the *categories* and *severity levels* of event messages that the software saves.

Defining Categories

The category of an event message defines the SRC component that generated the event message. If you want to view only event logs in a specific category, you can define a variable <category>, which is a text string that matches the name of a category. This variable is not case sensitive. To view the names of categories for event messages, view a log file for one of the default filters.

For example, the category Cops defines event messages generated by the COPS server. Similarly, the category CopsMsg defines a particular sort of event message that the COPS server generates.

Juniper Networks Customer Service can also provide names of categories, especially for troubleshooting purposes.

Defining Severity Levels

The event filter provides 128 levels of severity numbered 1–127. A higher number indicates a higher level of severity. Common levels of severity also have a specific name, as shown in Table 4.

CAUTION: Enabling the generation of debug log messages has a negative affect on system performance. Do not enable debug log messages unless you are instructed to do so by Juniper Networks Technical Assistance Center (JTAC).

Table 4: Named Severity Levels

Name	Severity Level
logmin	1
debug	10
info	20
notice	30
warning	40
error	50
crit	60
alert	70
emerg	80

Table 4: Named Severity Levels (continued)

Name	Severity Level
panic	90
logmax	127

You can define a severity level as follows:

- Specify an explicit severity. For example:
  - debug—Defines only debug messages
- Specify a minimum severity and a maximum severity. For example:
  - info-warning—Defines messages of minimum severity level of info and a maximum severity level of warning
  - Accept the default minimum (logmin) or maximum (logmax) severity by omitting the minimum or maximum severity. For example:
  - info-—Defines messages of minimum severity level info and maximum severity level logmax
  - -warning—Defines messages of minimum severity level logmin and maximum severity level warning
- Specify no severities to log all event messages.

The syntax for the severity takes the format:

[< severity >] | [< minimumSeverity >]-[< maximumSeverity >]

Use either the name or the number of a severity level shown in Table 4 for the variables in this syntax.

Defining Filters

You specify a filter by defining an expression with the following format:

singlematch [,singlematch]*

- singlematch—[!] (< category > | ([< category >]/[< severity >] | [< minimumSeverity >]-[< maximumSeverity >]))
- !—Do not log matching events
- < category > —See *Defining Categories* on page 8
- [< severity >] | [< minimumSeverity >]-[< maximumSeverity >]—See *Defining Severity Levels* on page 8.

The software filters events by evaluating each subexpression in order from left to right. When the software determines that an event message matches a subexpression, the software logs or ignores the message accordingly. You can specify an unlimited number of subexpressions; however, the order in which you specify the subexpressions affects the result.

Table 5 shows some examples of filters.

Table 5: Examples of Filters for Event Messages

Syntax	Event Messages Saved
/	All event messages
/info-	Event messages of level info and above from all categories
Cops/debug	Debug events from COPS category only
!Cops,/debug	All debug events except those from COPS category
CopsMsg/info-,!CopsMsg,Cops	All messages from COPS category, except those from CopsMsg category with level less than info

Rotation of Log Files

On C-series platforms, log files that contain entries are rotated daily when other daily system tasks run on the system. The system retails 5 log files for a component before overwriting the oldest file.

When a new log file is opened to replace a file from the previous day that contains content, a number (1–4) is appended to the name of the older file. For example, *sae_debug.log.4* would be the oldest file in the rotation, s*ae_debug.log.1* would be the newest file in the rotation; *sae_debug.log* would be the active log file for SAE.

On C-series platforms, the software compresses log files and appends the *.gz* suffix; for example, *sae_debug.log.4.gz*. Log files are stored in the */opt/UMC/component-name/var/log directory*; for example, */opt/UMC/sae/var/log*.

If you are using the SRC software on a Solaris platform, you can use **logadm** on Solaris version 9 or greater, or you can install the log rotate application from the following Web site:

http://www.sunfreeware.com

Chapter 3

Configuring Logging for SRC Components with the CLI

This chapter describes how use the SRC CLI to configure logging for SRC components. You can use the CLI to configure logging on a Solaris platform or on a C-series platform. Topics include:

You can also use SRC configuration applications to configure component logging on a Solaris platform. See *Chapter 4, Configuring Logging for SRC Components on a Solaris Platform*.

Topics in this chapter include:

Before You Configure Logging

Before you configure logging for SRC components, you should be familiar with the logging filters that you can configure. If you use a syslog log facility, you should be familiar with the syslog protocol. For information about logging filters see, *Chapter 2, Configuring Logging for SRC Components*.

Configuration Statements for Component Logging

Use the following configuration statements to configure logging for SRC components. You access these statements from the hierarchy for a component, such as:

- [edit shared acp configuration]
- [edit shared sae configuration]
- [edit shared nic scenario *scenario-name*]
- [edit snmp agent]
- [edit slot 0 jps].

```
logger name{
    file-logger {
        filter filter;
        filename filename;
        rollover-filename rollover-filename;
        maximum-file-size maximum-file-size;
    }

    syslog-logger {
        filter filter;
        syslog-host syslog-host;
        syslog-facility syslog-facility;
        format format;
    }
}
```

For detailed information about each configuration statement, see *SRC-PE CLI Command Reference.*

Configuring a Component to Store Log Messages in a File

Use the following statements to configure an SRC component to store log messages in a file:

```
logger name file {
    filter filter;
    filename filename;
    rollover-filename rollover-filename;
    maximum-file-size maximum-file-size;
}
```

When you enable logging to a file, by default SRC components and applications write log files in the */opt/UMC/*<*component-directory*>*/var/log* folder for a component, such as */opt/UMC/sae/var/log*.

All log files with the file extension .log in a *var/log* directory are rotated daily. When a new log file is created, the previous day's file is compressed and saved.

If you plan to filter log messages, you should be familiar with severity levels and filters for logging before you configure system logging for a component. See *Chapter 2, Configuring Logging for SRC Components*.

To configure component logging to a file:

1. From configuration mode, access the configuration statement that configures the logging destination for the component.

   [edit]
   user@host# *component-hierarchy* **logger** *name* **file**

   For example:

   [edit]
   user@host# **edit shared sae configuration logger sae-file-log-1 file**

   [edit]
   user@host# **edit snmp agent logger snmp-file-log-1 file**

   [edit]
   user@host# **edit slot 0 jps logger jps-file-log-1 file**

2. Specify the filter to define which event messages the software logs or disregards.

   [edit shared sae configuration logger sae-file-log-1 file]
   user@host# **set filter** *filter*

   If you do not specify a filter, logging to the specified file is disabled.

   Filters can specify the logging level, such as debug, or can specify expressions.

3. Specify the absolute path of the filename that contains the current log files.

   [edit shared sae configuration logger sae-file-log-1 file]
   user@host# **set filename** *filename*

   Make sure that the user under which the J2EE application server or Web application server runs has write access to this folder. If this user does not have write access to the default folder, configure the component or application to write logs in folders to which the user has write access.

4. (Optional)—Solaris platform; not recommended for the C-series platform) Specify the absolute path of the filename that contains the log history.

   [edit shared sae configuration logger sae-file-log-1 file]
   user@host# **set rollover-filename** *rollover-filename*

When the log file reaches the maximum size, the software closes the log file and renames it with the name you specify for the rollover file. If a previous rollover file exists, the software overwrites it. The software then reopens the log file and continues to save event messages in it.

NOTE: On a C-series platform, log files are automatically rotated on a daily basis. Consider whether specifying a rollover filename is needed for SRC software running on a C-series platform. If you do configure a rollover file when files are rotated, the software creates five compressed versions of partial log files, and one uncompressed log file.

5. (Optional)—Solaris platform; not recommended for the C-series platform) Specify the maximum size of the log file and the rollover file.

   [edit shared sae configuration logger sae-file-log-1 file]
   user@host# **set maximum-file-size** *maximum-file-size*

   Do not set the maximum file size to a value greater than the available disk space.

NOTE: On a C-series platform, log files are automatically rotated on a daily basis. Typically you do not specify a maximum file size when log files are rotated.

Configuring System Logging

Use the following statements to configure the SRC software to send log messages to the system logging facility:

```
logger name syslog {
    filter filter;
    host host;
    facility facility;
    format format;
}
```

You can configure components to send log messages to the system log server (also called a syslog server) on the platform on which the SRC software is running.

If you plan to filter log messages, you should be familiar with severity levels and filters for logging before you configure system logging for a component. See *Chapter 2, Configuring Logging for SRC Components*.

To component logging to the system log server:

1. From configuration mode, access the configuration statement that configures the logging destination for the component. For example:

   [edit]
   user@host# *component-hierarchy* **logger** *name* **syslog**

   For example:

   [edit]
   user@host# **edit shared sae configuration logger sae-sys-1 syslog**

   [edit]
   user@host# **edit snmp agent logger snmp-sys-1 syslog**

   [edit]
   user@host# **edit slot 0 jps logger jps-sys-1 syslog**

2. (Optional) Specify the filter to define which event messages the software logs or disregards.

   [edit shared sae configuration logger sae-sys-1 syslog]
   user@host# **set filter** *filter*

   Filters can specify the logging level, such as debug, or can specify expressions.

3. (Optional) Change the IP address or name of a host that collects event messages by means of a standard system logging daemon.

   [edit shared sae configuration logger sae-sys-1 syslog]
   user@host# **set host** *host*

   By default, the host is loghost for the syslog server on the local host. (Configuration in the */etc/hosts* file sets loghost to localhost.)

   Make sure that the user under which the J2EE application server or Web application server runs has write access to this folder. If this user does not have write access to the default folder, configure the component or application to write logs in folders to which the user has write access.

4. (Optional) Specify the type of system log in accordance with the system logging protocol, a value of 0–23.

   [edit shared sae configuration logger sae-sys-1 syslog]
   user@host# **set facility** *facility*

5. (Optional) Specify the MessageFormat string that indicates how the information in an event message is printed.

   [edit shared sae configuration logger sae-sys-1 syslog]
   user@host# **set format** *format*

   Specify a MessageFormat string as defined in

   http://java.sun.com/j2se/1.4.2/docs/api/java/text/MessageFormat.html

   The fields available for events are:

   - 0—Time and date of the event
   - 1—Name of the thread generating the event
   - 2—Text message of the event
   - 3—Category of the event
   - 4—Priority of the event

Chapter 4

Configuring Logging for SRC Components on a Solaris Platform

This chapter describes how to configure logging for SRC components and applications on a Solaris platform using the SRC configuration applications that run only on Solaris platforms.

You can also use the CLI that runs on Solaris platforms and the C-series platform to configure the component logging. See *Chapter 3, Configuring Logging for SRC Components with the CLI*.

Topics in this chapter include:

Before You Configure Logging

Before you configure logging on a Solaris system for SRC components, you should be familiar with the logging filters that you can configure, If you use a syslog log facility, you should be familiar with the syslog protocol.

For more information see, *Chapter 2, Configuring Logging for SRC Components*.

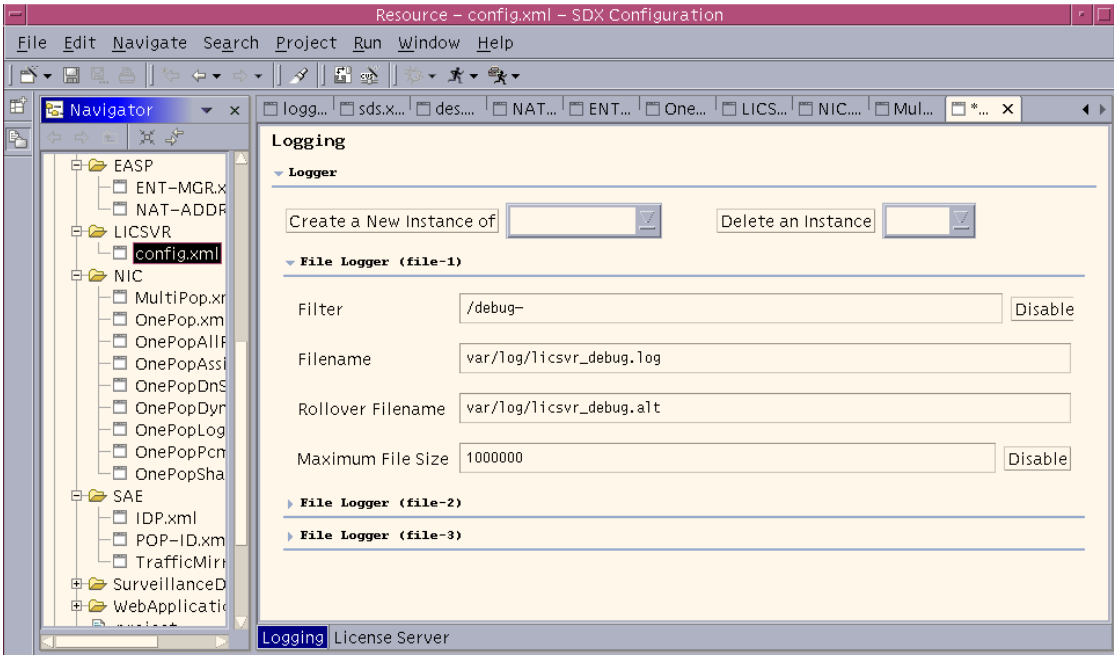
Accessing the Logging Configuration for All Components Except the NIC

To use SDX Configuration Editor to access a component's logging configuration:

1. In the navigation pane, select the configuration file for the component for which you want to configure logging.

2. Select the **Logging** tab, and expand the Logger section.

   Each SRC component comes with a default logging configuration. The Logging pane changes depending on the component that you select in the navigation pane. The following pane shows the file logging configuration for a license server.



Most components have default logging configurations that you can use as they are or modify.

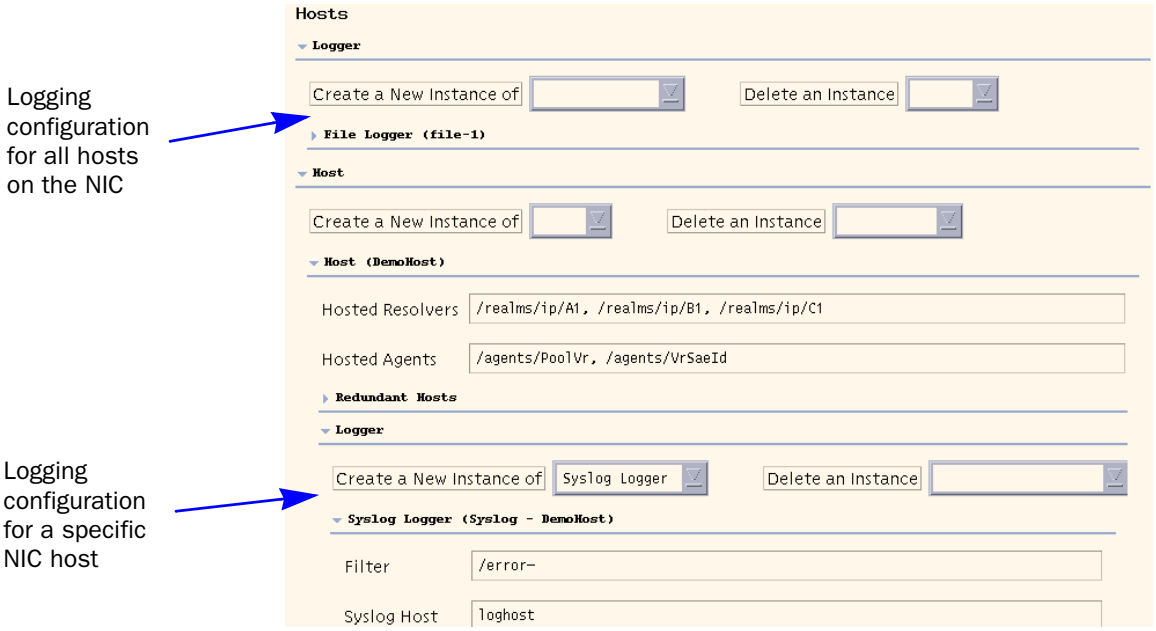
Accessing the Logging Configuration for the NIC

To use SDX Configuration Editor to access logging configuration for a NIC configuration scenario:

1. In the navigation pane, select the NIC configuration scenario for which you want to configure logging.

2. Select the **Host**s tab, and expand the Logger section.

   In the Hosts pane, you can configure logging for all NIC hosts for the NIC configuration scenario that you selected, or you can configure logging separately for each NIC host.



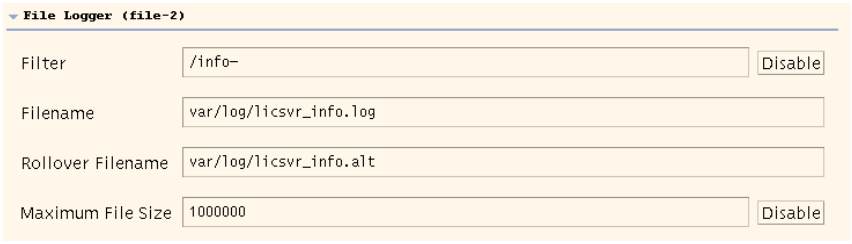
Saving Event Messages in Text Files

To use SDX Configuration Editor to configure the software to save event messages in text files:

1. In the navigation pane, select the component for which you want to configure logging for text files.

2. Select the **Logging** tab. (For NIC components, select the **Hosts** tab.)

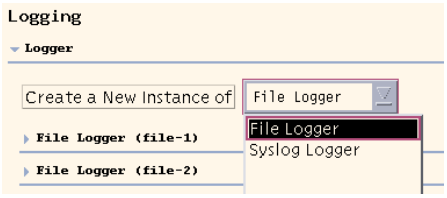
   The following example shows the file logging configuration fields.



   Each logging configuration can have multiple instances, with each instance sending different types of logs to different files.

3. (Optional) To create a new logging instance:

   a. Select **File Logger** in the Create a New Instance of list, and **select Create a New Instance of**.



      The Create a New Instance dialog box appears.

   b. Assign a name to the instance, and click **OK**.

      The instance appears in the Logging or Hosts pane.

4. In the section for an individual logger, edit or accept the default values for the fields.

   See *File Logging Fields* on page 21.

5. Select **File > Save**.

6. Right-click the configuration file, and select **SDX System Configuration > Export to LDAP Directory**.

File Logging Fields

In SDX Configuration Editor, you can modify the following fields in a logger section of the Logging pane in a configuration file.

You can also modify the values in this section in a text file that contains logging properties for an SRC component.

Filter

- Disables or enables and specifies a filter that determines the type of messages that this log file contains.
- Value— < Filter >

  See *Deleting Logs and Process Files for SRC Components* on page 24
- Default—The default value is different for each type of component.

Filename

- Absolute path of the filename that contains the current logs.
- Value—Text string
- Default—By default, SRC components and applications write log files in the folder where the application is started. However, the user under which the J2EE application server or Web application server runs may not have write access to this folder. For logging to work properly, configure the component or application to write logs in folders to which this user has write access. If you are using the version of JBoss packaged with the SRC software, add the absolute path */opt/UMC/jboss/server/default/log/* to the filenames and rollover filename for each log. For example, for the debug log, use the filename */opt/UMC/jboss/server/default/log/vta_debug.log*.
- Example—*/opt/UMC/jboss/server/default/log/*

Rollover Filename

- Absolute path of the filename that contains the log history. When the log file reaches the maximum size, the software closes the log file and renames it with the name you specify for the rollover file. If a previous rollover file exists, the software overwrites it. The software then reopens the log file and continues to save event messages in it.
- Value—Text string
- Default—The default value is different for each type of component.
- Example—*/opt/UMC/jboss/server/default/log/*

Maximum File Size

- Disables or enables and sets the maximum size of the log file and the rollover file.
- Value—Number of kilobytes in the range 0–4294967295
- Guidelines—Do not set the maximum file size to a value greater than the available disk space.
- Default—1000000

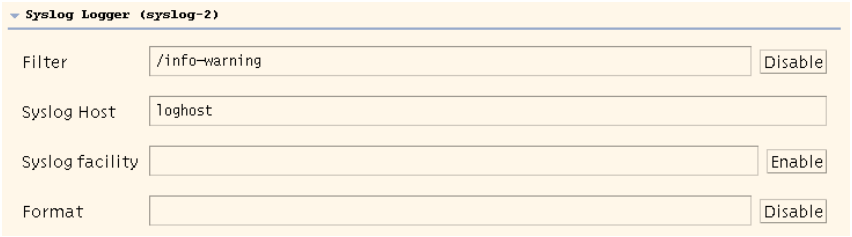
Saving Event Messages on a Logging Server

You can configure the software to save event messages on a host that you have configured as a system logging server. You can also specify the facility for system logging and the format in which the messages will be saved on the host.

To use SDX Configuration Editor to configure the software to save event messages in text files:

1. In the navigation pane, select the component for which you want to configure logging to a system logging server.
2. Select the **Logging** tab. (For NIC components, select the **Hosts** tab.)

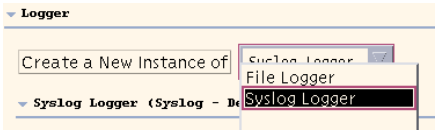
   The following example shows the system logging configuration fields.



   Each logging configuration can have multiple instances, with each instance sending different types of logs to different system logging servers.

3. (Optional) To create a new logging instance:

   a. Select **Syslog Logger** in the Create a New Instance of list, and click **Create a New Instance of**.



   The Create a New Instance dialog box appears.

   b. Assign a name to the instance, and click **OK**.

   The instance appears in the Logging or Hosts pane.

4. In the section for an individual logger, edit or accept the default values in the fields.

   See *System Logging Fields* on page 23.

   In the filter field of each type of log, you can specify an expression that defines the *categories* and *severity levels* of event messages that the software saves.

5. Select **File > Save**.

6. Right-click the configuration file, and select **SDX System Configuration > Export to LDAP Directory**.

System Logging Fields

In SDX Configuration Editor, you can modify the following fields in a system logger section of the Logging pane in a configuration file to configure logging to a system log file.

Filter

- Disables or enables and specifies a filter that determines the type of messages that this log file contains.
- Value— < Filter >

  For information about defining filters, see *Chapter 2, Configuring Logging for SRC Components*.
- Default—The default value is different for each type of component.

Syslog Host

- IP address or name of a host that collects event messages by means of a standard system logging daemon.
- Value—IP address or text string
- Default—loghost

Syslog facility

- Type of system log in accordance with the system logging protocol.
- Value—Integer in the range 0–23; each integer corresponds to the standard number for a system logging client
- Default—3

Format

- Specifies how the information in an event message is printed.
- Value—MessageFormat string as specified in

  http://java.sun.com/j2se/1.4.2/docs/api/java/text/MessageFormat.html

  The fields available for events are:
  - 0—Time and date of the event
  - 1—Name of the thread generating the event
  - 2—Text message of the event
  - 3—Category of the event
  - 4—Priority of the event.
- Default—None
- Example for text files—{0,time,HH:mm:ss.SSS z} {0,date,dd.MM.yyyy} [{1}] [{3}] [{4}] {2}

  A sample message for the sample setting is:

  14:13:24.366 EST 19.01.2004 [main] [Start-up module] [20] SAE STARTUP DONE

- Example for syslog—SSP[{1}] [{3}] [{4}] {2}

  Because the system log system usually timestamps all log messages, no time information is included in the default format. A sample message for the sample setting is:

  SSP[main] [Start-up module] [20] SAE STARTUP DONE

Deleting Logs and Process Files for SRC Components

For the following SRC components, you can issue a command to clean (delete) certain files that are generated by the process for that component.

- License server
- NIC hosts and monitors
- SAE
- SNMP agent

This command cleans:

- Text files that contain event messages.
- The files to which the machine on which you installed the component redirects the stderr and stdout outputs for that the component.
- Other types of files that the process generates and that are not used to reestablish the state of the SRC component when you restart it. These files vary according to each SRC component.

This command does not delete:

- Configurations in the directory or in local files.
- Information generated by the system logging facilities.
- Files that are required to reestablish the state of the SRC component when you restart it.

We recommend that you clean these files for a component when you stop it. When you restart the component, the SRC software creates new files with the same names as the ones you deleted. Cleaning the files keeps the file size small so that you can find data in the files more easily.

Deleting Log Files for SRC Components

To delete (clean) the log files for an SRC component:

1. On the host on which you installed the SRC component, log in as `root` or as another authorized user.
2. Access the folder in which you installed the component.

   cd /opt/UMC/<sdxComponent>/etc

   <sdxComponent> is the name of the folder in which the SRC component is installed.

   For information about component names, see *SRC-PE Getting Started Guide, Chapter 28, Installing the SRC Software on a Solaris Platform*.
3. Stop the component.

   ./<sdxComponent> stop
4. Clean the logs.

   ./<sdxComponent> clean

   The system responds with a status message.

5. Restart the SRC component.

   ./<sdxComponent> start

For example, to clean files for the SAE, enter the following commands:

```
cd /opt/UMC/sae/etc
./sae stop
./sae clean
./sae start
```

Part 3

Using Simulated Router Drivers and Simulated Subscribers for Testing

Chapter 5

Configuring a Simulated Router Driver for Testing with the SRC CLI

This chapter describes how to configure a simulated router driver with the SRC CLI.

You can also use SDX Configuration Editor, which runs on Solaris platforms, to configure simulated router drivers. See *Chapter 6, Configuring a Simulated Router Driver for Testing with SDX Configuration Editor*.

Topics in this chapter include:

Overview of Simulated Router Drivers

Simulated router drivers allow you to create subscriber sessions without connecting to a router. You can then use the simulated subscriber sessions to test SAE applications.

The SRC software has a default simulated router driver instance called default@simJunos.

Configuring Simulated Router Drivers

You configure a simulated router in the same way that you configure a real router.

Before you configure a simulated router driver:

- Make sure that you configure an interface classification script for the simulated router.

  See *SRC-PE Subscribers and Subscriptions Guide, Chapter 6, Classifying Interfaces and Subscribers with the SRC CLI*.

- Configure the SAE to instantiate a simulated router driver for each simulated router that you create.

- (Optional) Configure a session store for a simulated router driver. The driver uses the session store to store subscriber sessions, service sessions, and policies.

  See *SRC-PE Network Guide, Chapter 2, Configuring the SAE with the SRC CLI.*

Use the following configuration statements to configure simulated router drivers:

```
shared sae configuration driver simulated name {
    driver-type (junos | junose | pcmm);
    router-version router-version;
    driver-address driver-address;
    transport-router transport-router;
}
```

To configure simulated router drivers:

1. From configuration mode, access the configuration statement that configures simulated router drivers. In this sample procedure, west-region is the name of the SAE group, and default@simjunos is the name of the simulated router driver.

   ```
   [edit]
   user@host# edit shared sae group west-region configuration driver simulated
   default@simJunos
   ```

2. Configure the type of device that the simulated driver simulates.

   ```
   [edit shared sae group west-region configuration driver simulated
   default@simJunos]
   user@host# set driver-type (junos | junose | pcmm)
   ```

3. (Optional) Configure the version of the router software to simulate. This is the software version that is sent by the router.

   ```
   [edit shared sae group west-region configuration driver simulated
   default@simJunos]
   user@host# set router-version router-version
   ```

4. Configure the IP address of the device driver.

   ```
   [edit shared sae group west-region configuration driver simulated
   default@simJunos]
   user@host# set driver-address driver-address
   ```

5. (Optional) Configure the name of a virtual router that is used to connect to the SAE. This value is passed to the router initialization script. It is not supported on the JUNOS routing platform.

   ```
   [edit shared sae group west-region configuration driver simulated
   default@simJunos]
   user@host# set transport-router transport-router
   ```

6. (Optional) Verify the configuration of the simulated driver.

```
[edit shared sae group west-region configuration driver simulated
default@simJunos]
user@host# show
driver-type junos;
router-version 8.4;
driver-address 10.10.90.5;
```

Related Information

For additional information, see the following source:

- For information about setting up SAE groups, see *SRC-PE Getting Started Guide, Chapter 16, Setting Up an SAE with the SRC CLI.*

Chapter 6

Configuring a Simulated Router Driver for Testing with SDX Configuration Editor

This chapter describes how to configure a simulated router driver with SDX Configuration Editor. You can also use the SRC CLI that runs on Solaris platforms and the C-series platform to configure simulated router drivers. See *Chapter 5, Configuring a Simulated Router Driver for Testing with the SRC CLI*. Topics in this chapter include:

Overview of Simulated Router Drivers

Simulated router drivers allow you to create subscriber sessions without connecting to a router. You can then use the simulated subscriber sessions to test SAE applications.

The SRC software has a default simulated router driver instance called default@simJunos.

Configuring Simulated Router Drivers

You configure a simulated router in the directory in the same way that you configure a real router.

Before you configure a simulated router driver:

- Make sure that you configure an interface classification script for the simulated router.

  See *SRC-PE Subscribers and Subscriptions Guide, Chapter 7, Classifying Interfaces and Subscribers on a Solaris Platform*.

- Configure the SAE to instantiate a simulated router driver for each simulated router that you create.

- (Optional) Configure a session store for a simulated router driver. The driver uses the session store to store subscriber sessions, service sessions, and policies.

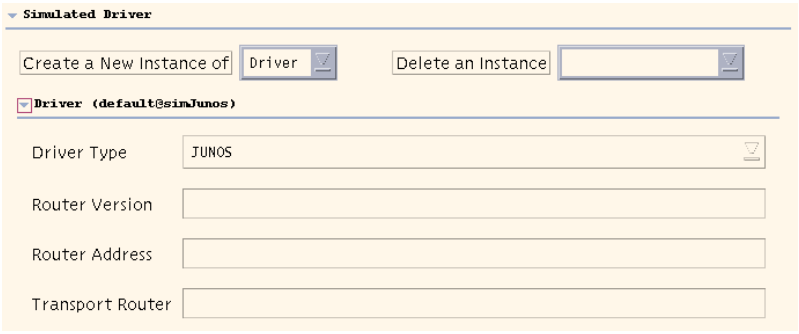
  See *SRC-PE Network Guide, Chapter 3, Configuring the SAE with SDX Configuration Editor*.

To use SDX Configuration Editor to create simulated router driver instances:

1. In the navigation pane, select an SAE configuration file for a POP.
2. Select the **Router** tab, and expand the Simulated Driver section.
3. In the Simulated Driver section next to the Create a New Instance of button, select **Driver**, and click **Create a New Instance of**.

   The Create New Instance dialog box appears.
4. Assign a name to the instance, and click **OK**.

   The new instance appears in the Simulated Driver area.



5. In the section for the new simulated router driver, edit or accept the default values for the fields.

   See *Simulated Driver Fields* on page 35.
6. Select **File > Save**.
7. Right-click the configuration file, and select **SDX System Configuration > Export to LDAP Directory**.

Simulated Driver Fields

In SDX Configuration Editor, you can modify the following fields in the Simulated Driver section of the Router pane in an SAE configuration file.

Driver Type

- Type of device that the simulated driver simulates.
- Value—JUNOS, JUNOSe, or PCMM
- Default—JUNOS
- Property name—Router.sim.<simulated router name>.type

Router Version

- Version of the router to simulate.
- Value—Software version that is sent by the router; for example, 6.4
- Default—No value
- Property name—Router.sim.<simulated router name>.version

Router Address

- Address of the router that is available for router initialization scripts.
- Value—IP address
- Default—10.0.0.1
- Property name—Router.sim.<simulated router name>.routerIp

Transport Router

- Name of a virtual router that is used to connect to the SAE. This value is passed to the router initialization script. It is not supported on the JUNOS routing platform.
- Value—Name of a virtual router
- Default—No value
- Property name—Router.sim.<simulated router name>.transportRouter

Chapter 7

Using Simulated Subscribers for Testing with the SRC CLI

This chapter describes how to log in and log out simulated subscribers with the CLI. Topics include:

Overview of Simulated Subscribers

Simulated subscribers allow you to create subscriber sessions without connecting to a router or other device. When developing a portal, you can log in as a simulated subscriber to test a portal without a router or a client PC.

Commands to Manage Simulated Subscribers

You can use the following operational mode commands to manage simulated subscribers.

- request sae login ipv4 authenticated-dhcp
- request sae login ipv4 authenticated-interface
- request sae login ipv4 unauthenticated-dhcp
- request sae login ipv4 unauthenticated-interface
- request sae logout dn
- request sae logout ip
- request sae logout login-name
- request sae logout session-id

- show sae subscribers
- show sae subscribers dn
- show sae subscribers ip
- show sae subscribers login-name
- show sae subscribers session-id

For detailed information about each command, see the *SRC-PE CLI Command Reference*.

Logging in Simulated Subscribers with the CLI

You can log in IPv4 subscribers who are:

- Authenticated DHCP subscribers
- Authenticated interface subscribers
- Unauthenticated DHCP subscribers
- Unauthenticated interface subscribers

Logging in simulated subscribers allows you to test your SRC application without the need for a router or other device.

You can log out from the simulated subscriber session in the same way that you log out from other subscriber sessions.

Logging In Authenticated DHCP Subscribers

Use the following command to log in simulated IPv4 authenticated DHCP subscribers:

request sae login ipv4 authenticated-dhcp virtual-router *virtual-router* address *address* login-name *login-name* mac-address *mac-address* <service-bundle *service-bundle*> <radius-class *radius-class*> <interface-name *interface-name*> <interface-alias *interface-alias*> <interface-description *interface-description*> <nas-port-id *nas-port-id*>

To log in a simulated IPv4 authenticated DHCP subscriber:

1. Issue the request sae login ipv4 authenticated-dhcp command. Specify the virtual-router, address, login-name, and mac-address options.

   user@host> **request sae login ipv4 authenticated-dhcp virtual-router** *virtual-router* **address** *address* **login-name** *login-name* **mac-address** *mac-address*

2. (Optional) To specify the service bundle used when logging in the simulated subscriber, use the service-bundle option.

3. (Optional) To specify the RADIUS class used when logging in the simulated subscriber, use the radius-class option.

4. (Optional) To specify the virtual interface used when logging in the simulated subscriber, use the interface-name option.

5. (Optional) To specify the interface description used when logging in the simulated subscriber, use the interface-alias option.

   If you are simulating JUNOSe routers, the interface alias is the description that is configured on JUNOSe routers with the interface description command.

6. (Optional) To specify the alternate interface name used when logging in the simulated subscriber, use the interface-description option.

7. (Optional) To specify the port identifier of an interface used when logging in the simulated subscriber, use the nas-port-id option.

Logging In Authenticated Interface Subscribers

Use the following command to log in simulated IPv4 authenticated interface subscribers:

request sae login ipv4 authenticated-interface virtual-router *virtual-router* address *address* login-name *login-name* <service-bundle *service-bundle*> <radius-class *radius-class*> <interface-name *interface-name*> <interface-alias *interface-alias*> <interface-description *interface-description*> <nas-port-id *nas-port-id*>

To log in a simulated IPv4 authenticated interface subscriber:

1. Issue the request sae login ipv4 authenticated-interface command. Specify the virtual-router, address, and login-name options.

   user@host> **request sae login ipv4 authenticated-interface virtual-router** *virtual-router* **address** *address* **login-name** *login-name*

2. (Optional) To specify the service bundle used when logging in the simulated subscriber, use the service-bundle option.

3. (Optional) To specify the RADIUS class used when logging in the simulated subscriber, use the radius-class option.

4. (Optional) To specify the virtual interface used when logging in the simulated subscriber, use the interface-name option.

5. (Optional) To specify the interface description used when logging in the simulated subscriber, use the interface-alias option.

   If you are simulating JUNOSe routers, the interface alias is the description that is configured on JUNOSe routers with the interface description command.

6. (Optional) To specify the alternate interface name used when logging in the simulated subscriber, use the interface-description option.

7. (Optional) To specify the port identifier of an interface used when logging in the simulated subscriber, use the nas-port-id option.

Logging In Unauthenticated DHCP Subscribers

Use the following command to log in simulated IPv4 unauthenticated DHCP subscribers:

request sae login ipv4 unauthenticated-dhcp virtual-router *virtual-router* address *address* mac-address *mac-address* <login-name *login-name*> <service-bundle *service-bundle*> <radius-class *radius-class*> <interface-name *interface-name*> <interface-alias *interface-alias*> <interface-description *interface-description*> <nas-port-id *nas-port-id*>

To log in a simulated IPv4 unauthenticated DHCP subscriber:

1. Issue the request sae login ipv4 unauthenticated-dhcp command. Specify the virtual-router, address, and mac-address options.

   user@host> **request sae login ipv4 unauthenticated-dhcp virtual-router** *virtual-router* **address** *address* **mac-address** *mac-address*

2. (Optional) To specify the fully-qualified name used to log in the simulated subscriber, use the login-name option.

3. (Optional) To specify the service bundle used when logging in the simulated subscriber, use the service-bundle option.

4. (Optional) To specify the RADIUS class used when logging in the simulated subscriber, use the radius-class option.

5. (Optional) To specify the virtual interface used when logging in the simulated subscriber, use the interface-name option.

6. (Optional) To specify the interface description used when logging in the simulated subscriber, use the interface-alias option.

   If you are simulating JUNOSe routers, the interface alias is the description that is configured on JUNOSe routers with the interface description command.

7. (Optional) To specify the alternate interface name used when logging in the simulated subscriber, use the interface-description option.

8. (Optional) To specify the port identifier of an interface used when logging in the simulated subscriber, use the nas-port-id option.

Logging In Unauthenticated Interface Subscribers

Use the following command to log in simulated IPv4 unauthenticated interface subscribers:

request sae login ipv4 unauthenticated-interface virtual-router *virtual-router* interface-name *interface-name* <address *address*> <login-name *login-name*> <service-bundle *service-bundle*> <radius-class *radius-class*> <interface-alias *interface-alias*> <interface-description *interface-description*> <nas-port-id *nas-port-id*>

To log in a simulated IPv4 authenticated interface subscriber:

1. Issue the request sae login ipv4 authenticated-interface command. Specify the virtual-router and interface-name options.

   user@host> **request sae login ipv4 authenticated-interface virtual-router** *virtual-router* **interface-name** *interface-name*

2. (Optional) To specify the IP address from which you log in the simulated subscriber, use the address option.

3. (Optional) To specify the fully-qualified name used to log in the simulated subscriber, use the login-name option.

4. (Optional) To specify the service bundle used when logging in the simulated subscriber, use the service-bundle option.

5. (Optional) To specify the RADIUS class used when logging in the simulated subscriber, use the radius-class option.

6. (Optional) To specify the interface description used when logging in the simulated subscriber, use the interface-alias option.

   If you are simulating JUNOSe routers, the interface alias is the description that is configured on JUNOSe routers with the interface description command.

7. (Optional) To specify the alternate interface name used when logging in the simulated subscriber, use the interface-description option.

8. (Optional) To specify the port identifier of an interface used when logging in the simulated subscriber, use the nas-port-id option.

Logging Out Simulated Subscribers with the CLI

You can log out subscribers who are accessible by:

- DN
- IP address
- Login name
- Session ID

To view all subscriber sessions:

user@host> **show sae subscribers**

Logging Out Subscribers by DN

To log out subscribers who are accessible by DN:

1. Issue the show sae subscribers dn command to view the subscribers who are accessible by DN.
2. Issue the request sae logout dn command to log out all subscribers who are accessible by DN.
   - To log out specific subscribers, use the filter option and specify all or part of the DN for the subscribers that you want to log out.

     user@host> **request sae logout dn filter** *filter*
   - To specify that no confirmation is requested before the software logs out the subscribers, use the force option.

     user@host> **request sae logout dn force**
     user@host> **request sae logout dn filter** *filter* **force**

Logging Out Subscribers by IP Address

To log out subscribers who are accessible by IP address:

1. Issue the show sae subscribers ip command to view the subscribers who are accessible by IP address.
2. Issue the request sae logout ip command to log out all subscribers who are accessible by IP address.
   - To log out specific subscribers, use the filter option and specify the IP address for the subscribers that you want to log out.

     user@host> **request sae logout ip filter** *filter*

- To specify that no confirmation is requested before the software logs out the subscribers, use the force option.

  user@host> **request sae logout ip force**
  user@host> **request sae logout ip filter** *filter* **force**

Logging Out Subscribers by Login Name

To log out subscribers who are accessible by login name:

1. Issue the show sae subscribers login-name command to view the subscribers accessible by login name.

2. Issue the request sae logout login-name command to log out all subscribers accessible by login name.

   - To log out specific subscribers, use the filter option and specify all or part of the login name for the subscribers that you want to log out.

     user@host> **request sae logout login-name filter** *filter*

   - To specify that no confirmation is requested before the software logs out the subscribers, use the force option.

     user@host> **request sae logout login-name force**
     user@host> **request sae logout login-name filter** *filter* **force**

Logging Out Subscribers by Session ID

To log out subscribers who are accessible by session ID:

1. Issue the show sae subscribers session-id command to view the subscribers accessible by session ID.

2. Issue the request sae logout session-id command to log out all subscribers accessible by session ID.

   - To log out specific subscribers, use the filter option and specify all or part of the session ID for the subscribers that you want to log out.

     user@host> **request sae logout session-id filter** *filter*

   - To specify that no confirmation is requested before the software logs out the subscribers, use the force option.

     user@host> **request sae logout session-id force**
     user@host> **request sae logout session-id filter** *filter* **force**

Part 4

Using SNMP for Monitoring and Troubleshooting

Chapter 8

Configuring the SNMP Traps with the SRC CLI

This chapter describes how to use the SRC CLI to configure traps with the Simple Network Management Protocol (SNMP) agent. You can use the CLI to configure traps on a Solaris platform or on a C-series platform.

You can also use configuration applications to configure traps on a Solaris platform. See *Chapter 9, Configuring the SNMP Traps on a Solaris Platform*.

Topics in this chapter include:

Overview of SNMP Traps

The SNMP agent provides network management systems with SNMP trap notifications in case of component failure or when critical resources are out of configurable limits. This information is captured in a Management Information Base (MIB).

The SNMP agent can be run on each SRC host. It can monitor any SRC process running on the host and is preconfigured to monitor SRC processes. Additionally, it provides detailed monitoring and configuration of SRC server components.

MIBs

The SNMP agent monitors MIB variables. Most variables measure the performance of the system. Some variables are counters, such as the saeLogins variable, which counts the total number of subscriber logins since startup. Some variables are gauges, and their numbers go up and down, such as the saeHeapUsed variable, which measures the Java Virtual Machine heap that is currently in use.

A MIB defines a trap type that is associated with many MIB variables. For traps based on counters, the SNMP agent periodically polls each specified variable. It takes the difference between the previous and current values of the variable and compares that difference with the threshold. If the difference has moved up across thresholds, the SNMP agent sends a trap raising an alarm (minor, major, or critical) for the highest threshold crossed to all configured receivers. If the difference has moved down across thresholds, the agent sends a trap clearing the alarm of the lowest threshold crossed.

You can configure the polling interval between samples. If you change the polling interval, also adjust the thresholds. For instance, if the critical threshold for SAE logins is 1,000 and the interval is 60 seconds, then a critical alarm is raised if there are more than 1,000 logins in 60 seconds. But if you change the interval to 600 seconds, then you would need to change the threshold to 10,000 to have the same meaning.

For traps based on gauges, the previous value is not needed; the current value is compared with the thresholds.

In the trap tables, there is a field named R/AV, where R means rate, and AV means absolute value. Rate is used for variables that are counters, and it measures the rate of change of the counter. Absolute value is used for variables that are gauges.

For a list of all traps, see *Chapter 10, Understanding Traps*.

Traps

Traps are individual events that the SNMP agent can monitor, such as the number of timeouts or errors that have occurred or connections that have opened or closed. There are two types of traps:

- Performance traps—Traps that poll MIB variables associated with the trap to determine whether a variable has crossed configured thresholds. If the variable crosses a threshold, an alarm is triggered and a trap is sent to the list of configured receivers.

- Event traps—Traps that are sent when an event occurs; for example, when a connection is established or closed.

For a list and description of all traps, see *Chapter 10, Understanding Traps*.

SNMP Traps and Informs

SNMP notifications can be sent as traps or inform requests. SNMP traps are unconfirmed notifications. SNMP informs are confirmed notifications.

SNMP traps are defined in either standard or enterprise-specific MIBs. The standard and enterprise-specific traps are compiled into the network management software. For more information on the SRC traps, see *Chapter 10, Understanding Traps*. For information on system logging severity levels for SNMP traps, see *Chapter 2, Configuring Logging for SRC Components*.

With traps, the receiver does not send any acknowledgment when it receives a trap and the sender cannot determine if the trap was received. To increase reliability, SNMP informs are supported in SNMPv3. With an inform, the receiver acknowledges the message with a response. For information about configuring SNMP notification handling, see *SRC-PE Getting Started Guide, Chapter 23, Configuring and Starting the SNMP Agent with the SRC CLI*.

Configuration Statements for the SNMP Traps

Use the following configuration statements to configure the SNMP traps at the [edit] hierarchy level.

snmp notify alarm category *category-name* ...

```
snmp notify alarm category category-name alarm alarm-name {
    interval interval;
    critical critical;
    major major;
    minor minor;
}
```

snmp notify event category *category-name* ...

snmp notify event category *category-name* event *event-name* ...

For detailed information about each configuration statement, see the *SRC-PE CLI Command Reference.*

Configuring Performance Traps

Use the following configuration statements to configure performance traps:

snmp notify alarm category *category-name* ...

```
snmp notify alarm category category-name alarm alarm-name {
    interval interval;
    critical critical;
    major major;
    minor minor;
}
```

To configure performance traps:

1. From configuration mode, access the configuration statement that configures the type of performance trap.

   ```
   [edit]
   user@host# edit snmp notify
   ```

2. Specify the type of trap and the trap name.

   ```
   [edit snmp notify]
   user@host# set alarm category category-name alarm alarm-name
   ```

   You can select from the list of trap types and their associated traps or create new traps.

3. (Optional) Specify the interval at which the variable associated with the trap is polled.

   ```
   [edit snmp notify alarm category category-name alarm alarm-name]
   user@host# set interval interval
   ```

4. Specify the threshold above which a critical alarm is generated.

   ```
   [edit snmp notify alarm category category-name alarm alarm-name]
   user@host# set critical critical
   ```

5. Specify the threshold above which a major alarm is generated.

   ```
   [edit snmp notify alarm category category-name alarm alarm-name]
   user@host# set major major
   ```

6. Specify the threshold above which a minor alarm is generated.

   ```
   [edit snmp notify alarm category category-name alarm alarm-name]
   user@host# set minor minor
   ```

Configuring Event Traps

Use the following configuration statements to configure event traps:

snmp notify event category *category-name* ...

snmp notify event category *category-name* event *event-name* ...

To configure event traps:

1. From configuration mode, access the configuration statement that configures the type of event trap.

   ```
   [edit]
   user@host# edit snmp notify
   ```

2. Specify the type of trap and the trap name.

   ```
   [edit snmp notify]
   user@host# set event category category-name event event-name
   ```

   You can select from the list of trap types and their associated traps or create new traps.

Chapter 9

Configuring the SNMP Traps on a Solaris Platform

This chapter describes how to configure and use the Simple Network Management Protocol (SNMP) agent on a Solaris platform using the configuration applications that run only on Solaris platforms.

You can also use the CLI that runs on Solaris platforms and the C-series platforms to configure the SNMP agents. See *Chapter 8, Configuring the SNMP Traps with the SRC CLI*.

Topics in this chapter include:

Overview of SNMP Traps

The SNMP agent provides network management systems with SNMP trap notifications in case of component failure or when critical resources are out of configurable limits. This information is captured in a Management Information Base (MIB).

The SNMP agent can be run on each SRC host. It can monitor any SRC process running on the host and is preconfigured to monitor SRC processes. Additionally, it provides detailed monitoring and configuration of SRC server components.

The SNMP agent automatically discovers SRC components that expose component-specific management information and components that are directory eventing system (DES) clients (that is, have a directory connection managed by DES). When the SNMP agent discovers a component, it adds variables and table entries to its MIB to export the component's management capabilities.

For components that are automatically discovered, the SNMP agent communicates directly with a management server built into the components. For these components, the agent can perform exhaustive tests to determine operability rather than just determining process status. The SNMP agent ensures that the management infrastructure built into the component continues to respond to management requests.

In addition to monitoring components that it automatically discovers, you can also configure the SNMP agent to monitor any process or collection of processes running on its host. The SNMP agent monitors processes by looking at entries in the process table. For many processes that are run only once, such as directory servers, it is sufficient to monitor the single entry in the process table that includes the command used to start the process.

When a component is written in Java or Python, you need to differentiate between the different instances of the Java or Python process because there will be multiple processes in which the executed command is **java** or **python**. The technical name field in the component definition allows you to make this differentiation. The technical name of a component is the command that is used to start the process for the component. In the case of a Java program, the technical name is the name of the main Java class that is specified as an argument to the **java** command. For a Python program, it is the name of the script that is specified as an argument to the **python** command.

MIBs

The SNMP agent monitors MIB variables. Most variables measure the performance of the system. Some variables are counters, such as the saeLogins variable, which counts the total number of subscriber logins since startup. Some variables are gauges, and their numbers go up and down, such as the saeHeapUsed variable, which measures the Java Virtual Machine heap that is currently in use.

A MIB defines a trap type that is associated with many MIB variables. For traps based on counters, the SNMP agent periodically polls each specified variable. It takes the difference between the previous and current values of the variable and compares that difference with the threshold. If the value has moved up across thresholds, the SNMP agent sends a trap raising an alarm (minor, major, or critical) for the highest threshold crossed to all configured receivers. If the value has moved down across thresholds, the agent sends a trap clearing the alarm of the lowest threshold crossed.

You can configure the polling interval between samples. If you change the polling interval, also adjust the thresholds. For instance, if the critical threshold for SAE logins is 1,000 and the interval is 60 seconds, then a critical alarm is raised if there are more than 1,000 logins in 60 seconds. But if you change the interval to 600 seconds, then you would need to change the threshold to 10,000 to have the same meaning.

For traps based on gauges, the previous value is not needed; the current value is compared with the thresholds.

In the trap tables, there is a field named R/AV, where R means rate, and AV means absolute value. Rate is used for variables that are counters, and it measures the rate of change of the counter. Absolute value is used for variables that are gauges.

For a list of all traps, see *Chapter 10, Understanding Traps*.

IOR Files

An SRC component writes its object references to an interoperable object reference (IOR) file, and the SNMP agent discovers components by monitoring IOR files.

SRC components have a property called sysman.iordirectory that specifies the location of the IOR file for the component. The default value for the location is the *var* folder relative to the SNMP agent folder (*/opt/UMC/agent/var*). If you install the SNMP agent in a folder other than the default, or if you previously changed the sysman.iordirectory property to a folder other than */opt/UMC/agent/var,* you need to change the property so that it points to the folder where the IOR file currently resides.

The following sections provide the location and name of the property file for each component.

SNMP Agent

Use this information to access the SNMP agent property file and change the location of the IOR file.

- Location of property file—*/opt/UMC/agent/config*
- Name of property file—smagent.prop
- Property name—smagent.sysman.iordirectory
- Default value—*var*

You can change the location of the IOR file for the SNMP agent with the local configuration tool for the SNMP agent. Set this property in the Sysman Agent IOR Directory field.

See *SRC-PE Getting Started Guide, Chapter 31, Configuring and Starting the SDX SNMP Agent on a Solaris Platform*.

SAE

Use this information to access the SAE property file and change the location of the IOR file.

- Location of property file—*/opt/UMC/sae/etc*
- Name of property file—default.properties
- Property name—sysman.iordirectory
- Default value—*/opt/UMC/agent/var*

You can change the location of the IOR file for the SAE with the local configuration tool for the SAE. Set this property in the Sysman Agent IOR Directory field.

See *SRC-PE Getting Started Guide, Chapter 30, Setting Up an SAE on a Solaris Platform*.

License Server

Use this information to access the license server property file and change the location of the IOR file.

- Location of property file—*/opt/UMC/licsvr/etc*
- Name of property file—bootstrap.properties
- Property name—sysman.iordirectory
- Default value—*/opt/UMC/agent/var*

You can change the location of the IOR file for the license with the local configuration tool for the license server. Set this property in the Sysman Agent IOR Directory field.

For information about license server, see *SRC-PE Getting Started Guide, Chapter 12, Customizing and Managing the License Server*.

NIC Host

Use this information to access the network information collector (NIC) property file and change the location of the IOR file.

- Location of property file—*/opt/UMC/nic/etc*
- Name of property file—nic.properties
- Property name—sysman.iordirectory
- Default value—*/opt/UMC/agent/var*

You can also change the location of the IOR file for the NIC host with the local configuration tool for the NIC. Set this property in the Sysman IOR field.

For information about NIC hosts, see *SRC-PE Network Guide, Chapter 11, Configuring NIC on a Solaris Platform*.

Web Redirector

Use this information to access the Web redirector property file and change the location of the IOR file.

- Location of property file—*/opt/UMC/redir/etc*
- Name of property file—redir.properties
- Property name—agent.path
- Default value—*../agent/var*

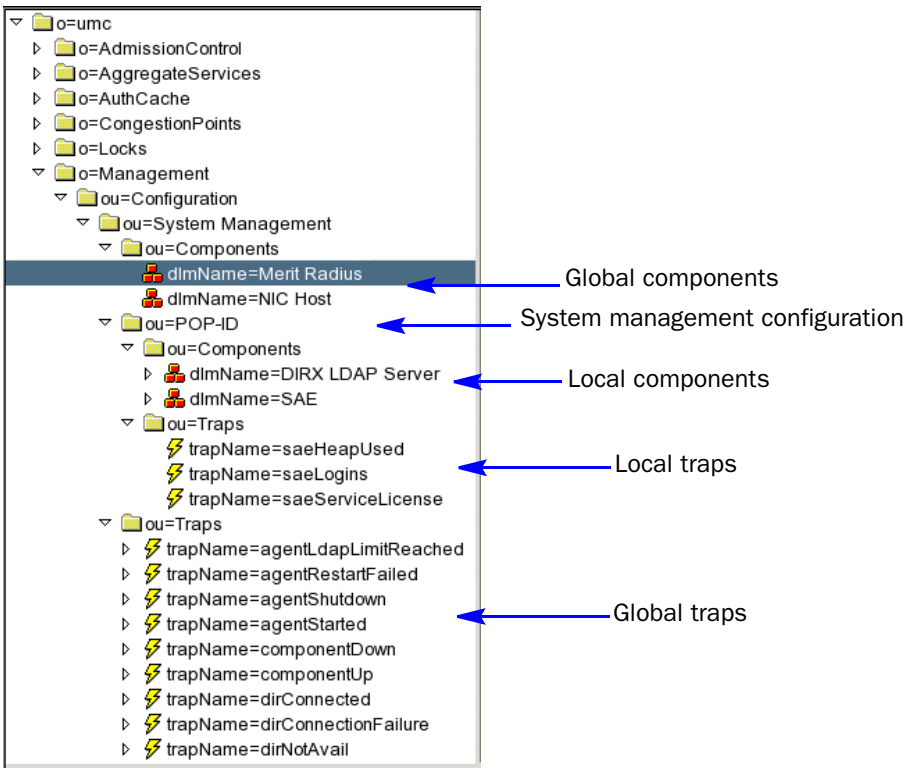
SNMP Agent Hierarchy and Objects

The SNMP agent configuration consists of:

- System management configuration
- Subfolders
- Components (local and global)
- Traps (local and global)

Figure 1 shows a sample set of system management objects that make up the SNMP agent.

Figure 1: SNMP Object Hierarchy in SDX Admin



System Management Configurations

A system management configuration consists of components and traps. The SRC software comes with a default system management configuration that has an *ou = components* object and an *ou = traps* object. The components and traps in the default system management configuration are called global components and global traps.

You can add components to, delete components from, or modify components in the global components object. You can modify the trap configurations in the global traps object, but you cannot add or delete traps in the global traps object.

You can create additional system management configurations with their own components and traps. System management configurations are a convenient way to specify a configuration for multiple SNMP agents installed on multiple hosts that all run the same set of components.

For instance, if you have a host in a point of presence (POP) that runs an SAE and shadow directory, you could set up a POPHost system management configuration for the POP host. You could also have a host in a back office that runs a master directory, a NIC host, and a RADIUS server. For this setup, you could create a BackOfficeHost system management configuration. Typical deployments have a small number of roles for hosts, and the system management configuration can be shared across a potentially large number of hosts with the same role.

For a given system management configuration, both the local and global components and traps are considered part of the configuration. Traps in parent system management configurations or subordinate system management configurations are not considered. If a component or trap occurs in both the global and local folder, then the local version overrides the global one.

Subfolders

SDX Admin lets you create subfolders to organize your system management configurations.

Components

Components are SRC and other network components that you can monitor with the SNMP agent; for example, the SAE, NIC hosts, RADIUS servers, directory servers, and SRC license servers.

The SNMP agent automatically creates local components for each SRC package that is installed on the host where it runs. In this case, most attributes of the component are automatically configured, including the type, start, and stop commands, and the installation date and version.

A global component is a component that is defined for all system management configurations. The global component saves you from defining the local component for each individual system management configuration when the local component definitions would all be the same. If you define a global component and a particular system management configuration requires a different definition, you can define a local component that would override the global component definition.

You can also create a container component and put subcomponents into it. Generally, container components are for monitoring components that require multiple processes, such as DirX. The SNMP agent considers the operational status of a container component as up only when all subcomponents are up, and it considers the container down if any of the subcomponents is down.

The container component start and stop commands are ignored when SNMP is used to set the administrative state of the container component. The start and stop commands of the container component are used to start and stop the whole component and are assumed to manage the starting and stopping of the processes corresponding to the contained components.

Traps

Traps are individual events that the SNMP agent can monitor, such as the number of timeouts or errors that have occurred or connections that have opened or closed. There are two types of traps:

- Performance traps—Traps that poll MIB variables associated with the trap to determine whether a variable has crossed configured thresholds. If the variable crosses a threshold, an alarm is triggered and a trap is sent to the list of receivers configured in the master agent.

  A global performance trap provides thresholds and polling intervals that are used by default wherever the trap is enabled. To enable a trap for a particular system management configuration, you must create a local version of the trap. Any local definitions of thresholds or polling intervals will override the global definitions.

- Event traps—Traps that are sent when an event occurs; for example, when a connection is established or closed.

  Global event traps do not have any effect on the system management configuration. To enable an event trap for a particular system management configuration, you must create a local version of the trap. To define trap receivers, you must configure the trap receivers in the master agent configuration.

For a list and description of all traps, see *Chapter 10, Understanding Traps*.

SNMP Traps and Informs

SNMP notifications can be sent as traps or inform requests. SNMP traps are unconfirmed notifications. SNMP informs are confirmed notifications.

SNMP traps are defined in either standard or enterprise-specific MIBs. The standard and enterprise-specific traps are compiled into the network management software. For more information on SRC traps, see *Chapter 10, Understanding Traps*. For information on system logging severity levels for SNMP traps, see *Chapter 2, Configuring Logging for SRC Components*.

With traps, the receiver does not send any acknowledgment when it receives a trap and the sender cannot determine if the trap was received. To increase reliability, SNMP informs are supported in SNMPv3. With an inform, the receiver acknowledges the message with a response. For information about configuring SNMP notification handling, see the master agent documentation.

Adding Subfolders in SDX Admin for an SNMP Agent

To use SDX Admin to add a subfolder:

1. In the navigation pane, right-click a system management configuration object or a subfolder object, and select **New > SubFolder**.
2. Enter a folder name in the dialog box, and click **OK**.

   Do not name a subfolder Components or Traps.

Deleting Subfolders in SDX Admin for an SNMP Agent

To use SDX Admin to delete a subfolder:

1. Delete all objects within the subfolder.
2. Right-click the subfolder, and select **Delete**.

Adding System Management Configuration for an SNMP Agent

To use SDX Admin to add a system management configuration:

1. In the navigation pane, right-click *ou = System Management* or a subfolder, and select **New > System Management Configuration**.
2. Enter a name in the dialog box, and click **OK**.

   Do not name a system management configuration Components or Traps.

   The software automatically creates a components and traps folder within the system management configuration folder.

You configure the SNMP agent on the desired host(s) to use the system management configuration by setting the Configuration Directory Base DN field in the SNMP agent local configuration tool.

See *SRC-PE Getting Started Guide, Chapter 31, Configuring and Starting the SDX SNMP Agent on a Solaris Platform*.

Deleting System Management Configuration for an SNMP Agent

To use SDX Admin to delete a system management configuration:

1. In the navigation pane, right-click any component or trap object subordinate to the system management configuration, and select **Delete**; repeat for all such objects.
2. Right-click the subordinate Components object, and select **Delete**; repeat for Traps.
3. Right-click the system management configuration object, and select **Delete**.

Adding an SNMP Agent Component

To use SDX Admin to add a component:

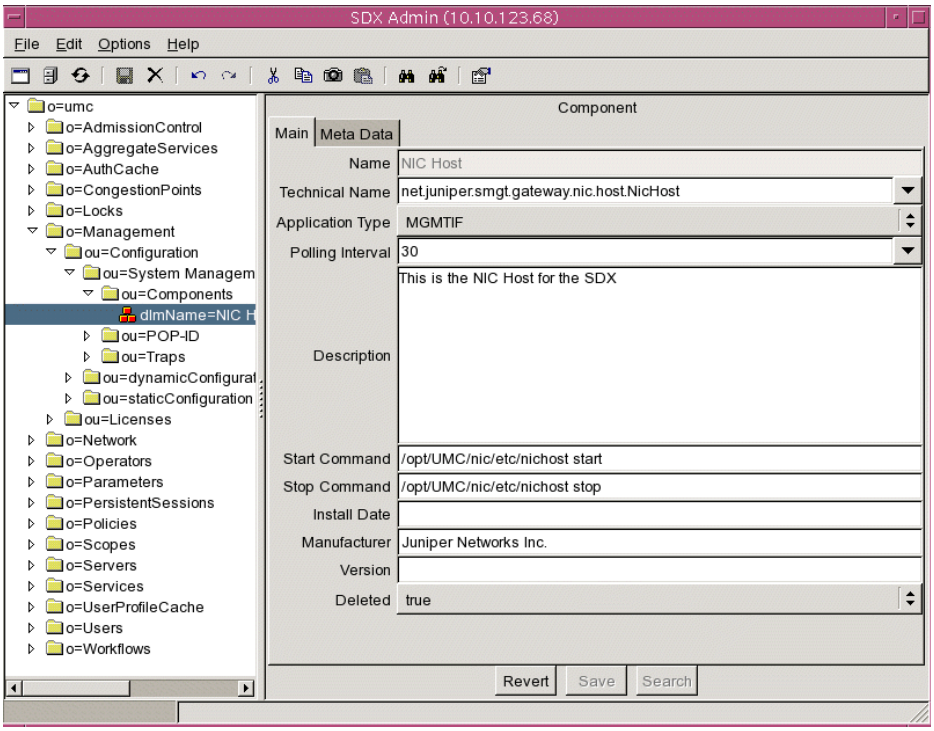
1. In the navigation pane, select a component folder. For example:

   ou = Components, ou = System Management, ou = Configuration, o = Management, o = umc

2. Right-click *ou = Components*, and select **New > Component**.

3. In the New Component dialog box, enter a name or select a name from the drop-down list. Names must be no more than 50 characters.

   The Component pane appears. If you selected a name from the drop-down list, the software fills in default values.



4. Edit or accept the default values for the SNMP fields.

   See *SNMP Component Fields* on page 63.

5. Click **Save**.

6. Restart the SNMP agent to update the agent with the changes.

SNMP Component Fields

In SDX Admin, you can modify the following fields in the content pane for SNMP components.

Technical Name

- Technical name for the component.
- Value—You can enter a value or select a value from the drop-down list. The value depends on the application type:
  - For a PYTHON application type, use the path to the file that contains the Python program that is executed by the Python process as it appears on the command line of the executed Python command. (Because all Python components run in a process in which the command name is **python**, you must provide the path to distinguish the Python program from other Python components running on the same host.)
  - For a PROCESS application type, use the executed command.
  - For a JAVA application type, use the full package/class name of the class with the "main" function that appears as an argument to the Java command that starts the component. (Because all Java components run in a process in which the command name is **java**, you must provide the name of the main class for a Java component to distinguish it from other Java components running on the same host.)
  - For CONTAINER and MGMTIF application types, the technical name of the component is not necessary and is ignored.
- Default—If you selected a name in the New Component dialog box, the software enters a technical name for you. Otherwise, there is no default.
- Example—net.juniper.smgt.gateway.nic.host.NicHost

Application Type

- The application type of the component.
- Value
  - JAVA—Java process
  - MGMTIF—Management interface used to monitor SRC-based components, such as subscriber portals or the Workflow application.
  - PROCESS—UNIX process, such as Merit RADIUS
  - PYTHON—Python process
  - CONTAINER—Component that groups related components that need to be monitored as a group. In the MIB, a container component sends a trap if any of its contained components fails. See *Components* on page 59.
- Guidelines—A container component cannot contain another container. It can contain only Python, process, Java, or mgmtif components.
- Default—If you selected a name in the New Component dialog box, the software enters an application type for you. Otherwise, there is no default.

Polling Interval

- Length of the interval between checks by the SNMP agent that the component is running.
- Value—Number of seconds in the range 1–3600. You can enter a value or select a value from the drop-down list.
- Default—Depends on the type of component

Description

- Text description of the component.
- Value—String
- Guidelines—Optional
- Default—No value

Start Command

- Software command that starts the component.
- Value—Path and command
- Guidelines—The software must be configured to start the component with SNMP. When SNMP is used to set the administrative state of a container component, it ignores the start and stop commands of the container component. The start and stop commands of the container component are used to start and stop the whole component and are assumed to manage the starting and stopping of the processes that correspond to the subcomponents.
- Default—For most SRC components, the software enters the correct start command as long as the component is installed in the default location.
- Example—/opt/UMC/sae/etc/sae start

Stop Command

- Software command that stops the component.
- Value—Path and command
- Guidelines—The software must be configured to stop the component with SNMP. When SNMP is used to set the administrative state of a container component, it ignores the start and stop commands of the container component. The start and stop commands of the container component are used to start and stop the whole component and are assumed to manage the starting and stopping of the processes that correspond to the subcomponents.
- Default—For most SRC components, the software enters the correct stop command as long as the component is installed in the default location.
- Example—/opt/UMC/sae/etc/sae stop

Install Date

- Date component was installed.
- Value—Date in the format YYYYMMDD or YYYYMMDDhhmmssZ
  - YYYYMMDD indicates the year, the month, and the day
  - hhmmss indicates the hour, the minute, and the second
  - Z = Coordinated Universal Time (UTC)
- Guidelines—Optional
- Default—No value

Manufacturer

- Component manufacturer.
- Value—Text name of a manufacturer
- Guidelines—Optional
- Default—If you selected a name in the New Component dialog box, the software enters a manufacturer for you. Otherwise, there is no default.

Version

- Software version of the component.
- Value—Text or integer
- Guidelines—Optional
- Default—No value

Deleted

- Specifies the availability of this entry to other SRC components connected to the directory.
- Value
  - Blank—Other SRC components can access this entry in the directory.
  - True—Other SRC components cannot use this entry in the directory, although the object still exists.
  - False—Other SRC components can access this entry in the directory.
- Default—Blank

Deleting an SNMP Agent Component

To use SDX Admin to delete a component:

1. In the navigation pane, right-click an object and select **Delete**.
2. Restart the SNMP agent to update the agent with the changes.

About Configuring Traps

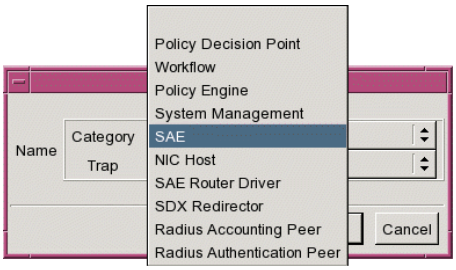
You can modify the trap configurations in the global traps folder, but you cannot add or delete traps in the global traps folder. You can add or delete traps in system management configurations that you create.

Chapter 10, Understanding Traps lists all the traps.

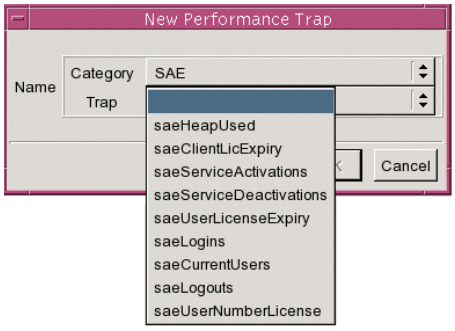
Adding Traps

To use SDX Admin to add a trap:

1. In the navigation pane, select a system management configuration.
2. Right-click *ou = Traps*, and select **New > Event Trap** or **New > Performance Trap**.
3. In the New Performance Trap or New Event Trap dialog box, select a category from the Category drop-down list. The categories displayed in the list depend on the type of trap that you are creating.



4. Select an item from the Trap drop-down list. The traps displayed in the list depend on the category you selected in the previous step.



5. Click **OK**.

   The Trap pane appears, showing default values for the trap you selected. Figure 2 shows a performance trap. Figure 3 shows an event trap.

6. Edit or accept default values for the SNMP Trap fields to configure the trap.

   See *SNMP Trap Fields* on page 68.

7. Click **Save**.

8. Restart the SNMP agent to update the agent with the changes.

Figure 2: Performance Trap Pane

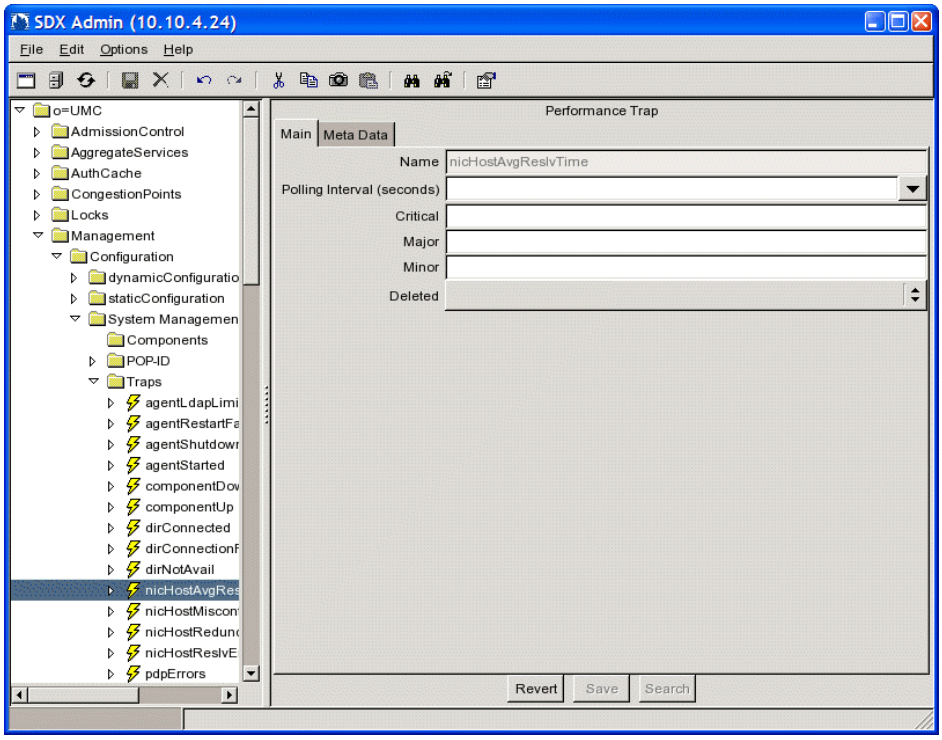
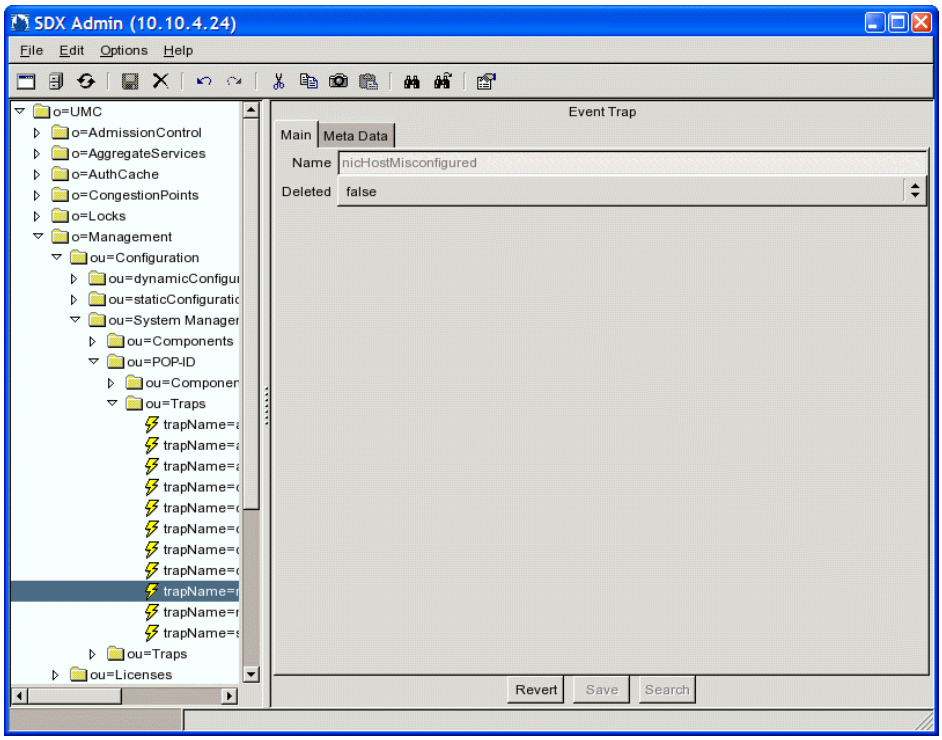


Figure 3: Event Trap Pane



SNMP Trap Fields

In SDX Admin, you can modify the following fields in the content pane for an SNMP trap.

Polling Interval

- Interval at which the variable associated with the trap is polled.
- Value —Number of seconds in the range 0–3600. You can enter a specific value or select a value from the drop-down list. If you leave this field blank, the counter is disabled.
- Default—Depends on the type of trap.

Critical

- Threshold above which a critical alarm is generated.
- Value—Integer. The valid range depends on the type of trap. See the tool tip help for the valid range for a trap.
- Default—Depends on the type of trap.

Major

- Threshold above which a major alarm is generated.
- Value—Integer. The valid range depends on the type of trap. See the tool tip help for the valid range for a trap.
- Default—Depends on the type of trap.

Minor

- Threshold above which a minor alarm is generated.
- Value—Integer. The valid range depends on the type of trap. See the tool tip help for the valid range for a trap.
- Default—Depends on the type of trap.

Deleted

- Specifies the availability of this entry to other SRC components connected to the directory.
- Value
  - Blank—Other SRC components can access this entry in the directory.
  - True—Other SRC components cannot use this entry in the directory, although the object still exists.
  - False—Other SRC components can access this entry in the directory.
- Default—Blank

Deleting Traps

To use SDX Admin to delete a trap:

1. In the navigation pane, right-click the trap object, and select **Delete**.
2. Restart the SNMP agent to update the agent with the changes.

Chapter 10

Understanding Traps

This chapter describes the trap information for performance and event traps and provides alarm state information. Topics include:

For information about using the SRC CLI that runs on Solaris platforms and the C-series platforms to configure traps, see *Chapter 8, Configuring the SNMP Traps with the SRC CLI*.

For information about using configuration applications to configure traps on a Solaris platform, see *Chapter 9, Configuring the SNMP Traps on a Solaris Platform*.

Performance Traps

Trap tables list all the traps supported by the SNMP agent, the text displayed for each trap, trap thresholds and intervals, and any special notes pertaining to the trap.

Table 6 describes the symbols used in the performance traps tables.

Table 6: Symbols in Performance Traps Tables

Symbol	Description
$S	Severity level of the trap: MINOR, MAJOR, CRITICAL, or CLEAR
$D	Status data
$P	Polling interval
$T	Threshold value
$A	Trap action; displayed as RAISED or CLEARED
$L	“Exceeded” if the trap is raised; “is below” if the trap is cleared

R/AV

Each performance trap table has a field called R/AV. R means rate, and AV means absolute value.

- Rate is used for variables that are counters. The rate is the difference between the current value of the underlying MIB variable being monitored and its previous value, which was read <interval> time ago. The interval length affects those values that are appropriate for the thresholds; that is, the longer the interval, the larger the thresholds must be. For instance, saeLogins is a counter of the total number of SAE logins. With the default interval of 60 seconds, the critical threshold of 2,000 means that a critical trap is sent if there are more than 2,000 logins within one minute. If you change the interval to 300 seconds (5 minutes), to keep the critical threshold at 2,000 logins a minute, you need to change the threshold to 10,000 (the number of logins in 5 minutes for a rate of 2,000 per minute).

- Absolute value is used for variables that are gauges, and they transition from one alarm threshold level to the next.

Decoding Trap Numbers in Performance Traps

Performance traps contain a trap ID, a severity, and an action. The trap ID, severity, and action are encoded in the trap number to make it easy to configure trap receivers, such as HP OpenView, to color and highlight traps.

Every performance trap has four trap definitions: one for critical, major, and minor severity levels, and one for the clear action. For critical, major, and minor severity levels, the action is raise. For the clear action, there is no severity level, because the severity level is implied by the last raise action for the trap ID.

Severity levels are assigned the following numbers:

- Critical = 1
- Major = 2
- Minor = 3
- Information = 5

The JuniSdxTrapID ::= TEXTUAL-CONVENTION section in the Juniper-SDX-TC MIB lists the trap IDs for all traps. The Juniper-SDX-TRAP MIB defines the SDX traps.

Tasks to decode trap numbers are:

- Decoding Trap Numbers for Raised Trap Actions on page 73
- Decoding Trap Numbers for Clear Trap Actions on page 73

You can access the MIBs on the Juniper Web site at

http://www.juniper.net/techpubs/software/management/sdx

Decoding Trap Numbers for Raised Trap Actions

To decode a trap number for raised trap actions:

- Use the following equation:

  Trap number = Trap ID * 10 + severity

For example, if the trap number is 43, then the trap ID is 4 (saeServiceActivations) and the severity is 3 (MINOR). Therefore, a trap number of 43 means that a MINOR event has occurred for the saeServiceActivations trap.

Decoding Trap Numbers for Clear Trap Actions

To decode a trap number for clear trap actions:

- Use the following equation:

  Trap number = Trap ID * 10

For example, if the trap number is 250, then the trap ID is 25 (saeAccPendingRequests). Therefore, a trap number of 250 means that the saeAccPendingRequests alarm has been cleared.

SAE Performance Traps

Table 7 lists the performance traps for the SAE.

Table 7: Performance Traps–SAE

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
saeHeapUsed	1	$S:SAE:$D% of Java VM heap is in use. This $L the threshold of $T %.:$A	95	90	80	60	AV
saeLogins	2	$S:SAE:During the last $Ps, $D logins occurred. This $L the threshold of $T logins.:$A	2000	1000	400	60	R
saeLogouts	3	$S:SAE:During the last $Ps, $D logouts occurred. This $L the threshold of $T logouts.:$A	2000	1000	400	60	R
saeServiceActivations	4	$S:SAE:During the last $Ps, $D services were activated. This $L the threshold of $T service activations.:$A	2000	1000	500	60	R
saeServiceDeactivations	5	$S:SAE:During the last $Ps, $D services were deactivated. This $L the threshold of $T service deactivations.:$A	2000	1000	500	60	R
saeCurrentUsers	6	$S:SAE:The number of user sessions is $D. This $L the threshold of $T users sessions.:$A	18000	14000	12000	60	AV

Table 7: Performance Traps–SAE (continued)

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
saeUserNumberLicense	7	$S:SAE:$D % of the available licenses are in use. This $L the threshold of $T.:$A	99	95	90	60	AV
saeUserLicenseExpiry	8	$S:SAE:The SAE license is about to expire in $D days. This $L the threshold of $T.:$A	1	10	14	3500	AV
saeClientLicExpiry	12	$S:SAE:The client has consumed $D % of its available license. This $L the threshold of $T.:$A	90	70	40	900	AV

Accounting Performance Traps

Table 8 lists the performance traps for accounting.

Table 8: Performance Traps–Accounting

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
saeAccInvalidServerAddresses	20	$S:SAE RADIUS Accounting Client:During the last $Ps, $D invalid server address errors occurred. This $L the threshold of $T invalid server address errors.:$A	5	2	1	60	R
saeAccRoundTripTime	21	$S:SAE RADIUS Accounting Client:The round trip message time is $Dms. This $L the threshold of $Tms.:$A	2250	1500	750	60	AV
saeAccRetransmissions	22	$S:SAE RADIUS Accounting Client:During the last $Ps, $D retransmissions occurred. This $L the threshold of $T retransmissions.:$A	5	2	1	60	R
saeAccMalformedResponses	23	$S:SAE RADIUS Accounting Client:During the last $Ps, $D malformed responses occurred. This $L the threshold of $T malformed responses.:$A	5	2	1	60	R
saeAccBadAuthenticators	24	$S:SAE RADIUS Accounting Client:During the last $Ps, $D bad authenticator error occurred. This $L the threshold of $T bad authenticators errors.:$A	5	2	1	60	R

Table 8: Performance Traps–Accounting (continued)

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
saeAccPendingRequests	25	$S:SAE RADIUS Accounting Client:The number of pending requests is $D. This $L the threshold of $T pending requests:$A	50	25	10	60	AV
saeAccTimeouts	26	$S:SAE RADIUS Accounting Client:During the last $Ps, $D timeouts occurred. This $L the threshold of $T timeouts.:$A	30	20	10	60	R
saeAccUnknownTypes	27	$S:SAE RADIUS Accounting Client:During the last $Ps, $D unknown type errors occurred. This $L the threshold of $T unknown type errors.:$A	30	20	10	60	R
saeAccPacketsDropped	28	$S:SAE RADIUS Accounting Client:During the last $Ps, $D packets were dropped. This $L the threshold of $T dropped packets.:$A	30	20	10	60	AV

Authentication Performance Traps

Table 9 lists the performance traps for authentication.

Table 9: Performance Traps–Authentication

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
saeAuthInvalidServerAddresses	40	$S:SAE RADIUS Authentication Client:During the last $Ps, $D invalid server address errors occurred. This $L the threshold of $T invalid server address errors.:$A	10	5	1	60	AV
saeAuthRoundTripTime	41	$S:SAE RADIUS Authentication Client:The round trip message time is $Dms. This $L the threshold of $Tms:$A	2250	1500	750	60	R
saeAuthAccessRetransmissions	42	$S:SAE RADIUS Authentication Client:During the last $Ps, $D retransmissions occurred. This $L the threshold of $T retransmissions.:$A	5	2	1	60	R

Table 9: Performance Traps–Authentication (continued)

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
saeAuthMalformedAccessResponses	43	$S:SAE RADIUS Authentication Client:During the last $Ps, $D malformed responses occurred. This $L the threshold of $T malformed responses.:$A	5	2	1	60	R
saeAuthBadAuthenticators	44	$S:SAE RADIUS Authentication Client:During the last $Ps, $D bad authenticators errors occurred. This $L the threshold of $T.:$A	5	2	1	60	
saeAuthPendingRequests	45	$S:SAE RADIUS Authentication Client:The number of pending requests is $D. This $L the threshold of $T pending requests:$A	50	25	10	60	AV
saeAuthTimeouts	46	$S:SAE RADIUS Authentication Client:During the last $Ps, $D timeouts occurred. This $L the threshold of $T timeouts.:$A	5	2	1	60	R
saeAuthUnknownTypes	47	$S:SAE RADIUS Authentication Client:During the last $Ps, $D unknown type errors occurred. This $L the threshold of $T unknown type errors.:$A	5	2	1	60	R
saeAuthPacketsDropped	48	$S:SAE RADIUS Authentication Client:During the last $Ps, $D packets were dropped. This $L the threshold of $T dropped packets.:$A	5	2	1	60	R

NIC Performance Traps

Table 10 lists the performance traps for NIC.

Table 10: Performance Traps–NIC

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
nicHostReslvErrors	230	$S:NIC Host: During the last $Ps, the number of resolution errors that occurred is $D. This $L is the threshold of $T errors.:$A	10	5	1	60	R
nicHostAvgReslvTime	231	$S:NIC Host: During the last $Ps, the average time this NIC Host spent on resolutions is $Dms. This $L the threshold of $Tms.:$A	1000	500	250	60	R

Router Driver Performance Traps

Table 11 lists the performance traps for router drivers.

Table 11: Performance Traps–Router Drivers

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
routerMsgErrors	190	$S:SAE Router Driver ($juniSaeRouterClientId):During the last $Ps, $D router errors occurred. This $L the threshold of $T errors.:$A	10	5	1	60	R
routerMsgTimeouts	191	$S:SAE Router Driver ($juniSaeRouterClientId):During the last $Ps, $D router timeouts occurred. This $L the threshold of $T timeouts.:$A	10	5	1	60	R
routerAvgJobQTime	192	$S:SAE Router Driver ($juniSaeRouterClientId):During the last $Ps, the average time that incoming router messages waited to be processed is $Dms. This $L the threshold of $Tms.:$A	500	250	100	60	R
routerJobQLength	193	$S:SAE Router Driver ($juniSaeRouterClientId):The number of unprocessed incoming router messages is $D. This $L the threshold of $T messages.:$A	2500	500	100	60	AV
routerJobQAge	194	$S:SAE Router Driver ($juniSaeRouterClientId):The oldest unprocessed router message has been waiting for $Dms. This $L the threshold of $Tms.:$A	30000	10000	5000	60	AV
routerAvgAddTime	195	$S:SAE Router Driver ($juniSaeRouterClientId): During the last $Ps, the average time (in milliseconds) this router driver spent handling 'object added' notifications is $Dms. This $L the threshold of $Tms.:$A	1000	500	100	60	R
routerAvgChgTime	196	$S:SAE Router Driver ($juniSaeRouterClientId): During the last polling interval, the average time (in milliseconds) this router driver spent handling 'object changed' notifications is $Dms. This $L the threshold of $Tms.:$A	1000	500	100	60	R

Table 11: Performance Traps–Router Drivers (continued)

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
routerAvgDelTime	197	$S:SAE Router Driver ($juniSaeRouterClientId): During the last polling interval, the average time (in milliseconds) this router driver spent handling 'object deleted' notifications is $Dms. This $L the threshold of $Tms.:$A	1000	500	100	60	R

Workflow Performance Traps

Table 12 lists the performance traps for workflows.

Table 12: Performance Traps–Workflow

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
wkfInstanceFileSize	90	$S:Workflow:The instance data allocated for each active workflow is $Dk. This $L the threshold of $Tk.:$A	7	5	2	60	AV
wkfEventFileSize	91	$S:Workflow:The pending events filesize is $Dk. This $L the threshold of $Tk.:$A	500	250	100	60	AV
wkfReportFileSize	92	$S:Workflow:The pending reports filesize is $Dk. This $L the threshold of $Tk.:$A	250	125	50	60	AV
wkfPersistentFileSize	93	$S:Workflow:The persistent storage allocated for each active workflow is $Dk. This $L the threshold of $Tk.:$A	70	50	20	60	AV
wkfCancelledWorkflows	94	$S:Workflow:During the last $Ps, $D workflows have been cancelled. This $L the threshold of $T cancelled workflows.:$A	100	50	10	60	R
wkfPendingEvents	95	$S:Workflow:The number of pending events is $D. This $L the threshold of $T pending events.:$A	1000	500	100	60	AV
wkfActiveWorkflows	96	$S:Workflow:The number of active workflows is $D. This $L the threshold of $T active workflows.:$A	1000	500	100	60	AV
wkfRunningWorkflows	97	$S:Workflow:The number of running workflows is $D. This $L the threshold of $T workflows.:$A	1000	500	100	60	AV

System Management Performance Traps

Table 13 lists the performance traps for system management event.

Table 13: Performance Traps–System Management Event

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
agentLdapLimitReached	113	$S: Ldap: The Ldap Limit has been reached: $D entries, during the last $Ps. This $L the threshold of $T entries.:$A.	100% of MAX	95% of MAX	90% of MAX	30	AV

Policy Engine Performance Traps

Table 14 lists the performance traps for policy engine.

Table 14: Performance Traps–Policy Engine

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
penAvgPGModProcTime	150	$S:Policy Engine:The average policy group modification processing time is $D ms. This $L the threshold of $T ms.:$A	200	500	1000	60	AV
penAvgICMModProcTime	151	$S:Policy Engine:The average interface classifier modification processing time is $D ms. This $L the threshold of $T ms.:$A	200	500	1000	60	AV
pdpErrors	152	$S:Policy Decision Point:During the last $Ps, $D errors occurred. This $L the threshold of $T PDP errors.:$A	10	5	1	30	R

SRC Redirector Performance Traps

Table 15 lists the performance traps for SRC redirector.

Table 15: Performance Traps–SRC Redirector

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
redirGBLimitReached	170	$S:SDX Redirector:During the last $Ps, the global bucket limit has been reached for $D times. This $L the threshold of $T times.:$A	3	2	1	900	R

SRC-ACP Performance Traps

Table 16 lists the performance traps for the SRC-Admission Control Plug-In (SRC-ACP) application.

Table 16: Performance Traps–SRC-ACP

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
acpHeapUsed	280	$S:ACP:$D% of Java VM heap is in use. This $L the threshold of $T%.:$A	95%	90%	80%	60	AV

JPS Performance Traps

Table 17 lists the performance traps for the Juniper Policy Server (JPS).

Table 17: Performance Traps–JPS

			Alarm Threshold Levels (default values)				
Trap Event	**Trap ID**	**Text Displayed**	**Critical**	**Major**	**Minor**	**Interval (sec)**	**R/AV**
jpsHeapUsed	250	$S:JPS:$D% of Java VM heap is in use. This $L the threshold of $T%.:$A	95%	90%	80%	60	AV
jpsCmtsAvgSyncTime	251	$S:JPS:During the last $Ps, the average time this JPS spent on CMTS synchronizations is $Dms. This $L the threshold of $Tms.:$A	900s	600s	200s	60	R
jpsCmtsAvgDecTime	252	$S:JPS:During the last $Ps, the average time the CMTS connection spent on successfully completed DEC/RPT transactions is $Dms. This $L the threshold of $Tms.:$A	3s	2s	1s	60	R
jpsMsgHdlrProcTime	253	$S:JPS:During the last $Ps, the average time the JPS message handler spent on message handling is $Dms. This $L the threshold of $Tms.:$A	10s	5s	2s	60	R
jpsMsgFlowProcTime	254	$S:JPS:During the last $Ps, the average time the JPS message flow spent on message handling is $Dms. This $L the threshold of $Tms.:$A	30s	15s	6s	60	R
jpsMsgFlowDroppedMsgs	255	$S:JPS:During the last $Ps, the number of messages dropped by a JPS message flow is $D. This $L the threshold of $T.:$A	1000	100	1	60	R

Event Traps

Table 18 lists the event traps.

Table 18: Event Traps

Trap Event	Trap ID	Text Displayed
saeLicenseNetworkCapacity	9	$S:SAE:The total number of sum-weighted line cards allocated in this SRC network is $LINE_CARD_NUMBER ($THRESHOLD_PERCENTAGE)%. This $L the network ERX capacity threshold of $T sum-weighted line cards.: $A
saeServiceSessionLicense	11	$S:LICENSE SERVER:$SERVICE_SESSIONS ($SERVICES_PERCENTAGE%) of the available licensed service sessions are in use.: $A
routerConnClosed	211	When juniSaeRouterUseFailOver is FALSE: INFORMATION:SAE Router Driver:The router connection to $juniSaeRouterClientId has been closed.:RAISE When juniSaeRouterUseFailOver is TRUE: INFORMATION:SAE Router Driver:The router connection to $juniSaeRouterClientId has been closed and redirected to $juniSaeRouterFailOverIp:$juniSaeRouterFailOverPort:RAISE
routerConnDown	212	INFORMATION:SAE Router Driver:The router connection to $juniSaeRouterClientId went down.:RAISE
routerConnRejected	213	INFORMATION:SAE Router Driver:The router connection from $juniSaeRouterClientId has been rejected.:RAISE
routerConnUp	210	INFORMATION:SAE Router Driver:A new router connection was established with $juniSaeRouterClientId.:RAISE
routerConfOutOfSynch	214	When the trap is raised, the text displayed is: INFORMATION:SAE Router Driver: The configured state of router $juniSaeRouterClientId is out of synch with SAE. The configured action to be taken by SAE is $configuredAction.:RAISE When the trap is cleared, the text displayed is: INFORMATION:SAE Router Driver: The configured state of router $juniSaeRouterClientId is successfully resynchronized with SAE.:CLEAR
agentStarted	110	INFORMATION:Agent:The agent has started.:RAISE
agentRestartFailed	111	CRITICAL: Agent: The agent has failed to restart after $ATTEMPTS attempts:RAISE
agentShutdown	112	INFORMATION:Agent:The agent has shutdown.:RAISE
componentUp	114	INFORMATION:$I: This component is up.:RAISE
componentDown	115	INFORMATION:$I: This component is down:RAISE
dirConnected	130	INFORMATION:$I:The directory connection has been established with $LDAP_HOST on port $LDAP_PORT, and has a type of $CONNECTION_TYPE.:RAISE
dirConnectionFailure	131	CRITICAL:$I:The directory connection with $LDAP_HOST has failed.:RAISE
dirNotAvail	132	CRITICAL:$I:A directory connection is not available.:RAISE
nicHostRedundStateSwitched	240	INFORMATION:NIC Host:The redundancy state of the NIC Host has switched to $juniNicHostRedundState.:RAISE
nicHostMisconfigured	241	INFORMATION:NIC Host: The NIC Host failed to start due to misconfiguration. The error message is "$MESSAGE".:RAISE
acpSyncCompleted	290	INFORMATION:ACP State Sync:ACP finished state sync with SAE for $juniAcpVirtualRouterName.:RAISE

Table 18: Event Traps (continued)

Trap Event	Trap ID	Text Displayed
acpRedundStateSwitched	291	INFORMATION:ACP Host:The redundancy state of the ACP Host has switched to $juniAcpRedundState.:RAISE
jpsAmConnUp	260	INFORMATION:JPS:A new application manager connection was established.:RAISE
jpsAmConnDown	261	INFORMATION:JPS:The application manager connection went down.:RAISE
jpsCmtsConnUp	262	INFORMATION:JPS:A new CMTS connection was established.:RAISE
jpsCmtsConnDown	263	INFORMATION:JPS:A CMTS connection went down.:RAISE

Alarm State Transitions

Table 19 lists the alarm state transitions.

Table 19: Alarm State Transitions

Last Data Threshold	Current Data Threshold	Action(s)	
NONE	NONE	No action	
NONE	MINOR	Raise minor event	
NONE	MAJOR	Raise major event	
NONE	CRITICAL	Raise critical event	
MINOR	NONE	Clear minor event	
MINOR	MINOR	No action	
MINOR	MAJOR	Raise major event	
MINOR	CRITICAL	Raise critical event	
MAJOR	NONE	Clear critical event	
MAJOR	MINOR	Clear major event	Raise minor event
MAJOR	MAJOR	No action	
MAJOR	CRITICAL	Raise critical event	
CRITICAL	NONE	Clear critical event	
CRITICAL	MINOR	Clear critical event	Raise minor event
CRITICAL	MAJOR	Clear critical event	Raise major event
CRITICAL	CRITICAL	No action	

Chapter 11

Monitoring with the SRC CLI and the C-Web Interface

This chapter describes how to use the SRC CLI and the C-Web interface to monitor your SRC environment. Topics include:

Monitoring with the SRC CLI and the C-Web Interface

You can use the show commands available with the SRC CLI to monitor the operation and configuration of your SRC environment. For more information about setting up the initial configuration for the SRC CLI, see the *SRC-PE Getting Started Guide*.

The C-Web graphical user interface (GUI) allows you to monitor the operation and configuration of your SRC environment by using a Web browser with Hypertext Transfer Protocol (HTTP) or HTTP over Secure Sockets Layer (HTTPS) enabled.

SRC Monitoring Options

The *SRC-PE Monitoring and Troubleshooting Guide* contains monitoring information for core SRC components. Monitoring information for licensed applications such as SRC Admission Control Plug-In (SRC-ACP) is located in the *SRC-PE Application Library*. Monitoring information for solutions such as Juniper Policy Server (JPS) is located in the *SRC-PE Solutions Guide*.

Table 20 lists and compares the monitoring options for the C-Web interface and the SRC CLI.

Table 20: Comparison of SRC Monitoring Options

C-Web Interface Monitor Option	Information Displayed	Corresponding SRC CLI Commands
ACP	Admission Control Plug-In (ACP) data and statistics	■ show acp backbone congestion-point congestion-point-expression ■ show acp backbone congestion-point dn ■ show acp backbone service ■ show acp edge congestion-point dn ■ show acp edge congestion-point subscriber-session-id ■ show acp edge subscriber ■ show acp remote-update congestion-point dn ■ show acp remote-update congestion-point name ■ show acp remote-update subscriber ■ show acp statistics directory ■ show acp statistics general ■ show acp statistics router
CLI	SRC CLI level and authorization data	■ show cli ■ show cli authorization
Component	Installed components	■ show component
Date	System date and time	■ show date
Disk	System disk status	■ show disk status
Interfaces	System interfaces	■ show interfaces
Iptables	Filtered traffic statistics from the iptables LINUX tool	■ show iptables
JPS	Juniper Policy Server (JPS) data and statistics	■ show jps statistics ■ show jps statistics am ■ show jps statistics am connections ■ show jps statistics cmts-locator ■ show jps statistics cmts ■ show jps statistics_cmts connections ■ show jps statistics message-handler ■ show jps statistics message-handler message-flow ■ show jps statistics process ■ show jps statistics rks

Table 20: Comparison of SRC Monitoring Options (continued)

C-Web Interface Monitor Option	Information Displayed	Corresponding SRC CLI Commands
NIC	Network information collector (NIC) component configuration data and statistics, including NIC agents, resolvers, process	■ show nic data ■ show nic data agent ■ show nic data resolver ■ show nic statistics ■ show nic statistics agent ■ show nic statistics host ■ show nic statistics process ■ show nic statistics resolver ■ show nic slot number data ■ show nic slot number statistics
NTP	Network Time Protocol (NTP) configuration data and statistics	■ show ntp associations ■ show ntp statistics ■ show ntp status
Redirect server	Redirect server statistics	■ show redirect server statistics
Route	Route data from the local system to a remote host	■ show route

Table 20: Comparison of SRC Monitoring Options (continued)

C-Web Interface Monitor Option	Information Displayed	Corresponding SRC CLI Commands
SAE	SAE configuration data and statistics	■ show sae interfaces ■ show sae licenses ■ show sae policies ■ show sae registered equipment ■ show sae registered login ■ show sae routers ■ show sae services ■ show sae statistics directory ■ show sae statistics directory connections ■ show sae statistics license client ■ show sae statistics license local ■ show sae statistics license virtual-router ■ show sae statistics policy-management ■ show sae statistics process ■ show sae statistics radius ■ show sae statistics radius client ■ show sae statistics router ■ show sae statistics router common ■ show sae statistics sessions ■ show sae subscribers ■ show sae subscribers dn ■ show sae subscribers ip ■ show sae subscribers login-name ■ show sae subscribers service-name ■ show sae subscribers session-id ■ show sae threads
Security	Security certificate configuration and statistics	■ show security certificate
System	SRC software and C-series platform configuration data	■ show configuration ■ show system boot-messages ■ show system information

Starting the C-Web Interface

For information about setting up the initial configuration for the C-Web interface, see the *SRC Getting Started Guide*.

To start the C-Web interface:

1. Start the Web browser.
2. Enter the name or IP address of the SAE and the port number for the C-Web interface using one of the following formats:

   http://<SRC-host>[:<port>]
   https://<SRC-host>[:<port>]

   The C-Web login page appears.
3. On the login page, type your username and password, and click **Log In**.

   To correct or change the username or password you typed, click **Reset**, type the new entry or entries, and click **Log In**.

   The Monitor page appears.

   To explicitly terminate a C-Web session at any time, click **Logout** in the top pane.

Layout of the C-Web Interface

Each page of the C-Web interface is divided into the following panes, as shown in Figure 4.

Figure 4: C-Web Layout

- Top pane—Displays identifying information and links.
- Main pane—Location where you monitor the SRC software or the C-series platform by entering information in text boxes, making selections, and clicking buttons.
- Side pane—Displays subtasks of the Monitor task currently displayed in the main pane. Click an item to access it in the main pane.
- Bottom pane—Displays copyright and trademark information.

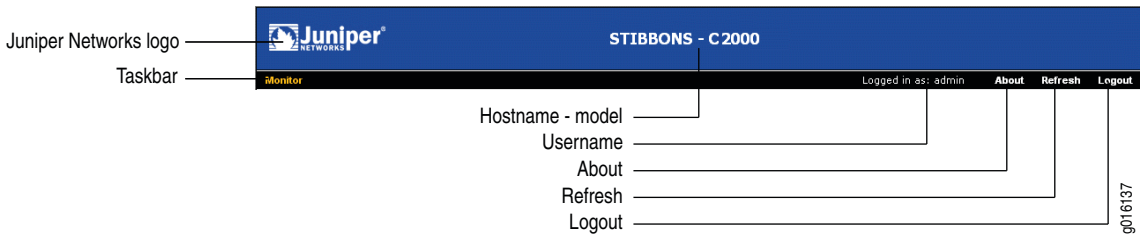
Elements of the C-Web Interface

This section summarizes the elements of the top pane, side pane, and main pane of the C-Web interface.

Top Pane Elements

The top pane comprises the elements shown in Figure 5 on page 88.

Figure 5: Top Pane Elements

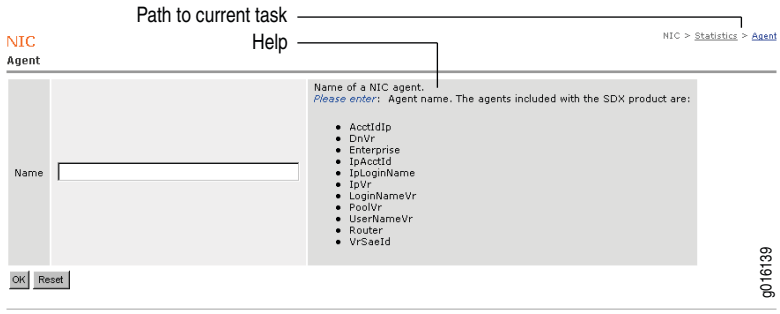


- Juniper Networks logo—Link to http://www.juniper.net in a new browser window.
- *hostname – model*—Hostname and model of the C-series platform.
- Logged in as: *username*—Username you used to log in to the C-series platform or the SRC software.
- About—Link to information about the C-Web interface, such as the version number.
- Logout—Ends your current login session with the C-Web interface and returns you to the login page.
- Taskbar—Menu of C-Web tasks. Click the Monitor task to view information about configuration on the C-series platform or the SRC software.

Main Pane Elements

The main pane comprises the elements shown in Figure 6.

Figure 6: Main Pane Elements



- Help—Displays field-specific information, such as the definition, format, and valid range of the field.
- Path to current task—Shows the successive C-Web tasks and subtasks that you selected to display the current main and side panes.

Side Pane Elements

The side pane comprises the elements shown in Figure 7.

Figure 7: Side Pane Elements

Each subtask displays options related to the selected task in the C-Web taskbar. Click the arrow signs (>) to expand individual items.

Navigating the C-Web Interface

The layout of the panes allows you to quickly navigate through the interface. You navigate the C-Web interface, move forward and backward, scroll pages, and expand and collapse elements as you do in a typical Web browser interface.

From the taskbar, select the C-Web task that you want to perform. Selecting the task displays related subtasks in the side pane. The side pane and taskbar are available from all pages, allowing you to skip from one task or subtask to the other from any page in the interface.

The path displayed in the top right corner of each page provides a context. Use this path to see your location in the monitoring tasks.

You can easily navigate to most subtasks by selecting them from the side pane. On pages where you are required to take an action, buttons and links allow you to move to the next or previous page as you perform certain actions.

Getting Help in the C-Web Interface

The C-Web interface provides Help for the monitoring options. Each field description contains information about the definition, format, and valid range of the field.

Part 5

Monitoring the SRC Software and the C-series Platform with the C-Web Interface and with the SRC CLI

Chapter 12

Monitoring the System with the SRC CLI

This chapter describes how to monitor the C-series platform with the SRC CLI. Topics include:

Viewing Information About the System with the SRC CLI

To view information about a C-series platform:

```
user@host> show system information
System Identification
Hostname         my-server
Manufacturer     Juniper Networks
Product Name     SDX-2000
Version          1.0
Serial Number    0207082006000001
UUID             48384441-5254-0030-4859-0030485977EE
Hostid           e30a2e07
Software version SRC-PE Release 7.0 [A.7.0.0-151]

System Time
Current time              2007-01-02 17:29:19 EST
Uptime                    15 days, 1:07
Number of active users    3
Load Averages (1m/5m/15m) 0.23/0.22/0.14

Memory
Total 15G
Free  12G

CPU Info
Number of CPU 4
CPU Model     Dual Core AMD Opteron(tm) Processor 265
Clock Speed   1804.132 MHz

Disk Information
  Mountpoint       Total Used  Use%
  /                2015M  956M  47%
  /altroot         2015M   35M   1%
```

```
  /altvar            29G   75M   0%
  /boot              98M   14M  14%
  /var               31G  216M   0%

Temperature
System +23 C
CPU-1  +33 C
CPU-2  +35 C

Fan speed
Fan-1 9375 RPM
Fan-2 9375 RPM
```

Viewing Information About Components Installed with the SRC CLI

To view release and status information for SRC components installed on a system:

```
user@host> show component
Installed Components
Name      Version                                          Status
cli       Release: 7.0 Build: CLI.A.7.0.0.0171             running
acp       Release: 7.0 Build: ACP.A.7.0.0.0174             disabled
jdb       Release: 7.0 Build: DIRXA.A.7.0.0.0176           running
editor    Release: 7.0 Build: EDITOR.A.7.0.0.0176          running
redir     Release: 7.0 Build: REDIR.A.7.0.0.0176           disabled
licSvr    Release: 7.0 Build: LICSVR.A.7.0.0.0179          stopped
nic       Release: 7.0 Build: GATEWAY.A.7.0.0.0170         disabled
sae       Release: 7.0 Build: SAE.A.7.0.0.0166             running
www       Release: 7.0 Build: UMC.A.7.0.0.0169             disabled
jps       Release: 7.0 Build: JPS.A.7.0.0.0172             disabled
agent     Release: 7.0 Build: SYSMAN.A.7.0.0.0174          running
webadm    Release: 7.0 Build: WEBADM.A.7.0.0.0173          disabled
```

Table 21 describes the output fields for the show component command. Output fields are listed in the order in which they appear.

Table 21: show component Output Fields

Field Name	Field Description
Name	Name of the component
Version	Version of the component
Status	State of the component, running or disabled

Viewing Information About Boot Messages with the SRC CLI

If you encounter system problems in a C-series platform after you start the system, you can view information about the boot process.

To view messages generated during system boot:

```
user@host> show system boot-messages

Bootdata ok (command line is ro root=/dev/vg0/root console=tty0
console=ttyS0,96
00)
```

```
Linux version 2.6.9-42.0.3.ELsmp (buildcentos@x8664-build.centos.org) (gcc
versi
on 3.4.6 20060404 (Red Hat 3.4.6-3)) #1 SMP Fri Oct 6 06:28:26 CDT 2006
BIOS-provided physical RAM map:
 BIOS-e820: 0000000000000000 - 000000000009ac00 (usable)
 BIOS-e820: 000000000009ac00 - 00000000000a0000 (reserved)
 BIOS-e820: 00000000000ea070 - 0000000000100000 (reserved)
 BIOS-e820: 0000000000100000 - 00000000dffc0000 (usable)
 BIOS-e820: 00000000dffc0000 - 00000000dffcf000 (ACPI data)
 BIOS-e820: 00000000dffcf000 - 00000000dfff0000 (ACPI NVS)
 BIOS-e820: 00000000dfff0000 - 00000000e0000000 (reserved)
 BIOS-e820: 00000000fec00000 - 00000000fec86000 (reserved)
 BIOS-e820: 00000000fee00000 - 00000000fee01000 (reserved)
 BIOS-e820: 00000000ffb00000 - 0000000100000000 (reserved)
 BIOS-e820: 0000000100000000 - 0000000220000000 (usable)
ACPI: RSDP (v000 ACPIAM                                    ) @
0x00000000000f7760
ACPI: RSDT (v001 A M I  OEMRSDT  0x03000529 MSFT 0x00000097) @
0x00000000dffc000
0
ACPI: FADT (v002 A M I  OEMFACP  0x03000529 MSFT 0x00000097) @
0x00000000dffc020
0
ACPI: MADT (v001 A M I  OEMAPIC  0x03000529 MSFT 0x00000097) @
0x00000000dffc039
0
ACPI: OEMB (v001 A M I  AMI_OEM  0x03000529 MSFT 0x00000097) @
0x00000000dffcf04
0
ACPI: DSDT (v001  DVLG2 DVLG2007 0x00000007 INTL 0x02002026) @
0x0000000000000000
0
No NUMA configuration found
Faking a node at 0000000000000000-0000000220000000
Bootmem setup node 0 0000000000000000-0000000220000000
No mptable found.
On node 0 totalpages: 2228224
  DMA zone: 4096 pages, LIFO batch:1
  Normal zone: 2224128 pages, LIFO batch:16
  HighMem zone: 0 pages, LIFO batch:1
DMI 2.3 present.
ACPI: PM-Timer IO Port: 0x408
ACPI: Local APIC address 0xfee00000
ACPI: LAPIC (acpi_id[0x01] lapic_id[0x00] enabled)
Processor #0 15:4 APIC version 16
ACPI: LAPIC (acpi_id[0x02] lapic_id[0x06] enabled)
Processor #6 15:4 APIC version 16
ACPI: LAPIC (acpi_id[0x03] lapic_id[0x01] enabled)
Processor #1 15:4 APIC version 16
ACPI: LAPIC (acpi_id[0x04] lapic_id[0x07] enabled)
Processor #7 15:4 APIC version 16
Setting APIC routing to flat
ACPI: IOAPIC (id[0x08] address[0xfec00000] gsi_base[0])
IOAPIC[0]: apic_id 8, version 32, address 0xfec00000, GSI 0-23
ACPI: IOAPIC (id[0x09] address[0xfec10000] gsi_base[24])
IOAPIC[1]: apic_id 9, version 32, address 0xfec10000, GSI 24-4
ACPI: INT_SRC_OVR (bus 0 bus_irq 0 global_irq 2 dfl dfl)
ACPI: INT_SRC_OVR (bus 0 bus_irq 9 global_irq 9 high level)
ACPI: IRQ0 used by override.
ACPI: IRQ2 used by override.
ACPI: IRQ9 used by override.
Using ACPI (MADT) for SMP configuration information
Allocating PCI resources starting at e2000000 (gap: e0000000:1ec00000)
```

```
Checking aperture...
Built 1 zonelists
Kernel command line: ro root=/dev/vg0/root console=tty0 console=ttyS0,9600
Initializing CPU#0
PID hash table entries: 4096 (order: 12, 131072 bytes)
time.c: Using 3.579545 MHz PM timer.
time.c: Detected 3200.267 MHz processor.
Console: colour VGA+ 80x25
Dentry cache hash table entries: 2097152 (order: 12, 16777216 bytes)
Inode-cache hash table entries: 1048576 (order: 11, 8388608 bytes)
Placing software IO TLB between 0x28c1000 - 0x68c1000
Memory: 8168568k/8912896k available (2106k kernel code, 0k reserved, 1297k
data,
 196k init)
Calibrating delay using timer specific routine.. 6406.43 BogoMIPS
(lpj=3203218)
Security Scaffold v1.0.0 initialized
SELinux:  Initializing.
SELinux:  Starting in permissive mode
There is already a security framework initialized, register_security failed.
selinux_register_security:  Registering secondary module capability
Capability LSM initialized as secondary
Mount-cache hash table entries: 256 (order: 0, 4096 bytes)
CPU: Trace cache: 12K uops, L1 D cache: 16K
CPU: L2 cache: 2048K
using mwait in idle threads.
CPU0: Initial APIC ID: 0, Physical Processor ID: 0
Using IO APIC NMI watchdog
CPU: Trace cache: 12K uops, L1 D cache: 16K
CPU: L2 cache: 2048K
CPU0: Initial APIC ID: 0, Physical Processor ID: 0
CPU0:                   Intel(R) Xeon(TM) CPU 3.20GHz stepping 03
per-CPU timeslice cutoff: 705.82 usecs.
task migration cache decay timeout: 1 msecs.
Booting processor 1/6 rip 6000 rsp 10006945f58
Initializing CPU#1
Calibrating delay using timer specific routine.. 6399.38 BogoMIPS
(lpj=3199690)
CPU: Trace cache: 12K uops, L1 D cache: 16K
CPU: L2 cache: 2048K
CPU1: Initial APIC ID: 6, Physical Processor ID: 3
                 Intel(R) Xeon(TM) CPU 3.20GHz stepping 03
Booting processor 2/1 rip 6000 rsp 1000697df58
Initializing CPU#2
Calibrating delay using timer specific routine.. 6399.32 BogoMIPS
(lpj=3199664)
CPU: Trace cache: 12K uops, L1 D cache: 16K
CPU: L2 cache: 2048K
```

Viewing Information About Security Certificates with the SRC CLI

To view information about security certificates that reside on the system:

```
user@host> show security certificate
web subject:CN=myhost
CAcert1 subject:CN=myhost
```

If no security certificates reside on the system, the CLI return a message to that effect:

```
user@host> show security certificate
No entity certificates in key store
```

Chapter 12

Monitoring the System with the C-Web Interface

This chapter describes how to use the C-Web interface to monitor the SRC software and the C-series platform. Topics include:

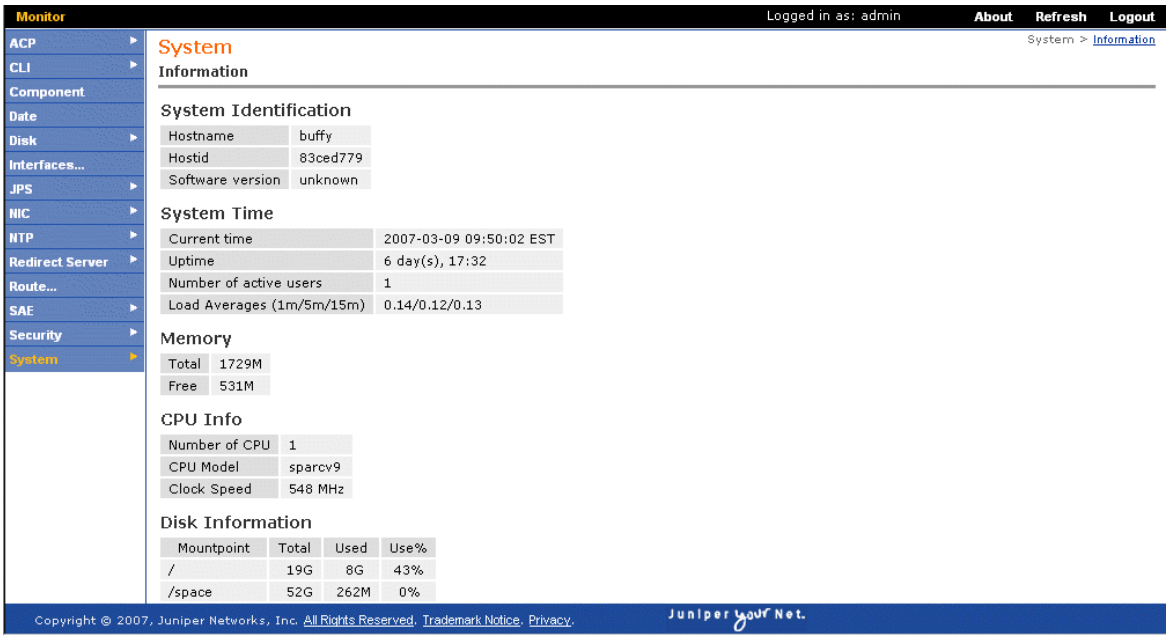
Viewing Information About the System with the C-Web Interface

You can view information about the SRC software, including system identification and the system time. You can also view information about the environment of the C-series platform, including memory, temperature, and fan speeds.

To view system information:

- Select **System** from the side pane, and click **Information**.

  The Information pane displays the system information.

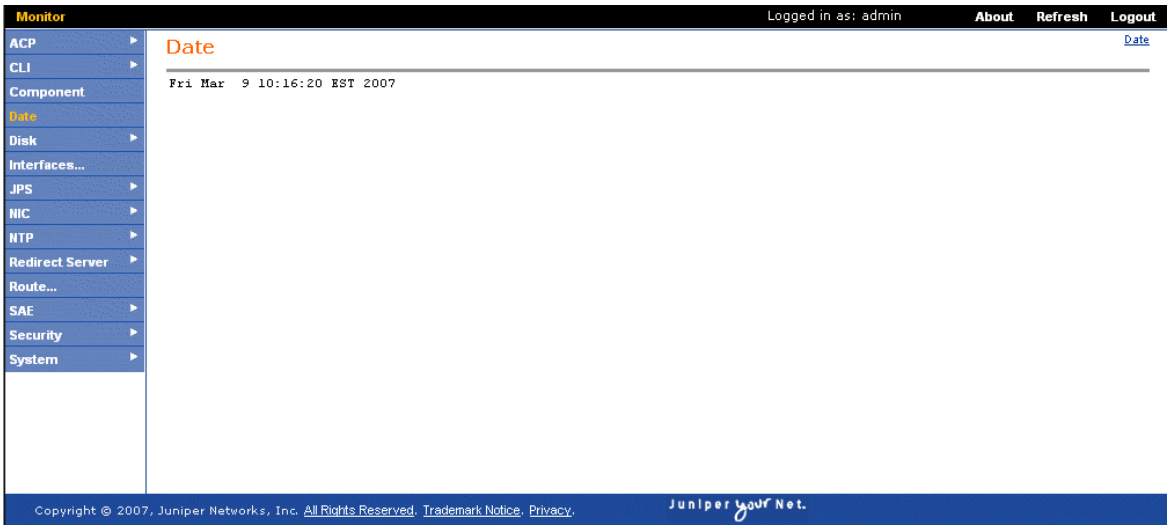


Viewing the System Date and Time with the C-Web Interface

To view the system date and time:

- Select **Date** from the side pane.

  The Date pane displays the date and time of the system.

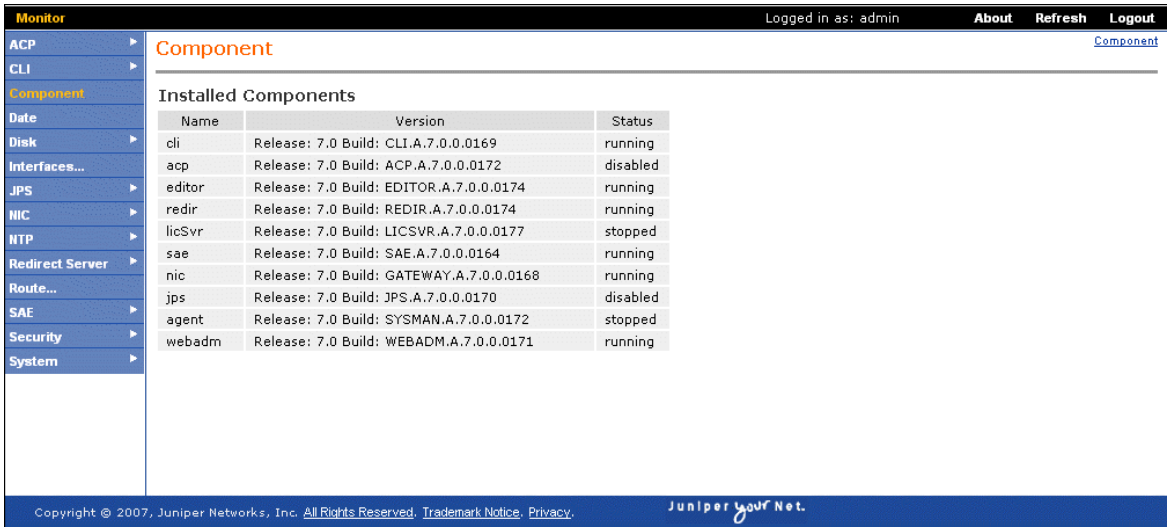


Viewing Information About Components Installed with the C-Web Interface

To view the installed SRC components:

- Select **Component** from the side pane.

  The Component pane displays the status of each installed component.

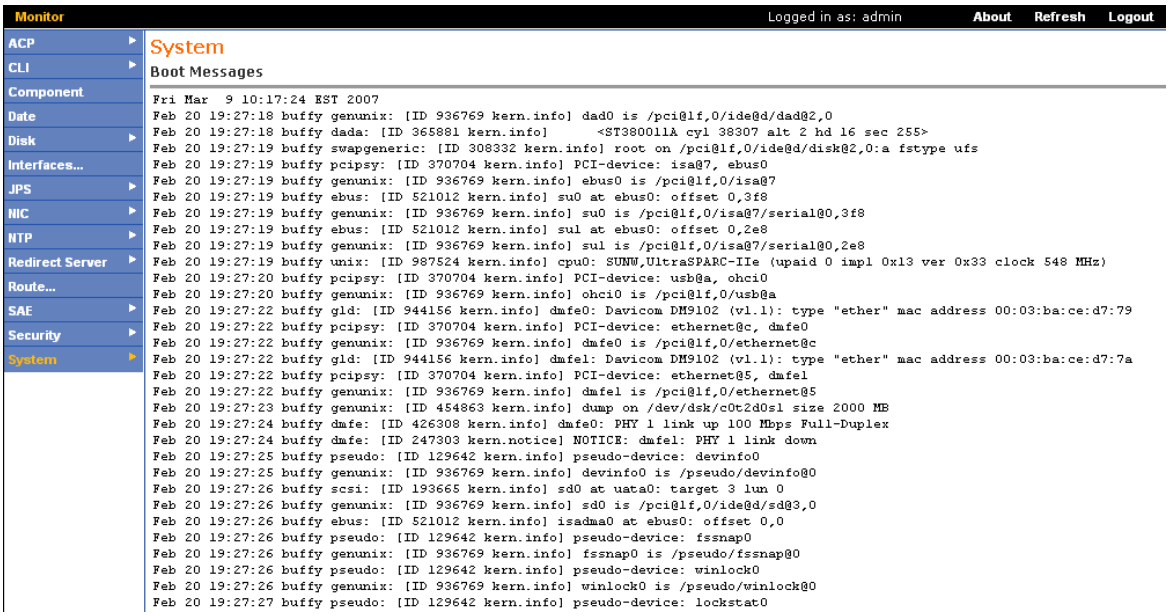


Viewing Information About Boot Messages with the C-Web Interface

To view messages generated during SRC software startup:

- Select **System** from the side pane, and click **Boot Messages**.

  The Boot Messages pane displays the boot messages.

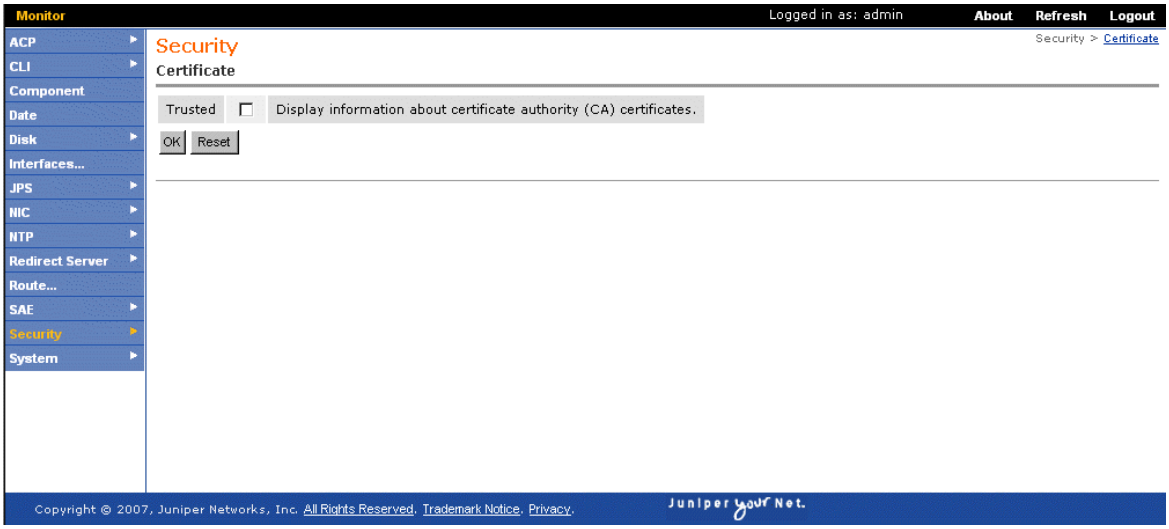


Viewing Information About Security Certificates with the C-Web Interface

To view messages generated during SRC software startup:

1. Select **Security** from the side pane, and click **Certificate**.

   The Certificate pane appears.



2. To display authority certificates, select the **Trusted** check box.
3. Click **OK**.

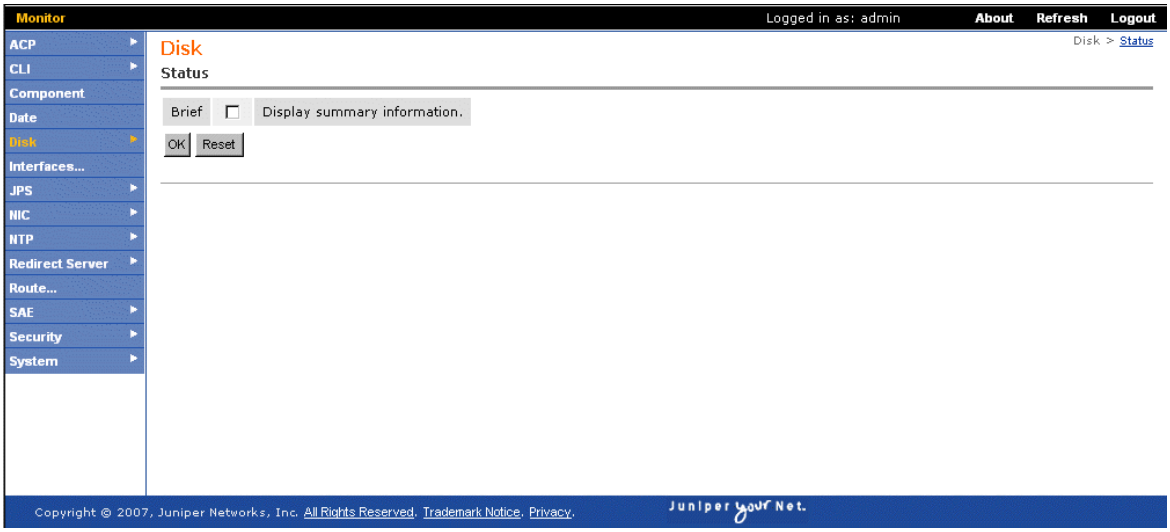
   The Certificate pane displays the security certificates.

Viewing Information About System Disk Status

To view information about the system disk status:

1. Select **Disk** from the side pane, and click **Status**.

   The Status pane appears.



2. To display a summary of the system disk status, select the **Brief** check box.
3. Click **OK**.

   The Status pane displays the system disk status.

Viewing Information About the SRC CLI with the C-Web Interface

You can view information about the current user's permissions and editing level for the SRC CLI.

Viewing Information About SRC CLI User Permissions

To display information about the current user's permissions for the SRC CLI:

- Select **CLI** from the side pane, and click **Authorization**.

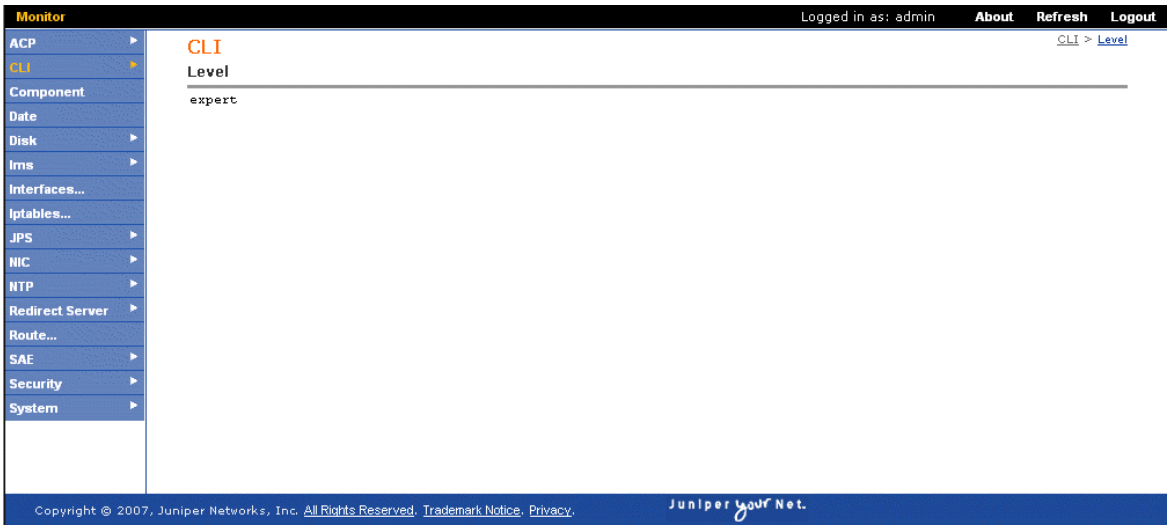
  The Authorization pane appears and displays the current user's permissions for each SRC CLI option.

Viewing Information About the SRC CLI User Level

To view information about the current user's editing level for the SRC CLI:

- Select **CLI** from the side pane, and click **Level**.

  The Level pane appears and displays the current user's editing level.



Chapter 13

Monitoring SAE Data with the SRC CLI

This chapter describes how to monitor the SAE with the CLI. Topics include:

Viewing SAE Data with the CLI

You can view information about the SAE active configuration. You can view data currently stored in the SAE server's memory for:

- Directory blacklist

  See Viewing Information About the Directory Blacklist with the CLI on page 110.

- Device drivers

  See Viewing Information About Device Drivers with the CLI on page 110.

- Interfaces

  See Viewing Information About Interfaces with the CLI on page 111.

- Licenses

  See Viewing Information About Licenses with the CLI on page 112.

- Policies

  See Viewing Information About Policies with the CLI on page 112.

- Registrations

  See Viewing Login Registrations with the CLI on page 113 and Viewing Equipment Registrations with the CLI on page 114.

- Services

  See Viewing Information About Services with the CLI on page 114.

- Threads

  See Viewing Information About Threads with the CLI on page 116.

Viewing Information About the Directory Blacklist with the CLI

To view information about the directory blacklist configured on the SAE:

user@host> **show sae directory-black-list**

Viewing Information About Device Drivers with the CLI

Each device driver manages one logical router instance. To view information about the state of SAE device drivers:

```
user@host> show sae drivers
JUNOSe Driver
Device name                          default@dryad
Device type                          junose
Device IP                            10.227.7.244
Local IP                             10.227.7.172
TransportRouter                      default@dryad
Device version                       7.2.0
Start time                           Tue Feb 13 14:18:44 EST 2007
Number of notifications              20
Number of processed added            14
Number of processed changed          0
Number of processed deleted          6
Number of provisioning attempt       30
Number of provisioning attempt failed 0
Number of outstanding decisions      0
Number of SAP                        7
Number of PAP                        1

  Job Queue
  Size                 0
  Age (ms)             1
  Total enqueued       28
  Total dequeued       28
  Average job time (ms) 426

  State Synchronization
  Number recovered subscriber sessions              0
  Number recovered service sessions                 0
  Number recovered interface sessions               0
  Number invalid subscriber sessions                0
  Number invalid service sessions                   0
  Number invalid interface sessions                 0
  Background restoration start time                 Tue Feb 13 14:18:49 EST 2007
  Background restoration end time                   Tue Feb 13 14:18:49 EST 2007
  Number subscriber sessions restored in background 0
  Number of provisioning objects left to collect    0
  Total number of provisioning objects to collect   11
  Start time                                        Tue Feb 13 14:18:45 EST 2007
  End time                                          Tue Feb 13 14:18:47 EST 2007
```

```
Number of synched contexts                          7
Number of post-sync jobs                            6
```

To view information about the state of a particular device driver, specify all or part of the virtual router name. For JUNOS router drivers and PCMM drivers, use the format default@routerName.

user@host> **show sae drivers device-name** *device-name*

To view only the virtual router names for the device driver:

```
user@host> show sae drivers brief
Router Drivers
Router Name              Router Type
default@simJunos            junos
```

To restrict the number of displayed results:

user@host> **show sae drivers maximum-results** *maximum-results*

Viewing Information About Interfaces with the CLI

We recommend that you do not enter the **show sae interfaces** command without specifying an interface, virtual router, brief, or maximum results to filter the results. Entering the **show sae interfaces** command can generate a large quantity of results, and processing these results can place a load on the C-series platform.

To view information about the router interfaces:

user@host> **show sae interfaces**

To view information about particular router interfaces, specify all or part of the interface name.

user@host> **show sae interfaces interface-name** *interface-name*

To view information about interfaces for a particular virtual router, specify all or part of the VR name.

user@host> **show sae interfaces virtual-router-name** *virtual-router-name*

To view only the interface names:

user@host> **show sae interfaces brief**

To restrict the number of displayed results:

user@host> **show sae interfaces maximum-results** *maximum-results*

Viewing Information About Licenses with the CLI

To view the installed licenses:

```
user@host> show sae licenses
SSC License Key Checker V3.0



Type of license: Pilot. Status: OK.

The following valid licenses are found:

License: cn=83ced779,ou=Licenses,o=Management,o=UMC
license.val.component = 1
license.val.customer = buffy
license.val.expiry = 2007-02-23
license.val.nodeid = 83ced779
license.val.release = 7.*
license.val.seqnum = 00555
license.val.type = pilot
license.val.userSessions = 100
```

Viewing Information About Policies with the CLI

To view information about the policies available on the SAE:

user@host> **show sae policies**

To view information about particular policies, specify all or part of the policy list name:

user@host> **show sae policies filter** *filter*

For example, if you wanted to view the policy called brickwall:

```
user@host> show sae policies filter brickwall
Policy Group
Policy Group Name brickwall
Absolute ID       policyGroupName=brickwall,ou=entjunos,o=Policies,o=UMC

  Policy Object
  applicability  both
  Name           both
  policyRoles    JUNOS
  accountingRule false
  Name           block
  priority       601
  ruleType       JUNOS ASP
  matchDirection both
  Name           all
  Name           drop
  Name           packet
```

To view only the policy list names for the policies:

```
user@host> show sae policies brief
Policies
ADSL-Basic
basicBod
```

```
BestEffort64
block
bod
bodVpn
both_fwr_filter
both_fwr_fwd
both_fwr_reject
brickwall
brickwall
content-provider
content-provider-tiered
custom_policer
default
default
DHCP
DocsisParameter
DownStream
dynsrcnat
eglimit
emailweb
emailweb
EntDefault
filter

More results available. Display has reached the maximum number of results.
Number of skipped results: 43
```

To restrict the number of displayed results:

user@host> **show sae policies maximum-results** *maximum-results*

Viewing Login Registrations with the CLI

You can view all login registrations, or you can view a specific registration.

For information about login registrations, see *SRC-PE Subscribers and Subscriptions Guide, Chapter 4, Configuring Subscriber–Related Properties on the SAE with the SRC CLI*.

To view information about all login registrations:

user@host> **show sae registered login**

To view a specific registration, specify the media access control (MAC) address for the registration that you want to display:

user@host> **show sae registered login mac-address** *mac-address*

To view only the MAC address of the registrations:

user@host> **show sae registered login brief**

To restrict the number of displayed results:

user@host> **show sae registered login maximum-results** *maximum-results*

Viewing Equipment Registrations with the CLI

You can view all equipment registrations, or you can view a specific registration.

For information about equipment registrations, see *SRC-PE Subscribers and Subscriptions Guide, Chapter 17, How Subscribers Use the Sample Residential Portal*.

To view information about all equipment registrations:

user@host> **show sae registered equipment**

To view a specific registration, specify the media access control (MAC) address for the registration that you want to display:

user@host> **show sae registered equipment mac-address** *mac-address*

To view only the MAC address of the registrations:

user@host> **show sae registered equipment brief**

To restrict the number of displayed results:

user@host> **show sae registered equipment maximum-results** *maximum-results*

Viewing Information About Services with the CLI

To view information about the services available on the SAE:

user@host> **show sae services**

To view information about particular services, specify all or part of the service name:

user@host> **show sae services filter** *filter*

For example, if you wanted to view the service called BrickWall:

```
user@host> show sae services filter brickwall
Service
available      true
description    This firewall blocks all incoming and outgoing traffic.
location       l=entjunos,o=scopes,o=umc
policygroupref policyGroupName=brickwall,ou=entjunos,o=Policies,o=UMC
servicename    BrickWall
servicetype    7
sspcategory    basicFirewall
ssptype        Normal
status         2
available      true
description    This firewall blocks all incoming and outgoing traffic.
location       l=entjunosstatelessfw,o=scopes,o=umc
policygroupref
policyGroupName=brickwall,ou=entjunos_statelessfw,o=Policies,o=UMC
servicename    BrickWall
servicetype    7
sspcategory    basicFirewall
ssptype        Normal
status         2
```

To view all the hidden services:

```
user@host> show sae services secret
Service
available      true
description    This firewall blocks all incoming traffic and allows only
               outgoing email and web traffic.
location       l=entjunos,o=scopes,o=umc
policygroupref policyGroupName=emailweb,ou=entjunos,o=Policies,o=UMC
servicename    EmailAndWeb
servicetype    7
sspcategory    basicFirewall
sspradiusclass EmailAndWeb
ssptype        Normal
status         2
available      true
description    This firewall blocks all incoming traffic and allows only
               outgoing email and web traffic.
location       l=entjunosstatelessfw,o=scopes,o=umc
policygroupref policyGroupName=emailweb,ou=entjunos_statelessfw,o=Policies,o=UMC
servicename    EmailAndWeb
servicetype    7
sspcategory    basicFirewall
sspradiusclass EmailAndWeb
ssptype        Normal
status         2

Service
available             true
                      This service is activated automatically when the
description           subscriber is the source or destination of a network
                      attack
location              l=idp-subscriber,o=scopes,o=umc
parametersubstitution captiveAddress=66.13.2.11
policygroupref        policyGroupName=quarantine,ou=idp,o=Policies,o=UMC
servicename           Quarantine
servicetype           7
sspradiusclass        Quarantine
ssptype               Normal
status                2
```

To view only the service names for the services:

```
user@host> show sae services brief
Services
EmailAndWeb
Quarantine
Audio-Silver
Internet-Gold
Internet-Silver
DynSrcNat
FWR_Filter_Out
StaticDestNat
PingDoSProtect
MirrorFragment
SubrIntfFragment
BrickWall
Audio-Bronze
Internet-Bronze
Limit500kbs
News
```

```
Gold_VPN
Limit1Mbs
Video-Silver
Audio-Gold
RouterFragment
1.0 Mbps
DynSrcNat
FWR_Filter_Out
StaticDestNat
PingDoSProtect
MirrorFragment
SubrIntfFragment
BrickWall
Audio-Bronze
Internet-Bronze
Limit500kbs
News
Gold_VPN
Limit1Mbs
Video-Silver
Audio-Gold
RouterFragment
1.0 Mbps
FWR_Rej_In
MirrorAggregate
Video-Bronze

More results available. Display has reached the maximum number of results.
Number of skipped results: 26
```

To restrict the number of displayed results:

user@host> **show sae services maximum-results** *maximum-results*

Viewing Information About Threads with the CLI

To view information about the threads and their priority on the SAE:

```
user@host> show sae threads
Thread Group
Thread group name system
Active threads    112
Active groups     11
Max priority      10

  Thread name          Priority Daemon thread
  Reference Handler    10        true
  Finalizer             8        true
  Signal Dispatcher     9        true

...

Thread Group
Thread group name RKSTrackingQueue
Active threads    5
Active groups     0
Max priority      10

  Thread name          Priority Daemon thread
  RKSTrackingQueue-0    5        true
  RKSTrackingQueue-1    5        true
```

```
RKSTrackingQueue-2    5        true
RKSTrackingQueue-3    5        true
RKSTrackingQueue-4    5        true
```

Viewing Information About Subscriber Sessions with the CLI

You can list subscriber sessions by:

- The distinguished name (DN) of the subscriber entry in the directory

  See Viewing Information About Subscriber Sessions by DN with the CLI on page 118.

- IP address

  See Viewing Information About Subscriber Sessions by IP Address with the CLI on page 118.

- Login name

  See Viewing Information About Subscriber Sessions by Login Name with the CLI on page 119.

- Service name

  See Viewing Information About Subscriber Sessions by Service Name with the CLI on page 119.

- Session ID

  See Viewing Information About Subscriber Sessions by Session ID with the CLI on page 120.

To view information about all subscriber sessions:

user@host> **show sae subscribers**

To view the subscriptions and service sessions from hidden services:

user@host> **show sae subscribers secret**

To view only the subscriber session information without service sessions:

user@host> **show sae subscribers brief**

To view the subscriber session ID, login name, and IP address:

user@host> **show sae subscribers terse**

To restrict the number of displayed results:

user@host> **show sae subscribers maximum-results** *maximum-results*

Viewing Information About Subscriber Sessions by DN with the CLI

To view information about subscriber sessions accessible by DN:

user@host> **show sae subscribers dn**

To view information about particular subscriber sessions, specify all or part of the DN:

user@host> **show sae subscribers dn filter** *filter*

To view the subscriptions and service sessions from hidden services:

user@host> **show sae subscribers dn secret**
user@host> **show sae subscribers dn filter** *filter* **secret**

To view only the subscriber session information without service sessions:

user@host> **show sae subscribers dn brief**
user@host> **show sae subscribers dn filter** *filter* **brief**

To view the subscriber session ID, login name, and IP address:

user@host> **show sae subscribers dn terse**
user@host> **show sae subscribers dn filter** *filter* **terse**

To restrict the number of displayed results:

user@host> **show sae subscribers dn maximum-results** *maximum-results*
user@host> **show sae subscribers dn filter** *filter* **maximum-results** *maximum-results*

Viewing Information About Subscriber Sessions by IP Address with the CLI

You can list subscriber sessions by IP address for Dynamic Host Configuration Protocol (DHCP) subscribers, authenticated Point-to-Point Protocol (PPP) subscribers, and static IP subscribers who have logged in to the portal.

To view information about subscriber sessions accessible by IP address:

user@host> **show sae subscribers ip**

To view information about particular subscriber sessions, specify the IP address:

user@host> **show sae subscribers ip filter** *filter*

To view the subscriptions and service sessions from hidden services:

user@host> **show sae subscribers ip secret**
user@host> **show sae subscribers ip filter** *filter* **secret**

To view only the subscriber session information without service sessions:

user@host> **show sae subscribers ip brief**
user@host> **show sae subscribers ip filter** *filter* **brief**

To view the subscriber session ID, login name, and IP address:

user@host> **show sae subscribers ip terse**
user@host> **show sae subscribers ip filter** *filter* **terse**

To restrict the number of displayed results:

user@host> **show sae subscribers ip maximum-results** *maximum-results*
user@host> **show sae subscribers ip filter** *filter* **maximum-results** *maximum-results*

Viewing Information About Subscriber Sessions by Login Name with the CLI

To view information about subscriber sessions accessible by login name:

user@host> **show sae subscribers login-name**

To view information about particular subscriber sessions, specify all or part of the login name:

user@host> **show sae subscribers login-name filter** *filter*

To view the subscriptions and service sessions from hidden services:

user@host> **show sae subscribers login-name secret**
user@host> **show sae subscribers login-name filter** *filter* **secret**

To view only the subscriber session information without service sessions:

user@host> **show sae subscribers login-name brief**
user@host> **show sae subscribers login-name filter** *filter* **brief**

To view the subscriber session ID, login name, and IP address:

user@host> **show sae subscribers login-name terse**
user@host> **show sae subscribers login-name filter** *filter* **terse**

To restrict the number of displayed results:

user@host> **show sae subscribers login-name maximum-results** *maximum-results*
user@host> **show sae subscribers login-name filter** *filter* **maximum-results** *maximum-results*

Viewing Information About Subscriber Sessions by Service Name with the CLI

To view information about subscriber sessions activated by a subscription to an active service session:

user@host> **show sae subscribers service-name**

To view information about particular subscriber sessions, specify all or part of the service name:

user@host> **show sae subscribers service-name filter** *filter*

To view the subscriptions and service sessions from hidden services:

user@host> **show sae subscribers service-name secret**
user@host> **show sae subscribers service-name filter** *filter* **secret**

To view only the subscriber session information without service sessions:

user@host> **show sae subscribers service-name brief**
user@host> **show sae subscribers service-name filter** *filter* **brief**

To view the subscriber session ID, login name, and IP address:

user@host> **show sae subscribers service-name terse**
user@host> **show sae subscribers service-name filter** *filter* **terse**

To restrict the number of displayed results:

user@host> **show sae subscribers service-name maximum-results** *maximum-results*
user@host> **show sae subscribers service-name filter** *filter* **maximum-results** *maximum-results*

Viewing Information About Subscriber Sessions by Session ID with the CLI

To view information about subscriber sessions by session ID:

user@host> **show sae subscribers session-id**

To view information about particular subscriber sessions, specify all or part of the subscriber session ID:

user@host> **show sae subscribers session-id filter** *filter*

To view the subscriptions and service sessions from hidden services:

user@host> **show sae subscribers session-id secret**
user@host> **show sae subscribers session-id filter** *filter* **secret**

To view only the subscriber session information without service sessions:

user@host> **show sae subscribers session-id brief**
user@host> **show sae subscribers session-id filter** *filter* **brief**

To view the subscriber session ID, login name, and IP address:

user@host> **show sae subscribers session-id terse**
user@host> **show sae subscribers session-id filter** *filter* **terse**

To restrict the number of displayed results:

user@host> **show sae subscribers session-id maximum-results** *maximum-results*
user@host> **show sae subscribers session-id filter** *filter* **maximum-results** *maximum-results*

Viewing SAE SNMP Information with the CLI

You can view state information that is also available through SNMP, including information about counters that describe the SAE history of activity. This information is the same as the information you can view from the SAE SNMP interface.

You can view SNMP information for:

- Directory

  See Viewing Statistics About the Directory with the CLI on page 122 and Viewing Statistics for Directory Connections with the CLI on page 122.

- Licenses

  See Viewing SNMP Information for Client Licenses with the CLI on page 123, Viewing SNMP Information for Local Licenses with the CLI on page 123, and Viewing SNMP Information for Licenses on Virtual Routers with the CLI on page 124.

- Policies

  See Viewing SNMP Information for Policies with the CLI on page 124.

- SAE server process

  See Viewing SNMP Information for the SAE Server Process with the CLI on page 124.

- RADIUS clients

  See Viewing Statistics for RADIUS Clients with the CLI on page 125 and Viewing SNMP Information for RADIUS Clients with the CLI on page 125.

- Routers and devices

  See Viewing Statistics for Device Drivers with the CLI on page 126 and Viewing Statistics for Specific Device Drivers with the CLI on page 126.

- Subscriber and service sessions

  See Viewing Statistics for Subscriber and Service Sessions with the CLI on page 127.

Viewing Statistics About the Directory with the CLI

To view statistics about the directory:

```
user@host> show sae statistics directory
SNMP Statistics
Services read         51
Services written      0
Subscriptions read    0
Subscriptions written 0
Users read            0
Users written         0
```

Viewing Statistics for Directory Connections with the CLI

To view statistics for directory connections:

```
user@host> show sae statistics directory connections
DES connection
Connection ID            FEEDBACK_DATA_MANAGER
Number of read           93
Number of write          93
Number of events sent    0
Number of events dropped 0
Average read time        2
Average write time       23
Directory host           127.0.0.1
Directory port           389
Directory type           primary
Primary restore time     83218
Event queue length       0

...

DES connection
Connection ID            ldapAuth-LdapAuthenticator
Number of read           0
Number of write          0
Number of events sent    0
Number of events dropped 0
Average read time        0
Average write time       0
Directory host           127.0.0.1
Directory port           389
Directory type           primary
Primary restore time     83200
Event queue length       0
```

To view information about particular directory connections, specify all or part of the connection ID.

user@host> **show sae statistics directory connections filter** *filter*

For example, if you wanted to view the directory connection that contained ldap in its connection ID:

```
user@host> show sae statistics directory connections filter ldap
DES connection
Connection ID            ldapAuth-LdapAuthenticator
Number of read           0
```

```
Number of write          0
Number of events sent    0
Number of events dropped 0
Average read time        0
Average write time       0
Directory host           127.0.0.1
Directory port           389
Directory type           primary
Primary restore time     83608
Event queue length       0
```

To view only the directory connection IDs:

```
user@host> show sae statistics directory connections brief
Directory Connections
FEEDBACK_DATA_MANAGER
EQUIPMENT_DATA_MANAGER
POM_Engine
LICENSE_MANAGER
SAE_ConfigMgr
adminLdap-LdapAuthenticator
SERVICE_DATA_MANAGER
USER_DATA_MANAGER
SAE_ConfigMgr(dynamicProps)
ldapAuth-LdapAuthenticator
```

Viewing SNMP Information for Client Licenses with the CLI

To view SNMP information about the state of client licenses:

user@host> **show sae statistics license client**

Viewing SNMP Information for Local Licenses with the CLI

To view SNMP information about the state of local licenses:

```
user@host> show sae statistics license local
Client License State
Mode                     Pilot
Number of licensed users 100
Number of current users  0
Expiry                   2007-02-23
```

Viewing SNMP Information for Licenses on Virtual Routers with the CLI

To view SNMP information about the state of licenses on specified virtual routers:

user@host> **show sae statistics license virtual-router**

To view information about the state of licenses for a particular virtual router, specify all or part of the VR name. For JUNOS router drivers and PCMM drivers, use the format default@routerName.

user@host> **show sae statistics license virtual-router filter** *filter*

To view only the virtual router names:

user@host> **show sae statistics license virtual-router brief**

Viewing SNMP Information for Policies with the CLI

To view SNMP information for the policy engine, policy decision point, and the shared object repository where the policy objects are stored:

```
user@host> show sae statistics policy-management
SNMP Statistics
Average time for processing interface    0
classifer modification
Average time for processing policy group 0
modification
Current total number of policy groups    68
loaded
Total number of default policy decisions 0
Total number of errors                   0
Total number of interface classifier     0
modifications
Total number of policy group             0
modifications
Total number of service policy decisions 0
Up time                                  81107 seconds since Tue Jan 23 19:52:53
                                         EST 2007
```

Viewing SNMP Information for the SAE Server Process with the CLI

To view SNMP information for the SAE server process:

```
user@host> show sae statistics process
SNMP Statistics
Heap in use 19211 kilo bytes (2%)
Heap limit  910016 kilo bytes
Threads     96
Up time     80877 seconds since Tue Jan 23 19:51:42 EST 2007
```

Viewing Statistics for RADIUS Clients with the CLI

To view SNMP statistics for RADIUS clients:

```
user@host> show sae statistics radius
SNMP Statistics
Accounting ACKs from unrecognized IP     0
Authentication ACKs from unrecognized IP 0
Radius client ID                         SAE.buffy
```

Viewing SNMP Information for RADIUS Clients with the CLI

To view SNMP information for RADIUS accounting clients:

user@host> **show sae statistics radius client accounting**

To view SNMP information for RADIUS authentication clients:

user@host> **show sae statistics radius client authentication**

To view information for a particular RADIUS client by IP address:

user@host> **show sae statistics radius client ip-address** *ip-address*
user@host> **show sae statistics radius client accounting ip-address** *ip-address*
user@host> **show sae statistics radius client authentication ip-address** *ip-address*

To view information for a particular RADIUS client by UDP port number:

user@host> **show sae statistics radius client udp-port** *udp-port*
user@host> **show sae statistics radius client accounting udp-port** *udp-port*
user@host> **show sae statistics radius client authentication udp-port** *udp-port*

To view only the RADIUS clients that were accessible by IP address and port number:

user@host> **show sae statistics radius client brief**
user@host> **show sae statistics radius client accounting brief**
user@host> **show sae statistics radius client authentication brief**

Viewing SNMP Information for Routers and Devices with the CLI

To view SNMP information for routers and devices that the SAE is managing:

user@host> **show sae statistics router**

To view information for a particular router, specify all or part of the VR name. For JUNOS router drivers and PCMM drivers, use the format default@routerName.

user@host> **show sae statistics router filter** *filter*

To view only the RADIUS clients that were accessible by IP address and port number:

user@host> **show sae statistics router brief**

Viewing Statistics for Device Drivers with the CLI

To view SNMP statistics for all device drivers:

```
user@host> show sae statistics router common
SNMP Statistics
Driver type                    JUNOSE COPS
Number of close requests       0
Number of connections accepted 0
Number of current connections  0
Number of open requests        0
Server address                 0.0.0.0
Server port                    3288
Time since last redirect       0

SNMP Statistics
Driver type                    PACKETCABLE COPS
Number of close requests       0
Number of connections accepted 0
Number of current connections  0
Number of open requests        0
Server address                 0.0.0.0
Server port                    0
Time since last redirect       0

SNMP Statistics
Driver type                    JUNOS
Number of close requests       0
Number of connections accepted 0
Number of current connections  0
Number of open requests        0
Server address                 0.0.0.0
Server port                    3333
Time since last redirect       0
```

The value of the server address can be either an IPv4 or IPv6 address, depending on the platform.

Viewing Statistics for Specific Device Drivers with the CLI

To view SNMP statistics for JUNOS router drivers:

user@host> **show sae statistics router common junos**

To view SNMP statistics for JUNOSe router drivers:

user@host> **show sae statistics router common junose-cops**

To view SNMP statistics for PCMM device drivers:

user@host> **show sae statistics router common packetcable-cops**

To view SNMP statistics for third-party device drivers:

user@host> **show sae statistics router common proxy**

For example, to view SNMP statistics for JUNOS router drivers:

```
user@host> show sae statistics router common junos
SNMP Statistics
Driver type                    JUNOS
Number of close requests       0
Number of connections accepted 0
Number of current connections  0
Number of open requests        0
Server address                 0.0.0.0
Server port                    3333
Time since last redirect       0
```

Viewing Statistics for Subscriber and Service Sessions with the CLI

To view SNMP statistics for subscriber and service sessions:

```
user@host> show sae statistics sessions
SNMP Statistics
Current service sessions                          0
Current user sessions                             0
Logins (includes sync. and static IP portal logins) 0
Logouts                                           0
Service session idle timeouts                     0
Service sessions started                          0
Service sessions stopped                          0
Service session timeouts                          0
```

Chapter 14

Monitoring SAE Data with the C-Web Interface

This chapter describes how to use the C-Web interface to monitor SAE data. Topics include:

Viewing SAE Data with the C-Web Interface

You can view data currently stored in the SAE server's memory for:

- Directory blacklist
- Services
- Licenses
- Policies
- Devices
- Interfaces
- Login registrations
- Equipment registrations
- Threads
- Subscriber Sessions

Viewing Information About the Directory Blacklist

To view information about the directory blacklist configured on the SAE:

- Select **SAE** from the side pane, and click **Directory Blacklist**.

  The Directory Blacklist pane appears.

Viewing Information About Services

To view information about the services available on the SAE:

1. Select **SAE** from the side pane, and click **Services**.

   The Services pane appears.

2. In the Service Name box, enter a full or partial service name for which you want to display information, or leave the box blank to display all services.

3. Select the **Secret** check box to set a flag indicating that secret services are displayed.

4. Select an output style from the Style list.

5. In the Maximum Results box, enter the maximum number of results that you want to receive.

6. Click **OK**.

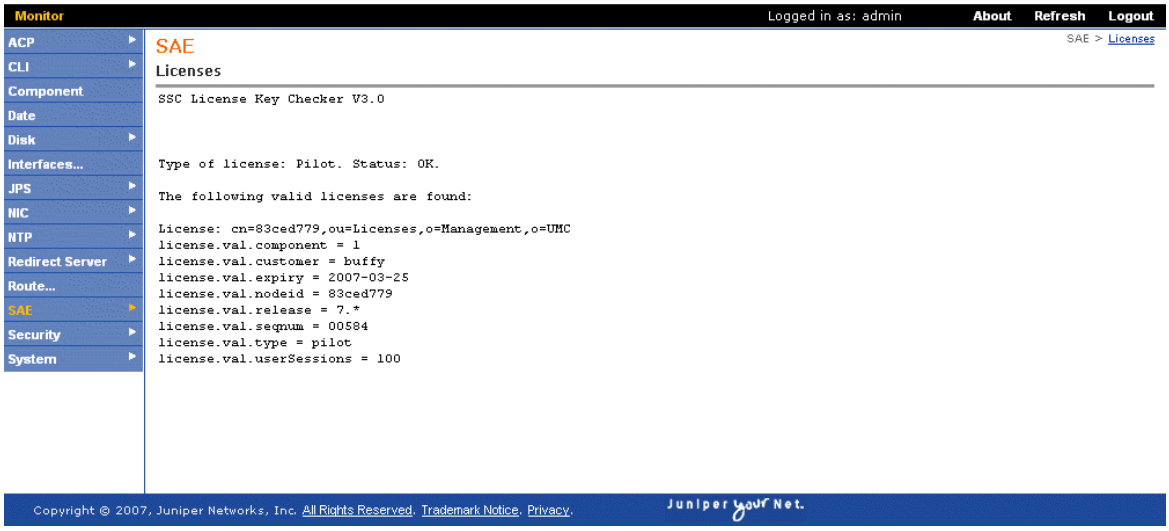
   The Services pane displays the status of the services running on the SAE.

Viewing Information About Licenses

To view information about licenses:

- Select **SAE** from the side pane, and click **License**.

  The Licenses pane displays statistics for licenses.

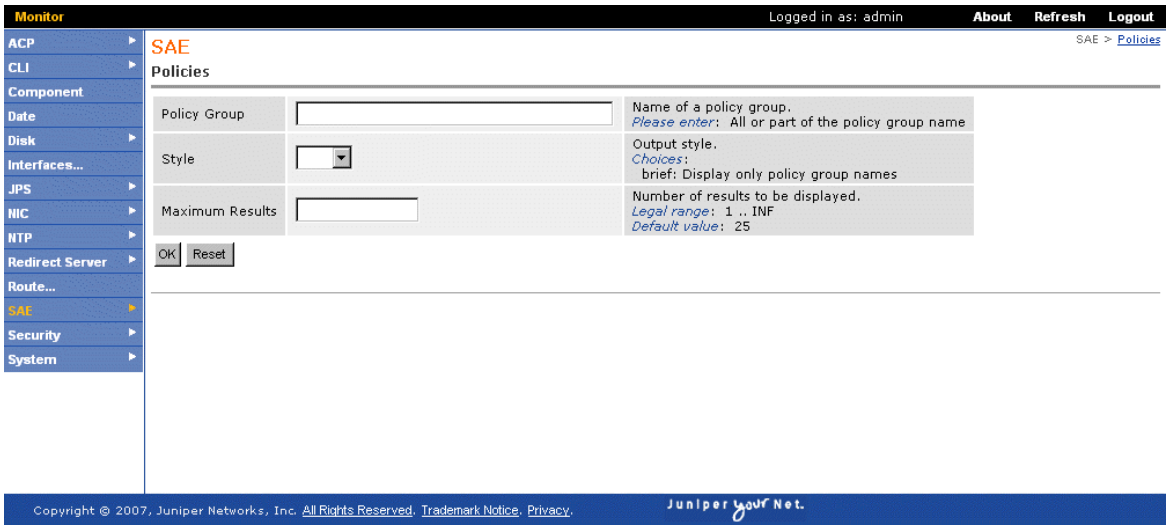


Viewing Information About Policies

To view information about the policies available on the SAE:

1. Select **SAE** from the side pane, and click **Policies**.

   The Policies pane appears.



2. In the Policy Group box, enter a full or partial policy name for which you want to display information, or leave the box blank to display all policies.

3. Select an output style from the Style list.

4. In the Maximum Results box, enter the maximum number of results that you want to receive.

5. Click **OK**.

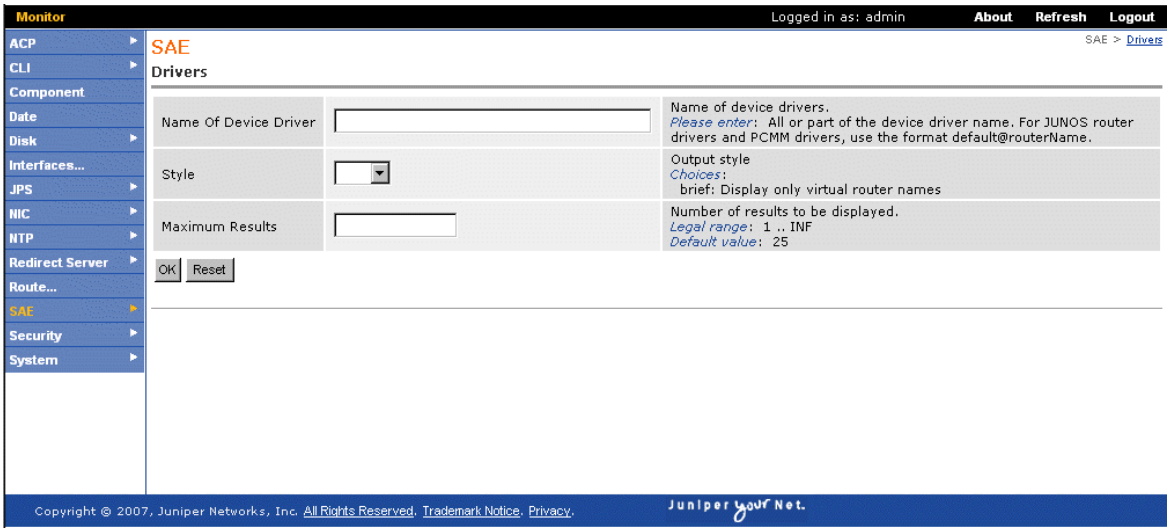
   The Policies pane displays the status of the policies configured on the SAE.

Viewing Information About Device Drivers

To view information about the device drivers available on the SAE:

1. Select **SAE** from the side pane, and click **Drivers**.

   The Drivers pane appears.



2. In the Name of Device Driver box, enter a full or partial device driver name for which you want to display information, or leave the box blank to display all devices.

   For JUNOSe router drivers, use the format:

   <virtual router name>@<router name>

   For JUNOS router drivers and PCMM drivers, use the format:

   default@<router name>

3. Select an output style from the Style list.

4. In the Maximum Results box, enter the maximum number of results that you want to receive.

5. Click **OK**.

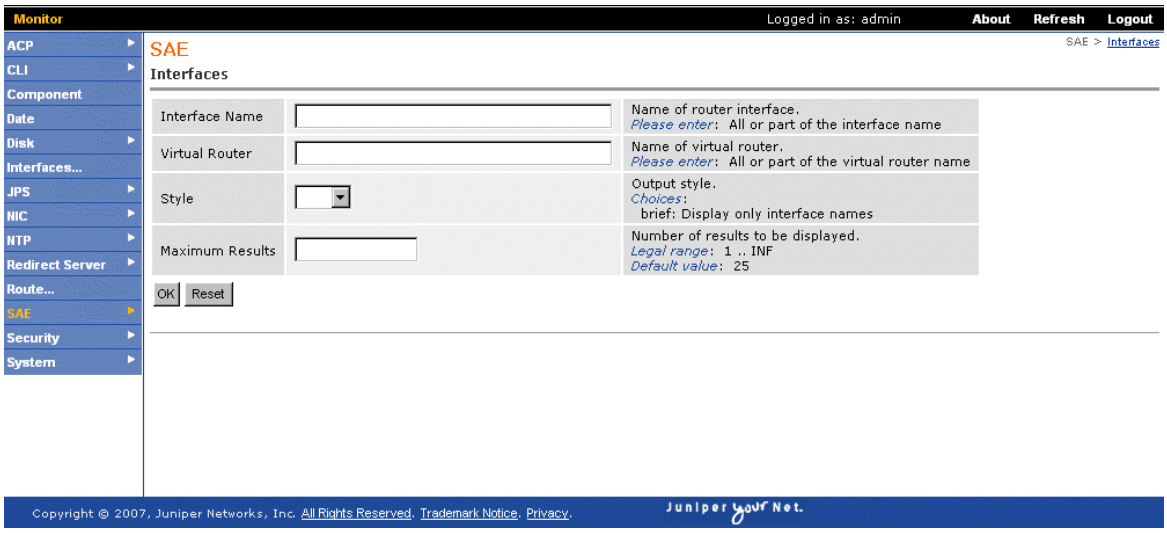
   The Drivers pane displays the status of the routers running on the SAE.

Viewing Information About Interfaces

To view information about the interfaces available on the router:

1. Select **SAE** from the side pane, and click **Interfaces**.

   The Interfaces pane appears.



2. In the Interface Name box, enter the name of the router interface for which you want to display information. or leave the box blank to display information about all router interfaces.

3. In the Virtual Router box, enter the name of the virtual router for which you want to display interfaces, or leave the box blank to display information for all virtual routers.

4. Select an output style from the Style list.

5. In the Maximum Results box, enter the maximum number of results that you want to receive.

6. Click **OK**.

   The Interfaces pane displays the interfaces available on the router.

Viewing Login Registrations

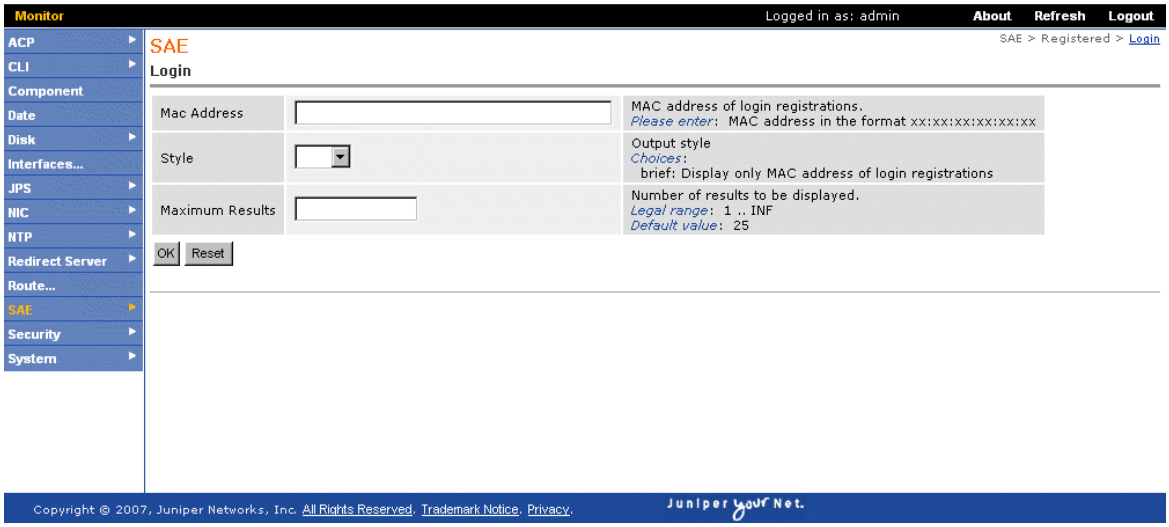
You can view all login registrations, or you can view a specific registration.

For information about login and equipment registrations, see *SRC-PE Subscribers and Subscriptions Guide, Chapter 17, How Subscribers Use the Sample Residential Portal*.

To view information about login registrations:

1. Select **Registered** from the side pane, and click **Login**.

   The Login pane appears.



2. In the MAC Address box, enter a MAC address that specifies the login registrations that you want to display.

   Use the format:

   xx:xx:xx:xx:xx:xx

3. Select an output style from the Style list.

4. In the Maximum Results box, enter the maximum number of results that you want to receive.

5. Click **OK**.

   The Login pane displays information about the login registrations.

Viewing Equipment Registrations

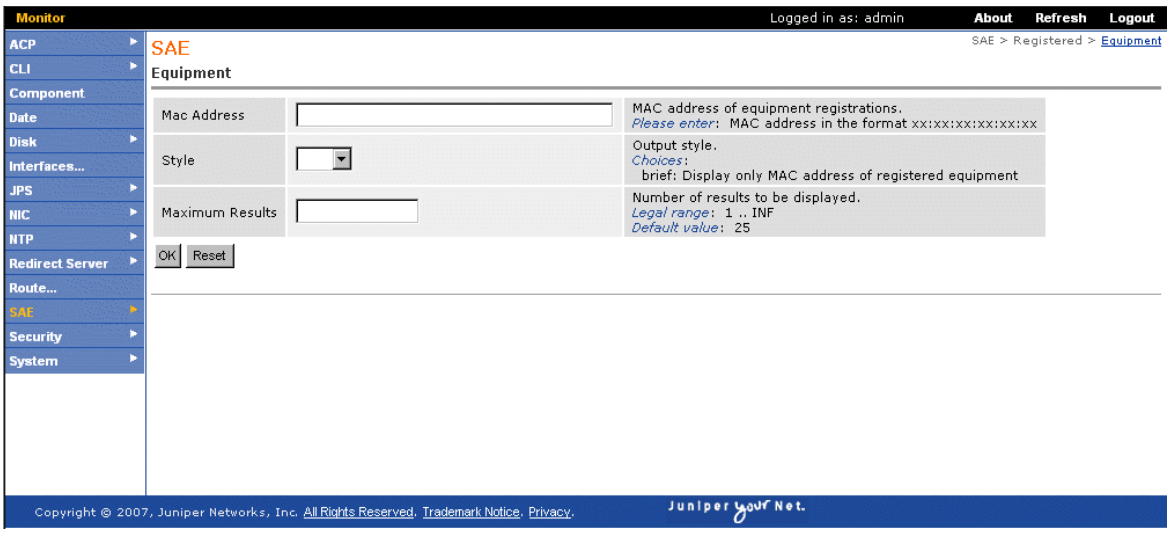
You can view all equipment registrations, or you can view a specific registration.

For information about login and equipment registrations, see *SRC-PE Subscribers and Subscriptions Guide, Chapter 17, How Subscribers Use the Sample Residential Portal*.

To view information about equipment registrations:

1. Select **Registered** from the side pane, and click **Equipment**.

   The Equipment pane appears.



2. In the MAC Address box, enter a MAC address that specifies the equipment registrations that you want to display.

   Use the format:

   xx:xx:xx:xx:xx:xx

3. Select an output style from the Style list.

4. In the Maximum Results box, enter the maximum number of results that you want to receive.

5. Click **OK**.

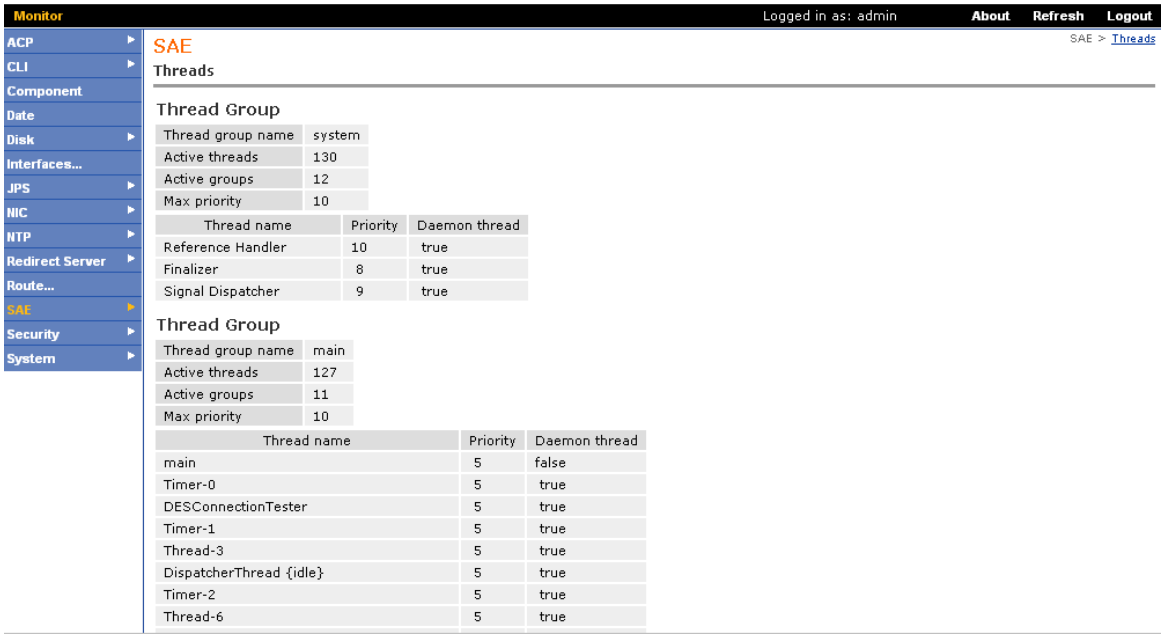
   The Equipment pane displays information about the equipment registrations.

Viewing Information About Threads

To view information about the threads and their priority on the SAE:

- Select **SAE** from the side pane, and click **Threads**.

  The Threads pane displays information about threads.



Viewing Information About Subscriber Sessions with the C-Web Interface

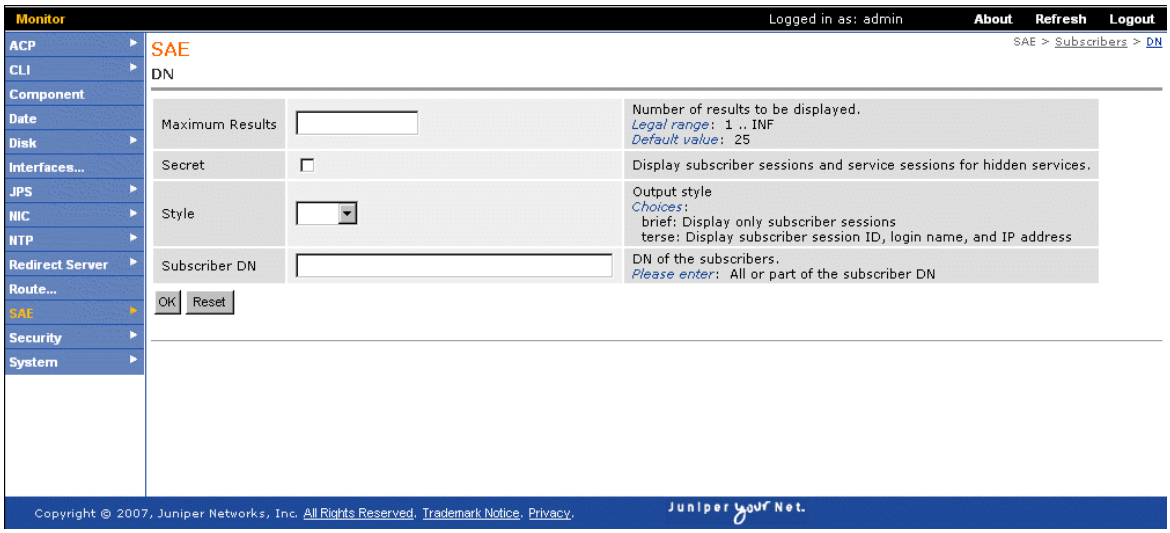
You can list subscriber sessions by the distinguished name (DN) of the subscriber entry in the directory, by login name, or by session ID. You can also list subscriber sessions by IP address for Dynamic Host Configuration Protocol (DHCP) subscribers, authenticated Point-to-Point Protocol (PPP) subscribers, and static IP subscribers who are being managed by the SAE.

Viewing Information About Subscriber Sessions by DN

To view information about subscriber sessions by DN:

1. Select **SAE** from the side pane, click **Subscribers**, and then click **DN**.

   The DN pane appears.



2. In the Maximum Results box, enter the maximum number of results that you want to receive.

3. Select the **Secret** check box to set a flag indicating that subscriptions and service sessions from hidden services are displayed.

4. Select an output style from the Style list.

5. In the Subscriber DN box, enter a full or partial subscriber DN for which you want to display information, or leave the box blank to display all subscriber sessions.

6. Click **OK**.

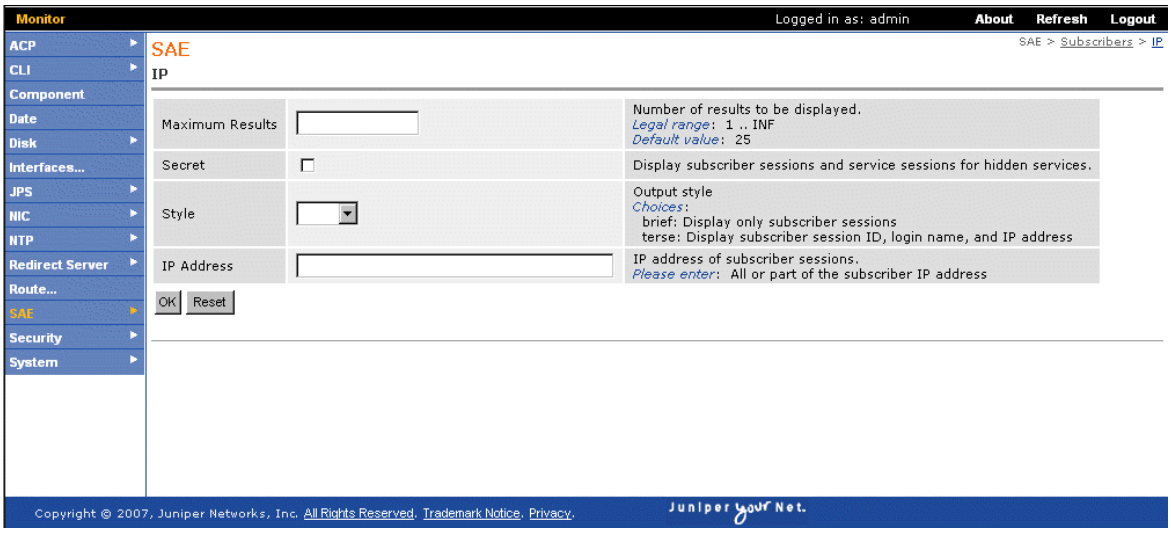
   The DN pane displays information about subscriber sessions.

Viewing Information About Subscribers by IP Address

To view information about subscriber sessions by IP address:

1. Select **SAE** from the side pane, click **Subscribers**, and then click **IP**.

   The IP pane appears.



2. In the Maximum Results box, enter the maximum number of results that you want to receive.

3. Select the **Secret** check box to set a flag indicating that subscriptions and service sessions from hidden services are displayed.

4. Select an output style from the Style list.

5. In the IP Address box, enter a full or partial IP address for which you want to display information, or leave the box blank to display all subscriber sessions.

6. Click **OK**.

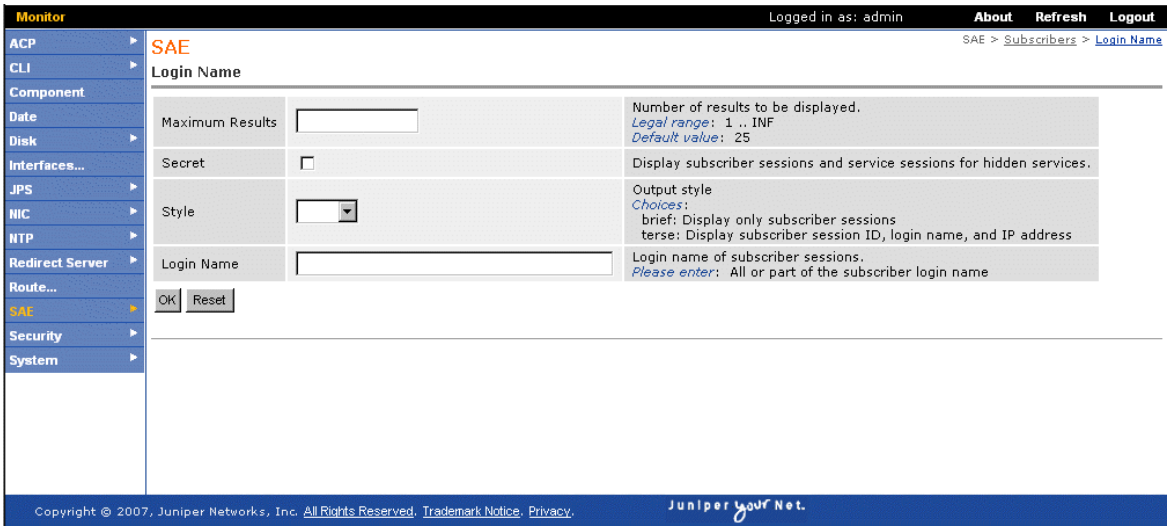
   The IP pane displays information about subscriber sessions.

Viewing Information About Subscriber Sessions by Login Name

To view information about subscriber sessions by login name:

1. Select **SAE** from the side pane, click **Subscribers**, and then click **Login Name**.

   The Login Name pane appears.



2. In the Maximum Results box, enter the maximum number of results that you want to receive.

3. Select the **Secret** check box to set a flag indicating that subscriptions and service sessions from hidden services are displayed.

4. Select an output style from the Style list.

5. In the Login Name box, enter a full or partial login name for which you want to display information, or leave the box blank to display all subscriber sessions.

6. Click **OK**.

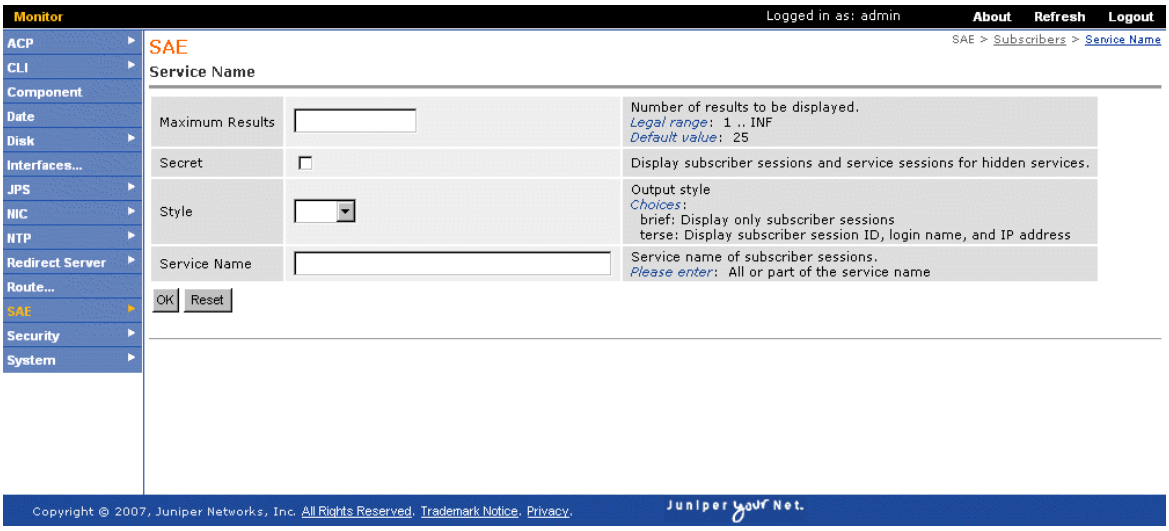
   The Login Name pane displays information about subscriber sessions.

Viewing Information About Subscriber Sessions by Service Name

To view information about subscriber sessions by service name:

1. Select **SAE** from the side pane, click **Subscribers**, and then click **Service Name**.

   The Service Name pane appears.



2. In the Maximum Results box, enter the maximum number of results that you want to receive.

3. Select the **Secret** check box to set a flag indicating that subscriptions and service sessions from hidden services are displayed.

4. Select an output style from the Style list.

5. In the Service Name box, enter a full or partial service name for which you want to display information, or leave the box blank to display all subscriber sessions.

6. Click **OK**.

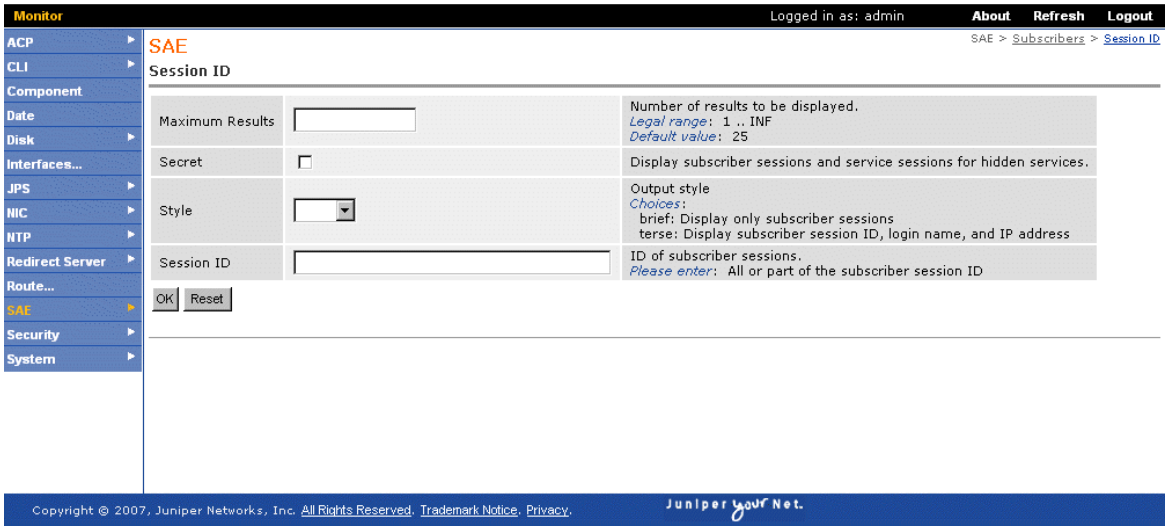
   The Service Name pane displays information about subscriber sessions.

Viewing Information About Subscriber Sessions by Session ID

To view information about subscriber sessions by session ID:

1. Select **SAE** from the side pane, click **Subscribers**, and then click **Session ID**.

   The Session ID pane appears.



2. In the Maximum Results box, enter the maximum number of results that you want to receive.

3. Select the **Secret** check box to set a flag indicating that subscriptions and service sessions from hidden services are displayed.

4. Select an output style from the Style list.

5. In the Session ID box, enter a full or partial session ID name for which you want to display information, or leave the box blank to display all subscriber sessions.

6. Click **OK**.

   The Session ID pane displays information about subscriber sessions.

Viewing SNMP Information with the C-Web Interface

You can use the C-Web interface to view SNMP statistics for the SAE configuration of:

- Directory
- Licenses
- Policies

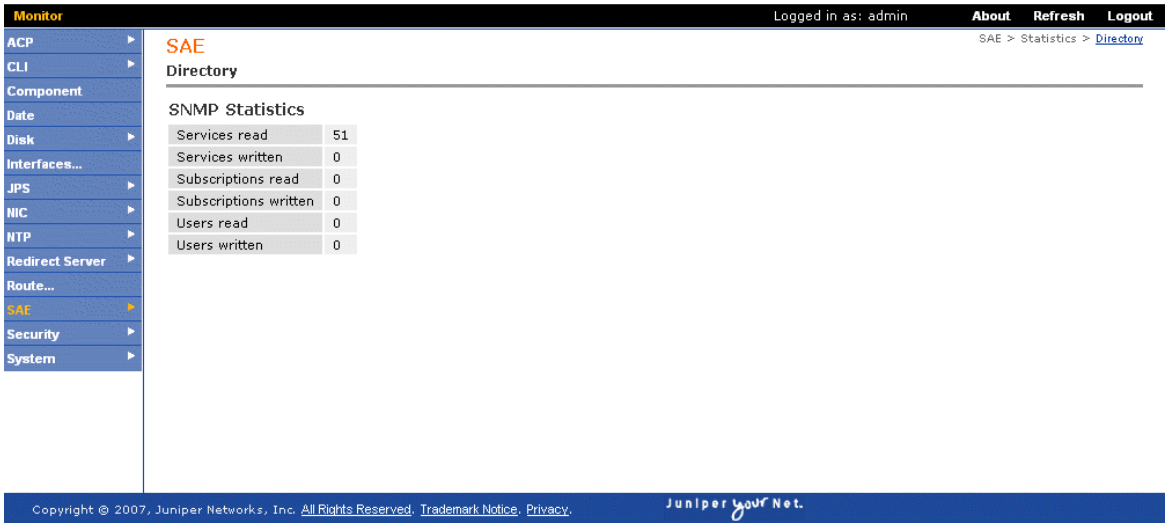
- Server processes
- RADIUS
- Devices
- Subscriber sessions and service sessions

Viewing SNMP Statistics for the Directory

To view SNMP statistics for the directory:

- Select **SAE** from the side pane, click **Statistics**, and then click **Directory**.

  The Directory pane displays statistics for the directory.

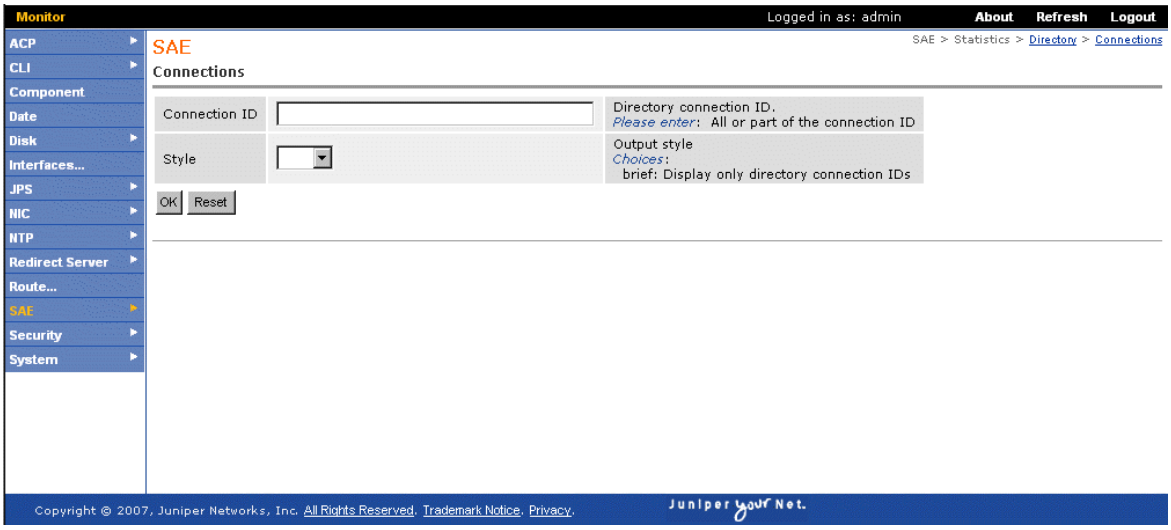


Viewing SNMP Statistics for Directory Connections

To view SNMP statistics for directory connections:

1. Select **SAE** from the side pane, click **Statistics**, click **Directory**, and then click **Connections**.

   The Connections pane appears.



2. In the Connection ID box, enter a full or partial connection ID for which you want to display information, or leave the box blank to display all SNMP statistics for all directory connections.

3. Select an output style from the Style list.

4. Click **OK**.

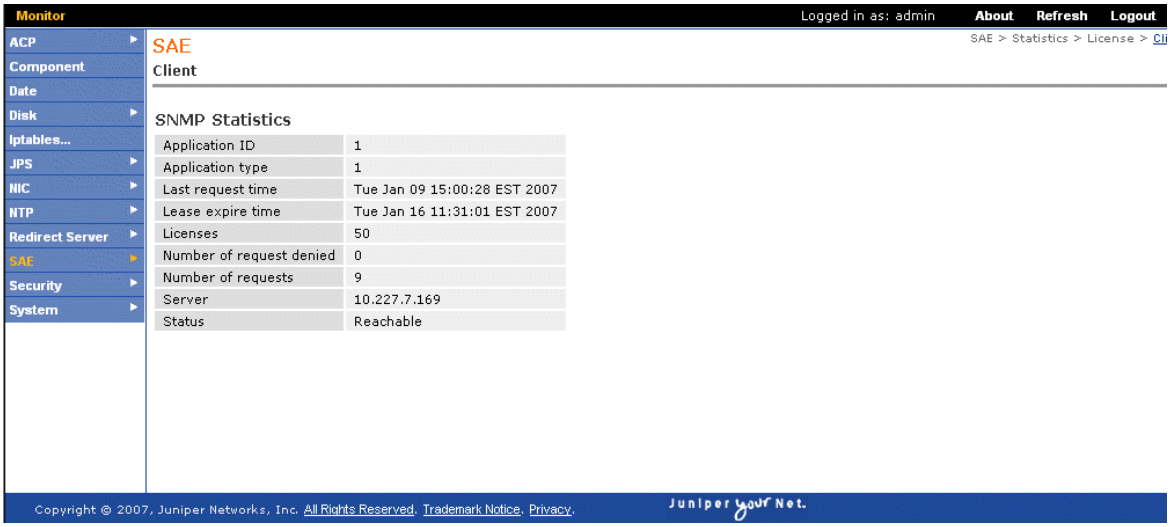
   The Connections pane displays statistics for directory connections.

Viewing SNMP Statistics for Client Licenses

To view SNMP statistics for client licenses:

- Select **SAE** from the side pane, click **Statistics**, click **License**, and then click **Client**.

  The Client pane displays statistics for client licenses.

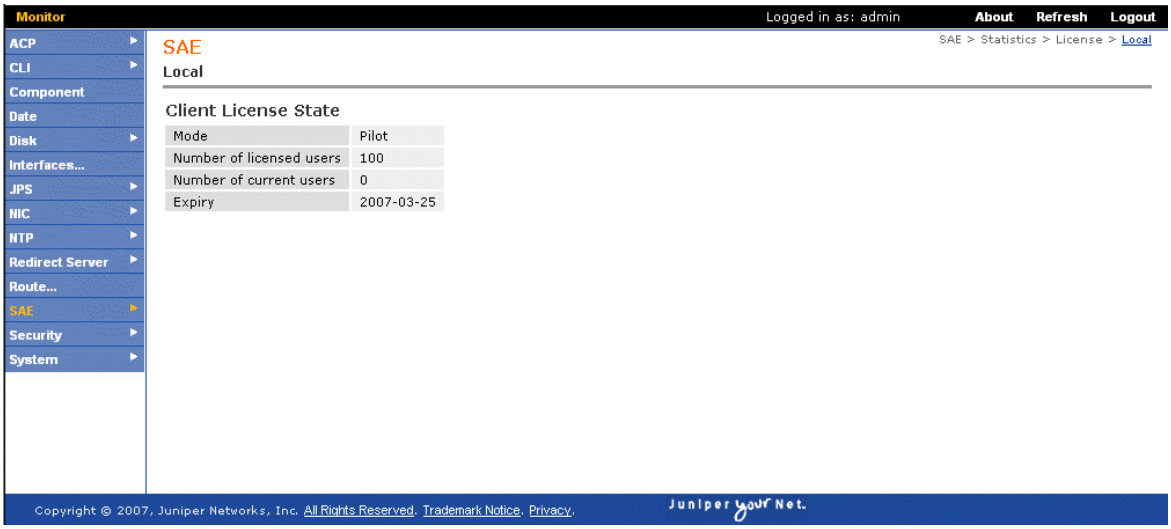


Viewing SNMP Statistics for Local Licenses

To view SNMP statistics for local licenses:

- Select **SAE** from the side pane, click **Statistics**, click **License**, and then click **Local**.

  The Local pane displays statistics for local licenses.



Viewing SNMP Statistics for Licenses by Device

To view SNMP statistics for licenses by device:

1. Select **SAE** from the side pane, click **Statistics**, click **License**, and then click **Device**.

   The Device pane appears.

2. In the Device Name box, enter a full or partial device name for which you want to display information, or leave the box blank to display SNMP statistics for all devices.

   For JUNOSe router drivers, use the format:

   <virtual router name>@<router name>

   For JUNOS router drivers and PCMM drivers, use the format:

   default@<router name>

3. Select an output style from the Style list.

4. Click **OK**.

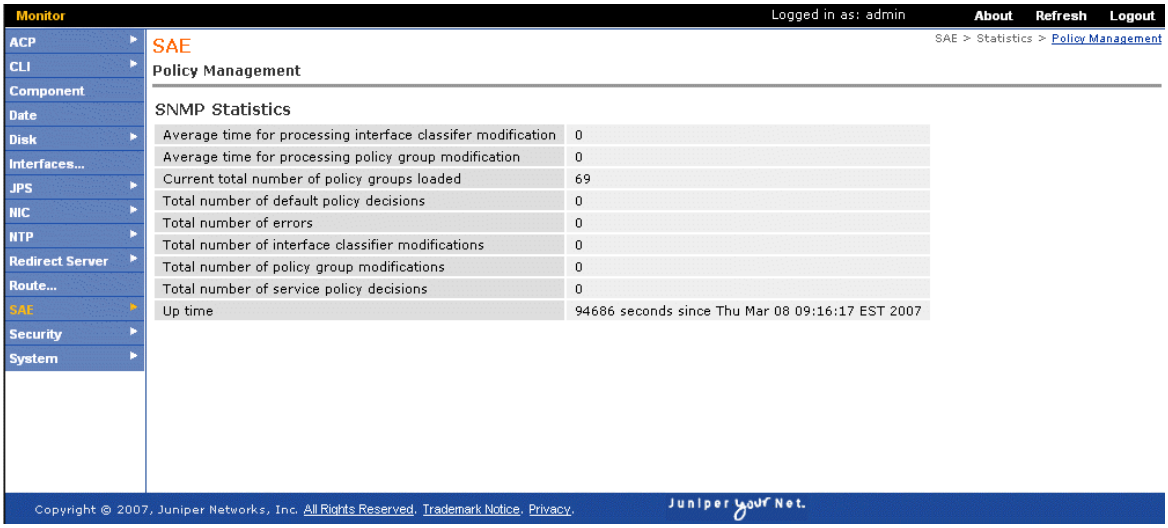
   The Device pane displays statistics for virtual router licenses.

Viewing SNMP Statistics About Policies

To view SNMP statistics about policies:

- Select **SAE** from the side pane, click **Statistics**, and then click **Policy Management**.

  The Policy Management pane displays statistics for policies.



Viewing SNMP Statistics About Server Processes

To view SNMP statistics about server processes:

- Select **SAE** from the side pane, click **Statistics**, and then click **Process**.

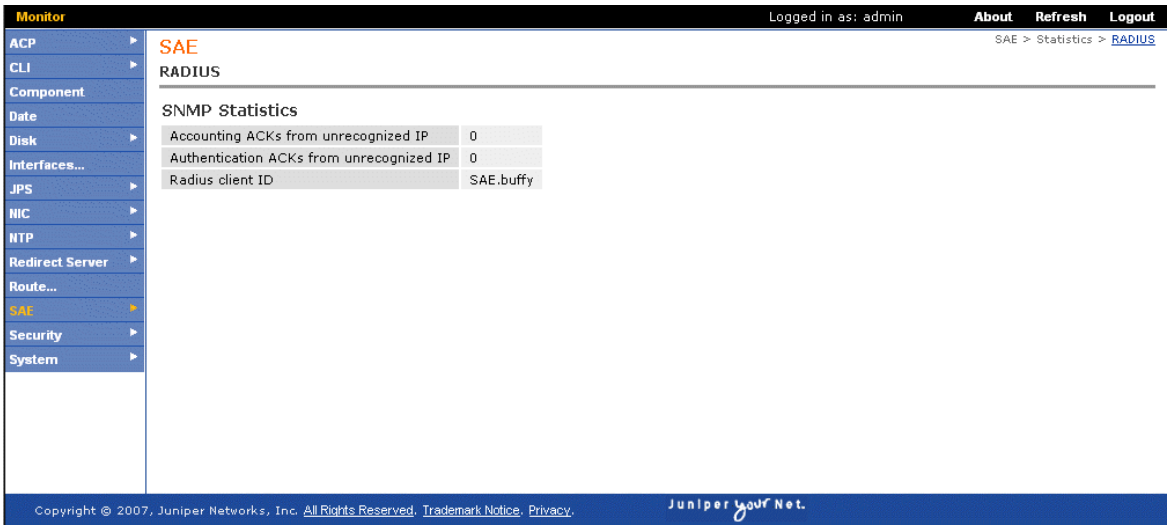
  The Process pane displays statistics for server processes.

Viewing SNMP Statistics About RADIUS

To view SNMP statistics about RADIUS:

- Select **SAE** from the side pane, click **Statistics**, and then click **RADIUS**.

  The RADIUS pane displays statistics for RADIUS.

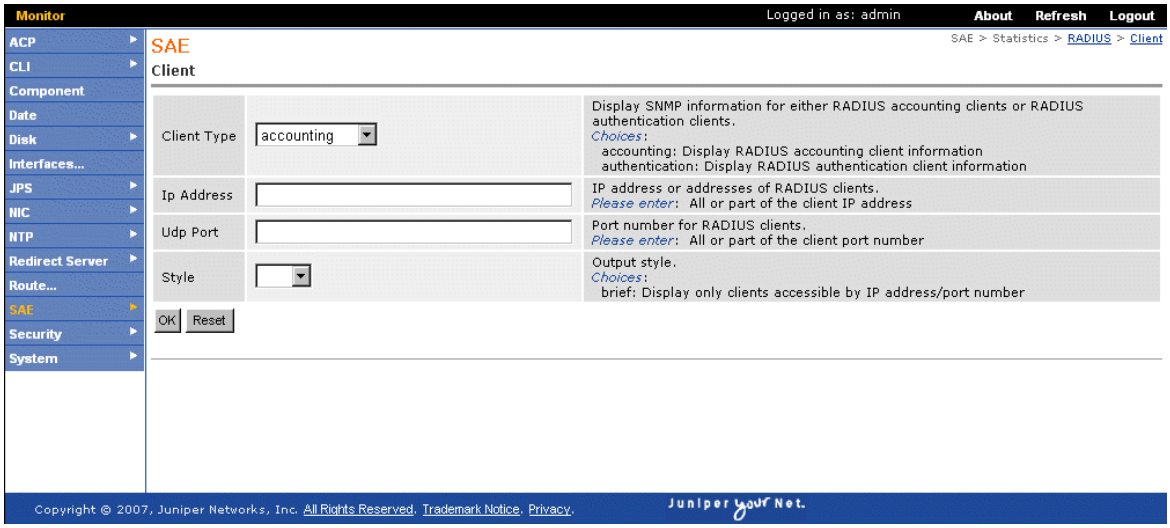


Viewing SNMP Statistics About RADIUS Clients

To view SNMP statistics about RADIUS clients:

1. Select **SAE** from the side pane, click **Statistics**, click **RADIUS**, and then click **Client**.

   The Client pane appears.



2. Select a client type from the Client Type list:

   - accounting—Displays RADIUS accounting information
   - authentication—Displays RADIUS client authentication information

3. In the IP Address box, enter the client IP address to display SNMP information for a specific RADIUS client, or leave the box blank to display SNMP information for all RADIUS clients.

4. In the UDP Port box, enter a port number to display SNMP information for a specific RADIUS client, or leave the box blank to display SNMP information for all RADIUS clients.

5. Select an output style from the Style list.

6. Click **OK**.

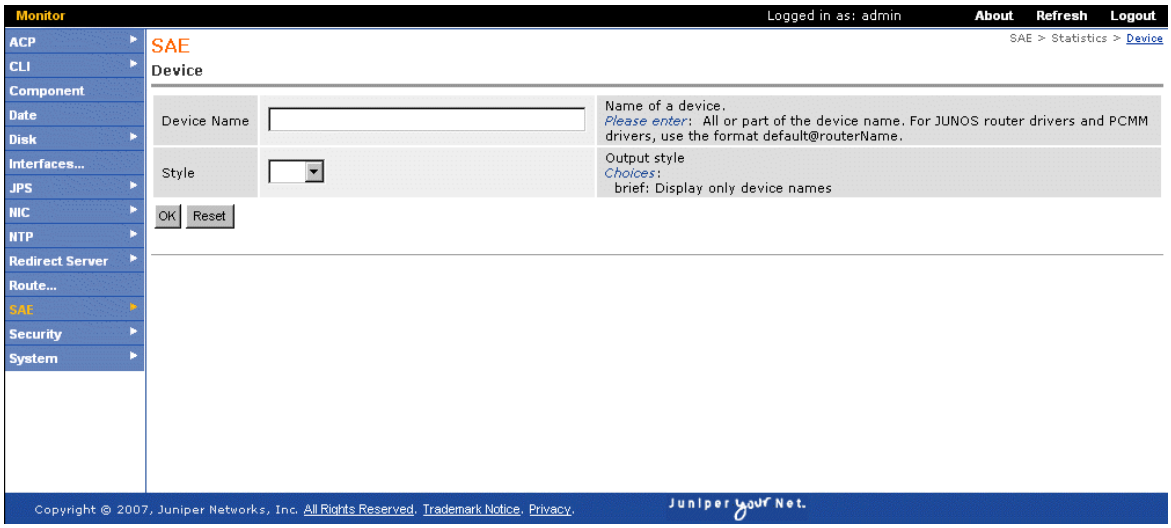
   The Client pane displays statistics for RADIUS clients.

Viewing SNMP Statistics for Devices

To view SNMP statistics about devices:

1. Select **SAE** from the side pane, click **Statistics**, and then click **Device**.

   The Device pane appears.



2. In the Device Name box, enter a full or partial device name for which you want to display information, or leave the box blank to display all devices.

3. Select an output style from the Style list.

4. Click **OK**.

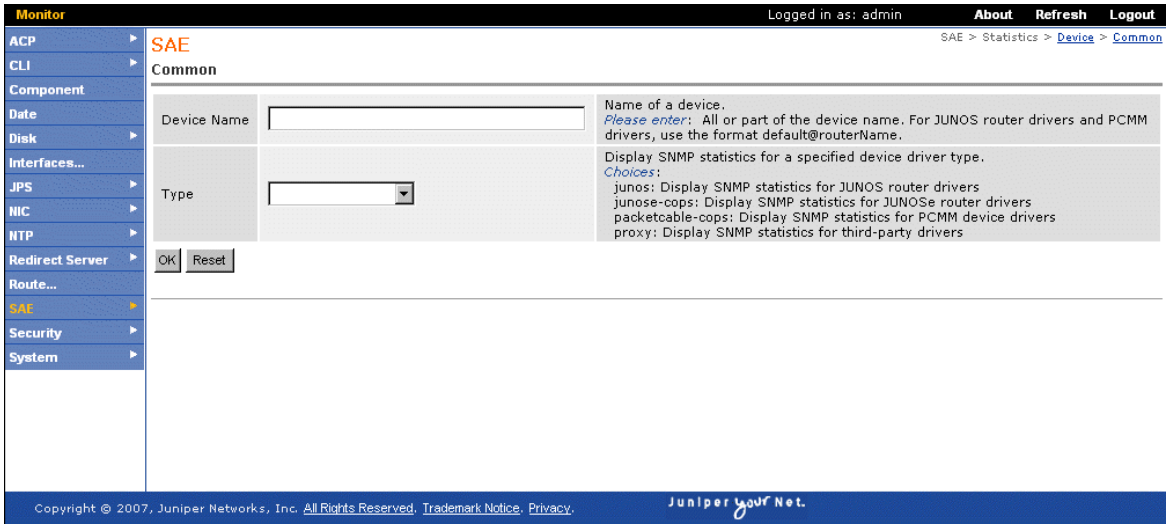
   The Device pane displays statistics for all devices.

Viewing SNMP Statistics for Specific Devices

To view SNMP statistics about specific devices:

1. Select **SAE** from the side pane, click **Statistics**, click **Device**, and then click **Common**.

   The Common pane appears.



2. In the Device Name box, enter a full or partial device name for which you want to display information, or leave the box blank to display all devices.

3. Select a device type from the Type list:

   - junos—Displays SNMP statistics for JUNOS router drivers
   - junose-cops—Displays SNMP statistics for JUNOSe router drivers
   - packetcable-COPS—Displays SNMP statistics for PCMM device drivers
   - proxy—Displays SNMP statistics for third-party drivers

4. Click **OK**.

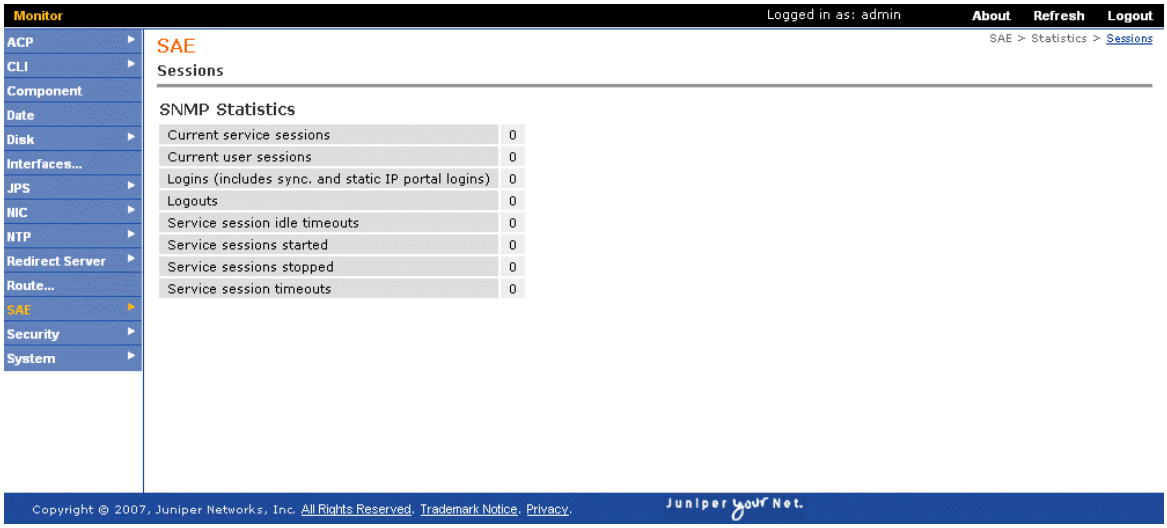
   The Common pane displays statistics for the specified device.

Viewing SNMP Statistics for Subscriber Sessions and Service Sessions

To view SNMP statistics about subscriber sessions and service sessions:

- Select **SAE** from the side pane, click **Statistics**, and then click **Sessions**.

  The Sessions pane displays statistics for subscriber sessions and service sessions.



Chapter 15

Monitoring and Troubleshooting NIC with the SRC CLI

This chapter describes how to monitor the network information collector (NIC) with the SRC CLI. Topics include:

Viewing Statistics About NIC Operations

You can view statistics for the NIC process and for various NIC components. Table 22 lists the commands you use to view NIC statistics.

Table 22: Commands to Display NIC Statistics

Command	Output Displayed
show nic statistics	All NIC statistics. The output for this command includes the output for the other show nic statistics commands.
show nic statistics agent	NIC statistics for agents.
show nic statistics host	NIC statistics for a NIC host.
show nic statistics process	NIC statistics for the NIC process.
show nic statistics resolver	NIC statistics for resolvers.
show nic statistics slot	All NIC statistics for a specified slot. The output for this command includes the output for the show nic statistics agent, show nic statistics host, show nic statistics process, and show nic statistics resolver commands.

Viewing Statistics for the NIC Process

To view statistics for the NIC process:

```
user@host> show nic statistics process
Component Statistics
Component Name process
Heap in use    456194 bytes (87%)
Heap limit     524288 bytes
Threads        42
Up time        747848 seconds since Wed Jan 31 19:35:57 EST 2007
```

Table 23 describes the output fields for the show nic statistics process command. Output fields are listed in the order in which they appear.

Table 23: show nic statistics process Output Fields

Field Name	Field Description
Component name	Name of component—process indicates the NIC process.
Heap in use	Heap size allocated by the Java Virtual Machine. The percentage indicates the percentage of the heap in use. We recommend that if the percent in use is more than 90% additional heap be allocated for the NIC.
Heap limit	Size of Java heap configured for the NIC.
Threads	Number of threads in use.
Up time	Length of time NIC has been running on the system. Includes the date and time at which NIC was last started.

Viewing Statistics for a NIC Host

To view statistics for a NIC host:

```
user@host> show nic statistics host
Component Statistics
Component Name                 /hosts
Number of Components Restart   0
Number of No Match Resolutions 0
Number of Resolution Errors    0
Number of Resolutions          0
```

Table 24 describes the output fields for the show nic statistics host command. Output fields are listed in the order in which they appear.

Table 24: show nic statistics host Output Fields

Field Name	Field Description
Component name	Name of component—/hosts indicates NIC host. A specific host has the format /hosts/*hostname*.
Number of Components Restart	Number of NIC resolvers and agents that have restarted in the host.
Number of No Match Resolutions	Number of resolution requests that did not return data.
Number of Resolution Errors	Number of errors encountered when processing resolutions requests.
Number of Resolutions	Number of successful data resolutions; for example, the SAE reference for a specified IP address, the login name for a specified IP address, or the SAE reference for a specified login name.

Viewing Statistics for NIC Resolvers

To interpret the statistics for NIC resolvers, make sure that you have a good understanding of the NIC resolutions process.

See *SRC-PE Network Guide, Chapter 18, NIC Resolution Process*.

To view statistics for NIC resolvers:

```
user@host> show nic statistics resolver
Component Statistics
Component Name           /realms/login/A1
Number of Data Sources   0
Resolver Size            0

Component Statistics
Component Name           /realms/login/B1
Number of Data Sources   1
Resolver Size            0

Component Statistics
Component Name           /realms/login/C1
Number of Data Sources   1
Resolver Size            2140

Component Statistics
Component Name           /realms/login/D1
Number of Data Sources   2
Resolver Size            0
```

Table 25 describes the output fields for the show nic statistics resolver command. Output fields are listed in the order in which they appear.

Table 25: show nic statistics resolver Output Fields

Field Name	Field Description
Component name	Name of a resolver. Resolver names have the format /realms/*realm-name*/*resolver name*.
Number of Data Sources	The number of sources from which the resolver obtains data. A data source can be an agent or another resolver.
Resolver Size	The number of keys (or number of mappings) required to perform this resolution.

Viewing Statistics for NIC Agents

To interpret the statistics for NIC agents, make sure that you have a good understanding of the NIC agents.

See *SRC-PE Network Guide, Chapter 9, Locating Subscriber Information with the NIC*.

To view statistics for NIC agents:

```
user@host> show nic statistics agent
Component Statistics
Component Name            /agents/LoginNameVr
Agent Type                Passive
Connection to Data Source Up
Data Size                 262141

Component Statistics
Component Name            /agents/VrSaeId
Agent Type                Active
Connection to Data Source Up
Data Size                 2212

Component Statistics
Component Name            /agents/IpLoginName
Agent Type                Passive
Connection to Data Source Up
Data Size                 262141

Component Statistics
Component Name            /agents/Pool
Agent Type                Active
Connection to Data Source Up
Data Size                 3
```

Table 26 describes the output fields for the show nic statistics agent command. Output fields are listed in the order in which they appear.

Table 26: show nic statistics agent Output Fields

Field Name	Field Description
Component name	Name of an agent. Agent names have the format /agents/*agent-name*.
Agent Type	Type of agent—active or passive. Active agents publish data whether or not a resolver requests the data. Passive agents provide information only when a resolver requests it.
Connection to Data Source	Whether or not the agent has a connection to its data source; for example, a directory agent to the directory, or an SAE plug-in agent to the CORBA naming server.
Data Size	Number of key to value mappings for the agent.

Viewing NIC Resolution Data

You can view the data that NIC uses during a resolution. You can view all resolution data, or data for a specified NIC component. Table 27 lists the commands you use to view NIC resolution information.

Table 27: Commands to Display NIC Data

Command	Output Displayed
show nic data	All NIC data. The output for this command includes the output for the other show nic data commands.
show nic data maximum-results	All or a specified quantity of NIC resolution data.
show nic data agent	NIC resolution data for a specified agent.
show nic data resolver	NIC resolution data for a specified resolver.
show nic data slot	All NIC data for a specified slot. The output for this command includes the output for the show nic data agent and show nic data resolver commands.

Viewing Data for NIC Resolvers

To interpret the data for resolvers, make sure that you have a good understanding of the NIC resolution process.

See *SRC-PE Network Guide, Chapter 18, NIC Resolution Process*.

To view all NIC resolver data:

```
user@host> show nic data resolver
Component name
/realms/login/C1
Key
  Type
Vr
  String
default@dw2
Value
  Type
```

```
SaeId
  String
IOR:
000000000000003549444C3A736D67742E6A756E697065722E6E65742F7361652F5365727...
41637469766174696F6E456E67696E653A312E3000000000000000002000000000000000780...
0000000C31302E3232372E362E343300226100000000022676172 6B6269742E6B616E6C6...
6E70722E6E65742F736165504F412F5341450000000000020000000000000008000000004...
000000010000001C000000000001000100000001050100010001010900000001050100010...
0000002C000000000000000100000001000000 1C000000000001000100000001050100010...
0000000105010001...
Key
  Type
Vr
  String
vr1495@marvin
Value
  Type
SaeId
  String
...
```

Table 28 describes the output fields for the show nic data resolver command. Output fields are listed in the order in which they appear.

Table 28: show nic data resolver Output Fields

Field Name	Field Description
Component name	Name of a resolver. Resolver names have the format /realms/*realm-name*/*resolver name*.
Key	Data type and value of a NIC key. The value is the actual value of the NIC key, not the NIC value to which the key maps.
Value	Data type and value of the NIC value that maps to the associated NIC key.

Viewing Data for NIC Agents

To interpret the data for agents, make sure that you have a good understanding of the NIC resolution process.

See *SRC-PE Network Guide, Chapter 18, NIC Resolution Process*.

To view all NIC resolver data:

```
user@host> show nic data agent
Component name
/agents/LoginNameVr
Key
  Type
Ip
  String
192.170.179.0
Value
  Type
Vr
  String
vorbis-13@prsim
Key
  Type
```

```
Ip
  String
192.170.179.3
Value
  Type
Vr
  String
vorbis-13@prsim


...

Key
  Type
Vr
  String
default@sys1
Value
  Type
SaeId
  String
IOR:
000000000000003549444C3A736D67742E6A756E697065722E6E65742F7361652F5365727669
6365
41637469766174696F6E456E67696E653A312E3000000000000000002000000000000000780001
0200
0000000C31302E3232372E362E343300226100000000002267617 26B6269742E6B616E6C6162
2E6A
6E70722E6E65742F736165504F412F534145000000000002000000000000000080000000004A41
4300
000000010000001C000000000001000100000001050100010001010900000001050100010000
0001
0000002C000000000000000010000000100000001C000000000001000100000001050100010001
0109
0000000105010001
```

Table 29 describes the output fields for the show nic data agent command. Output fields are listed in the order in which they appear.

Table 29: show nic data agent Output Fields

Field Name	Field Description
Component name	Name of an agent. Agent names have the format /agents/*agent-name*.
Key	Data type and value of a NIC key. The value is the actual value of the NIC key, not the NIC value to which the key maps.
Value	Data type and value of the NIC value that maps to the associated NIC key.

Troubleshooting NIC Data Resolution

Troubleshooting NIC data resolution is a complex task that requires a good understanding of how NIC operates, how it resolves resolution requests, and how the NIC configuration scenario that you are using performs resolutions. See:

- *SRC-PE Network Guide, Chapter 9, Locating Subscriber Information with the NIC*
- *SRC-PE Network Guide, Chapter 18, NIC Resolution Process*
- *SRC-PE Network Guide, Chapter 21, NIC Configuration Scenarios*

This section presents high-level troubleshooting information. For assistance troubleshooting NIC operation and NIC resolutions, contact the Juniper Technical Support Center.

Troubleshooting NIC Operation

To troubleshoot NIC operation:

1. Make sure that the heap size configured for NIC is adequate and that the process is up:

```
user@host> show nic statistics process
Component Statistics
Component Name process
Heap in use    456194 bytes (87%)
Heap limit     524288 bytes
Threads        42
Up time        747848 seconds since Wed Jan 31 19:35:57 EST 2007
```

2. Determine whether there are any NIC resolution errors and whether NIC successfully completed any resolution requests:

```
user@host> show nic statistics host
Component Statistics
Component Name                 /hosts
Number of Components Restart   0
Number of No Match Resolutions 0
Number of Resolution Errors    0
Number of Resolutions          0
```

3. Test the resolution process by using the test nic resolve command.

   See *SRC-PE Network Guide, Chapter 10, Configuring NIC with the SRC CLI*.

Troubleshooting NIC Resolution

If you are unsure whether NIC is resolving resolution requests, you can view data about those requests to see whether NIC is receiving data.

1. Verify that NIC is receiving data by running the show nic data resolver command.

   See *Viewing Data for NIC Resolvers* on page 161.

   For each resolver, which is identified by a component name such as /realms/login/C1, the output should show a value, such as default@sys1 for the key Vr, and the NIC value for that key such as the IOR that identifies an SAE.

2. If NIC is not receiving data, determine which agent or agents are not receiving data by running the show nic data agent command.

   See *Viewing Data for NIC Agents* on page 162.

3. Review your NIC configuration to make sure that NIC is configured correctly by running the show command for the NIC configuration scenario. For example:

   ```
   [edit shared nic scenario OnePop
   user@host# show
   ```

Chapter 16

Monitoring the NIC with the C-Web Interface

This chapter describes how to monitor NIC components with the C-Web interface. Topics include:

Viewing Hosts with the C-Web Interface

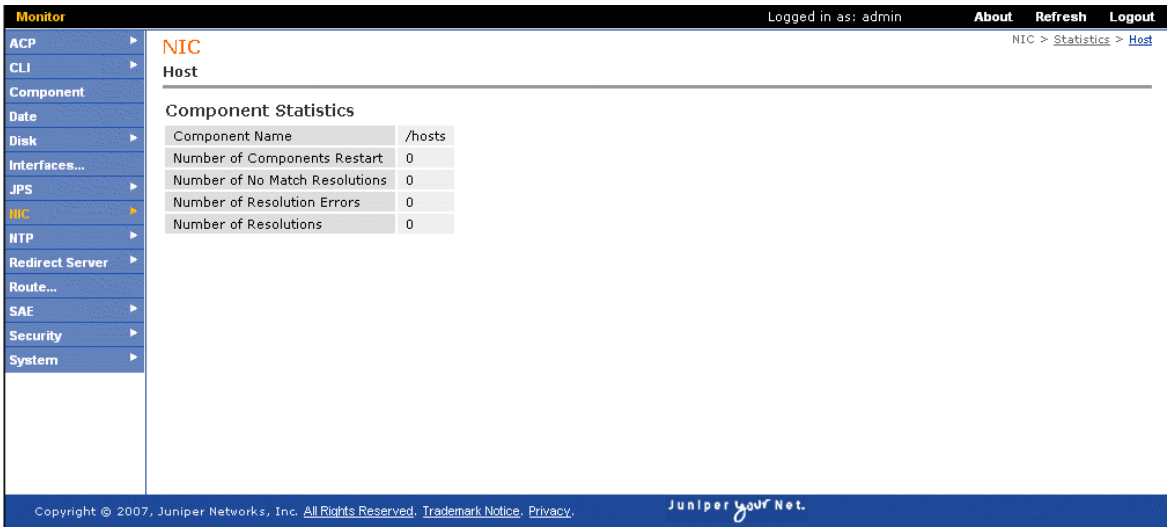
You can view statistics for hosts and the host process.

Viewing Host Statistics

To view NIC host statistics:

- Select **NIC** from the side pane, click **Statistics**, and then click **Host**.

  The Host pane displays the properties for the agent.

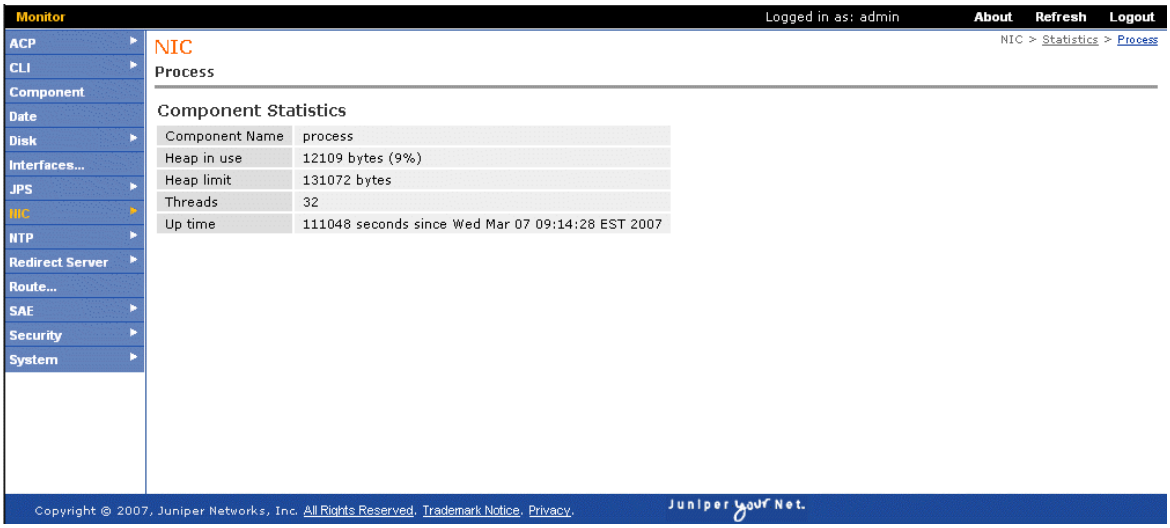


Viewing Host Process Statistics

To view NIC host process statistics:

- Select **NIC** from the side pane, click **Statistics**, and then click **Process**.

  The Process pane displays the statistics for the host process.



Viewing Resolvers with the C-Web Interface

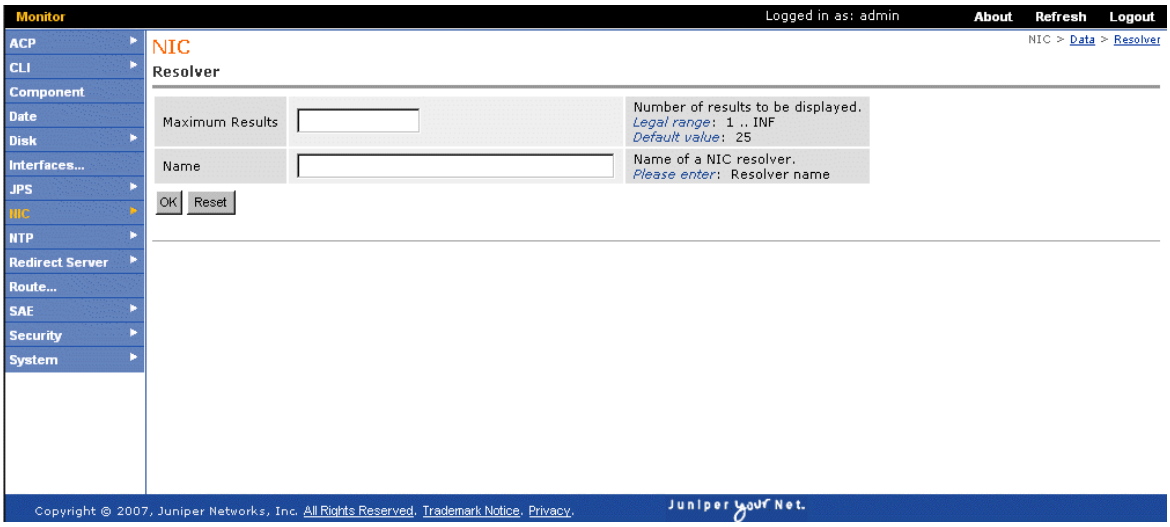
You can view resolvers and monitor resolver statistics with the C-Web interface.

Viewing Resolvers

To view information about a resolver:

1. Select **NIC** from the side pane, click **Data**, and then click **Resolver**.

   The Resolver pane appears.



2. In the Maximum Results box, enter the maximum number of results that you want to receive.

3. In the Name box, enter the name of the resolver for which you want to view data.

4. Click **OK**.

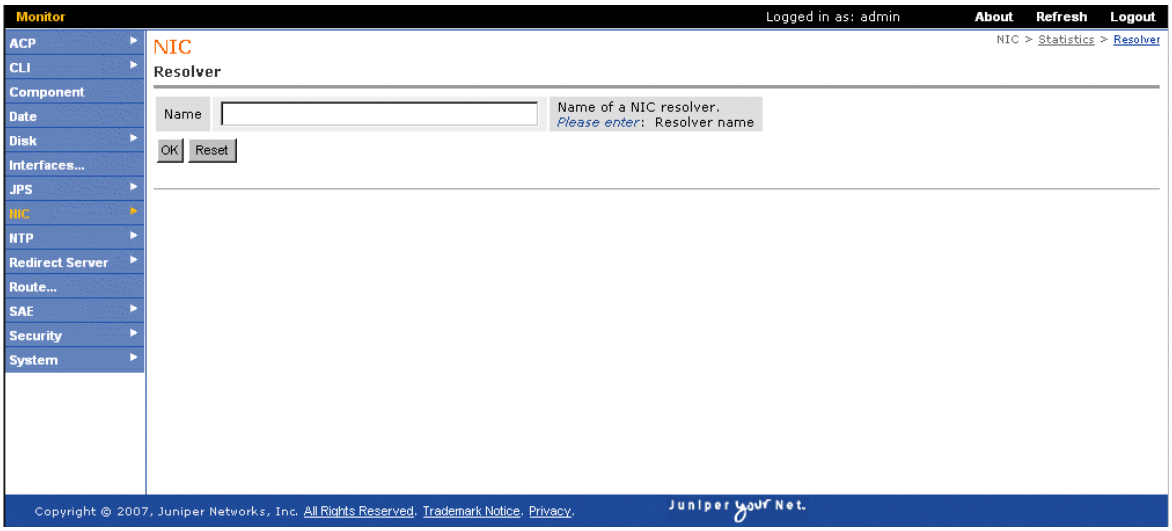
   The Resolver pane displays the properties for the resolver.

Viewing Resolver Statistics

To view statistics about resolvers:

1. Select **NIC** from the side pane, click **Statistics**, and then click **Resolver**.

   The Resolver pane appears.



2. In the Name box, enter the name of the resolver for which you want to view statistics.

3. Click **OK**.

   The Resolver pane displays the statistics for the resolver.

Viewing Agents with the C-Web Interface

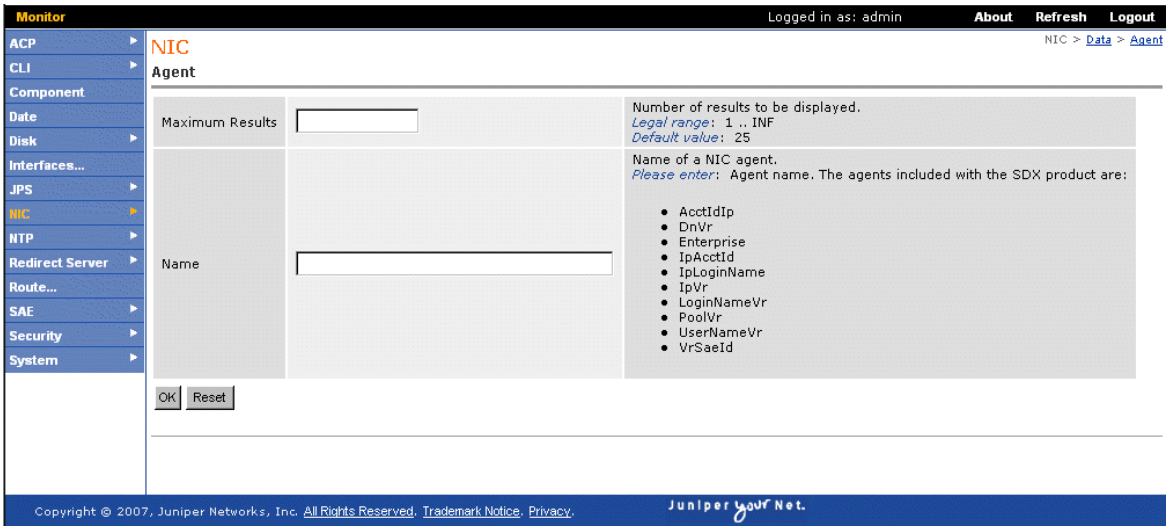
You can view agent properties or agent statistics using the C-Web interface.

Viewing Agents

To view information about an agent:

1. Select **NIC** from the side pane, click **Data**, and then click **Agent**.

   The Agent pane appears.



2. In the Maximum Results box, enter the maximum number of results that you want to receive.
3. In the Name box, enter the name of the agent for which you want to view data.
4. Click **OK**.

   The Agent pane displays the properties for the agent.

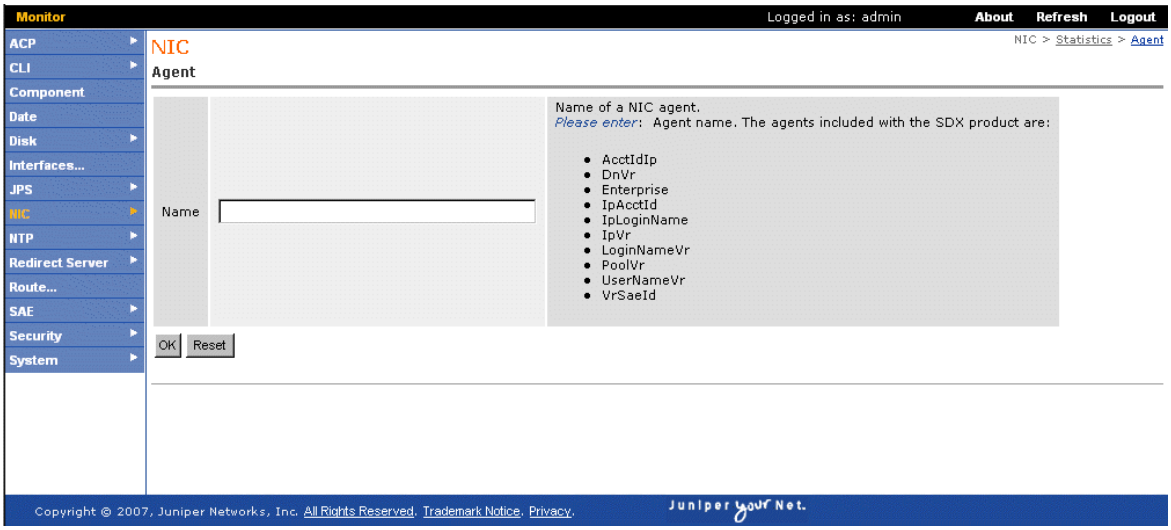
For information about the meaning of the properties, see *SRC-PE Network Guide, Chapter 20, Reviewing the NIC Configuration*.

Viewing Agent Statistics

To view statistics for an agent:

1. Select **NIC** from the side pane, click **Statistics**, and then click **Agent**.

   The Agent pane appears.



2. In the Name box, enter the name of the agent for which you want to view statistics.

3. Click **OK**.

   The Agent pane displays the properties for the agent.

For information about the meaning of the properties, see *SRC-PE Network Guide, Chapter 20, Reviewing the NIC Configuration*.

Chapter 17

Monitoring NTP with the SRC CLI

This chapter describes how to monitor the Network Time Protocol (NTP) with the SRC CLI. You can monitor NTP on Solaris platforms as well as C-series platforms. Topics include:

Viewing NTP Peers with the SRC CLI

To view a list of NTP peers with the SRC CLI:

```
user@host> show ntp associations
     remote           local      st poll reach  delay   offset    disp
==============================================================================
*myserver.jnpr.n 192.0.7.46      3 1024  377 0.00038 -0.000573 0.12178
```

Table 30 describes the output fields for the show ntp associations command. Output fields are listed in the approximate order in which they appear.

Table 30: show ntp associations Output Fields

Field Name	Field Description
remote	Address or name of the remote NTP peer
local	Address or name used by NTP on the local system
st	Stratum of the remote peer
poll	Polling interval, in seconds
reach	Reachability register, in octal
delay	Current estimated delay of the peer, in milliseconds
offset	Current estimated offset of the peer, in milliseconds
disp	Current estimated dispersion of the peer, in milliseconds

Viewing Statistics for NTP with the SRC CLI

To view statistics for NTP with the SRC CLI:

```
user@host> show ntp statistics
time since restart:     2371617
time since reset:       2371617
packets received:       38765
packets processed:      2573
current version:        38761
previous version:       0
bad version:            0
access denied:          36188
bad length or format:   0
bad authentication:     0
rate exceeded:          0
```

Viewing Internal Variables for NTP with the SRC CLI

To view information about internal variables for NTP with the SRC CLI:

```
user@host> show ntp status
system peer:          menemsha.jnpr.net
system peer mode:     client
leap indicator:       00
stratum:              4
precision:            -20
root distance:        0.02245 s
root dispersion:      0.07689 s
reference ID:         [10.227.2.100]
reference time:       c922b152.86dd0529  Thu, Dec  7 2006 10:27:14.526
system flags:         auth monitor ntp kernel stats
jitter:               0.000183 s
stability:            1.728 ppm
broadcastdelay:       0.003998 s
authdelay:            0.000000 s
```

Chapter 18

Monitoring NTP with the C-Web Interface

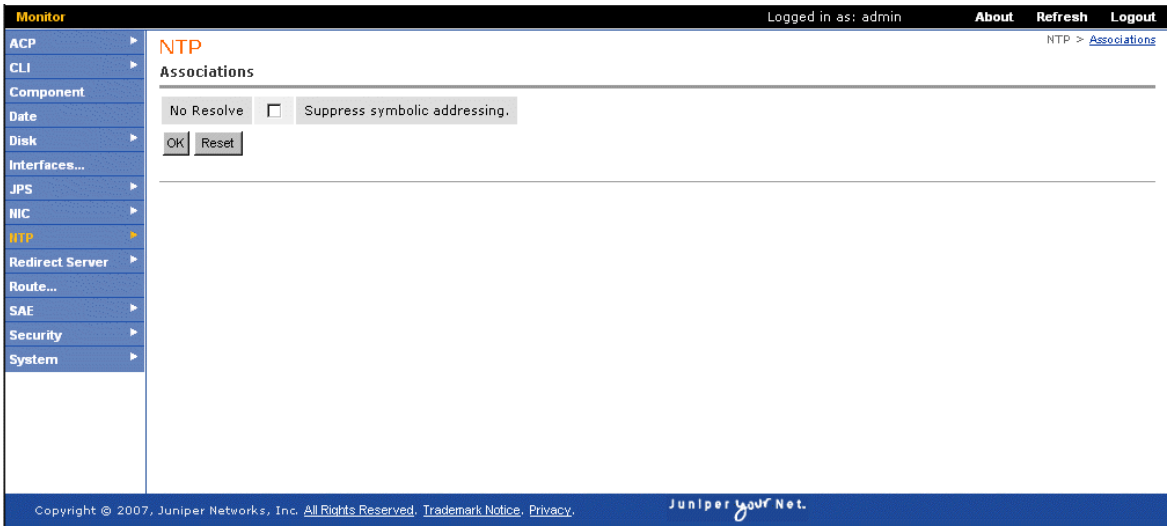
This chapter describes how to monitor the Network Time Protocol (NTP) server with the C-Web interface. Topics include:

Viewing NTP Peers with the C-Web Interface

To view a list of NTP peers:

1. Select **NTP** from the side pane, and click **Associations**.

   The Associations pane appears.



2. To suppress symbolic addressing, select the **No Resolve** box.
3. Click **OK**.

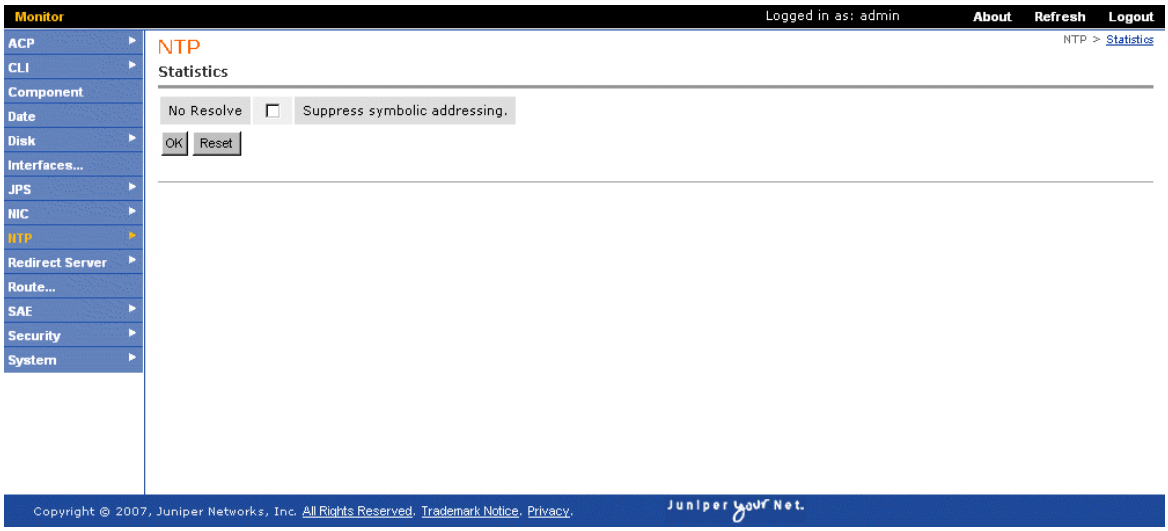
   The Associations pane displays the list of NTP peers.

Viewing Statistics for NTP with the C-Web Interface

To display statistics for NTP:

1. Select **NTP** from the side pane, and click **Statistics**.

   The Statistics pane appears.



2. To suppress symbolic addressing, select the **No Resolve** box.
3. Click **OK**.

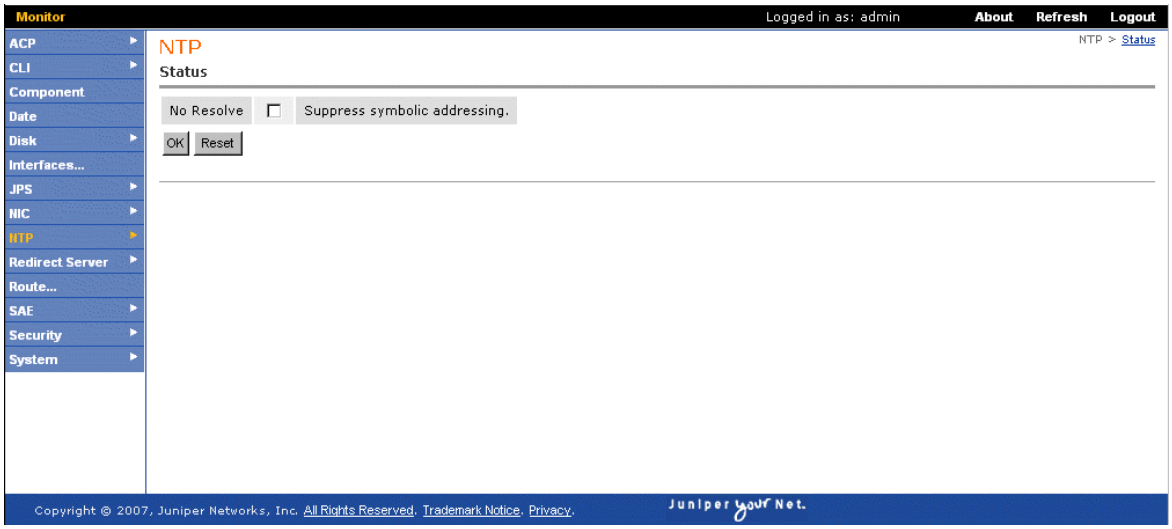
   The Statistics pane displays statistics for NTP.

Viewing NTP Status with the C-Web Interface

To display status for NTP:

1. Select **NTP** from the side pane, and click **Status**.

   The Status pane appears.



2. To suppress symbolic addressing, select the **No Resolve** box.
3. Click **OK**.

   The Status pane displays NTP status.

Chapter 19

Monitoring Redirect Server with the SRC CLI

This chapter describes how to monitor the redirect server with the SRC CLI. Topics include:

Viewing Statistics for the Redirect Server with the SRC CLI

To view statistics for redirect server:

```
user@host> show redirect-server statistics
Redirect Server
Uptime: 1270724.713 s
Accepted Requests: 25
Rejected Requests: 0
User limit leaky buckets: 0
User limits reached: 0
Global limits reached: 0
```

Viewing Statistics for Filtered Traffic

You can obtain information about the packets filtered on a C-series platform by accessing statistics for the iptables Linux tool. You can also reset the counters for this tool.

To view information about packet filtering on a C-series platform:

```
user@host> show iptables <nat | filter | mangle> <reset-counters>
```

where

- nat—Displays information for the nat table for the iptables tool. The nat table provides rules for rewriting packet addresses.
- filter—Displays information for the filter table for the iptables tool. The filter table provides rules for defining packet filters.

- mangle—Displays information for the mangle table for the iptables tool. The mangle table provides rules for adjusting packet options, such as quality of service.

For example:

```
user@host> show iptables
Chain INPUT (policy ACCEPT 25M packets, 9401M bytes)
 pkts bytes target     prot opt in     out     source
destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
destination

Chain OUTPUT (policy ACCEPT 24M packets, 4506M bytes)
 pkts bytes target     prot opt in     out     source
destinationreset-counters
```

To reset the values in the output for the show iptables command:

user@host> **show iptables reset counters**

Chapter 20

Monitoring the Redirect Server and Filtered Traffic with the C-Web Interface

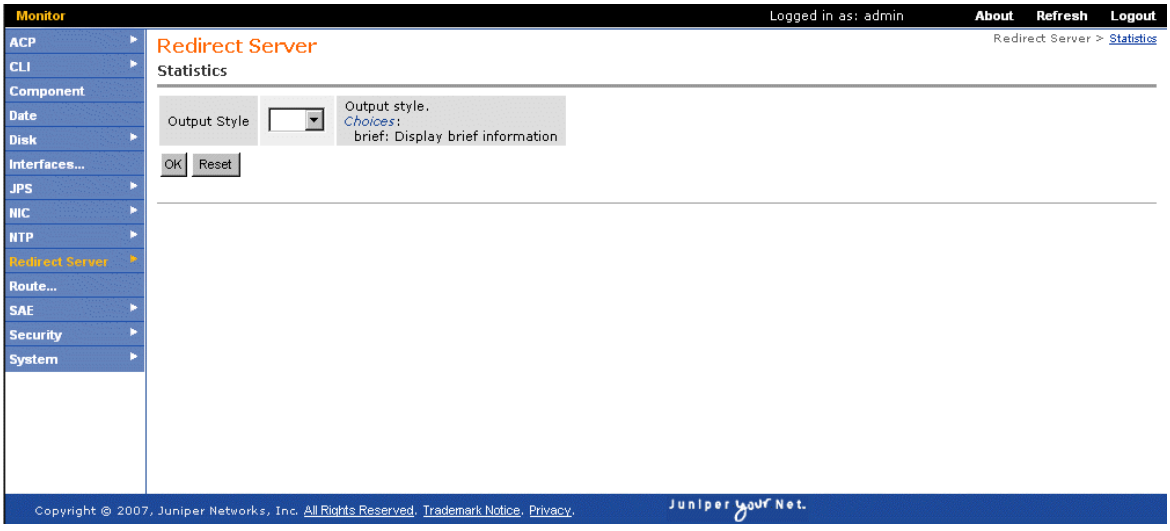
This chapter describes how to use the C-Web interface to monitor the redirect server and filtered traffic with the iptables LINUX tool. Topics include:

Viewing Statistics for the Redirect Server with the C-Web Interface

To view statistics for the redirect server:

1. Select **Redirect Server** from the side pane, and click **Statistics**.

   The Statistics pane appears.



2. Select a style from the Output Style list.
3. Click **OK**.

   The Statistics pane displays the redirect server statistics.

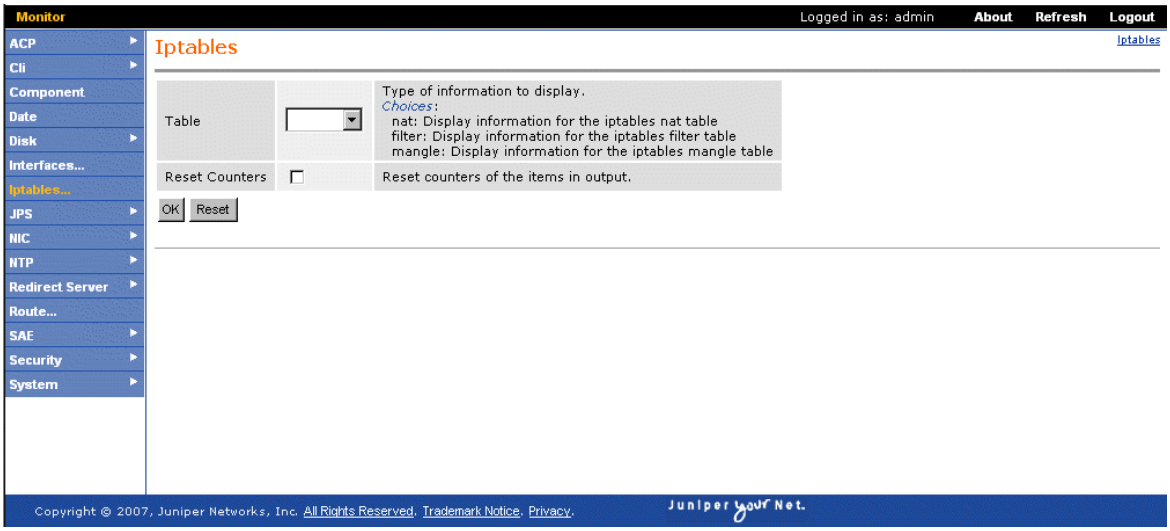
Viewing Information About Filtered Traffic with the C-Web Interface

You can view information about filtered traffic with the iptables Linux tool when you are using C-Web to monitor the C-series platform.

To view information about the filtered traffic:

1. Select **Iptables** from the side pane.

   The Iptables pane appears.



2. Select the type of table that you want to display from the Table list:
   - nat—Display information for the iptables NAT table
   - filter—Display information for the iptables filter table
   - mangle—Display information for the iptables mangle table
3. Select the **Reset Counters** check box to rest the counters of items in the output.
4. Click **OK**.

   The Iptables pane displays information about filtered traffic.

Chapter 21

Troubleshooting Network Connectivity with the SRC CLI

This chapter describes how to troubleshoot connections to remote hosts. Topics include:

Overview of Commands to Troubleshoot Connections to Remote Hosts

If you are troubleshooting problems with the SRC software that might be caused by connectivity problems to remote hosts, you can use the following commands:

- ping—Test connectivity to a remote host.
- traceroute—Display the route from the local host to a remote host and back.
- show interfaces—Display information about system interfaces.
- show route—Display information form the system routing table.

Testing Connectivity to Remote Hosts

To test connectivity to a remote host:

```
user@host> ping
PING 10.227.7.45 (10.227.7.45) 56(84) bytes of data.
64 bytes from 10.227.7.45: icmp_seq=0 ttl=63 time=0.560 ms
64 bytes from 10.227.7.45: icmp_seq=1 ttl=63 time=0.613 ms
64 bytes from 10.227.7.45: icmp_seq=2 ttl=63 time=0.641 ms
64 bytes from 10.227.7.45: icmp_seq=3 ttl=63 time=0.653 ms
64 bytes from 10.227.7.45: icmp_seq=4 ttl=63 time=0.651 ms
64 bytes from 10.227.7.45: icmp_seq=5 ttl=63 time=0.418 ms
```

```
64 bytes from 10.227.7.45: icmp_seq=6 ttl=63 time=0.440 ms
64 bytes from 10.227.7.45: icmp_seq=7 ttl=63 time=0.454 ms
64 bytes from 10.227.7.45: icmp_seq=8 ttl=63 time=0.466 ms
64 bytes from 10.227.7.45: icmp_seq=9 ttl=63 time=0.478 ms
64 bytes from 10.227.7.45: icmp_seq=10 ttl=63 time=0.488 ms

Ctrl-C

--- 10.227.7.45 ping statistics ---
94 packets transmitted, 94 received, 0% packet loss, time 93038ms
rtt min/avg/max/mdev = 0.418/0.560/0.791/0.089 ms, pipe 2
```

For information about all the options for the ping command, see the *SRC-PE CLI Command Reference.*

Viewing the Route Information

You can use the traceroute command to get information about the hops between the local system and a remote host.

To view route information:

```
user@host> traceroute 192.2.7.48
traceroute to 192.2.7.48 (192.2.7.48), 30 hops max, 46 byte packets
 1  host (192.2.7.45)  3000.716 ms !H  3000.733 ms !H  3001.272 ms !H
```

For information about all the options for the traceroute command, see the *SRC-PE CLI Command Reference.*

Viewing Routing Table Information

You can display brief or detailed information about the route from the local system to a remote host.

To view brief route information:

```
user@host> show route
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.2.2.0       *               255.255.255.0   U         0 0          0 eth0
default         srclab1.mylab.  0.0.0.0         UG        0 0          0 eth0
```

To view detailed route information:

```
user@host> show route detail
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface MSS   Window irtt
192.2.2.0       *               255.255.255.0   U     0      0        0 eth0   0     0      0
default         srclab1.mylab.  0.0.0.0         UG    0      0        0 eth0   0     0      0
```

The detailed output includes the additional Metric, Ref, and Use fields.

Viewing Interface Information

You can view information about all system interfaces, or about a specified interface.

To view information about all system interfaces:

```
user@host> show interfaces
eth0      Link encap:Ethernet  HWaddr 00:30:48:55:B6:FC
          inet addr:10.227.6.42  Bcast:10.227.6.255  Mask:255.255.255.0
          inet6 addr: fe80::230:48ff:fe55:b6fc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:482467 errors:0 dropped:0 overruns:0 frame:0
          TX packets:57573 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:38147790 (36.3 MiB)  TX bytes:4396018 (4.1 MiB)
          Base address:0xcc00 Memory:fc9c0000-fc9e0000

eth1      Link encap:Ethernet  HWaddr 00:30:48:55:B6:FD
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Base address:0xc800 Memory:fc9a0000-fc9c0000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1946394 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1946394 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:260604464 (248.5 MiB)  TX bytes:260604464 (248.5 MiB)

lo:1      Link encap:Local Loopback
          inet addr:192.168.254.1  Mask:255.255.255.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1

sit0      Link encap:IPv6-in-IPv4
          NOARP  MTU:1480  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

Chapter 22

Monitoring Network Connectivity with the C-Web Interface

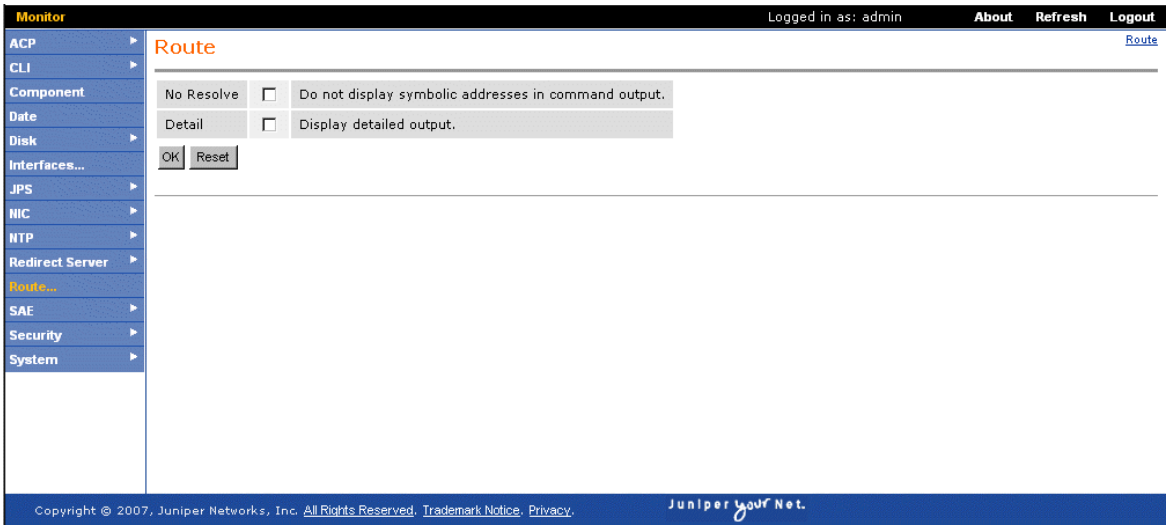
This chapter describes how to use the C-Web interface to monitor network connectivity. Topics include:

Viewing Information About the Routing Table with the C-Web Interface

To view information about the route from the local system to a remote host:

1. Select **Route** from the side pane.

   The Route pane appears.



2. To suppress symbolic addressing, select the **No Resolve** box.

3. To display detailed output, select the **Detail** box.

4. Click **OK**.

Viewing Information About System Interfaces with the C-Web Interface

To view information about all system interfaces:

1. Select **Interfaces** from the side pane.

   The Interfaces pane appears.

2. In the Interface name box, enter the name of the interface for which you want to view data.

3. Click **OK**.

Index

T