

SRC PE Software

CLI Command Reference, Volume 1

Release

4.0.x



Published: 2010-06-03

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

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

SRC PE Software CLI Command Reference, Volume 1
Release 4.0.x
Copyright © 2010, Juniper Networks, Inc.
All rights reserved. Printed in USA.

Writing: Linda Creed, Colleen Feerick, Justine Kangas, Betty Lew
Editing: Fran Mues
Illustration: Nathaniel Woodward
Cover Design: Edmonds Design

Revision History
May 2010—Revision 1

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

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. The Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

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 (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) 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, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the 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 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 or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations 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 Embedded Software on non-Juniper equipment; (j) use Embedded 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 payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

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 présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

About the Documentation

- SRC Documentation and Release Notes on page vii
- Audience on page vii
- Documentation Conventions on page vii
- Documentation Feedback on page ix
- Requesting Technical Support on page ix

SRC Documentation and Release Notes

For a list of related SRC documentation, see <http://www.juniper.net/techpubs/>.

If the information in the latest *SRC Release Notes* differs from the information in the SRC guides, follow the *SRC Release Notes*.

Audience

This documentation is intended for experienced system and network specialists working with routers running JUNOS® and JUNOSe Software in an Internet access environment. We assume that readers know how to use the routers, directories, and RADIUS servers that they will deploy in their SRC networks. 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

Table 1 on page viii defines the notice icons used in this guide. Table 2 on page viii defines text conventions used throughout this 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 or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2: Text Conventions

Convention	Description	Examples
Bold text like this	<ul style="list-style-type: none"> Represents keywords, scripts, and tools in text. Represents a GUI element that the user selects, clicks, checks, or clears. 	<ul style="list-style-type: none"> Specify the keyword exp-msg. Run the install.sh script. Use the pkgadd tool. To cancel the configuration, click Cancel.
Bold text like this	Represents text that the user must type.	user@host# set cache-entry-age cache-entry-age
Fixed-width text like this	Represents information as displayed on your terminal's screen, such as CLI commands in output displays.	<pre>nic-locators { login { resolution { resolver-name /realms/ login/A1; key-type LoginName; value-type SaeId; } } }</pre>
Regular sans serif typeface	<ul style="list-style-type: none"> Represents configuration statements. Indicates SRC CLI commands and options in text. Represents examples in procedures. Represents URLs. 	<ul style="list-style-type: none"> 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/src/api-index.html
<i>Italic sans serif typeface</i>	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.

Table 2: Text Conventions (*continued*)

Key names linked with a plus sign (+)	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
<i>Italic typeface</i>	<ul style="list-style-type: none"> Emphasizes words. Identifies book names. Identifies distinguished names. Identifies files, directories, and paths in text but not in command examples. 	<ul style="list-style-type: none"> There are two levels of access: <i>user</i> and <i>privileged</i>. <i>SRC PE Getting Started Guide</i> <i>o=Users, o=UMC</i> The <i>/etc/default.properties</i> file.
Backslash	At the end of a line, indicates that the text wraps to the next line.	Plugin.radiusAcct-1.class=\net.juniper.smgmt.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

Documentation Feedback

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

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/> .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html> .

SRC CLI

This document summarizes the SRC command-line interface (SRC CLI).

Configuration statements and operational commands are listed in alphabetical order for the following components in the *SRC PE CLI Command Reference, Volume 1*:

- CLI and System
- Juniper Networks Database
- SAE
- Network Information Collector (NIC)
- Session State Registrar (SSR)
- Subscriber Information Collector (SIC)
- SNMP Agent
- SRC Admission Control Plug-In (SRC ACP)
- SRC License Management
- COS Naming Service

Configuration statements and operational commands are listed in alphabetical order for the following components in the *SRC PE CLI Command Reference, Volume 2*:

- Service CLI
- Policy CLI
- Subscriber CLI
- Redirect Server
- External Subscriber Monitor
- Dynamic Service Activator
- IP Multimedia Subsystem (IMS)
- Diameter Application
- Juniper Policy Server (JPS)

CLI and System

The following table summarizes the SRC command-line interface (SRC CLI) for controlling and using the SRC CLI environment and for managing the C Series Controller. Configuration statements and operational commands are listed in alphabetical order.

- [Configuration commands and statements](#)
- [Filter commands](#)
- [Operational commands](#)

CLI and System
Configuration Commands and Statements
commit
copy
delete
display set
edit
exit
help
help configuration
history
insert
interfaces
interfaces name group
interfaces name tunnel
interfaces name unit
interfaces name unit unit-number family inet
interfaces name unit unit-number family inet6 address
load factory-default
load merge

load override
load replace
load set
rename
rollback
routing-options static route
run
save
set
show
slot
system
system ipmi
system ipmi user
system ldap client
system login
system login class
system login user
system login user user-name authentication
system ntp
system ntp authentication-key
system ntp broadcast
system ntp multicast-client
system ntp peer
system ntp server
system radius-server
system services

system services editor
system services editor policy-editor
system services netconf
system services ssh
system services web-management http
system services web-management https
system services web-management logger
system services web-management logger name file
system services web-management logger name syslog
system static-host-mapping
system syslog file
system syslog file file-name
system syslog host
system syslog host log-host-name
system syslog user
system syslog user user-name
system tacplus-server
top
up
Filter Commands
compare
count
display (changed running)
display level level
display xml
except
find

last
match
no-more
save
Operational Commands
clear security certificate
clear security certificate-request
clear security ssh
configure
disable
enable
exit
file archive
file checksum md5
file compare
file copy
file create
file delete
file list
file monitor
file rename
file show
ipmisol close local-session
ipmisol close remote-session
ipmisol open
ping
request disk disable

request disk enable
request disk identify
request disk initialize
request ipmi power
request network discovery
request security enroll
request security generate-certificate-request
request security get-ca-certificate
request security import-certificate
request support information
request system halt
request system install
request system prepare-partitions
request system reboot
request system restore
request system snapshot
request system uninstall
request system upgrade
restart
set cli complete-on-space
set cli directory
set cli language
set cli level
set cli password
set cli prompt
set cli screen-length
set cli screen-width

set cli terminal
set date
set date ntp
show cli
show cli authorization
show cli directory
show cli level
show component
show configuration
show date
show disk status
show interfaces
show ipmi chassis
show ipmi power
show iptables
show ntp associations
show ntp statistics
show ntp status
show route
show security certificate
show system boot-messages
show system information
show system snapshot
show system users
ssh
start shell
telnet

[traceroute](#)

commit

Syntax

```
commit <check> <and-quit>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Commit the set of changes and cause the changes to take operational effect.

Options

`check`—(Optional) Verify whether the syntax is correct, but do not apply changes.

`and-quit`—(Optional) Exit from configuration mode if the commit operation is successful.

Required Privilege Level

config-control

copy

Syntax

```
copy parent1 identifier1 (to) parent2 identifier2
```

Release Information

Command introduced in SRC Release 3.0.0

Description

Copy an existing configuration statement or identifier.

Options

parent1— Path to an existing configuration statement or identifier.

Value—Path of a collection object

identifier1— Existing identifier or statement.

Value— Identifier or statement

Configuration path.

Value

- *to*— Transition.

parent2— Path to a new configuration statement or identifier.

Value—Path of a collection object

identifier2— New identifier or statement.

Value— Identifier or statement

Required Privilege Level

config-control

delete

Syntax

```
delete < force object value >
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Delete a configuration statement or identifier. All subordinate statements and identifiers contained within the specified statement path are deleted with it.

Options

force— Flag indicating that no confirmation is requested before the software clears the configuration.

Default—false

object— Name of the statement or identifier to delete.

Value—Path of a configuration object

value— Value of the statement to delete.

Value—Valid value for selected object

Required Privilege Level

config-control

display set

Syntax

```
display set <relative>
```

Release Information

Command introduced in SRC Release 3.1.0

Description

Display the configuration in the format of **set** commands.

Options

`relative`—(Optional) Display the configuration for a hierarchy level in the format of **set** commands.

Required Privilege Level

No specific privilege required.

edit

Syntax

`edit object`

Release Information

Command introduced in SRC Release 1.0.0

Description

Specify edit level in the configuration hierarchy. This command lets you go directly to the specified edit level; for example, to [edit system login]. If you specify a path to a level that does not exist, the software creates the path for you. If you navigate to a different level without creating other statements (for example, by using a **top**, **up**, or **exit** command), the configuration statement may be deleted.

To edit the configuration statement to which you navigated by using the **edit** command, use the **set**, **delete**, **rename**, or **insert** commands.

Options

object— Edit level; for example, **edit system login**.

Required Privilege Level

No specific privilege required.

exit

Syntax

```
exit <configuration-mode>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Exit from this level in the CLI to the level above. At the top level in configuration mode, exit from configuration mode.

Alias

quit

Options

`configuration-mode`—(Optional) Exit from configuration mode.

Required Privilege Level

No specific privilege required.

help

Syntax

`help <command>`

Release Information

Command introduced in SRC Release 1.0.0

Description

Display help about commands. Enter help followed a command name to view information.

Options

command—(Optional) Name of command for which to display help help text.

Value—Operational command

Required Privilege Level

No specific privilege required.

help configuration

Syntax

```
help configuration <object>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display help for a configuration statement. Enter help followed by the statement to view information.

Options

object—(Optional) Configuration statement or object for which to provide help.

Value—Path of a configuration object

Required Privilege Level

No specific privilege required.

history

Syntax

```
history <clear>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display the list of the commands executed—from least recent to most recent.

Options

`clear`—(Optional) Clear command history.

Required Privilege Level

No specific privilege required.

insert

Syntax

```
insert parent identifier1 (after | before) identifier2
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Insert an identifier into an existing configuration hierarchy. You must configure the identifiers before you reorder them. The **insert** command does not create new identifiers.

Options

parent— Path in the configuration hierarchy to an existing configuration statement.

Value— Hierarchy path

identifier1— Existing identifier.

Value— Name of existing identifier

Ordering of identifiers.

Value

- *after*— Place *identifier1* after *identifier2*.
- *before*— Place *identifier1* before *identifier2*.

identifier2— New identifier to insert.

Value—Valid value for selected object

Required Privilege Level

config-control

interfaces

Syntax

```
interfaces name {
    disable;
    trusted;
}
```

Hierarchy Level

```
[edit interfaces]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure interfaces on the C Series Controller.

Options

name *name*— Name of interface

Value— Interface name

disable—(Optional) Disable this interface

Editing Level—Basic

trusted—(Optional) Untrusted interfaces can be connected to untrusted networks. If not set, eth1 will be untrusted, any other interface will be trusted.

Editing Level—Basic

Required Privilege Level

interface

Required Editing Level

Basic

interfaces *name* group

Syntax

```
interfaces name group {
    mode (balance-rr | active-backup | balance-xor | broadcast | 802.3ad |
balance-tlb | balance-alb);
    downdelay downdelay;
    updelay updelay;
    lacp-rate (slow | fast);
    mii-monitoring-interval mii-monitoring-interval;
    interfaces [interfaces...];
    primary primary;
    transmit-hash-policy (layer2 | layer34);
}
```

Hierarchy Level

```
[edit interfaces name group]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure Ethernet group interfaces. Group interfaces let you aggregate network interfaces into a single logical interface to support Ethernet redundancy.

When you configure group interfaces:

- The group interface name must not be one of the Ethernet interface names (that is, eth0, eth1, eth2, eth3).
- If an Ethernet interface is listed inside a group interface, it must not be configured as an interface by itself.
- Group interface and tunnel interface configurations are mutually exclusive. You cannot configure both types at the same time.

Options

```
mode (balance-rr | active-backup | balance-xor | broadcast | 802.3ad
| balance-tlb | balance-alb)— Grouping mode.
```

Value

- `balance-rr`— Round-robin policy: Transmit packets in

sequential order from the first available device through the last. This mode provides load balancing and fault tolerance.

- `active-backup`— Active-backup policy: Create only one device that is active. A different device becomes active if, and only if, the active device fails.

When a failover occurs in active-backup mode, bonding will issue one or more gratuitous ARPs on the newly active device. One gratuitous ARP is issued for the bonding master interface and each VLAN interface configured above it, provided that the interface has at least one IP address configured. Gratuitous ARPs issued for VLAN interfaces are tagged with the appropriate VLAN ID.

This mode provides fault tolerance. The primary option affects the behavior of this mode.

- `balance-xor`— XOR policy: Transmit based on the selected transmit hash policy. Alternate transmit policies can be selected with the transmit hash policy option. This mode provides load balancing and fault tolerance.
- `broadcast`— Broadcast policy: Transmit everything on all device interfaces. This mode provides fault tolerance.
- `802.3ad`— IEEE 802.3ad Dynamic link aggregation: Create aggregation groups that share the same speed and duplex settings. Utilizes all devices in the active aggregator according to the 802.3ad specification.

Device selection for outgoing traffic is done according to the transmit hash policy, which can be changed from the default simple XOR policy via the transmit hash policy option. Note that not all transmit policies may be 802.3ad compliant, particularly in regards to the packet mis-ordering requirements of section 43.2.4 of the 802.3ad standard. Differing peer implementations will have varying tolerances for noncompliance.

- `balance-tlb`— Adaptive transmit load balancing: Create channel bonding that does not require any special switch support. The outgoing traffic is distributed according to the current load (computed relative to the speed) on each device. Incoming traffic is received by the current device. If the receiving device fails, another device takes over the MAC address of the failed receiving device.
- `balance-alb`— Adaptive load balancing: Include adaptive transmit load balancing plus receive load balancing (rlb) for IPV4 traffic, and does not require any special switch support. The receive load balancing is achieved by ARP negotiation. The bonding driver intercepts the ARP replies sent by the local system on their way out and overwrites the source hardware address with the unique hardware address of one of the devices in the bond such that different peers use different hardware addresses for the server.

Receive traffic from connections created by the server is also balanced. When the local system sends an ARP request the bonding driver copies and saves the peer's IP information from the ARP packet. When the ARP reply arrives from the peer, its hardware address is retrieved and the bonding driver initiates an ARP reply to this peer assigning it to one of the devices in the bond. A problematic outcome of using ARP negotiation for balancing is that each time that an ARP request is broadcast it uses the hardware address of the bond. Hence, peers learn the hardware address of the bond and the balancing of receive traffic

collapses to the current device. This is handled by sending updates (ARP replies) to all the peers with their individually assigned hardware address such that the traffic is redistributed. Receive traffic is also redistributed when a new device is added to the bond and when an inactive device is re-activated. The receive load is distributed sequentially (round robin) among the group of highest speed devices in the bond.

When a link is reconnected or a new device joins the bond the receive traffic is redistributed among all active devices in the bond by initiating ARP Replies with the selected MAC address to each of the clients. The updelay option must be set to a value equal or greater than the switch's forwarding delay so that the ARP replies sent to the peers will not be blocked by the switch.

Editing Level—Basic

`downdelay downdelay`—(Optional) Time to wait before disabling a device after a link failure has been detected. This option is valid only for the MII monitor. The downdelay value should be a multiple of the MII monitoring interval; if not, it will be rounded down to the nearest multiple.

Value—Integer in the range 0–2147483647 ms

Editing Level—Basic

`updelay updelay`—(Optional) Time to wait before enabling a device after a link recovery has been detected. This option is valid only for the MII monitor. The updelay value should be a multiple of the MII monitoring interval; if not, it will be rounded down to the nearest multiple.

Value—Integer in the range 0–2147483647 ms

Editing Level—Basic

`lacp-rate (slow | fast)`—(Optional) Rate at which the link partner is requested to transmit LACPDU packets in 802.3ad mode. This option is valid only for the 802.3ad mode.

Value

- `slow`— Request partner to transmit LACPDUs every 30 seconds.
- `fast`— Request partner to transmit LACPDUs every 1 second.

Editing Level—Basic

`mii-monitoring-interval mii-monitoring-interval`—(Optional) MII link monitoring frequency. This option is valid only for the MII monitor.

Value—Integer in the range -2147483648–2147483647 ms

Editing Level—Basic

`interfaces [interfaces...]`— Ethernet interfaces in this group.

Value—Text

Editing Level—Basic

`primary primary`—(Optional) Name of device that will always be the active device while it is available. Only when the primary is off-line will alternate devices be used. This is useful when one device is preferred over another, for example, when one device has higher throughput than another. This option is valid only for active-backup mode.

Value—Text

Editing Level—Basic

`transmit-hash-policy (layer2 | layer34)`—(Optional) Transmit hash policy to use for device selection in balance-xor and 802.3ad modes.

Value

- `layer2`— Uses XOR of hardware MAC addresses to generate the hash. The formula is:
(source MAC XOR destination MAC) modulo slave count
This algorithm will place all traffic to a particular network peer on the same device. This algorithm is 802.3ad compliant.
- `layer34`— Uses upper layer protocol information, when available, to generate the hash. This allows for traffic to a particular network peer to span multiple devices, although a single connection will not span multiple devices.
The formula for unfragmented TCP and UDP packets is
((source port XOR dest port) XOR ((source IP XOR dest IP) AND 0xffff) modulo slave count
For fragmented TCP or UDP packets and all other IP protocol traffic, the source and destination port information is omitted. For non-IP traffic, the formula is the same as for the layer2 transmit hash policy.
This algorithm is not fully 802.3ad compliant. A single TCP or UDP conversation containing both fragmented and unfragmented packets will see packets striped across two interfaces. This may result in out of order delivery. Most traffic types will not meet this criteria, as TCP rarely fragments traffic, and most UDP traffic is not involved in extended conversations. Other implementations of 802.3ad may or may not tolerate this noncompliance.

Editing Level—Basic

Required Privilege Level

interface

Required Editing Level

Basic

interfaces *name* tunnel

Syntax

```
interfaces name tunnel {
    mode (ipip | gre | sit);
    destination destination;
    source source;
    key key;
    interface interface;
    ttl ttl;
}
```

Hierarchy Level

```
[edit interfaces name tunnel]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a tunnel interface. A tunnel allows direct connection between a remote location and an application running on the C Series Controller; a tunnel lets you use the redirect server in deployments where the JUNOSe router does not have a direct connection to the C Series Controller.

Options

`mode (ipip | gre | sit)`—Type of tunnel interface.

Value

- `ipip`—IP-over-IP. Encapsulates IP packets within IP packets.
- `gre`—GRE. Encapsulates traffic that uses various routing protocols within IP.
- `sit`—IPv6 in IPv4 tunnel

Default—No value

Editing Level—Basic

`destination destination`—IP address of the remote end of the tunnel.

Value—IP address

Default— No value
Editing Level—Basic

`source source`—(Optional) Local IP address, that will not change, to receive tunneled packets. If you specify a source address, also specify a local interface.

Value—IP address
Default— No value
Editing Level—Basic

`key key`—(Optional) For a GRE tunnel, a GRE key.

Value—Integer in the range -2147483648–2147483647
Default— No value
Editing Level—Basic

`interface interface`—(Optional) Existing physical interface. If you configured a source address, specify an interface.

Value— Name of interface.

Example: eth0

Default— No value
Editing Level—Basic

`ttl ttl`—(Optional) Lifetime of tunneled packets.

Value—Integer in the range 1–255
Editing Level—Basic

Required Privilege Level

interface

Required Editing Level

Basic

interfaces *name* unit

Syntax

```
interfaces name unit unit-number ...
```

Hierarchy Level

```
[edit interfaces name unit]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure logical interfaces on a physical Ethernet interface on the C Series Controller. You can create different units to configure numerous IP addresses on an interface.

Options

unit-number unit-number— Number of the unit (logical interface).

Value—Integer in the range 0–16385

Required Privilege Level

interface

Required Editing Level

Basic

interfaces *name* unit *unit-number* family inet

Syntax

```
interfaces name unit unit-number family inet {
    address address;
    broadcast broadcast;
}
```

Hierarchy Level

```
[edit interfaces name unit unit-number family inet]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure properties for IPv4.

Options

`address address`—(Optional) IP address with destination prefix for interface.

Value— IP address/destination prefix

Default— No value

Editing Level—Basic

`broadcast broadcast`—(Optional) Broadcast address.

Value—IP address

Default— No value

Editing Level—Basic

Required Privilege Level

interface

Required Editing Level

Basic

interfaces *name* unit *unit-number* family inet6 address

Syntax

```
interfaces name unit unit-number family inet6 address address ...
```

Hierarchy Level

```
[edit interfaces name unit unit-number family inet6 address]
```

Release Information

Statement introduced in SRC Release 1.1.0

Description

Configure properties for IPv6.

Options

address address— IP address with destination prefix for interface.

Value— IP address/destination prefix

Required Privilege Level

interface

Required Editing Level

Basic

load factory-default

Syntax

```
load factory-default
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Load the default configuration supplied with the SRC software.

Required Privilege Level

config-control

load merge

Syntax

```
load merge filename <relative> <format (text | xml) >
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Combine the configuration that is currently shown in the CLI and the configuration in the specified file.

Options

filename— Path and filename of the file on the C-series Controller to load.

Value— Complete filename on the C-series Controller *path/filename*.

relative—(Optional) Hierarchy level relative to the current location.

format (text | xml) —(Optional) The configuration format.

Value

- *text*— Text format
- *xml*— XML format

Required Privilege Level

config-control

load override

Syntax

```
load override filename <format (text | xml) >
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Discard the entire configuration that is currently shown in the CLI, and load the entire configuration in the specified file. The statement also marks every object as changed.

Options

filename— Path and filename of the file on the C-series Controller to load.

Value— Complete filename on the SRC Controller *path/filename*.

format (text | xml) —(Optional) The configuration format

Value

- *text*— Text format
- *xml*— XML format

Required Privilege Level

config-control

load replace

Syntax

```
load replace filename <relative> <format (text | xml) >
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Replace identifiers or values in a configuration.

Options

filename— Path and filename of the file on the C-series Controller to load.

Value— Complete filename on the C-series Controller *path/filename*.

relative—(Optional) Hierarchy level relative to the current location.

format (text | xml) —(Optional) The configuration format

Value

- *text*— Text format
- *xml*— XML format

Required Privilege Level

config-control

load set

Syntax

```
load set filename <relative>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Execute the set of commands listed in the specified file.

Options

filename— Path and filename of the file on the C-series Controller to load.

Value— Complete filename on the C-series Controller *path/filename*.

relative—(Optional) Hierarchy level relative to the current location.

Required Privilege Level

config-control

rename

Syntax

```
rename parent identifier1 (to) identifier2
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Rename an existing configuration statement or identifier.

Options

parent— Path to an existing configuration statement or identifier.

Value—Path of a collection object

identifier1— Existing identifier or statement.

Value— Identifier or statement

Configuration path.

Value

- to— Transition.

identifier2— New identifier or statement.

Value—Valid value for selected object

Required Privilege Level

config-control

rollback

Syntax

rollback

Release Information

Command introduced in SRC Release 1.0.0

Description

Return to a previously committed configuration.

Note: You can enter the **rollback** command only at the top level of the configuration hierarchy.

Required Privilege Level

config-control

routing-options static route

Syntax

```
routing-options static route destination {
    next-hop [next-hop...];
    reject;
}
```

Hierarchy Level

```
[edit routing-options static route]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure static routes to point to routers that connect to other networks to allow connectivity to devices on other networks.

Options

destination destination— Destination network and mask. To configure the default route use destination 0.0.0.0/0

Value—Text

next-hop [next-hop...]—(Optional) Address of next hop from the C Series Controller to the destination.

Value—IP address

Default— No value

Editing Level—Basic

reject—(Optional) Drop packets to the specified destination, and send an ICMP unreachable message.

Editing Level—Basic

Required Privilege Level

routing

Required Editing Level

Basic

run

Syntax

`run command`

Release Information

Command introduced in SRC Release 1.0.0

Description

Run an operational mode command without exiting from configuration mode.

Options

command— Name of command to run.

Value—Operational command

Required Privilege Level

No specific privilege required.

save

Syntax

```
save filename <format (text | xml) >
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Save the configuration to an ASCII file. The contents of the current level of the statement hierarchy and below are saved, along with the statement hierarchy containing it.

Options

filename— Name of file to contain the saved configuration.

Value— One of the following:

- Local filename, including path— *path/file*.
- File URL.
- FTP format—*ftp://username@hostname/ filename* or *ftp://username:password @hostname/filename*. (**Note:** Password appears at the CLI in clear text.)

format (text | xml) —(Optional) The configuration format

Value

- *text*— Text format
- *xml*— XML format

Required Privilege Level

view

set

Syntax

set object value

Release Information

Command introduced in SRC Release 1.0.0

Description

Create a statement hierarchy and set identifier values. When you enter a **set** command, the current level in the hierarchy does not change.

Options

object— Configuration statement or identifier

Value—Path of a configuration object

value— Value configured for a configuration statement.

Value—Valid value for selected object

Required Privilege Level

config-control

show

Syntax

```
show <object>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display information about a configuration object.

Options

object—(Optional) Configuration object for which to display information. The object can be a configuration statement or an identifier for a statement.

Value—Path of a configuration object

Required Privilege Level

config-view

slot

Syntax

```
slot number ...
```

Hierarchy Level

```
[edit slot]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure slot number for component.

Options

number number— Number of the slot for which you want to configure values.

Value— Currently, the chassis has only one slot. The valid value is 0.

Default—0

Required Privilege Level

system

Required Editing Level

Basic

system

Syntax

```
system {
    host-name host-name;
    domain-name domain-name;
    domain-search [domain-search...];
    name-server [name-server...];
    authentication-order [(radius | tacplus | password)...];
    time-zone time-zone;
}
```

Hierarchy Level

[edit system]

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure system properties.

Options

`host-name host-name`—Hostname for the C Series Controller.

Value— hostname

Default— No value

Editing Level—Basic

`domain-name domain-name`—(Optional) Name of the domain in which the C Series Controller is located. This is the default domain name that is appended to hostnames that are not fully qualified.

Value— domain name

Default— No value

Editing Level—Basic

`domain-search [domain-search...]`—(Optional) List of domains to search.

Value— domain name

Default— No value
Editing Level—Basic

`name-server [name-server...]`—(Optional) Domain name server(s).

Value— name server
Default— No value
Editing Level—Basic

`authentication-order [(radius | tacplus | password)...]`—(Optional) Order in which the software tries different user authentication methods when attempting to authenticate a user. For each login attempt, the software tries the authentication methods in order configured, until the password matches.

Value

- `radius`— RADIUS authentication
- `tacplus`—TACACS+ authentication services
- `password`—Traditional password authentication

Editing Level—Basic

`time-zone time-zone`—(Optional) Name of the local time zone.

Value— time-zone
Default—UTC
Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

system ipmi

Syntax

```
system ipmi {
    address address;
    gateway gateway;
    gateway-mac-address gateway-mac-address;
}
```

Hierarchy Level

```
[edit system ipmi]
```

Release Information

Statement introduced in SRC Release 2.0.0

Description

Configure the IPMI interface.

Options

address address—(Optional) IP address/destination prefix of IPMI interface. You must enter a value for the C2000 Controller. For the C4000 Controller, the address is automatically set to the IP address of the eth0 unit 0 interface.

Value—Text
Editing Level—Basic

gateway gateway— IP address of the gateway.

Value—IP address
Editing Level—Basic

gateway-mac-address gateway-mac-address—(Optional) MAC address of the gateway. If not specified, ARP will be used to get the gateway's MAC address.

Value—Text
Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

system ipmi user

Syntax

```
system ipmi user name {
    plain-text-password;
    encrypted-password encrypted-password;
}
```

Hierarchy Level

```
[edit system ipmi user]
```

Release Information

Statement introduced in SRC Release 2.0.0

Description

Configure the IPMI user account.

Options

name name— Username that is used to login to the IPMI interface of a C Series Controller.

Value— username

plain-text-password—(Optional) Prompt for a plain-text password.

Editing Level—Basic

encrypted-password encrypted-password— Password in plaintext format.

Value— plain-text-password

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

system ldap client

Syntax

```
system ldap client {
    base-dn base-dn;
    url url;
    backup-urls [backup-urls...];
    principal principal;
    credentials credentials;
    timeout timeout;
    time-limit time-limit;
    eventing;
    polling-interval polling-interval;
    connection-manager-id connection-manager-id;
    dispatcher-pool-size dispatcher-pool-size;
    event-base-dn event-base-dn;
    signature-dn signature-dn;
    blacklist;
}
```

Hierarchy Level

```
[edit system ldap client]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure directory properties used by the CLI to connect to the directory that contains SRC data.

On a C-series Controller, you use the Juniper Networks database and typically use the default configuration for the directory connection. You can add backup directories and change the password to the directory.

Options

base-dn base-dn—(Optional) DN of the root directory for SRC components and applications.

Value— DN

Default—o=UMC

Editing Level—Expert

`url url`—(Optional) URL that identifies the location of the primary directory server.

Value—URL

Default—`ldap://127.0.0.1:389`

Editing Level—Expert

`backup-urls [backup-urls...]`—(Optional) URLs that identify the locations of backup directory servers. Backup servers are used if the primary directory server is not accessible.

Value—URL

Default—No value

Editing Level—Normal

`principal principal`—(Optional) DN that defines the username with which an SRC component accesses the directory.

Value—DN

Default—`cn=conf,o=Operators,<base>`

Editing Level—Expert

`credentials credentials`—(Optional) Password used for authentication with the directory server.

Value—Secret text

Default—`conf`

Editing Level—Expert

`timeout timeout`—(Optional) Maximum amount of time during which the directory must respond to a connection request.

Value—Integer in the range 0–600 s

Default—No value

Editing Level—Expert

`time-limit time-limit`—(Optional) The number of milliseconds to wait for directory results before returning. If set to 0, wait indefinitely.

Value—Integer in the range 0–2147483647 ms

Default—5000

Editing Level—Expert

`eventing`—(Optional) Enable an SRC component to poll the directory for changes.

Default—TRUE

Editing Level—Expert

`polling-interval` *polling-interval*—(Optional) Interval at which an SRC component polls the directory to check for directory changes.

Value—Integer in the range 15–86400 s

Default— No value

Editing Level—Expert

`connection-manager-id` *connection-manager-id*—(Optional) CLI identifier of the connection manager for the directory eventing system (within the JNDI framework).

Value— Identifier for connection manager

Example—DIRAGENT_POOL_VR

Editing Level—Expert

`dispatcher-pool-size` *dispatcher-pool-size*—(Optional) Number of directory change notifications that can be sent simultaneously to the SRC component.

Value—Integer in the range 0–2147483647

Editing Level—Expert

`event-base-dn` *event-base-dn*—(Optional)

DN of an entry superior to the data associated with an SRC component in the directory.

If you are storing non-SRC data in the directory, and that data changes frequently whereas the SRC data does not, you may need to adjust the default value to improve performance. For optimal performance, set the value to the DN of an entry superior to both the SRC data and the changing non-SRC data.

Value— DN

Default— o=umc, <base>

Editing Level—Expert

`signature-dn` *signature-dn*—(Optional) DN of the directory entry that specifies the `usedDirectory` attribute for the SRC CLI. The `usedDirectory` attribute identifies the vendor of the directory server.

Value— DN

Editing Level—Expert

`blacklist`—(Optional) Specifies whether the directory monitoring system prevents connection to a directory if the directory fails to respond during 10 polling intervals.

Editing Level—Expert

Required Privilege Level

system

Required Editing Level

Basic

system login

Syntax

```
system login {
    announcement announcement;
}
```

Hierarchy Level

```
[edit system login]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure system announcement to be displayed at user login.

Options

announcement announcement—(Optional) Announcement displayed to every user after login.

Value— Announcement text

Default— No value

Editing Level—Basic

Required Privilege Level

system admin

Required Editing Level

Basic

system login class

Syntax

```
system login class name {
    allow-commands allow-commands;
    allow-configuration allow-configuration;
    deny-commands deny-commands;
    deny-configuration deny-configuration;
    idle-timeout idle-timeout;
    permissions [(admin | admin-control | all | clear | configure | control |
field | firewall | firewall-control | interface | interface-control | maintenance
| network | reset | routing | routing-control | secret | secret-control |
security | security-control | shell | snmp | snmp-control | system | system-
control | view | view-configuration | service | service-control | subscriber |
subscriber-control)...];
}
```

Hierarchy Level

```
[edit system login class]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Define login classes. You can define any number of login classes.

Options

name name— Name that you choose for a login class.

Value— Name

allow-commands allow-commands—(Optional) Operational mode commands that members of a login class can use.

If you omit this statement and the deny-commands statement, users can issue only those commands for which they have access privileges through the permissions statement.

You can use an extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.

Value— Operational-mode commands to allow

Default— No value

Editing Level—Basic

`allow-configuration` *allow-configuration*—(Optional) Configuration mode commands that members of a login class can use.

If you omit this statement and the `deny-configuration` statement, users can issue only those commands for which they have access privileges through the permissions statement

You can use an extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.

Value— Configuration-mode commands to allow

Default— No value

Editing Level—Basic

`deny-commands` *deny-commands*—(Optional) Operational mode commands that the user is denied permission to issue, even though the permissions set with the permissions statement would allow it.

If you omit this statement and the `allow-commands` statement, users can issue only those commands for which they have access privileges through the permissions statement.

You can use an extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any wildcard characters, enclose it in quotation marks.

Value— Operational mode commands to deny

Default— No value

Editing Level—Basic

`deny-configuration` *deny-configuration*—(Optional) Configuration mode commands that the user is denied permission to issue, even though the permissions set with the permissions statement would allow it.

If you omit this statement and the `allow-configuration` statement, users can issue only those commands for which they have access privileges through the permissions statement.

You can use extended (modern) regular expression as defined in POSIX 1003.2. If the regular expression contains any spaces, operators, or wildcard characters, enclose it in quotation marks.

Value— Configuration mode commands to deny

Default— No value

Editing Level—Basic

`idle-timeout` *idle-timeout*—(Optional) Maximum amount of time that a session can be idle before the user is logged off the C-series Controller. The session times out after remaining at the CLI operational mode prompt for the specified time.

If you omit this statement, a user is never forced off the system after extended idle times.

Value— Number of minutes

Default— No value

Editing Level—Basic

`permissions [(admin | admin-control | all | clear | configure | control | field | firewall | firewall-control | interface | interface-control | maintenance | network | reset | routing | routing-control | secret | secret-control | security | security-control | shell | snmp | snmp-control | system | system-control | view | view-configuration | service | service-control | subscriber | subscriber-control) ...]`—(Optional) Access privileges for each login class.

Value

- `admin`— Can view user account information in configuration mode and with the `show configuration` command.
- `admin-control`— Can view user accounts and configure them (at the [edit system login] hierarchy level).
- `all`— Has all permissions.
- `clear`— Can clear (delete) information learned from the network that is stored in various network databases (by using the `clear` commands).
- `configure`— Can enter configuration mode (by using the `configure` command).
- `control`— Can modify any configuration values.
- `field`— Reserved for field (debugging) support.
- `firewall`— Can view the firewall filter configuration in configuration mode.
- `firewall-control`— Can view and configure firewall filter information.
- `interface`— Can view the interface configuration in configuration mode and with the `show configuration operational mode` command.
- `interface-control`— Can modify interface configuration.
- `maintenance`— Can perform system maintenance, including starting a local shell on a C-series Controller, and can halt and reboot a C-series Controller (by using the `request system` commands).
- `network`— Can access the network by entering commands such as SSH or Telnet.
- `reset`— Can restart software processes by using the `restart` command and can configure whether software processes are enabled or disabled.
- `routing`— Can view routing information in configuration and operational modes.

- `routing-control`— Can view general routing information and modify routing configuration.
- `secret`— Can view passwords and other authentication keys in the configuration.
- `secret-control`— Can view passwords and other authentication keys in the configuration and can modify them in configuration mode.
- `security`— Can view security configuration in configuration mode and with the `show configuration operational mode` command.
- `security-control`— Can view security configuration in configuration mode and with the `show configuration operational mode` command.
- `shell`— Can start a local shell on the router by entering the `start shell` command.
- `snmp`— Can view SNMP configuration information in configuration and operational modes.
- `snmp-control`— Can view SNMP configuration information and configure SNMP (at the `[edit snmp]` hierarchy level).
- `system`— Can view system-level information in configuration and operational modes.
- `system-control`— Can view and configure system-level configuration information.
- `view`— Can use various commands to display current system-wide values and statistics.
- `view-configuration`— Can view all system configuration, excluding any secret configurations.
- `service`— Can view service and policy definitions.
- `service-control`— Can view and configure service definitions and policy definitions.
- `subscriber`— Can view information about subscriber definitions.
- `subscriber-control`— Can view and configure information about subscriber definitions.

Editing Level—Basic

Required Privilege Level

system admin

Required Editing Level

Basic

system login user

Syntax

```
system login user user-name {
    class class;
    full-name full-name;
    uid uid;
    gid gid;
    prompt prompt;
    level (basic | normal | advanced | expert);
    complete-on-space (on | off);
}
```

Hierarchy Level

```
[edit system login user]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure access permissions for individual users.

Options

user-name user-name— Username that is used to log in to a C-series Controller.

Value— Username

class class— User's login class. Configure one class for each user. The class referenced must already be configured.

Value— Class-name
Editing Level—Basic

full-name full-name— Full name of the user. If the name contains spaces, enclose it in quotation marks.

Value— Name
Editing Level—Basic

`uid uid`— User identifier for the login account.

Value—Integer in the range 0–64000

Editing Level—Basic

`gid gid`— Group identifier for the login account.

Value—Integer in the range 0–64000

Editing Level—Basic

`prompt prompt`—(Optional) Default prompt that this user sees at the SRC CLI.

Value— Prompt-text

Editing Level—Basic

`level (basic | normal | advanced | expert)`—(Optional) Editing level available to the user. The setting for the editing level determines which configuration commands are visible to the user.

Value

- `basic`— Minimal set of configuration statements and commands
— only the statements that must be configured are visible.
- `normal`— Normal set of configuration statements and commands
— the common and basic statements are visible.
- `advanced`— All configuration statements and commands,
including the common and basic ones, are visible.
- `expert`— All configuration statements, including common, basic,
and internal statements and commands used for debugging, are visible.

Default— Normal

Editing Level—Basic

`complete-on-space (on | off)`—(Optional) Set the CLI to complete a partial command entry when you type a space. This statement enables command completion for all user sessions for this user.

To enable command completion for an active user session, use the `set cli complete-on-space` operational mode command.

Value

- `on`— Turn on command completion—allow either a space or a tab to be used for command completion.
- `off`— Turn off command completion—a space or a tab after a partial command name does not complete the command.

Default— On
Editing Level—Basic

Required Privilege Level

system admin

Required Editing Level

Basic

system login user *user-name* authentication

Syntax

```
system login user user-name authentication {
    plain-text-password;
    encrypted-password encrypted-password;
    ssh-authorized-keys [ssh-authorized-keys...];
}
```

Hierarchy Level

```
[edit system login user user-name authentication]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Authentication methods that a user can use to log in to a C-series Controller. You can assign multiple authentication methods to a single user.

Options

`plain-text-password`—(Optional) Prompt for a plain-text password.

Editing Level—Basic

`encrypted-password` *encrypted-password*—(Optional) Password in encrypted format.

Value— Encrypted-password

Editing Level—Basic

`ssh-authorized-keys` [*ssh-authorized-keys...*]—(Optional) Public key for SSH.

Value— Public-key

Editing Level—Basic

Required Privilege Level

system admin

Required Editing Level

Basic

system ntp

Syntax

```
system ntp {
    boot-server boot-server;
    broadcast-client;
    trusted-key [trusted-key...];
}
```

Hierarchy Level

```
[edit system ntp]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure NTP.

We strongly recommend that you configure NTP on every server used for an SRC deployment. The system may not recognize subscriber sessions if the clocks are not synchronized.

Options

`boot-server boot-server`—(Optional) Server that NTP queries when at boot time to determine the local date and time.

When you boot the system on which the SRC software runs, the system issues an `ntpdate` request, which polls a network server to determine the local date and time. You can configure a server that the system uses to determine the time at startup. If no boot server is configured, NTP uses one of the configured servers to set the initial time.

Value— IP address of an NTP server

Default— No value

Editing Level—Basic

`broadcast-client`—(Optional) Listen for NTP broadcast messages on the local network to discover other servers on the same subnet.

Editing Level—Basic

`trusted-key [trusted-key . . .]`—(Optional) List of keys you are allowed to use when you configure the local system to synchronize its time with other systems on the network.

Value— Positive signed 32-bit integer (1–2147483647)
Default— No value
Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

system ntp authentication-key

Syntax

```
system ntp authentication-key key-number {
    value value;
}
```

Hierarchy Level

```
[edit system ntp authentication-key]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure NTP authentication keys so that the C-series Controller can send authenticated packets. If you configure the C-series Controller to operate in authenticated mode, you must configure a key.

NTP authentication uses the MD5 encryption algorithm.

Options

key-number key-number— Positive integer that identifies the NTP authentication key.

Value—Integer in the range 1–2147483647

value value— The value of the NTP authentication, which can contain 1–8 ASCII characters.

Value—Secret text

Default— No value

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

system ntp broadcast

Syntax

```
system ntp broadcast address {
    key key;
    ttl ttl;
    version version;
}
```

Hierarchy Level

```
[edit system ntp broadcast]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the C-series Controller to operate in broadcast mode with the remote system at the specified address. In this mode, the local system sends periodic broadcast messages to a client population at the specified broadcast or multicast address. Typically, you include this statement only when the local system is operating as a transmitter.

Options

address address— IP address to receive broadcast or multicast periodic broadcast messages.

Value— IP address

key key—(Optional) Value of the authentication key used to encrypt authentication fields in all packets sent to the broadcast or multicast address.

Value— Positive signed 32-bit integer (1–2147483647)

Default— No value

Editing Level—Basic

ttl ttl—(Optional) TTL value to transmit.

Value—Integer in the range 1–255

Default— No value

Editing Level—Basic

`version version`—(Optional) Version number of NTP to use in outgoing NTP packets.

Value—Integer in the range 1–4

Default— No value

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

system ntp multicast-client

Syntax

```
system ntp multicast-client {
    address;
}
```

Hierarchy Level

```
[edit system ntp multicast-client]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Listen for NTP multicast messages on the local network to discover other servers on the same subnet.

Options

address—(Optional) IP address(s). If you specify more than one address, the system joins those multicast groups.

Value—IP address

Default— No value

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

system ntp peer

Syntax

```
system ntp peer address {
    key key;
    version version;
    prefer;
}
```

Hierarchy Level

```
[edit system ntp peer]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the C-series Controller to operate in symmetric active mode with the remote system at the specified address. In this mode, the C-series Controller and the remote system can synchronize with each other. This configuration is useful in a network in which either the local router or the remote system might be a better source of time.

Options

`address address`— IP address of an NTP peer. Do not specify a hostname.

Value—IP address

`key key`—(Optional) Key number used to encrypt all authentication fields in packets sent to the specified address.

Value— Positive signed 32-bit integer (1–2147483647)

Default— No value

Editing Level—Basic

`version version`—(Optional) Version number of NTP to be used in outgoing packets.

Value—Integer in the range 1–4

Default— No value

Editing Level—Basic

`prefer`—(Optional) Remote system is the preferred host. This remote system is then selected for synchronization among a set of systems that are operating correctly.

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

system ntp server

Syntax

```
system ntp server address {
    key key;
    version version;
    prefer;
}
```

Hierarchy Level

```
[edit system ntp server]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the C-series Controller to operate in client mode with the remote system at the specified address. In this mode, the C-series Controller can be synchronized with the remote system, but the remote system can never be synchronized with the C-series Controller.

Options

`address address`— IP address of an NTP server. Do not specify a hostname.

Value—IP address

`key key`—(Optional) Key number used to encrypt all authentication fields in packets sent to the specified address.

Value— Positive signed 32-bit integer (1–2147483647)

Default— No value

Editing Level—Basic

`version version`—(Optional) Version number of NTP to be used in outgoing packets.

Value—Integer in the range 1–4

Default— No value

Editing Level—Basic

`prefer`—(Optional) Remote system is the preferred host. This remote system is then selected for synchronization among a set of systems that are operating correctly.

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

system radius-server

Syntax

```
system radius-server address {
    port port;
    secret secret;
    timeout timeout;
    retry retry;
}
```

Hierarchy Level

```
[edit system radius-server]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure RADIUS authentication. To use more than one RADIUS server, include a `radius-server` statement for each server. The software contacts the servers in order in a round-robin fashion until it receives a valid response from one of the servers or until the retry limit is reached for all servers.

To configure RADIUS for authentication, also include `radius` in the `authentication-order` option for the `system` statement.

For a user authenticated through RADIUS to be able to log in to the C Series Controller, you must create either a local profile or a remote profile to define common access privileges for all users authenticated through RADIUS or TACACS+. For information about creating user profiles, see the `system login user` statement.

Options

`address address`— IP address of RADIUS server.

Value— IP address

`port port`—(Optional) [Alias: authentication-port] Port number on which to connect to a RADIUS server.

Value—Integer in the range 0–65535

Default—1812

Editing Level—Basic

`secret secret`— Password to use with the RADIUS server. This secret password is used by the C Series Controller and must match the password on the RADIUS server.

Value— password
Editing Level—Basic

`timeout timeout`—(Optional) Amount of time that the C Series Controller waits to receive a response from the RADIUS server.

Value—Integer in the range 1–90 s
Default—3
Editing Level—Basic

`retry retry`—(Optional) Number of times the C Series Controller tries to contact a RADIUS server.

Value—Integer in the range 1–10
Default—3
Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

system services

Syntax

```
system services {  
    telnet;  
}
```

Hierarchy Level

```
[edit system services]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure system services.

Options

`telnet`—(Optional) Allow Telnet connections from remote systems to the C Series Controller.

Note: Telnet connections do not allow access through `root`.

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

system services editor

Syntax

```
system services editor {
    password-encryption (crypt | md5 | sha | plain);
}
```

Hierarchy Level

```
[edit system services editor]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure access properties for external access to the Policies, Services, and Subscribers Editor.

Options

`password-encryption (crypt | md5 | sha | plain)`—(Optional) Encrypt the passwords of users who remotely access the Policies, Services, and Subscribers Editor using the specified encryption algorithm.

Value

- `crypt`— UNIX crypt, a one-way encryption.
- `md5`— Message Digest 5 (MD5), a 128-bit message digest.
- `sha`— SHA message digest, a 160-bit message digest.
- `plain`— No encryption.

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

system services editor policy-editor

Syntax

```
system services editor policy-editor {
    directory-eventing;
}
```

Hierarchy Level

```
[edit system services editor policy-editor]
```

Release Information

Statement introduced in SRC Release 1.0.0

Options

`directory-eventing`—(Optional) Enable policy editor to poll the directory for changes.

Default—true

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

system services netconf

Syntax

```
system services netconf {  
    ssh;  
}
```

Hierarchy Level

```
[edit system services netconf]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Allow connections through NETCONF to the C Series Controller.

Options

`ssh`—(Optional) Use SSH for NETCONF connections.

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

system services ssh

Syntax

```
system services ssh {
    root-login (allow | deny | deny-password);
    protocol-version (v1 | v2);
}
```

Hierarchy Level

```
[edit system services ssh]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Allow SSH requests from remote systems to the C Series Controller.

Options

`root-login (allow | deny | deny-password)`—(Optional) Control user access through SSH.

Value

- `allow`— Allow users to login in to the C Series Controller as `root` through SSH.(Default)
- `deny`— Disable users from logging in to the C Series Controller as `root` through SSH.
- `deny-password`— Allow users to log in to the C Series Controller as `root` through SSH when the authentication method (for example, RSA authentication) does not require a password.

Editing Level—Basic

`protocol-version (v1 | v2)`—(Optional) SSH protocol versions accepted.

Value

- `v1`—SSH version 1

- v2—SSH version 2 (Default)

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

system services web-management http

Syntax

```
system services web-management http {
    port port;
    interface [interface...];
}
```

Hierarchy Level

```
[edit system services web-management http]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Use HTTP without encryption.

Options

port port—(Optional) TCP port to be used for incoming connections to the C-Web interface.

Value—Integer in the range 1–65535

Default—80

Editing Level—Basic

*interface [*interface...*]*—(Optional) List of network interfaces to accept incoming connections. If you do not specify any interfaces, the software accepts connections from all interfaces.

Value— Name of external interface, such as eth0.

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

system services web-management https

Syntax

```
system services web-management https {
    port port;
    interface [interface...];
    local-certificate local-certificate;
}
```

Hierarchy Level

```
[edit system services web-management https]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Use secure HTTP with encryption.

Options

`port port`—(Optional) TCP port to be used for incoming connections to the C-Web interface.

Value—Integer in the range 1–65535

Default—443

Editing Level—Basic

`interface [interface...]`—(Optional) List of network interfaces to accept incoming connections. If you do not specify any interfaces, the software accepts connections from all interfaces.

Value— Name of external interface, such as eth0.

Editing Level—Basic

`local-certificate local-certificate`—(Optional) Name of the security certificate (in X.509 format) on the local system. This certificate is used to secure connections from external Web browsers to the C-Web interface.

Value— Name of digital security certificate.

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

system services web-management logger

Syntax

```
system services web-management logger name ...
```

Hierarchy Level

```
[edit system services web-management logger]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a logging component for the C-Web interface. Logging can be to a file or to the system logging utility.

Options

name name— Name of a logging component.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

system services web-management logger *name* file

Syntax

```
system services web-management logger name file {
    filter filter;
    filename filename;
    rollover-filename rollover-filename;
    maximum-file-size maximum-file-size;
}
```

Hierarchy Level

```
[edit system services web-management logger name file]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure logging of messages to a file.

filter filter—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

Editing Level—Basic

filename filename— Absolute path of the filename that contains the current logs.

Note: 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.

Value— Filename

Default— By default, SRC components and applications write log files in the folder in which the component or application is started.

Editing Level—Basic

`rollover-filename rollover-filename`—(Optional) 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— Path of filename

Example—`/opt/UMC/sae/var/log/sae.alt`

Default— The default value is different for each type of component.

Editing Level—Normal

`maximum-file-size maximum-file-size`—(Optional) Maximum size of the log file and the rollover file.

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

Value—Integer in the range 0–2147483647 kbytes

Default— 1000000

Editing Level—Normal

Required Privilege Level

system system

Required Editing Level

Basic

system services web-management logger *name* syslog

Syntax

```
system services web-management logger name syslog {
    filter filter;
    host host;
    facility facility;
    format format;
}
```

Hierarchy Level

```
[edit system services web-management logger name syslog]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure logging of messages to system logging.

filter filter—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

Editing Level—Basic

host host— IP address or name of a host that collects event messages by means of a standard system logging daemon.

Value— IP address or hostname

Default—loghost

Editing Level—Basic

facility facility—(Optional) Type of system log in accordance with the system logging protocol.

Value—Integer in the range 0–23

Default— 3

Editing Level—Advanced

`format format`—(Optional) MessageFormat string that specifies how the information in an event message is printed. (The strings {#} are replaced with the log information [...]).

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

Editing Level—Advanced

Required Privilege Level

system system

Required Editing Level

Basic

system static-host-mapping

Syntax

```
system static-host-mapping host-name {
    inet [inet...];
    alias [alias...];
}
```

Hierarchy Level

```
[edit system static-host-mapping]
```

Release Information

Statement introduced in SRC Release 2.0.0

Description

Configure static mapping to resolve hostnames.

Options

host-name *host-name*— Fully-qualified name of the system.

Value—Text

inet [*inet...*]—(Optional) [Alias: inet4 inet6] IP addresses to which you want to map the hostname.

Value—IP address

Editing Level—Basic

alias [*alias...*]—(Optional) Aliases for the hostname.

Value—Text

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

system syslog file

Syntax

```
system syslog file file-name ...
```

Hierarchy Level

```
[edit system syslog file]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify a file to store information that has been collected.

Options

file-name file-name— Name of the file in which to log system messages.

Value— filename

Required Privilege Level

system

Required Editing Level

Basic

system syslog file *file-name*

Syntax

```
system syslog file file-name (any | authorization | daemon | ftp | kernel | user
| local7) {
    (any | emergency | alert | critical | error | warning | notice | info |
none);
}
```

Hierarchy Level

```
[edit system syslog file file-name]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the message groups and severity level of messages to be forwarded to a specified file, host, or user.

Options

Group of messages that are either generated by the same software process or concern a similar condition or activity (such as authentication attempts). A message group is referred to as a facility.

Value

- *any*— Messages from all facilities.
- *authorization*— Authentication and authorization attempts.
- *daemon*— Actions performed or errors encountered by various system processes.
- *ftp*— Actions performed or errors encountered by an FTP process.
- *kernel*— Actions performed or errors encountered by the kernel.
- *user*— Actions performed or errors encountered by various user processes.
- *local7*— Actions performed or errors encountered by different SRC processes.

Severity level

Value

- `any`— Messages for all severity levels.
- `emergency`— System panic or other condition that causes the system to stop functioning.
- `alert`— Conditions that require immediate correction.
- `critical`— Critical conditions, such as hard drive errors.
- `error`— Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels.
- `warning`— Conditions that warrant monitoring.
- `notice`— Conditions that are not errors but might warrant special handling.
- `info`— Events or nonerror conditions of interest.
- `none`— Messages are not generated for any condition.

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

system syslog host

Syntax

```
system syslog host log-host-name ...
```

Hierarchy Level

```
[edit system syslog host]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the IP address or hostname of the remote host to receive system log messages. The remote machine must be running a standard syslogd utility.

Options

log-host-name log-host-name— IP address or hostname of a remote system to receive system log messages. The remote machine must be running a standard syslogd utility.

Value— IP address or hostame

Required Privilege Level

system

Required Editing Level

Basic

system syslog host *log-host-name*

Syntax

```
system syslog host log-host-name (any | authorization | daemon | ftp | kernel |
user | local7) {
    (any | emergency | alert | critical | error | warning | notice | info |
none);
}
```

Hierarchy Level

```
[edit system syslog host log-host-name]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the message groups and severity level of messages to be forwarded to a specified file, host, or user.

Options

Group of messages that are either generated by the same software process or concern a similar condition or activity (such as authentication attempts). A message group is referred to as a facility.

Value

- *any*— Messages from all facilities.
- *authorization*— Authentication and authorization attempts.
- *daemon*— Actions performed or errors encountered by various system processes.
- *ftp*— Actions performed or errors encountered by an FTP process.
- *kernel*— Actions performed or errors encountered by the kernel.
- *user*— Actions performed or errors encountered by various user processes.
- *local7*— Actions performed or errors encountered by different SRC processes.

Severity level

Value

- **any**— Messages for all severity levels.
- **emergency**— System panic or other condition that causes the system to stop functioning.
- **alert**— Conditions that require immediate correction.
- **critical**— Critical conditions, such as hard drive errors.
- **error**— Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels.
- **warning**— Conditions that warrant monitoring.
- **notice**— Conditions that are not errors but might warrant special handling.
- **info**— Events or nonerror conditions of interest.
- **none**— Messages are not generated for any condition.

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

system syslog user

Syntax

```
system syslog user user-name ...
```

Hierarchy Level

```
[edit system syslog user]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Notify a specified user by means of a terminal session.

Options

user-name user-name— Name of user to receive messages.

Value— Username

Required Privilege Level

system

Required Editing Level

Basic

system syslog user *user-name*

Syntax

```
system syslog user user-name (any | authorization | daemon | ftp | kernel | user
| local7) {
    (any | emergency | alert | critical | error | warning | notice | info |
none);
}
```

Hierarchy Level

```
[edit system syslog user user-name]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the message groups and severity level of messages to be forwarded to a specified file, host, or user.

Options

Group of messages that are either generated by the same software process or concern a similar condition or activity (such as authentication attempts). A message group is referred to as a facility.

Value

- *any*— Messages from all facilities.
- *authorization*— Authentication and authorization attempts.
- *daemon*— Actions performed or errors encountered by various system processes.
- *ftp*— Actions performed or errors encountered by an FTP process.
- *kernel*— Actions performed or errors encountered by the kernel.
- *user*— Actions performed or errors encountered by various user processes.
- *local7*— Actions performed or errors encountered by different SRC processes.

Severity level

Value

- `any`— Messages for all severity levels.
- `emergency`— System panic or other condition that causes the system to stop functioning.
- `alert`— Conditions that require immediate correction.
- `critical`— Critical conditions, such as hard drive errors.
- `error`— Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels.
- `warning`— Conditions that warrant monitoring.
- `notice`— Conditions that are not errors but might warrant special handling.
- `info`— Events or nonerror conditions of interest.
- `none`— Messages are not generated for any condition.

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

system tacplus-server

Syntax

```
system tacplus-server {
    address [address...];
    secret secret;
}
```

Hierarchy Level

```
[edit system tacplus-server]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure TACACS+ authentication.

To configure TACACS+ for authentication, also include `tacplus` in the `authentication-order` option for the `system` statement.

For a user authenticated through TACACS+ to be able to log into the C Series Controller, you must create either a local profile or a remote profile to define common access privileges for all users authenticated via RADIUS or TACACS+. For information about creating user profiles, see the `system login user` statement.

Options

`address [address...]`— Address of TACACS+ authentication server.

Value— IP address
Default— No value
Editing Level—Basic

`secret secret`— Password to use with the RADIUS or TACACS+ server. The secret password used by the C Series Controller must match that used by the server.

Value—Secret text
Default— No value
Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

top

Syntax

`top <command>`

Release Information

Command introduced in SRC Release 1.0.0

Description

Return to the top level of the configuration hierarchy, which is indicated by the [edit] banner.

Options

command—(Optional) Name of command to run from the top of configuration hierarchy.

Note: The following commands are not supported: **exit**, **rollback**, **run**, **top**

Value— Name of command to run

Default— No value

Required Privilege Level

No specific privilege required.

up

Syntax

up <*number*>

Release Information

Command introduced in SRC Release 1.0.0

Description

Move up in the hierarchy of configuration statements.

Options

number—(Optional) Number of levels to move up in the hierarchy.

Value—Integer in the range 1–2147483647

Default—1

Required Privilege Level

No specific privilege required.

compare

Syntax

```
compare <filename>
```

Release Information

Command introduced in SRC Release 3.1.0

Description

Display comparison of configuration changes to the active (running) configuration.

Options

filename—(Optional) Name of file that contains the configuration changes. This file must be in plain-text format.

Value—Text

Required Privilege Level

No specific privilege required.

count

Syntax

count

Release Information

Command introduced in SRC Release 1.0.0

Description

Indicate number of occurrences.

Required Privilege Level

No specific privilege required.

display

Syntax

```
display (changed | running | hierarchy)
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display additional information.

Options

Type of information to display.

Value

- `changed`— Tag attributes with value changes.
- `running`— Display the most recently committed configuration.
- `hierarchy`— Display the configuration in a complete hierarchy from the top.

Required Privilege Level

No specific privilege required.

display

Syntax

```
display level level
```

Release Information

Command introduced in SRC Release 2.0.0

Description

Display additional information.

Options

level level— Display output for a hierarchy level, as indicated by the number of the hierarchy level. For example, NIC, SAE and ACP would be at hierarchy level 1.

Value—Integer in the range 0–2147483647

Default—1

Required Privilege Level

No specific privilege required.

display

Syntax

```
display (xml)
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display additional information.

Options

Type of information to display.

Value

- `xml`— Display information as XML tags.

Required Privilege Level

No specific privilege required.

except

Syntax

```
except pattern
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display text that does not match the specified pattern.

Options

pattern— Pattern to hide.

Value— Text that forms the pattern.

Required Privilege Level

No specific privilege required.

find

Syntax

```
find pattern
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Search for first occurrence of a specified pattern.

Options

pattern— Pattern to locate.

Value— Text that forms the pattern.

Required Privilege Level

No specific privilege required.

last

Syntax

```
last <lines>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display the last part of the output.

Options

lines—(Optional) Number of lines from the last line backward.

Value—Integer in the range 0–2147483647

Default—10

Required Privilege Level

No specific privilege required.

match

Syntax

```
match pattern
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display text that matches the specified pattern.

Options

pattern— Pattern to match.

Value— Pattern to locate.

Required Privilege Level

No specific privilege required.

no-more

Syntax

no-more

Release Information

Command introduced in SRC Release 1.0.0

Description

Do not paginate output.

Required Privilege Level

No specific privilege required.

save

Syntax

```
save filename
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Save output text to file.

Options

filename— Name or URL of file to which to save output.

Value— Filename or URL

Required Privilege Level

No specific privilege required.

clear security certificate

Syntax

```
clear security certificate <identifier identifier>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Delete a digital certificate from the system.

Options

identifier identifier—(Optional) Name of a local digital certificate.

Value—*Certificate name*

Required Privilege Level

security

clear security certificate-request

Syntax

```
clear security certificate-request <file-name file-name>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Delete a certificate request on the system.

Options

file-name file-name—(Optional) Name of certificate signing request file. This file is stored in the `/tmp` directory and has the file-extension `.csr`.

Value—*filename*

Default—certreq

Required Privilege Level

security

clear security ssh

Syntax

```
clear security ssh known-host known-host
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Clear (delete) cached SSH data.

Options

known-host *known-host*— Name of known host to remove

Value— Hostname

Required Privilege Level

security

configure

Syntax

```
configure <exclusive>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Enter configuration mode. In configuration mode, you enter hierarchical statements to define properties for the SRC software.

Alias

edit

Options

`exclusive`—(Optional) If you enter configuration mode with the exclusive lock on, you lock the candidate global configuration for as long as you remain in configuration mode.

Required Privilege Level

configure

disable

Syntax

```
disable component component
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Stop an SRC component that is running on the system.

Options

component component— Name of SRC component to stop.

To see a list of installed components, use the `show component` command.

Value— Component name

Required Privilege Level

reset

enable

Syntax

```
enable component component
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Start a specified SRC component that is installed on the system.

Options

component component— Name of SRC component to start.

Value— Component name

Required Privilege Level

reset

exit

Syntax

exit

Release Information

Command introduced in SRC Release 1.0.0

Description

Exit from the CLI session. If a session was established through SSH, you return to the local environment; if the session was established through Telnet or from a console, you return to the login prompt.

Alias

quit

Required Privilege Level

No specific privilege required.

file archive

Syntax

```
file archive <compress> source source destination destination
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Create an archive file on a C-series Controller.

Options

`compress`—(Optional) Compress an archive file by using the GNU `gzip` utility to create a TGZ file.

`source source`— Directory path to archive.

Value— Directory path

`destination destination`— Name of archive file to be created.

Value— Filename

Required Privilege Level

maintenance

file checksum md5

Syntax

```
file checksum md5 path
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Calculate an MD5 checksum of a file on a C-series Controller.

Options

path— Directory path of the file.

Value— Directory path

Required Privilege Level

maintenance

file compare

Syntax

```
file compare < (context | unified) > <ignore-white-space> files from-file to-file
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Compare files on a C-series Controller.

Options

(Optional)

Value

- **context**— Output shows the context for differences between the files. It shows which line was changed in one line listing, then the change for the line in a second line listing.
- **unified**— Output shows the differences between files in a unified format. A single listing of line numbers shows the line on which a change occurred, then the changed text.

ignore-white-space—(Optional) Differences in amount of white space ignored.

from-file—File to compare

Value— Filename

to-file—File to compare

Value— Filename

Required Privilege Level

maintenance

file copy

Syntax

```
file copy source destination
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Copy files.

Options

source— Source URL of file to copy.

Value— FTP or file URL

destination— Destination URL of file to copy.

Value— FTP or file URL

Required Privilege Level

maintenance

file create

Syntax

```
file create filename <encoding (base64) > content content
```

Release Information

Command introduced in SRC Release 3.1.0

Description

Create a file with the provided content

Options

filename— The filename must be created in an existing directory that is writable by the logged in user. If the name of an existing file is selected, the existing file will be overwritten.

Value—Text

encoding (base64) —(Optional) Type of content encoding.

Value

- *base64*— Content is base64 encoded and will be decoded before content is written to file.

content content— When using the CLI, the content can be provided in a "here-document" using "<<EOF". The here-document ends when *EOF* is entered on a line by itself. *EOF* is an arbitrary string.

Value—Text

Required Privilege Level

maintenance

file delete

Syntax

```
file delete file
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Delete a file on a C-series Controller.

Options

file— File to delete.

Value— Filename

Required Privilege Level

maintenance

file list

Syntax

```
file list <recursive> <detail> <path>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

List files in a directory on a C-series Controller.

Options

recursive—(Optional) Create recursive listing of files.

detail—(Optional) Provide information about the files in a listing of files, such as modification date and file size.

path—(Optional) Path to the directory in which you list files.

Value— Pathname

Required Privilege Level

maintenance

file monitor

Syntax

```
file monitor filename
```

Release Information

Command introduced in SRC Release 2.0.0

Description

Show online updates of a file

Options

filename—Filename to monitor

Value—Text

Required Privilege Level

maintenance

file rename

Syntax

```
file rename source destination
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Rename a file on a C-series Controller.

Options

source— File to rename.

Value— Filename

destination— New name for file to be renamed.

Value— Filename

Required Privilege Level

maintenance

file show

Syntax

```
file show <encoding (base64) > filename
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display content of a file.

Options

encoding (base64) —(Optional) Type of file encoding.

Value

- *base64*— File has base64 encoding.

filename— Name of file for which to display content.

Value— Filename

Required Privilege Level

maintenance

ipmisol close local-session

Syntax

```
ipmisol close local-session
```

Release Information

Command introduced in SRC Release 2.0.0

Description

Close the active IPMI connection to the local host. At any time, only one IPMI Serial-Over-LAN connection to an IPMI interface is allowed.

Required Privilege Level

network

ipmisol close remote-session

Syntax

```
ipmisol close remote-session host host user user
```

Release Information

Command introduced in SRC Release 2.0.0

Description

Close the active IPMI connection to a specific remote host. At any time, only one IPMI Serial-Over-LAN connection to an IPMI interface is allowed.

Options

`host host`— IP address of IPMI interface on the remote host.

Value— IP address

`user user`— IPMI username configured on the remote host.

Value— Username

Required Privilege Level

network

ipmisol open

Syntax

```
ipmisol open host host user user
```

Release Information

Command introduced in SRC Release 2.0.0

Description

Open a remote serial console using IPMI Serial-Over-LAN. The remote system must have IPMI configured.

Options

host host— IP address of IPMI interface on the remote host.

Value— IP address

user user— IPMI username configured on the remote host.

Value— Username

Required Privilege Level

network

ping

Syntax

```
ping <count count> <interval interval> <interface interface> <no-resolve> <tos
tos> <ttl ttl> <size size> <pattern pattern> host
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Determine whether a remote host is reachable by sending ping requests to the remote host.

Options

count count—(Optional) Number of ping requests to send.

Value—Integer in the range 1–2000000000 packets

interval interval—(Optional) Interval between ping requests.

Value—Integer in the range 1–2147483647 s

interface interface—(Optional) Interface from which to send a ping request.

Value— Interface name; for example, eth0.

no-resolve—(Optional) Do not display symbolic addresses in command output.

tos tos—(Optional) Value of IP type-of-service byte.

Value—Integer in the range 0–255

ttl ttl—(Optional) Maximum number of hops between the source and the destination.

Value— Number of hops

size size—(Optional) Number of bytes of data to be sent.

Value—Integer in the range 0–65468

Default— 56. This value translates to 64 ICMP bytes that includes the 8 bytes for ICMP header data.

pattern pattern—(Optional) Number of bytes to fill, or pad, the packet to send. You can use this option to diagnose data-dependent problems in a network. For example, pattern ff causes all ones to fill the sent packet.

Value— Hexadecimal fill pattern. Up to 16 bytes to fill the packet to send.

host— IP address or hostname of remote host.

Value— IP address or hostname

Required Privilege Level

network

request disk disable

Syntax

```
request disk disable <device device>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Disable a specified disk in the disk mount.

Options

device device—(Optional) Number assigned to the disk to be disabled, 0 or 1.

Value—Integer in the range 0–1

Default—0

Required Privilege Level

maintenance

request disk enable

Syntax

```
request disk enable <device device>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Enable a a specified disk in the disk mount.

Options

device device—(Optional) Number assigned to the disk to be enabled, 0 or 1.

Value—Integer in the range 0–1

Default—0

Required Privilege Level

maintenance

request disk identify

Syntax

```
request disk identify <device device>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Turn on LED blinking for a specified disk on a C-series Controller to identify which disk is disk 0 and which is disk 1.

Options

device device—(Optional) Number assigned to a disk, 0 or 1.

Value—Integer in the range 0–1

Default—0

Required Privilege Level

maintenance

request disk initialize

Syntax

```
request disk initialize <device device> <force>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Initialize a specified disk in the disk mount.

Options

device device—(Optional) Number assigned to the disk to be initialized, 0 or 1.

Value—Integer in the range 0–1

Default—0

force—(Optional) Initialize a specified disk.

Note:When you run this command and specify a disk that contains data, the command initializes the disk and the data on the disk is lost.

Required Privilege Level

maintenance

request ipmi power

Syntax

```
request ipmi power (on | off | soft-off | reset | cycle)
```

Release Information

Command introduced in SRC Release 3.0.0

Description

Execute an IPMI power command.

Options

Value

- `on`— Power up a C-series Controller.
- `off`— Power down a C-series Controller. This command does not initiate a clean shutdown of the operating system prior to powering down the system.
- `soft-off`— Power down a C-series Controller softly. This command initiates a soft shutdown of the operating system prior to powering down the system.
- `reset`— Perform a hard reset on a C-series Controller.
- `cycle`— Power off and then power on a C-series Controller.

Required Privilege Level

maintenance

request network discovery

Syntax

```
request network discovery network network <community community>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Discover all manageable network elements in an IP subnet. The devices must be online and respond to SNMP queries.

Options

network network— Address of the network to discover

Value— Address in dotted decimal notation

- Individual host—#. #. #. #
- Complete network—#. #. #. #/##

community community—(Optional) Name of SNMP community

Value— SNMP community name

Default—public

Required Privilege Level

network

request security enroll

Syntax

```
request security enroll <subject subject> <password password> url url ca-  
identifier ca-identifier identifier identifier
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Request that the certificate authority (CA) automatically sign the certificate request for the specified subject and challenge password and enroll the certificate through the Simple Certificate Enrollment Protocol (SCEP). Use the `request security get-ca-certificate` command to generate the certificate request.

Options

subject subject—(Optional) Name (as defined in the X.509 standard for public key infrastructure) used in the certificate name field. If you do not specify a value for *subject*, the SRC software uses the unqualified hostname of the system in the format `cn=hostname`. You can specify one subject for a certificate.

Value— Distinguished name in the format: `cn=name`.

Example

```
cn=sdx1,ou=pop,o=Juniper,l=kanata, st=ontario,c=Canada
```

password password—(Optional) Password on the CA for the specified subject. If you do not enter a password, the system prompts you for one.

Value— *password*

url url— URL of certificate authority (which is the SCEP server).

Value— *URL*

ca-identifier ca-identifier— Identifier that designates the certificate authority. Use the value provided by the CA.

Value— *CA identifier*

identifier identifier— Local name of a digital certificate.

Value— *Certificate name*

Required Privilege Level

security

request security generate-certificate-request

Syntax

```
request security generate-certificate-request <subject subject> <password
password> <file-name file-name> <encoding (binary | pem) >
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Create a self-signed certificate and a certificate signing request. You send the the certificate signing request file to a certificate authority (CA) for signing. Use the `request security import-certificate` command to import the issued certificate.

Options

`subject subject`—(Optional) Name (as defined in the X.509 standard for public key infrastructure) used in the certificate name field. If you do not specify a value for `subject`, the SRC software uses the unqualified hostname of the system in the format `cn=hostname`. You can specify one subject for a certificate.

Value— Distinguished name in the format: `cn=name`.

Example

```
cn=sdx1,ou=pop,o=Juniper,l=kanata, st=ontario,c=Canada
```

`password password`—(Optional) Password on the CA for the specified subject. If you do not enter a password, the system prompts you for one.

Value— `password`

`file-name file-name`—(Optional) Name of certificate signing request file. This file is stored in the `/tmp` directory with the file-extension `.csr`.

Value— `filename`

Default—`certreq`

`encoding (binary | pem)` —(Optional) Type of encoding used by the certificate signing

request.

Value

- `binary`— Binary encoding
- `pem`— Privacy enhanced mail encoding

Default—`pem`

Required Privilege Level

security

request security get-ca-certificate

Syntax

```
request security get-ca-certificate url url ca-identifier ca-identifier
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Request a certificate authority (CA) certificate through the Simple Certificate Enrollment Protocol (SCEP). After you request the certificate, use the `request security enroll` command to request digital certificates from this CA.

Options

`url url`— URL of certificate authority (which is the SCEP server).

Value— *URL*

`ca-identifier ca-identifier`— Identifier that designates the certificate authority. The identifier is not the name of the certificate authority.

Value— *Identifier*

Required Privilege Level

security

request security import-certificate

Syntax

```
request security import-certificate file-name file-name identifier identifier
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Import a digital certificate from a file. Run the `request security generate-certificate-request` command first to create a certificate signing request that you manually submit to the CA for signing.

Options

`file-name file-name`— Name of the certificate file.

Value— *filename*

`identifier identifier`— Name of a local digital certificate.

Value— *Certificate name*

Required Privilege Level

security

request support information

Syntax

```
request support information <days> < (acp | activity | agent | cli | appsvr |
diameter | dsa | extsubmon | ims | jdb | jps | licSvr | nic | redir | sae | sic |
webadm) >
```

Release Information

Command introduced in SRC Release 3.1.0

Description

Collects information about components.

Options

days—(Optional) Range of days for which information is collected. Files modified before this range are ignored.

Value—Integer in the range 1–36500

Default—7

(Optional) Components from which diagnostic information will be collected.

Value

- *acp*— Collects information from SRC ACP
- *activity*— Collects information from Activity Monitor
- *agent*— Collects information from the SNMP Agent
- *cli*— Collects information from the CLI
- *appsvr*— Collects information from the Application Server
- *diameter*— Collects information from Diameter application
- *dsa*— Collects information from Dynamic Service Activator
- *extsubmon*— Collects information from External Subscriber Monitor
- *ims*— Collects information from IP Multimedia Subsystem (IMS)
- *jdb*— Collects information from Juniper Networks Database
- *jps*— Collects information from Juniper Policy Server (JPS)
- *licSvr*— Collects information from the license server
- *nic*— Collects information from the Network Information Collector (NIC)
- *redir*— Collects information from the Redirect Server
- *sae*— Collects information from the SAE
- *sic*— Collects information from the SIC

- `webadm`— Collects information from the C-Web interface

Required Privilege Level

view

request system halt

Syntax

```
request system halt <force>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Stop system processes and halt the operating system.

Alias

poweroff

Options

`force`—(Optional) Stop the system without first performing a shutdown.

Required Privilege Level

maintenance

request system install

Syntax

```
request system install url url package package
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Install a specified SRC component.

Options

url url— URL of an SRC installable image. The URL can be one of the following:

- *usb:*—Local USB disk
- *ftp://host/path*—Path on an FTP site or on the local system

Value— URL

package package— Name of the SRC package to install.

Value— Package name

Required Privilege Level

maintenance

request system prepare-partitions

Syntax

```
request system prepare-partitions
```

Description

If you upgrade the system software to SRC Release 3.2.0 or later from earlier releases, you need to change the size of the disk partitions to make room for additional components and the Juniper Networks database. This command only needs to be run once.

Required Privilege Level

No specific privilege required.

request system reboot

Syntax

```
request system reboot <force>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Shut down then restart the C-series Controller.

Options

`force`—(Optional) Restart the C-series Controller without first performing a system shutdown.

Required Privilege Level

maintenance

request system restore

Syntax

```
request system restore
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Restore the root file system from a previously taken snapshot.

Note: The system will reboot twice while the snapshot is being restored.

Required Privilege Level

maintenance

request system snapshot

Syntax

```
request system snapshot <verbose>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Create a backup copy of the root file system.

After you issue the command, you cannot return to the previous version of the software because the running and backup copies of the software are identical.

Options

`verbose`—(Optional) Display detailed messages during the backup process.

Required Privilege Level

maintenance

request system uninstall

Syntax

```
request system uninstall package package
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Remove an SRC package that is installed on the system.

Options

package package— Name of the SRC package to remove.

Value— Package name

Required Privilege Level

maintenance

request system upgrade

Syntax

```
request system upgrade url url <no-reboot>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Upgrade the SRC software.

Options

`url url`— URL of an SRC installable image. The URL can be one of the following:

- `usb:`—Local USB disk
- `ftp://host/path`—Path on an FTP site or on the local system

Value— URL

`no-reboot`—(Optional) Do not reboot after upgrade

Required Privilege Level

maintenance

restart

Syntax

```
restart component component < (gracefully | immediately | soft) >
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Restart an SRC component that is running on the system.

Options

component *component*— Name of SRC component to restart.

Value— Name of component

(Optional) Method to use to restart component.

Value

- *gracefully*— Shutdown the component, then start it again.
- *immediately*— Send a signal kill (SIGKILL) signal to immediately stop the component, then start it again.
- *soft*— Send a signal hangup (SIGHUP) signal to the process for the component to restart the component.

Default—*gracefully*

Required Privilege Level

reset

set cli complete-on-space

Syntax

```
set cli complete-on-space (on | off)
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Set the CLI to complete a partial command entry when you type a space. This command enables command completion for the current user session.

To enable command completion for all user sessions for a specified user, use the **system login user** statement.

Options

Command completion

Value

- **on**— Turn on command completion to allow a space to be used for command completion.
- **off**— Turn off command completion; a space after a partial command name does not complete the command.

Required Privilege Level

No specific privilege required.

set cli directory

Syntax

```
set cli directory directory
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Set the path of the working directory.

Options

directory— Pathname of working directory.

Value— Directory path

Required Privilege Level

No specific privilege required.

set cli language

Syntax

```
set cli language <language>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Set the language and encoding appropriate to your terminal environment.

Options

language—(Optional) Language and encoding.

Value— Language and encoding in the format 2-character language code (lower case)_2-character country code (upper case). encoding. For example, en_US.UTF8.

Default—en_US.UTF8

Required Privilege Level

No specific privilege required.

set cli level

Syntax

```
set cli level (basic | normal | advanced | expert)
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Set the access level for the CLI commands. The access level controls the number of commands and configuration statements accessible to the user.

Options

Editing level

Value

- `basic`— Minimal set of configuration statements and commands. Only the statements that must be configured are visible.
- `normal`— Normal set of configuration statements and commands. The common and basic statements are visible.
- `advanced`— All configuration statements and commands, including the common and basic ones, are visible.
- `expert`— All configuration statements, including common, basic, and internal statements and commands used for debugging are visible.

Required Privilege Level

No specific privilege required.

set cli password

Syntax

```
set cli password
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Change the current password that is used to access the CLI.

Required Privilege Level

No specific privilege required.

set cli prompt

Syntax

```
set cli prompt cli-prompt
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Set the prompt that is displayed within the CLI.

Options

cli-prompt— Characters that appear at the CLI prompt.

Specify the characters \> to have > appear at the end of the prompt in operational mode and # at the end of the prompt in configuration mode.

Value— Text to appear at prompt

Required Privilege Level

No specific privilege required.

set cli screen-length

Syntax

```
set cli screen-length length
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Set the number of lines to appear on the screen.

Options

length— Number of lines to appear on a CLI screen. If the terminal supports reporting the screen size the screen size reported by the terminal takes precedence.

Value—Integer in the range 5–100000

Required Privilege Level

No specific privilege required.

set cli screen-width

Syntax

```
set cli screen-width width
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Set the screen width in number of columns to appear on the screen.

Options

width— Number of columns to appear on a CLI screen. If the terminal supports reporting the screen size the screen size reported by the terminal takes precedence.

Value—Integer in the range 0–100000

Required Privilege Level

No specific privilege required.

set cli terminal

Syntax

```
set cli terminal (ansi | vt100 | xterm | dumb)
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Set the terminal type.

Options

Terminal type

Value

- `ansi`—ANSI-compatible terminal
- `vt100`—VT100-compatible terminal
- `xterm`—Xterm window
- `dumb`—Dumb terminal

Required Privilege Level

No specific privilege required.

set date

Syntax

```
set date time
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Set the system date and time.

Options

time— System date and time.

Value— System date and time in the format YYYYMMDDhhmm.ss in which:

- YYYY—Year. Contains 4 digits.
- mm—Month. A number 1–12.
- DD—Day. A number 1–31
- mm—Minute. A number 0–59.
- ss—Second. A number 0–59.

For example, to enter the time 12:15 and 30 seconds on October 30, 2006 enter 200610301215.30.

Required Privilege Level

maintenance

set date ntp

Syntax

```
set date ntp servers
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Use NTP to set the date and time for the C-series Controller.

Note: For normal operation, we strongly recommended that you configure NTP to maintain local time. For additional information, see the **system ntp** configuration statement.

If NTP is enabled it is not possible to set the time manually.

Options

servers— List of the IP addresses of NTP servers to use.

Value— IP address(es)

Required Privilege Level

maintenance

show cli

Syntax

```
show cli
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display properties that have been set to control the CLI environment.

Required Privilege Level

No specific privilege required.

show cli authorization

Syntax

```
show cli authorization
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Identify the user logged in to the CLI session, and display the user's privilege level, the user's permissions to run specified operational and configuration commands, and the user's authorization to run commands.

Required Privilege Level

No specific privilege required.

show cli directory

Syntax

```
show cli directory
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display the current working directory.

Required Privilege Level

No specific privilege required.

show cli level

Syntax

```
show cli level
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display the current access level.

Required Privilege Level

No specific privilege required.

show component

Syntax

```
show component
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display information and status for SRC components installed.

Required Privilege Level

maintenance

show configuration

Syntax

```
show configuration <object>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display information about the SRC configuration.

Options

object—(Optional) Object for which to display information.

Value—Path of a configuration object

Required Privilege Level

config-view

show date

Syntax

```
show date
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display the time and date set on the system.

Alias

time

Required Privilege Level

No specific privilege required.

show disk status

Syntax

```
show disk status <brief>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display status information.

Options

`brief`—(Optional) Display summary information.

Required Privilege Level

view

show interfaces

Syntax

```
show interfaces <interface-name>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display information about interfaces configured on a C-series Controller, including but not limited to interface address, information about packets sent, and information about packets received.

Options

interface-name—(Optional) Name of an interface

Value— Interface name; for example eth0. If you do not specify an interface name, the command displays information for all interfaces.

Default— No value

Required Privilege Level

network

show ipmi chassis

Syntax

```
show ipmi chassis
```

Release Information

Command introduced in SRC Release 3.0.0

Description

Display IPMI chassis information.

Required Privilege Level

view

show ipmi power

Syntax

```
show ipmi power
```

Release Information

Command introduced in SRC Release 3.0.0

Description

Display the power status (on/off) of a specified C-series Controller through IPMI.

Required Privilege Level

view

show iptables

Syntax

```
show iptables < (nat | filter | mangle) > <reset-counters>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display information about the iptables Linux tool.

Options

(Optional) Type of information to display.

Value

- `nat`— Display information for the nat table for the iptables tool. The nat table provides rules for rewriting packet addresses.
- `filter`— Display information for the filter table for the iptables tool. The filter table provides rules for defining packet filters.
- `mangle`— Display information for the mangle table for the iptables tool. The mangle table provides rules for adjusting packet options, such as quality of service.

`reset-counters`—(Optional) Reset counters of the items in output.

Required Privilege Level

view

show ntp associations

Syntax

```
show ntp associations <no-resolve>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display NTP peers and their state.

Options

`no-resolve`—(Optional) Suppress symbolic addressing.

Required Privilege Level

view

show ntp statistics

Syntax

```
show ntp statistics <no-resolve>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display information about NTP.

Options

`no-resolve`—(Optional) Suppress symbolic addressing.

Required Privilege Level

view

show ntp status

Syntax

```
show ntp status <no-resolve>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display the values of internal variables returned by NTP peers.

Options

`no-resolve`—(Optional) Suppress symbolic addressing.

Required Privilege Level

view

show route

Syntax

```
show route <no-resolve> <detail>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display information from the routing table.

Options

`no-resolve`—(Optional) Do not display symbolic addresses in command output.

`detail`—(Optional) Display detailed output.

Required Privilege Level

network

show security certificate

Syntax

```
show security certificate <trusted>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display information about the certificates stored on the local system.

Options

`trusted`—(Optional) Display information about certificate authority (CA) certificates.

Required Privilege Level

security

show system boot-messages

Syntax

```
show system boot-messages
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display system messages generated during system startup.

Required Privilege Level

view

show system information

Syntax

```
show system information
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display information about the system. The command output includes the system hostname, information about the system hardware, the version of the SRC software installed on the system.

Required Privilege Level

No specific privilege required.

show system snapshot

Syntax

```
show system snapshot
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Show information of existing system snapshot

Required Privilege Level

view

show system users

Syntax

```
show system users <brief> <no-from>
```

Release Information

Command introduced in SRC Release 1.1.0

Description

Show users who are currently logged in

Options

`brief`—(Optional) Use the short format

`no-from`—(Optional) Do not show the FROM field

Required Privilege Level

view

ssh

Syntax

```
ssh host host < (v1 | v2) >
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Open an SSH session to another host.

Options

host host— Hostname or IP address of the remote host. You can specify a username by using the format *user@host* for *host*. If you do not specify a username, the command uses the username of the current user.

Value— Hostname, IP address, *user@hostname*, or *user@IP* address

(Optional) SSH version

Value

- *v1*— Use SSH version 1.
- *v2*— Use SSH version 2.

Default—

Required Privilege Level

network

start shell

Syntax

```
start shell (csh | sh | bash)
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Set type of shell to start.

Options

Type of shell to start.

Value

- `csh`— C shell
- `sh`— Bourne-style shell
- `bash`— GNU Bourne shell

Default—`csh`

Required Privilege Level

shell maintenance

telnet

Syntax

```
telnet host [<port port>]
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Open a Telnet session to another host.

Options

host— Hostname or address of the remote host.

Value— Hostname or IP address

port port—(Optional) Port number or service name on the remote host.

Value— Port number

Required Privilege Level

network

traceroute

Syntax

```
traceroute <gateway gateway> <interface interface> <tos tos> <ttl ttl> <wait wait> <no-resolve> <bypass-routing> <source source> host
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display the route from the local host, interface on the local host, or IP address on the local host to a remote host.

Options

gateway gateway—(Optional) Address of gateway through which route passes.

Value— IP address

interface interface—(Optional) Interface from which to send packets to trace a route. The IP address of this interface is the source IP address in packets sent to trace the route. Typically, you specify either the *interface* or *source* option to obtain the IP address for packets sent on a multi-homed host (a host that has more than one IP address).

Note: Only users with root permissions can execute this command with this option.

Value— Interface name; for example, eth0.

tos tos—(Optional) Value of IP type-of-service byte

Value—Integer in the range 0–255

ttl ttl—(Optional) Maximum number of hops between the source and the destination

Value— Number of hops

wait wait—(Optional) Number of seconds to wait for a response.

Value—Integer in the range 0–600 s

`no-resolve`—(Optional) Do not display symbolic addresses in command output.

`bypass-routing`—(Optional) Do not use the entries in the routing table when traceroute request is sent; use the interface specified by the `interface` option.

`source source`—(Optional) IP address from which to send packets to trace a route. The IP address is included in packets sent to trace the route. Typically, you specify either the `interface` or `source` option to obtain the IP address for packets sent on a multi-homed host (a host that has more than one IP address).

Value— IP address (not a hostname). If you specify an IP address that is not assigned to a system, you receive an error message to the effect that a traceroute request was not sent.

`host`— IP address or hostname of remote host.

Value— IP address or hostname

Required Privilege Level

network

Juniper Networks Database

The following table summarizes the SRC command-line interface (SRC CLI) for the Juniper Networks Database. Configuration statements and operational commands are listed in alphabetical order.

Juniper Networks Database
Configuration Statements
system ldap server
system ldap server community
system ldap server security
Operational Commands
request system ldap change-admin-password
request system ldap change-component-password
request system ldap community force-update
request system ldap community initialize
request system ldap load
request system ldap security export-certificate
show system ldap community
show system ldap statistics

system ldap server

Syntax

```
system ldap server {  
    (stand-alone);  
}
```

Hierarchy Level

```
[edit system ldap server]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Enable the Juniper Networks database to run in standalone mode. This database contains the SRC configuration information.

Typically, you run the database in standalone mode only in testing environments. If you want to run the Juniper Networks database in a community (or group) of databases, use the `system ldap server community` statement.

Enable the Juniper Networks database in either standalone or community mode; a Juniper Networks database can run either standalone or in a community, but not both. If you do not enable the database, it will not run.

Options

Value

- `stand-alone`— Standalone mode for the Juniper Networks database.

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

system ldap server community

Syntax

```
system ldap server community {
    role (primary | secondary);
    primary-neighbors [primary-neighbors...];
    secondary-neighbors [secondary-neighbors...];
}
```

Hierarchy Level

```
[edit system ldap server community]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Enable the Juniper Networks database to operate as part of a community (group) of other Juniper Networks databases. The Juniper Networks database contains the SRC configuration information.

If you want to run the Juniper Networks database standalone, use the `stand-alone` option at the `system ldap server hierarchy` level.

Enable the Juniper Networks database in either standalone or community mode; a Juniper Networks database can run either standalone or in a community, but not both. If you do not enable the database, it will not run.

Options

`role (primary | secondary)`— Role of the database. The role determines the read and write access to the database.

Value

- `primary`— A database that provides read and write access to client applications. It replicates its data and distributes changes to any Juniper Networks databases configured as neighbors.
- `secondary`— A database that provides read access to client applications. If client applications try to write data to this database, the database refers the client to a primary database.

Default— No value

Editing Level—Basic

`primary-neighbors [primary-neighbors...]`—(Optional) A database that propagates changes that it receives to other Juniper Networks databases configured as neighbors. A primary neighbor must be assigned a primary role.

Value— Primary neighbor identified by one of the following:

- IP address; for example, 192.2.4.0
- Hostname that the C-series Controller can resolve through the domain name system; for example, myhostname1
- Fully qualified hostname; for example, myhostname1.mycompany.com

Default— No value

Editing Level—Basic

`secondary-neighbors [secondary-neighbors...]`—(Optional) A database that only receives database changes. A secondary neighbor must be assigned a secondary role.

Value— Secondary neighbor identified by one of the following:

- IP address; for example, 192.2.4.0
- Hostname that the C-series Controller can resolve through the domain name system; for example, myhostname1
- Fully qualified hostname; for example, myhostname1.mycompany.com

Default— No value

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

system ldap server security

Syntax

```
system ldap server security {
    (enable | strict);
}
```

Hierarchy Level

```
[edit system ldap server security]
```

Release Information

Statement introduced in SRC Release 2.0.0

Description

You can secure connections to a Juniper Networks database by:

- Allowing only Secure Lightweight Directory Access Protocol (LDAPS) connections from remote systems. In this case, both database replication and remote SRC components connect through LDAPS. Restricting all remote connections through LDAPS is supported only on C-Series Controllers.
- Allowing only LDAPS connections for database replication, but LDAP or LDAPS connections for other applications. In this case, remote SRC components can connect through LDAP or LDAPS.

To allow access to the Juniper Networks database only through LDAP, use the `delete security` command at the `system ldap server` hierarchy level.

Options

Secure connections to the Juniper Networks database.

Value

- `enable`— Use LDAPS to secure connections to other Juniper Networks databases for data replication.
- `strict`— Use LDAPS to secure remote connections to the Juniper Networks database. Local SRC components have LDAP access the database.

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

request system ldap change-admin-password

Syntax

```
request system ldap change-admin-password new-password new-password
```

Release Information

Command introduced in SRC Release 1.0.1

Description

Change the administrative password for the Juniper Networks database.

Options

new-password new-password— New administrative password for the Juniper Networks database.

Value— *password*

Required Privilege Level

maintenance

request system ldap change-component-password

Syntax

```
request system ldap change-component-password (cli | licenseReader |
licenseWriter | nic | sae | conf) new-password new-password
```

Release Information

Command introduced in SRC Release 2.0.0

Description

Change the password that a specified SRC component uses to communicate with the Juniper Networks database.

Options

Name of an SRC component.

Value

- **cli**— Password that the SRC CLI uses to communicate with the Juniper Networks database.
- **licenseReader**— Password that the SRC license server uses to obtain licensing information from the Juniper Networks database.
- **licenseWriter**— Password that the SRC license server uses to provide licensing information to the Juniper Networks database.
- **nic**— Password that the Network Information Collector (NIC) uses to communicate with the Juniper Networks database.
- **sae**— Password that the SAE uses to communicate with the Juniper Networks database for changes to the following repositories in the database: Users, Services, Policies, and Networks.
- **conf**— Password used to communicate configuration information with the Juniper Networks database.

new-password new-password— New password SRC component

Value— *password*

Required Privilege Level

maintenance

request system ldap community force-update

Syntax

```
request system ldap community force-update neighbor neighbor
```

Release Information

Command introduced in SRC Release 2.0.0

Description

For a specified neighbor, update data that has changed since the neighbor database was last active.

Options

neighbor neighbor— Name of neighbor to be updated.

Value— Neighbor name

Required Privilege Level

maintenance

request system ldap community initialize

Syntax

```
request system ldap community initialize neighbor neighbor
```

Release Information

Command introduced in SRC Release 2.0.0

Description

Initialize data for a specified neighbor in a community of Juniper Networks databases.

Options

neighbor neighbor— Name of the neighbor to initialize.

Value— Neighbor name

Required Privilege Level

maintenance

request system ldap load

Syntax

```
request system ldap load (equipment-registration | isp-service-portal |
enterprise-portal | snmp-agent | dsa-configuration | hostchecker-configuration |
idp-configuration | tm-configuration) < (replace | merge) >
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Load sample data supplied with the SRC software.

Options

Type of data to be loaded.

Value

- `equipment-registration`— Sample data for the sample residential portal to demonstrate an application that provides an association between a subscriber and the equipment being used to make the DHCP connection.
- `isp-service-portal`— Sample data for the sample residential portal to demonstrate an application that provides a means for subscribers to directly log in to a subscriber session for their ISP.
- `enterprise-portal`— Sample data for the Enterprise Manager Portal and the sample enterprise service portal.
- `snmp-agent`— Sample data for SNMP traps for SNMP agent.
- `dsa-configuration`— Sample data for the Dynamic Service Activator.
- `hostchecker-configuration`— Sample data Instant Virtual Extremity (IVE) Host Checker integration application.
- `idp-configuration`— Sample data for the Intrusion Detection and Prevention (IDP) integration application.
- `tm-configuration`— Sample data for the traffic mirroring application.

(Optional) Replace all existing entries or only new entries. If it is first time to load one specific ldap sample data, the choice of replace or merge would make no difference.

Value

- `replace`— Replace all existing entries or adding new entries from a given Idif file
- `merge`— Replace only deleted entries or adding new entries from a given Idif file

Default— `merge`

Required Privilege Level

`maintenance`

request system ldap security export-certificate

Syntax

```
request system ldap security export-certificate file-name file-name
```

Release Information

Command introduced in SRC Release 3.0.0

Description

Export LDAP server CA certificate.

Options

file-name file-name— Name of the certificate file

Value—Text

Required Privilege Level

maintenance

show system ldap community

Syntax

```
show system ldap community
```

Release Information

Command introduced in SRC Release 2.0.0

Description

Display statistics for a community of Juniper Networks databases.

Required Privilege Level

view

show system ldap statistics

Syntax

```
show system ldap statistics
```

Release Information

Command introduced in SRC Release 2.0.0

Description

Display local operation statistics for the Juniper Networks database.

Required Privilege Level

view

SAE

The following table summarizes the SRC command-line interface (SRC CLI) for the SAE. Configuration statements and operational commands are listed in alphabetical order.

SAE
Configuration Statements
shared_auth-cache_cached-dhcp-profile
shared_classification-script_dhcp_classifier
shared_classification-script_dhcp_classifier_name_dhcp-classifier_rule
shared_classification-script_dhcp_classifier_name_dhcp-classifier_rule_name_condition
shared_classification-script_dhcp_classifier_name_dhcp-classifier_rule_name_script
shared_classification-script_interface_classifier
shared_classification-script_interface_classifier_name_interface-classifier_rule
shared_classification-script_interface_classifier_name_interface-classifier_rule_name_condition
shared_classification-script_interface_classifier_name_interface-classifier_rule_name_script
shared_classification-script_subscriber_classifier
shared_classification-script_subscriber_classifier_name_subscriber-classifier_rule
shared_classification-script_subscriber_classifier_name_subscriber-classifier_rule_name_condition
shared_classification-script_subscriber_classifier_name_subscriber-classifier_rule_name_script
shared_network_application-manager-group
shared_network_device
shared_network_device_name_interface-classifier_rule
shared_network_device_name_interface-classifier_rule_name_condition
shared_network_device_name_interface-classifier_rule_name_script
shared_network_device_name_virtual-router
shared_network_policy-decision-point
shared_sae_configuration

shared_sae_configuration_aggregate-services
shared_sae_configuration_driver
shared_sae_configuration_driver_aaa
shared_sae_configuration_driver_aaa_session-store
shared_sae_configuration_driver_junos
shared_sae_configuration_driver_junos_configuration-checking
shared_sae_configuration_driver_junos_lsp-tracking
shared_sae_configuration_driver_junos_security
shared_sae_configuration_driver_junos_session-store
shared_sae_configuration_driver_junos-ise
shared_sae_configuration_driver_junos-ise_session-store
shared_sae_configuration_driver_junos-ptsp
shared_sae_configuration_driver_junos-ptsp_session-store
shared_sae_configuration_driver_junose
shared_sae_configuration_driver_junose_session-store
shared_sae_configuration_driver_pcmm
shared_sae_configuration_driver_pcmm_cmts-specific-rks-plugin-ins
shared_sae_configuration_driver_pcmm_session-store
shared_sae_configuration_driver_scripts
shared_sae_configuration_driver_session-store
shared_sae_configuration_driver_simulated
shared_sae_configuration_driver_simulated_name_session-store
shared_sae_configuration_driver_snmp
shared_sae_configuration_driver_third-party
shared_sae_configuration_driver_third-party_session-store
shared_sae_configuration_dynamic-radius-server
shared_sae_configuration_external-interface-features

shared_sae_configuration_external-interface-features_name_CommunityManager
shared_sae_configuration_external-interface-features_name_EventAPI
shared_sae_configuration_external-interface-features_name_JavaScriptProcessor
shared_sae_configuration_external-interface-features_name_PythonScriptProcessor
shared_sae_configuration_external-interface-features_name_SAEAccess
shared_sae_configuration_external-interface-features_name_SAEFeature
shared_sae_configuration_external-interface-features_name_SAEFeature_properties
shared_sae_configuration_file-accounting-template
shared_sae_configuration_file-accounting-template_name_attributes
shared_sae_configuration_global-radius-udp-port
shared_sae_configuration_idle-timeout
shared_sae_configuration_interim-accounting
shared_sae_configuration_interim-session-job-manager
shared_sae_configuration_ldap
shared_sae_configuration_ldap_directory-eventing
shared_sae_configuration_ldap_persistent-login-cache
shared_sae_configuration_ldap_policy-data
shared_sae_configuration_ldap_service-data
shared_sae_configuration_ldap_subscriber-data
shared_sae_configuration_license-manager_client
shared_sae_configuration_license-manager_directory-access
shared_sae_configuration_logger
shared_sae_configuration_logger_name_file
shared_sae_configuration_logger_name_syslog
shared_sae_configuration_login-registration
shared_sae_configuration_nic-proxy-configuration
shared_sae_configuration_nic-proxy-configuration_name_cache

shared_sae_configuration_nic-proxy-configuration_name_nic-host-selection
shared_sae_configuration_nic-proxy-configuration_name_nic-host-selection_blacklisting
shared_sae_configuration_nic-proxy-configuration_name_resolution
shared_sae_configuration_nic-proxy-configuration_name_test-nic-bindings
shared_sae_configuration_nic-proxy-configuration_name_test-nic-bindings_key-values
shared_sae_configuration_plugin-ins
shared_sae_configuration_plugin-ins_event-publishers
shared_sae_configuration_plugin-ins_event-publishers_device-type-authentication
shared_sae_configuration_plugin-ins_manager
shared_sae_configuration_plugin-ins_name
shared_sae_configuration_plugin-ins_name_name_acp-interface-listener
shared_sae_configuration_plugin-ins_name_name_custom-radius-accounting
shared_sae_configuration_plugin-ins_name_name_custom-radius-accounting_peer-group
shared_sae_configuration_plugin-ins_name_name_custom-radius-authentication
shared_sae_configuration_plugin-ins_name_name_custom-radius-authentication_peer-group
shared_sae_configuration_plugin-ins_name_name_ejb-adaptor
shared_sae_configuration_plugin-ins_name_name_external
shared_sae_configuration_plugin-ins_name_name_file-accounting
shared_sae_configuration_plugin-ins_name_name_flex-radius-accounting
shared_sae_configuration_plugin-ins_name_name_flex-radius-accounting_peer-group
shared_sae_configuration_plugin-ins_name_name_flex-radius-accounting_radius-packet-definition
shared_sae_configuration_plugin-ins_name_name_flex-radius-accounting_radius-packet-definition_name_attributes
shared_sae_configuration_plugin-ins_name_name_flex-radius-accounting_radius-packet-definition_name_vendor-specific
shared_sae_configuration_plugin-ins_name_name_flex-radius-accounting_radius-packet-definition_name_vendor-specific_name_attributes
shared_sae_configuration_plugin-ins_name_name_flex-radius-accounting_radius-packet-definition_name_vendor-specific_name_type

[shared sae configuration plug-ins name name flex-radius-accounting radius-packet-definition name vendor-specific name type name attributes](#)

[shared sae configuration plug-ins name name flex-radius-accounting radius-packet-definition name vendor-specific-26](#)

[shared sae configuration plug-ins name name flex-radius-accounting radius-packet-definition name vendor-specific-26 name attributes](#)

[shared sae configuration plug-ins name name flex-radius-accounting radius-packet-definition name vendor-specific-26 name type](#)

[shared sae configuration plug-ins name name flex-radius-accounting radius-packet-definition name vendor-specific-26 name type name attributes](#)

[shared sae configuration plug-ins name name flex-radius-authentication](#)

[shared sae configuration plug-ins name name flex-radius-authentication_peer-group](#)

[shared sae configuration plug-ins name name flex-radius-authentication radius-packet-definition](#)

[shared sae configuration plug-ins name name flex-radius-authentication radius-packet-definition name attributes](#)

[shared sae configuration plug-ins name name flex-radius-authentication radius-packet-definition name vendor-specific](#)

[shared sae configuration plug-ins name name flex-radius-authentication radius-packet-definition name vendor-specific name attributes](#)

[shared sae configuration plug-ins name name flex-radius-authentication radius-packet-definition name vendor-specific name type](#)

[shared sae configuration plug-ins name name flex-radius-authentication radius-packet-definition name vendor-specific name type name attributes](#)

[shared sae configuration plug-ins name name flex-radius-authentication radius-packet-definition name vendor-specific-26](#)

[shared sae configuration plug-ins name name flex-radius-authentication radius-packet-definition name vendor-specific-26 name attributes](#)

[shared sae configuration plug-ins name name flex-radius-authentication radius-packet-definition name vendor-specific-26 name type](#)

[shared sae configuration plug-ins name name flex-radius-authentication radius-packet-definition name vendor-specific-26 name type name attributes](#)

[shared sae configuration plug-ins name name interface-subscriber-limit](#)

[shared sae configuration plug-ins name name internal](#)

<u>shared_sae_configuration Plug-ins name name internal_properties</u>
<u>shared_sae_configuration Plug-ins name name jms-adaptor</u>
<u>shared_sae_configuration Plug-ins name name ldap-authentication</u>
<u>shared_sae_configuration Plug-ins name name pcmm-rks</u>
<u>shared_sae_configuration Plug-ins name name pcmm-rks_peer-group</u>
<u>shared_sae_configuration Plug-ins name name qos-profile-tracking</u>
<u>shared_sae_configuration Plug-ins name name radius-accounting</u>
<u>shared_sae_configuration Plug-ins name name radius-accounting_peer-group</u>
<u>shared_sae_configuration Plug-ins name name radius-authentication</u>
<u>shared_sae_configuration Plug-ins name name radius-authentication_peer-group</u>
<u>shared_sae_configuration Plug-ins name name schedule-authorization</u>
<u>shared_sae_configuration Plug-ins name name ssr-reader</u>
<u>shared_sae_configuration Plug-ins state-synchronization</u>
<u>shared_sae_configuration policy-management-configuration</u>
<u>shared_sae_configuration radius-packet-template</u>
<u>shared_sae_configuration radius-packet-template name radius-attributes</u>
<u>shared_sae_configuration radius-packet-template name radius-attributes name attributes</u>
<u>shared_sae_configuration radius-packet-template name radius-attributes name vendor-specific</u>
<u>shared_sae_configuration radius-packet-template name radius-attributes name vendor-specific name attributes</u>
<u>shared_sae_configuration radius-packet-template name radius-attributes name vendor-specific name type</u>
<u>shared_sae_configuration radius-packet-template name radius-attributes name vendor-specific name type name attributes</u>
<u>shared_sae_configuration radius-packet-template name radius-attributes name vendor-specific-26</u>
<u>shared_sae_configuration radius-packet-template name radius-attributes name vendor-specific-26 name attributes</u>
<u>shared_sae_configuration radius-packet-template name radius-attributes name vendor-specific-26 name type</u>

shared sae configuration radius-packet-template name radius-attributes name vendor-specific-26 name type name attributes
shared sae configuration script-extension
shared sae configuration service-activation
shared sae configuration service-schedule
shared sae configuration session-job-manager
shared sae configuration subscriber-sessions
shared sae configuration time-based-policies
shared sae configuration timeout-session-job-manager
shared sae dhcp-classifier rule
shared sae dhcp-classifier rule name condition
shared sae dhcp-classifier rule name script
shared sae group
shared sae subscriber-classifier rule
shared sae subscriber-classifier rule name condition
shared sae subscriber-classifier rule name script
slot number sae
slot number sae initial
slot number sae initial directory-connection
slot number sae initial directory-eventing
slot number sae radius
Operational Commands
clear sae directory-blacklist
clear sae registered equipment
clear sae registered login
monitor sae statistics sessions
request sae load configuration

request sae load domain-map
request sae load interface-classification
request sae load services
request sae load subscriptions
request sae login ip authenticated-dhcp
request sae login ip authenticated-interface
request sae login ip unauthenticated-dhcp
request sae login ip unauthenticated-interface
request sae logout dn
request sae logout ip
request sae logout login-name
request sae logout session-id
request sae modify device failover
request sae shutdown device
request sae update ip-pools
request sae update qos-profiles
show sae directory-blacklist
show sae drivers
show sae interfaces
show sae policies
show sae registered equipment
show sae registered login
show sae services
show sae statistics device
show sae statistics device common
show sae statistics directory
show sae statistics directory connections

<u>show sae statistics license client</u>
<u>show sae statistics license device</u>
<u>show sae statistics license local</u>
<u>show sae statistics policy-management</u>
<u>show sae statistics process</u>
<u>show sae statistics radius</u>
<u>show sae statistics radius client</u>
<u>show sae statistics sessions</u>
<u>show sae subscribers</u>
<u>show sae subscribers dn</u>
<u>show sae subscribers ip</u>
<u>show sae subscribers login-name</u>
<u>show sae subscribers service-name</u>
<u>show sae subscribers session-id</u>
<u>show sae threads</u>

shared auth-cache cached-dhcp-profile

Syntax

```
shared auth-cache cached-dhcp-profile name {
    description description;
    pool-name pool-name;
    ip-address ip-address;
    dhcp-options dhcp-options;
    boot-server-name boot-server-name;
    boot-file-name boot-file-name;
    virtual-router virtual-router;
    local-interface local-interface;
    lease-time lease-time;
    user-name user-name;
    service-bundle service-bundle;
    radius-class radius-class;
}
```

Hierarchy Level

```
[edit shared auth-cache cached-dhcp-profile]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a cached DHCP profile.

Options

name name— Name of a cached DHCP profile.

Value— String

description description—(Optional) Description of the DHCP client device.

Value— String

Default— No value

Editing Level—Basic

`pool-name` *pool-name*—(Optional) Name of the IP address pool on the JUNOS router from which a DHCP address is selected.

Value— String

Default— No value

Editing Level—Basic

`ip-address` *ip-address*—(Optional) Fixed IP address that is offered to the DHCP client if the client is part of a network in the configured DHCP pool.

Value— IP address

Default— No value

Editing Level—Basic

`dhcp-options` *dhcp-options*—(Optional) Defines DHCP options that are used to configure DHCP clients.

Value— Define DHCP options in the format: option=value [,value...].

where option is the DHCP option name or number (see the customer documentation for a list of supported DHCP options) and values are entered based on the type of option:

- int32, int16, int8—Decimal or hex prefixed by 0x
- string—Optionally surrounded by double quotes
- ip-address—Dotted decimal
- data-string—Sequence of hex-encoded bytes separated by a : (colon) or a string surrounded by double quotes

Separate multiple options by line breaks.

Value is a string containing one or more options defined as 'name=value'. Multiple options are separated by line breaks.

To include nonstandard options in a DHCP profile, use the name option-*nnn*, where *nnn* is the option number, and the value is of type data-string; that is, either a string surrounded in double quotes, or a sequence of hex-encoded bytes, separated by a colon (:).

Default— No value

Editing Level—Basic

`boot-server-name` *boot-server-name*—(Optional) Name of the server used to boot the DHCP client.

Value— String, length < 64

Default— No value
Editing Level—Basic

`boot-file-name` *boot-file-name*—(Optional) Name of a boot file used to boot the DHCP client.

Value— String, length < 128
Default— No value
Editing Level—Basic

`virtual-router` *virtual-router*—(Optional) Name of the virtual router that holds the IP address pool.

Value— Name of the virtual router in the format *vrname@hostname*. An * (asterisk) means that the values for the virtual router are ignored when the cached profile is used. Use an * if you do not know the virtual router to which the subscriber will connect.
Default— No value
Editing Level—Basic

`local-interface` *local-interface*—(Optional) Name of the JUNOSe router interface that will receive the DHCP client device's request for an IP address.

Value— Name of the virtual router in the format *vrname@hostname*. An * (asterisk) means that the values for local interface are ignored when the cached profile is used. Use an * if you do not know the interface to which the subscriber will connect or if you want to allow the subscriber to connect through multiple interfaces.
Default— No value
Editing Level—Basic

`lease-time` *lease-time*—(Optional) Length of time the supplied IP address is valid. This parameter is not currently implemented on the JUNOSe router. The DHCP lease time that the SAE sends to the JUNOSe router is ignored.

Value— Number of seconds
Default— No value
Editing Level—Basic

`user-name` *user-name*—(Optional) Username of the DHCP subscriber without the domain name.

Value— String that specifies the information to the left of the @ character in *userName@domainName*.
Default— No value
Editing Level—Basic

`service-bundle` *service-bundle*—(Optional) Vendor-specific RADIUS attribute that specifies the SRC service bundle to use.

Value— String

Default— No value

Editing Level—Basic

`radius-class` *radius-class*—(Optional) RADIUS attribute class.

Value— String

Default— No value

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared classification-script dhcp classifier

Syntax

```
shared classification-script dhcp classifier name {
    description description;
}
```

Hierarchy Level

```
[edit shared classification-script dhcp classifier]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a subscriber classifier. For more information about subscriber classifiers, see the *SRC PE Subscribers and Subscription Guide*.

Options

`name name`— Name of the classification script

Value— Text

`description description`—(Optional) Description of the classification script.

Value— Text

Default— No value

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared classification-script dhcp classifier *name* dhcp-classifier rule

Syntax

```
shared classification-script dhcp classifier name dhcp-classifier rule name {
    target target;
}
```

Hierarchy Level

```
[edit shared classification-script dhcp classifier name dhcp-classifier rule]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify a script for a rule in a classification script. Classification scripts are organized into rules. Each rule has a target and one or more match conditions.

Options

name name— Rule in a classification script

Value—Text

target target—(Optional) Result of the classification script that is returned to the SAE.

Value— The result depends on the type of classification script:

- Subscriber classification script—An LDAP query that uniquely identifies a subscriber entry in the directory.
- DHCP classification script—DHCP profile.

Default— Not applicable

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared classification-script dhcp classifier *name* dhcp-classifier rule *name* condition

Syntax

```
shared classification-script dhcp classifier name dhcp-
classifier rule name condition name ...
```

Hierarchy Level

```
[edit shared classification-script dhcp classifier name dhcp-
classifier rule name condition]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure match conditions used to find a target. You can configure multiple conditions for each classifier rule.

Options

name name— Match conditions used to find a target. For information about configuring match conditions, see *Classifying Interfaces and Subscribers with the SRC CLI* in *SRC PE Subscribers and Subscriptions Guide*.

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared classification-script dhcp classifier *name* dhcp-classifier rule *name* script

Syntax

```
shared classification-script dhcp classifier name dhcp-
classifier rule name script {
    script-value;
}
```

Hierarchy Level

```
[edit shared classification-script dhcp classifier name dhcp-
classifier rule name script]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a classification script rule to use a script target.

Options

script-value—(Optional) Script target. The content of the script rule is interpreted when the classifier is initially loaded. The script rule can contain definitions of custom functions, which can be called during the matching process. Because you can insert arbitrary code into a script, you can use classification scripts to perform arbitrary tasks. Because script targets use asterisks, you cannot use asterisks in other types of targets.

Value— Script enclosed in quotation marks

Default— No value

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared classification-script interface classifier

Syntax

```
shared classification-script interface classifier name {
    description description;
}
```

Hierarchy Level

```
[edit shared classification-script interface classifier]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an interface classifier. For more information about subscriber classifiers, see the *SRC PE Subscribers and Subscription Guide*.

Options

name name— Name of the classification script

Value— Text

description description—(Optional) Description of the classification script.

Value— Text

Default— No value

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared classification-script interface classifier *name* interface-classifier rule

Syntax

```
shared classification-script interface classifier name interface-
classifier rule name {
    target target;
}
```

Hierarchy Level

```
[edit shared classification-script interface classifier name interface-
classifier rule]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an interface classification rule

Options

name name— Name of the rule in the interface classification script

Value— Text

target target—(Optional) Result of the classification script that gets returned to the SAE.

Value— Path to a policy group. For example, /sample/junose/DHCP.

Default— No value

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared classification-script interface classifier *name* interface-classifier rule *name* condition

Syntax

```
shared classification-script interface classifier name interface-
classifier rule name condition name ...
```

Hierarchy Level

```
[edit shared classification-script interface classifier name interface-
classifier rule name condition]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure match conditions used to find a target. You can configure multiple conditions for each classifier rule.

Options

name name— Match conditions used to find a target. For more information about configuring match conditions, see *Classifying Interfaces and Subscribers with the SRC CLI* in *SRC PE Subscribers and Subscriptions Guide*.

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared classification-script interface classifier *name* interface-classifier rule *name* script

Syntax

```
shared classification-script interface classifier name interface-
classifier rule name script {
    script-value;
}
```

Hierarchy Level

```
[edit shared classification-script interface classifier name interface-
classifier rule name script]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a classification script rule to use a script target.

Options

script-value—(Optional) Script target. A script that can contain definitions of custom functions that can be called during the matching process. The complete content of the script is interpreted when the classifier is initially loaded. Because you can insert code into a script target, you can use the classification script to perform various tasks.

Value— Script enclosed in quotation marks.

Default— No value

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared classification-script subscriber classifier

Syntax

```
shared classification-script subscriber classifier name {
    description description;
}
```

Hierarchy Level

```
[edit shared classification-script subscriber classifier]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a subscriber classifier. For more information about subscriber classifiers, see the *SRC PE Subscribers and Subscription Guide*.

Options

name name— Name of the classification script

Value— Text

description description—(Optional) Description of the classification script.

Value— Text

Default— No value

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared classification-script subscriber classifier *name* subscriber-classifier rule

Syntax

```
shared classification-script subscriber classifier name subscriber-
classifier rule name {
    target target;
}
```

Hierarchy Level

```
[edit shared classification-script subscriber classifier name subscriber-
classifier rule]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify a script for a rule in a classification script. Classification scripts are organized into rules. Each rule has a target and one or more match conditions.

Options

name name— Rule in a classification script

Value—Text

target target—(Optional) Result of the classification script that is returned to the SAE.

Value— The result depends on the type of classification script:

- Subscriber classification script—An LDAP query that uniquely identifies a subscriber entry in the directory.
- DHCP classification script—DHCP profile.

Default— Not applicable

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared classification-script subscriber classifier *name* subscriber-classifier rule *name* condition

Syntax

```
shared classification-script subscriber classifier name subscriber-
classifier rule name condition name ...
```

Hierarchy Level

```
[edit shared classification-script subscriber classifier name subscriber-
classifier rule name condition]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure match conditions used to find a target. You can configure multiple conditions for each classifier rule.

Options

name name— Match conditions used to find a target. For information about configuring match conditions, see *Classifying Interfaces and Subscribers with the SRC CLI* in *SRC PE Subscribers and Subscriptions Guide*.

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared classification-script subscriber classifier *name* subscriber-classifier rule *name* script

Syntax

```
shared classification-script subscriber classifier name subscriber-
classifier rule name script {
    script-value;
}
```

Hierarchy Level

```
[edit shared classification-script subscriber classifier name subscriber-
classifier rule name script]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a classification script rule to use a script target.

Options

script-value—(Optional) Script target. The content of the script rule is interpreted when the classifier is initially loaded. The script rule can contain definitions of custom functions, which can be called during the matching process. Because you can insert arbitrary code into a script, you can use classification scripts to perform arbitrary tasks. Because script targets use asterisks, you cannot use asterisks in other types of targets.

Value— Script enclosed in quotation marks

Default— No value

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared network application-manager-group

Syntax

```
shared network application-manager-group name {
    description description;
    application-manager-id application-manager-id;
    connected-sae [connected-sae...];
    pdp-group pdp-group;
    local-address-pools [local-address-pools...];
    managing-sae-ior managing-sae-ior;
}
```

Hierarchy Level

```
[edit shared network application-manager-group]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure application managers for the Juniper policy server (JPS).

Options

name name— Name of application manager group.

Value— Text string

description description—(Optional) Information about the SAE community.

Value— Text string

Default— No value

Editing Level—Basic

application-manager-id application-manager-id— Unique identifier within the domain of the service provider for the application manager that handles the service session; used to specify the application manager identifier (AMID) that is included in all messages sent to and from the policy server.

This option is required. The SAE constructs the AMID value by concatenating two fields: Application Manager Tag (this option) and Application Type (this value is obtained from a

service during activation).

Value— 2-byte unsigned integer

Default— No value

Editing Level—Basic

`connected-sae [connected-sae...]`— SAEs that are connected to the specified policy server group (PDP Group). This list becomes the community of SAEs.

This option is required. When you modify a community, wait for passive session stores of the new community members to be updated before you shut down the current active SAE.

Otherwise, a failover from the current active SAE to the new member is triggered immediately, and the new member's session store may not have received all data from the active SAE's session store.

Value— IP address or hostname

Default— No value

Editing Level—Basic

`pdp-group pdp-group`— Name of the policy server group associated with this SAE community.

Value— Text string

Default— No value

Editing Level—Basic

`local-address-pools [local-address-pools...]`—(Optional) List of IP address pools that this PDP group currently manages and stores. You must configure a local address pool if you are using the NIC so that the NIC can resolve the IP-to-SAE mapping.

Value— An address pool is specified by a sequence of zero or more address sets enclosed in parentheses (). An address set can be either a range of addresses or a subnetwork with or without address exclusions.

- Specify a range by entering a start and end address separated by a space and enclosed in square brackets. For example, `[10.10.10.5 10.10.10.250]` denotes the address set 10.10.10.5 to 10.10.10.250 inclusive.
- Specify a subnet with optional address exclusions in curly brackets. You must include a base address and a mask or prefix length separated by a forward slash. To exclude addresses, follow the forward slash with a comma and a comma-separated list of excluded addresses. For example:
 - `{10.20.20.0/24}` denotes all addresses that start with 10.20.20
 - `{10.21.0.0/255.255.0.0}` denotes all addresses that start with 10.21
 - `{10.20.30.0/24,10.20.30.0,10.20.30.255}` denotes all addresses that start with 10.20.30 except 10.20.30.0 and 10.20.30.255

Default— No value
Editing Level—Basic

`managing-sae-ior` *managing-sae-ior*—(Optional) Common Object Request Broker Architecture (CORBA) reference for the SAE managing this policy server group. The `amlorPublisher` script provides this information when the SAE connects to the policy server. If you do not select this script when configuring initialization scripts, enter a value.

Value— One of the following items:

- The actual CORBA reference for the SAE
- The absolute path to the interoperable object reference (IOR) file
- A corbaloc URL in the form `corbaloc::<host>:8801/SAE`
 - `<host>`—Name or IP address of the SAE host

The following examples show different CORBA references.

- Absolute path—`/opt/UMC/sae/var/run/sae.ior`
- corbaloc URL—`boston:8801/sae`
- Actual IOR—
`IOR:0000000000000002438444C3A736D67742E6A756E697...`

Default— No value
Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared network device

Syntax

```
shared network device name {
    description description;
    management-address management-address;
    device-type (junose | junos-ise | junos-ptsp | junos | pcmm | third-party);
    origin-host origin-host;
    qos-profile [qos-profile...];
    peers [peers...];
}
```

Hierarchy Level

```
[edit shared network device]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a device that the SAE manages.

Options

name name— Name of the router or other device that the SAE manages.

Value— Text; must use lowercase characters

description description—(Optional) Description of the device that the SAE manages.

Value— Text

Default— No value

Editing Level—Basic

management-address management-address—(Optional) IP address of the device. For networks with JUNOSE routers, the redirect component in redundant mode uses this address to send SNMP set messages to set a static route to the new redirect server after a failover.

Value— IP address

Default— No value

Editing Level—Basic

`device-type` (`junose` | `junos-ise` | `junos-ptsp` | `junos` | `pcmm` | `third-party`)—(Optional) Type of device that you are configuring.

Value

- `junose`— JUNOSe router
- `junos-ise`— Intelligent service edge
- `junos-ptsp`— Packet trigger subscriber policy
- `junos`— JUNOS routing platform
- `pcmm`— CMTS device
- `third-party`— Third-party device

Default— No value

Editing Level—Basic

`origin-host` *origin-host*—(Optional) Devices managed through Diameter are identified through their origin host. If the origin-host is not specified, it defaults to the device name.

Value—Text

Editing Level—Basic

`qos-profile` [*qos-profile...*]—(Optional) For JUNOSe routers, specifies quality of service (QoS) profiles that are configured on the router.

Value— Single QoS profile or a list of QoS profiles

Default— No value

Editing Level—Basic

`peers` [*peers...*]—(Optional) Peers.

Value—Text

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared network device *name* interface-classifier rule

Syntax

```
shared network device name interface-classifier rule name {
    target target;
}
```

Hierarchy Level

```
[edit shared network device name interface-classifier rule]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an interface classification rule.

Options

name name— Name of the rule in the interface classification script.

Value— Text

target target—(Optional) Result of the classification script that gets returned to the SAE.

Value— Path to a policy group. For example, /sample/junose/DHCP.

Default— No value

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared network device *name* interface-classifier rule *name* condition

Syntax

```
shared network device name interface-classifier rule name condition name ...
```

Hierarchy Level

```
[edit shared network device name interface-classifier rule name condition]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure match conditions used to find a target. You can configure multiple conditions for each classifier rule.

Options

name name— Match conditions used to find a target. For more information about configuring match conditions, see *Classifying Interfaces and Subscribers with the SRC CLI* in *SRC PE Subscribers and Subscriptions Guide*.

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared network device *name* interface-classifier rule *name* script

Syntax

```
shared network device name interface-classifier rule name script {
    script-value;
    include include;
}
```

Hierarchy Level

```
[edit shared network device name interface-classifier rule name script]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an interface classifier for a network device. For more information about interface classifiers, see the *SRC PE Subscribers and Subscriptions Guide*.

Options

script-value—(Optional) Script target. A script that can contain definitions of custom functions that can be called during the matching process. The complete content of the script is interpreted when the classifier is initially loaded. Because you can insert code into a script target, you can use the classification script to perform various tasks.

Value— Script enclosed in quotation marks.

Default— No value

Editing Level—Basic

include include—(Optional) Name of an existing script to include in the script you are configuring.

Value— *script-name*

Default— No value

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared network device *name* virtual-router

Syntax

```
shared network device name virtual-router name {
    sae-connection [sae-connection...];
    snmp-read-community snmp-read-community;
    snmp-write-community snmp-write-community;
    scope [scope...];
    local-address-pools local-address-pools;
    static-address-pools static-address-pools;
    tracking-plug-in [tracking-plug-in...];
    authentication-plug-in [authentication-plug-in...];
    vpn-id (VRF);
}
```

Hierarchy Level

```
[edit shared network device name virtual-router]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a virtual router object.

Options

name name— Name of the virtual router.

Value— One of the following:

- For JUNOSe routers, the name of the VR, which is case sensitive, must exactly match the name of the VR configured on the router.
- For JUNOS routing platforms, CMTS devices, and other third-party devices, use the name default

sae-connection [sae-connection...]—(Optional) IP addresses of the SAEs that can manage this device. This option is required for the SAE to work with the router.

To specify the active SAE and the standby SAE, enter an exclamation point (!) after the hostname or IP address of the SAEs.

Value— IP address or a list of IP addresses

Specify the active SAE and the redundant SAE by entering an exclamation point (!) after the hostname or IP address of the connected SAEs. For example: 10.3.219.10! 10.3.219.20!

Default— No value

Editing Level—Basic

`snmp-read-community snmp-read-community`—(Optional) SNMP community name associated with SNMP read-only operations for this virtual router. Read operations are typically used by router initialization scripts to read information, such as IP address pools, from the router.

Value— Text

Default— No value

Editing Level—Basic

`snmp-write-community snmp-write-community`—(Optional) SNMP community name associated with SNMP write operations for this virtual router. The write community is used only by the redirect server to set a static route.

Value— Text

Default— No value

Editing Level—Basic

`scope [scope...]`—(Optional) The virtual router can be associated with a number of service scopes. The scopes are available for subscribers connected to this virtual router for selecting customized versions of services.

Value— Text

Default— No value

Editing Level—Basic

`local-address-pools local-address-pools`—(Optional) For JUNOS virtual routers, address of local address pools on the JUNOS virtual router.

- If you do not configure the PoolPublisher router initialization script for a JUNOS virtual router, configure this option for a JUNOS virtual router.
- If you do configure the PoolPublisher router initialization script for a JUNOS virtual router, configure this option if pool data needs to be updated. This data needs to be updated if you change the address pools on a virtual router that is actively being managed by SAE. The reason is that the initialization script is triggered only when the COPS connection is started.

For CMTS devices, you must configure either a local address pool or a static address pool so

that the NIC can resolve the IP-to-SAE mapping.

Value— An address pool is specified by a sequence of zero or more address sets enclosed in parentheses (). An address set can be either a range of addresses or a subnetwork with or without address exclusions.

- Specify a range by entering a start and end address separated by a space and enclosed in square brackets. For example, [10.10.10.5 10.10.10.250] denotes the address set 10.10.10.5 to 10.10.10.250 inclusive.
- Specify a subnet with optional address exclusions in curly brackets. You must include a base address and a mask or prefix length separated by a forward slash. To exclude addresses, follow the forward slash with a comma and a comma-separated list of excluded addresses. For example:
 - {10.20.20.0/24} denotes all addresses that start with 10.20.20
 - {10.21.0.0/255.255.0.0} denotes all addresses that start with 10.21
 - {10.20.30.0/24,10.20.30.0,10.20.30.255} denotes all addresses that start with 10.20.30 except 10.20.30.0 and 10.20.30.255

Default— No value

Editing Level—Basic

`static-address-pools static-address-pools`—(Optional) IP address pools that a JUNOS virtual router manages but does not store on the router because the router is not managing the allocation of these addresses. For CMTS devices, you must configure either a local address pool or a static address pool so that the NIC can resolve the IP-to-SAE mapping.

Value—

Default— No value

Editing Level—Basic

`tracking-plugin-in [tracking-plugin-in...]`—(Optional) List of plug-ins that are notified of interface events for this virtual router.

Value— Single tracking plug-in or a list of tracking plug-ins

Default— No value

Editing Level—Basic

`authentication-plugin-in [authentication-plugin-in...]`—(Optional) List of plug-ins that are notified of interface events for this virtual router.

Value— Single authentication plug-in or a list of authentication plug-ins

Default— No value

Editing Level—Basic

`vpn-id (VRF)`—(Optional) If the VPN identifier is set to "VRF", then the VRF name reported by the device is used as the VPN identifier for subscriber sessions. Otherwise the VPN identifier is used as configured.

Value

- `VRF`—Use the VRF name reported by the device.

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared network policy-decision-point

Syntax

```
shared network policy-decision-point name {
    description description;
    pdp-address pdp-address;
    pdp-group pdp-group;
}
```

Hierarchy Level

```
[edit shared network policy-decision-point]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configures the policy server as a policy decision point.

Options

name name— Name of policy decision point.

Value— Text string

description description—(Optional) Information about this policy server.

Value— Text string

Default— No value

Editing Level—Basic

pdp-address pdp-address— IP address of the policy server. The SAE uses this address to establish a COPS connection with the policy server.

Value— IP address

Default— No value

Editing Level—Basic

pdp-group pdp-group— Name of the policy server group.

Value— Text string
Default— No value
Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration

Syntax

```
shared sae configuration {
    substitution-num-engines substitution-num-engines;
    substitution-cache-size substitution-cache-size;
    compress-session-data;
    session-id-old-format;
}
```

Hierarchy Level

```
[edit shared sae configuration]
```

Options

`substitution-num-engines` *substitution-num-engines*—(Optional) Number of Substitution Engines

Value—Integer in the range -2147483648–2147483647

Default—5

Editing Level—Expert

`substitution-cache-size` *substitution-cache-size*—(Optional) Substitution Engine Cache Size

Value—Integer in the range -2147483648–2147483647

Default—5000

Editing Level—Expert

`compress-session-data`—(Optional) Enable or disable compression of the serialized data when saving the state of the SAE. You can use serialized data compression to reduce the size of sessions objects that the SAE sends across the network for the session store feature.

Enabling this option reduces the size of objects, but increases the CPU load on the SAE. We recommend that you do not enable this option because of the increase to the CPU load.

Default— Disabled

Editing Level—Basic

`session-id-old-format`—(Optional) Revert to the old style of generating the user session accounting id.

Enabling this attribute will cause the generated user session id to not be suitable for use as a device session id in the session database. We recommend that you do not enable this option because of session database incompatibility

Default— false

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration aggregate-services

Syntax

```
shared sae configuration aggregate-services {
    keepalive-time keepalive-time;
    keepalive-retry-time keepalive-retry-time;
    activation-deactivation-time activation-deactivation-time;
    failed-notification-retry-time failed-notification-retry-time;
    reactivation-verification-time reactivation-verification-time;
}
```

Hierarchy Level

```
[edit shared sae configuration aggregate-services]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure timers and intervals associated with monitoring and activating aggregate sessions.

Options

keepalive-time keepalive-time— Interval at which keepalive messages are sent from an aggregate service session and an associated fragment service session.

Value— Number of seconds in the range 1–2147483647

Default— 86400

Editing Level—Basic

keepalive-retry-time keepalive-retry-time— Time to wait before resending unacknowledged keepalive messages.

Value— Number of seconds in the range 1–2147483647

Default— 900

Editing Level—Basic

activation-deactivation-time activation-deactivation-time— Time to wait before retrying failed activation or deactivation of the fragment service session.

Value— Number of seconds in the range 1–2147483647

Default— 900
Editing Level—Basic

`failed-notification-retry-time` *failed-notification-retry-time*— Length of time to continue sending failure notifications if an aggregate service cannot reach a fragment service, or a fragment service cannot reach an aggregate service during shutdown of the aggregate service.

Value— Number of seconds in the range 1–2147483647
Default— 86400
Editing Level—Basic

`reactivation-verification-time` *reactivation-verification-time*— Maximum time (in seconds) to verify fragment reactivation

Value—Integer in the range -2147483648–2147483647
Default—30
Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration driver

Syntax

```
shared sae configuration driver {
    unauthenticated-subscriber-dn unauthenticated-subscriber-dn;
    virtual-portal-address virtual-portal-address;
    mac-cache-expiration mac-cache-expiration;
}
```

Hierarchy Level

```
[edit shared sae configuration driver]
```

Options

unauthenticated-subscriber-dn unauthenticated-subscriber-dn—
Transitional profile for subscribers who are not logged in to the SAE. For example, if a subscriber logs out of the SAE using the API method `Subscriber.logout()`, an unauthenticated subscriber session is created. The unauthenticated subscriber profile must exist and can be subscribed to services available for unauthenticated subscribers. The portal implementation determines whether unauthenticated (anonymous) subscribers can access the portal.

Value— <DN>. You can use the special value <base> to refer to the globally configured base DN. The string <base> is replaced with the directory base DN.

Default— *uniqueID=unauthenticated,ou=local,retailerName=default,o=Users,<base>*

Editing Level—Normal

virtual-portal-address virtual-portal-address—(Optional) IP address that policies use as a substitution to send traffic to a captive portal.

Value— IP address

Default— No value

Editing Level—Normal

mac-cache-expiration mac-cache-expiration— Amount of time that a subscriber profile remains in the SAE's in-memory cache. Configure this parameter to be greater than the time required for a DHCP subscriber to transition from an unauthenticated IP address to an authenticated IP address or vice versa. The time required for a DHCP subscriber to transition from one IP address to another depends on the lease times configured on the JUNOS router and the instructions given to the subscriber on the Web portal, such as reboot your PC now.

Value— Number of seconds in the range 0–2147483647

Default— 1800

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration driver aaa

Syntax

```
shared sae configuration driver aaa {
    sae-community-manager sae-community-manager;
    transient-session-timeout transient-session-timeout;
    max-update-interval max-update-interval;
    update-grace-period update-grace-period;
    resume-unrecovered;
    keep-alive-timeout keep-alive-timeout;
    registry-retry-interval registry-retry-interval;
    reply-timeout reply-timeout;
    sequential-message-timeout sequential-message-timeout;
    thread-pool-size thread-pool-size;
    thread-idle-timeout thread-idle-timeout;
}
```

Hierarchy Level

```
[edit shared sae configuration driver aaa]
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the SAE to manage AAA NAS groups.

Options

sae-community-manager sae-community-manager— Name of the community manager that manages AAA NAS group communities. Active SAEs are selected from this community.

Value— Community name
Default— AAACommunityManager
Editing Level—Expert

transient-session-timeout transient-session-timeout—(Optional) Time to wait before expiring a temporary session.

Value— Number of seconds
Default— 90

Editing Level—Basic

`max-update-interval` *max-update-interval*—(Optional) Maximum interval of interim updates for user sessions.

Value— Number of seconds

Default— 3600

Editing Level—Basic

`update-grace-period` *update-grace-period*—(Optional) Grace period to expect an interim update for a user session.

Value— Number of seconds

Default— 900

Editing Level—Basic

`resume-unrecovered`—(Optional) Specifies whether a user session that has failed to recover from a failover should be resumed.

Value— true or false

Default— true

Editing Level—Basic

`keep-alive-timeout` *keep-alive-timeout*—(Optional) Time to wait before expiring the registry to a Diameter server.

Value— Number of seconds

Default— 60

Editing Level—Basic

`registry-retry-interval` *registry-retry-interval*—(Optional) Time to wait before retrying a failed registry to a Diameter server.

Value— Number of seconds

Default— 30

Editing Level—Basic

`reply-timeout` *reply-timeout*—(Optional) Time to wait before expiring a request sent to a Diameter server.

Value— Number of seconds

Default— 20

Editing Level—Basic

`sequential-message-timeout` *sequential-message-timeout*—(Optional) Time to wait before expiring an expected message.

Value— Number of seconds

Default— 20

Editing Level—Basic

`thread-pool-size` *thread-pool-size*—(Optional) Number of working threads that process requests.

Value— Thread pool size

Default— 50

Editing Level—Basic

`thread-idle-timeout` *thread-idle-timeout*—(Optional) Time to wait before stopping working threads after they become idle.

Value— Number of seconds

Default— 60

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration driver aaa session-store

Syntax

```
shared sae configuration driver aaa session-store {
    maximum-queue-age maximum-queue-age;
    maximum-queued-operations maximum-queued-operations;
    maximum-queue-size maximum-queue-size;
    maximum-file-size maximum-file-size;
    minimum-disk-space-usage minimum-disk-space-usage;
    rotation-batch-size rotation-batch-size;
    maximum-session-size maximum-session-size;
    disk-load-buffer-size disk-load-buffer-size;
    network-buffer-size network-buffer-size;
    retry-interval retry-interval;
    communications-timeout communications-timeout;
    load-timeout load-timeout;
    idle-timeout idle-timeout;
    maximum-backlog-ratio maximum-backlog-ratio;
    minimum-backlog minimum-backlog;
}
```

Hierarchy Level

```
[edit shared sae configuration driver aaa session-store]
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the session store for the device driver.

maximum-queue-age maximum-queue-age—(Optional) Maximum age that a queue of buffered store operations (such as adding a session to the store or removing a session from the store) can reach before the queue is written to a session store file.

Value— Number of milliseconds in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 5000

Editing Level—Advanced

maximum-queued-operations maximum-queued-operations—(Optional) Number of buffered store operations that are queued before the queue is written to a session store file.

Value— Integer in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 50

Editing Level—Advanced

`maximum-queue-size` *maximum-queue-size*—(Optional) Maximum size that a queue of buffered store operations can reach before the queue is written to a session store file.

Value— Number of bytes in the range 0–2147483647

Default— 51050

Editing Level—Advanced

`maximum-file-size` *maximum-file-size*—(Optional) Maximum size of session store files. When a file reaches this size, a new file is created.

Value— Number of bytes in the range 0–2147483647

Default— 25000000

Editing Level—Advanced

`minimum-disk-space-usage` *minimum-disk-space-usage*—(Optional) Percentage of space in all session store files that is used by live sessions. When the percentage of space in the session store files that is used by live sessions decreases to this percentage, the oldest session store file is compacted and appended to the newest session store file, and then the oldest session store file is deleted.

Value— Percentage of disk space in the range 1–100. We recommend a range of 30-50

Default— 25

Editing Level—Advanced

`rotation-batch-size` *rotation-batch-size*—(Optional) When the oldest session store file is rotated, specifies the number of sessions that are rotated from the oldest file to the newest file at the same time. While a set of sessions is rotated, no other session store activity can take place.

Value— Integer in the range 0–2147483647

Default— 50

Editing Level—Advanced

`maximum-session-size` *maximum-session-size*—(Optional) Maximum size of a single subscriber or service session. Use this parameter to reserve memory for an internal buffer.

Value— Number of bytes in the range 0–2147483647

Default— 10000

Editing Level—Advanced

`disk-load-buffer-size` *disk-load-buffer-size*—(Optional) Size of the buffer that is used to load all of a session store's files from disk at startup.

Value— Number of bytes in the range 0–2147483647

Default— 1000000

Editing Level—Advanced

`network-buffer-size` *network-buffer-size*—(Optional) Size of the buffer that holds messages or message segments that are waiting to be sent to passive session stores

Value— Number of bytes in the range 21+ <size of maximum session size field>–2147483647

Default— 51050

Editing Level—Advanced

`retry-interval` *retry-interval*—(Optional) Time interval between attempts by the active session store to connect to missing passive session stores.

Value— Number of milliseconds in the range 0–2147483647

Default— 5000

Editing Level—Advanced

`communications-timeout` *communications-timeout*—(Optional) Amount of time in milliseconds that a session store waits before closing when it is blocked from reading or writing a message. This timeout does not apply when a session store is waiting for a remote session store to load its state from disk. (A non-positive number means wait forever. This is not recommended.)

Value— Number of milliseconds

Default— 60000

Editing Level—Advanced

`load-timeout` *load-timeout*—(Optional) Amount of time in milliseconds that an active session store waits for a passive session store or a passive session store waits for an active session store to load its data from disk before it closes the connection to the session store. (A non-positive number means wait forever. This is not recommended.)

Value— Number of milliseconds

Default— 420000

Editing Level—Advanced

`idle-timeout` *idle-timeout*—(Optional) Amount of time that a passive session store waits for activity from the active session store before it closes the connection to the active

session store. This timeout applies after the session store startup and initial update processes are complete.

Value— Number of milliseconds in the range 0–2147483647

Default— 3600000

Editing Level—Advanced

`maximum-backlog-ratio` *maximum-backlog-ratio*—(Optional) Along with the minimum backlog size, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the backlog of unsent operations (in bytes) divided by the total size (in bytes) of all live store operations is greater than this number, the connection is closed.

Value— Floating point number

Default— 1.5

Editing Level—Advanced

`minimum-backlog` *minimum-backlog*—(Optional) Along with the maximum backlog ratio, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent to the passive session store. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the maximum backlog ratio is met, the active session store does not close the connection unless the backlog of messages (in bytes) is greater than this number.

Value— Number of bytes in the range 0–2147483647

Default— 5000000

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Advanced

shared sae configuration driver junos

Syntax

```
shared sae configuration driver junos {
    beep-server-port beep-server-port;
    tls-beep-server-port tls-beep-server-port;
    connection-attempts connection-attempts;
    keepalive-interval keepalive-interval;
    message-timeout message-timeout;
    batch-size batch-size;
    transaction-batch-time transaction-batch-time;
    sdx-group-name sdx-group-name;
    sdx-session-group-name sdx-session-group-name;
    send-commit-check send-commit-check;
}
```

Hierarchy Level

```
[edit shared sae configuration driver junos]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the SAE to manage JUNOS routing platforms. A JUNOS routing platform interacts with the SAE by using a JUNOS software process called `sdx`. When the `sdx` process establishes a TCP/IP connection to the SAE, the SAE begins to manage the router. The JUNOS router driver configuration defines parameters related to the interactions between the SAE and the `sdx` process.

`beep-server-port beep-server-port`— TCP port number that is used to communicate with the `sdx` process on JUNOS routing platforms. This port number must match the port number configured in the `sdx` process on the router.

Value— TCP port number; if this value is set to zero and the TLS BEEP server port is set, the SAE accepts only TLS connections.

If you change this port number, you need to restart the SAE before the change takes effect.

Default— 3333

Editing Level—Advanced

`tls-beep-server-port` *tls-beep-server-port*— TCP port number used to communicate with the `sdx` process on JUNOS routing platforms using a secure TLS connection.

Value— TLS port number; if this value is set to zero, the SAE does not accept TLS connections.

If you change this port number, you need to restart the SAE before the change takes effect.

Default— 3434

Editing Level—Advanced

`connection-attempts` *connection-attempts*— Number of outstanding connection attempts before the SAE starts dropping new connection attempts.

Value— Positive value greater than 0; if the value is equal to or less than 0, the default value is used.

Default— 50

Editing Level—Advanced

`keepalive-interval` *keepalive-interval*— Interval between keepalive messages sent from the router. The `sdx` process on the router monitors the connection to the SAE by sending keepalive messages at one-third the specified interval. If the `sdx` process does not receive the expected keepalive answer within the specified timeout, it closes the connection.

A short interval results in a high load on the BEEP interface.

A long interval results in a long time before a connection failure is detected.

Value— Number of seconds in the range 0-2147483647. A value of 0 means that timeout is disabled.

Default— 45

Editing Level—Advanced

`message-timeout` *message-timeout*— Amount of time that the router driver waits for a response from the `sdx` process. Under a high load the router may not be able to respond fast enough to requests.

Change this value only if a high number of timeout events appear in the error log.

Value— Number of milliseconds in the range 0–2147483647

Default— 30000

Editing Level—Advanced

`batch-size` *batch-size*— Minimum number of service configuration transactions that are committed at the same time. If any of the transactions in a batch fails, all transactions are aborted, and the associated service activations or deactivations fail.

To control maximum latency for a job when services are activated in parallel, specify 120% of the number of CORBA threads as the batch size.

Value— Integer in the range 0–2147483647

Default— 10

Editing Level—Advanced

`transaction-batch-time` *transaction-batch-time*— Maximum time to collect configuration transactions in a batch. The batch is completed if either the batch size or the batch time is reached.

The completion time is calculated from the creation of a batch. Note that the batch time is a function of the total configuration size and not of the number of commands in the configuration transactions.

Value— Number of milliseconds in the range 0–2147483647

Default— 2000

Editing Level—Advanced

`sdx-group-name` *sdx-group-name*— Name of group on the JUNOS routing platform in which provisioning objects are stored.

Value— Name configured on the JUNOS routing platform

Default— sdx

Editing Level—Advanced

`sdx-session-group-name` *sdx-session-group-name*— Name of group on the JUNOS routing platform in which session objects are stored.

Value— Name configured on the JUNOS routing platform

Default— sdx-sessions

Editing Level—Advanced

`send-commit-check` *send-commit-check*— Enables or disables commit check. If enabled, a more detailed error message is logged if a batch fails, which lets you verify individual transactions in a batch.

To maximize service activation performance, commit check should be disabled.

Value— true or false

Default— true

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration driver junos configuration-checking

Syntax

```
shared sae configuration driver junos configuration-checking {
    configuration-checking-schedule configuration-checking-schedule;
    configuration-checking-action (enforce | synchronize | detect);
}
```

Hierarchy Level

```
[edit shared sae configuration driver junos configuration-checking]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the SAE to periodically check the configuration of the JUNOS routing platform.

Options

`configuration-checking-schedule configuration-checking-schedule`—
(Optional) Specifies when the SAE checks the router configuration.

Value— The schedule format is modeled on the UNIX crontab Entry Format (see UNIX crontab man pages). It consists of seven fields separated by space or tabs and enclosed in double quotation marks. The fields specify:

- Minute (0-59)
- Hour (0-23)
- Day of month (1-31, or the first three letters of the day of month)
- Month of the year (1-12)
- Day of the week (0-6 with 0=Sunday, or the first three letters of the name of the day)
- Year (4 digits indicating the year)
- Time Zone ID: An * indicates the SAE local time zone.

For custom time zones, specify the format:

- zone = "GMT" ("+" | "-") (hour : minute | hour minute | hour)
- hour = digit digit
- minute = digit digit
- digit = 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9

Use the following guidelines when configuring the schedule:

- An asterisk (*) is interpreted as 0 for minutes and hours and as the SAE local time zone for time zone. For all other fields, it stands for "first-last."
- Ranges of numbers and names are allowed. Ranges are two values separated with a hyphen. The specified range is inclusive. For example, 1–5 for the hour field specifies checking at hours 1, 2, 3, 4, and 5.
- Lists are allowed. A list is a set of numbers (or ranges) separated by commas. For example: "1,2,5,9", "0-4,8-12".
- Step values can be used with ranges. Following a range with "<number>" specifies skips in the number's value through the range. For example, "0-23/2" in the hours field specifies event execution every other hour. Steps are also permitted after an asterisk, so "* /2" specifies every 2 hours.
- When determining the next event time based on a specific time pattern, the following rules apply: Seconds and milliseconds are ignored (that is, rounded up to the closest minute). If you set both a day of the month and a day of the week, only the day of month is used.

Default— No value

Editing Level—Advanced

`configuration-checking-action (enforce | synchronize | detect)`—
(Optional) Action that the SAE takes when it detects disparities between the configuration of the SAE and the configuration on the router.

Value— One of the following:

- `detect`—Reports disparities through the SAE router driver event trap called `routerConfOutOfSynch` and through the info log. The SAE does not make any changes on the router.
- `enforce`—Enforces the state of the session layer on the router. The SAE removes all sessions that have disparities and creates new sessions with the same activation parameters as the original ones
- `synchronize`—Synchronizes the state of the session layer on the router. The SAE removes all sessions that have disparities.

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Advanced

shared sae configuration driver junos lsp-tracking

Syntax

```
shared sae configuration driver junos lsp-tracking {
    match match;
    file file;
}
```

Hierarchy Level

```
[edit shared sae configuration driver junos lsp-tracking]
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure event tracking for JUNOS LSPs to provide information to an application, such as the sample IPTV application, that needs information about LSP status.

LSP tracking can configure the system log on managed JUNOS routing platforms to send notification messages to the managing SAE when LSPs are created and removed, and when bandwidth allocation for an LSP changes.

Options

`match match`—(Optional) A regular expression to identify a set of LSP names. If you do not define an expression, the SAE tracks all LSPs.

Value— Regular expression

Default— No value

Editing Level—Basic

`file file`—(Optional) Name of the file to store syslog event messages (that provide information about LSP state changes in a JUNOS routing platform).

Value— Filename

Default— mpls4sae

Editing Level—Expert

Required Privilege Level

system system

Required Editing Level

Normal

shared sae configuration driver junos security

Syntax

```
shared sae configuration driver junos security {
    need-client-authentication;
    local-certificate local-certificate;
}
```

Hierarchy Level

```
[edit shared sae configuration driver junos security]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure Transport Layer Security (TLS) on the SAE.

need-client-authentication—(Optional) Enables or disables whether or not the SAE requests a client certificate from the router

If enabled, the SAE asks the router for a client certificate when a connection to the router is established.

If disabled, the SAE does not ask the router for a client certificate when a connection to the router is established.

Default— Enabled

Editing Level—Normal

local-certificate *local-certificate*—(Optional) Name of certificate to be used for TLS communications

Value— Name of certificate

Default— No value

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Advanced

shared sae configuration driver junos session-store

Syntax

```
shared sae configuration driver junos session-store {
    maximum-queue-age maximum-queue-age;
    maximum-queued-operations maximum-queued-operations;
    maximum-queue-size maximum-queue-size;
    maximum-file-size maximum-file-size;
    minimum-disk-space-usage minimum-disk-space-usage;
    rotation-batch-size rotation-batch-size;
    maximum-session-size maximum-session-size;
    disk-load-buffer-size disk-load-buffer-size;
    network-buffer-size network-buffer-size;
    retry-interval retry-interval;
    communications-timeout communications-timeout;
    load-timeout load-timeout;
    idle-timeout idle-timeout;
    maximum-backlog-ratio maximum-backlog-ratio;
    minimum-backlog minimum-backlog;
}
```

Hierarchy Level

```
[edit shared sae configuration driver junos session-store]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the session store for the JUNOS driver.

maximum-queue-age maximum-queue-age—(Optional) Maximum age that a queue of buffered store operations (such as adding a session to the store or removing a session from the store) can reach before the queue is written to a session store file.

Value— Number of milliseconds in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 5000

Editing Level—Advanced

maximum-queued-operations maximum-queued-operations—(Optional) Number of buffered store operations that are queued before the queue is written to a session store file.

Value— Integer in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 50

Editing Level—Advanced

`maximum-queue-size` *maximum-queue-size*—(Optional) Maximum size that a queue of buffered store operations can reach before the queue is written to a session store file.

Value— Number of bytes in the range 0–2147483647

Default— 51050

Editing Level—Advanced

`maximum-file-size` *maximum-file-size*—(Optional) Maximum size of session store files. When a file reaches this size, a new file is created.

Value— Number of bytes in the range 0–2147483647

Default— 25000000

Editing Level—Advanced

`minimum-disk-space-usage` *minimum-disk-space-usage*—(Optional) Percentage of space in all session store files that is used by live sessions. When the percentage of space in the session store files that is used by live sessions decreases to this percentage, the oldest session store file is compacted and appended to the newest session store file, and then the oldest session store file is deleted.

Value— Percentage of disk space in the range 1–100. We recommend a range of 30-50

Default— 25

Editing Level—Advanced

`rotation-batch-size` *rotation-batch-size*—(Optional) When the oldest session store file is rotated, specifies the number of sessions that are rotated from the oldest file to the newest file at the same time. While a set of sessions is rotated, no other session store activity can take place.

Value— Integer in the range 0–2147483647

Default— 50

Editing Level—Advanced

`maximum-session-size` *maximum-session-size*—(Optional) Maximum size of a single subscriber or service session. Use this parameter to reserve memory for an internal buffer.

Value— Number of bytes in the range 0–2147483647

Default— 10000

Editing Level—Advanced

`disk-load-buffer-size` *disk-load-buffer-size*—(Optional) Size of the buffer that is used to load all of a session store's files from disk at startup.

Value— Number of bytes in the range 0–2147483647

Default— 1000000

Editing Level—Advanced

`network-buffer-size` *network-buffer-size*—(Optional) Size of the buffer that holds messages or message segments that are waiting to be sent to passive session stores

Value— Number of bytes in the range 21+ <size of maximum session size field>–2147483647

Default— 51050

Editing Level—Advanced

`retry-interval` *retry-interval*—(Optional) Time interval between attempts by the active session store to connect to missing passive session stores.

Value— Number of milliseconds in the range 0–2147483647

Default— 5000

Editing Level—Advanced

`communications-timeout` *communications-timeout*—(Optional) Amount of time in milliseconds that a session store waits before closing when it is blocked from reading or writing a message. This timeout does not apply when a session store is waiting for a remote session store to load its state from disk. (A non-positive number means wait forever. This is not recommended.)

Value— Number of milliseconds

Default— 60000

Editing Level—Advanced

`load-timeout` *load-timeout*—(Optional) Amount of time in milliseconds that an active session store waits for a passive session store or a passive session store waits for an active session store to load its data from disk before it closes the connection to the session store. (A non-positive number means wait forever. This is not recommended.)

Value— Number of milliseconds

Default— 420000

Editing Level—Advanced

`idle-timeout` *idle-timeout*—(Optional) Amount of time that a passive session store waits for activity from the active session store before it closes the connection to the active

session store. This timeout applies after the session store startup and initial update processes are complete.

Value— Number of milliseconds in the range 0–2147483647

Default— 3600000

Editing Level—Advanced

`maximum-backlog-ratio` *maximum-backlog-ratio*—(Optional) Along with the minimum backlog size, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the backlog of unsent operations (in bytes) divided by the total size (in bytes) of all live store operations is greater than this number, the connection is closed.

Value— Floating point number

Default— 1.5

Editing Level—Advanced

`minimum-backlog` *minimum-backlog*—(Optional) Along with the maximum backlog ratio, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent to the passive session store. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the maximum backlog ratio is met, the active session store does not close the connection unless the backlog of messages (in bytes) is greater than this number.

Value— Number of bytes in the range 0–2147483647

Default— 5000000

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Advanced

shared sae configuration driver junos-ise

Syntax

```
shared sae configuration driver junos-ise {
    sae-community-manager sae-community-manager;
    cached-driver-expiration cached-driver-expiration;
    keep-alive-timeout keep-alive-timeout;
    registry-retry-interval registry-retry-interval;
    reply-timeout reply-timeout;
    sequential-message-timeout sequential-message-timeout;
    thread-pool-size thread-pool-size;
    thread-idle-timeout thread-idle-timeout;
}
```

Hierarchy Level

```
[edit shared sae configuration driver junos-ise]
```

Release Information

Statement introduced in SRC Release 3.2.0

Description

Configure the SAE to manage ISE devices.

Alias

intelligent-service-edge

Options

sae-community-manager sae-community-manager— Name of the community manager that manages ISE device communities. Active SAEs are selected from this community.

Value— Community name

Default— ISECommunityManager

Editing Level—Expert

cached-driver-expiration cached-driver-expiration— Minimum amount of time to keep the state of a router driver after its Diameter connection is closed. You might want to change this value because the SAE can resynchronize more quickly if most of the state is still in memory and it does not need to be reread from the disk.

Value— Number of seconds in the range 0–2147483647

Default— 600

Editing Level—Advanced

`keep-alive-timeout` *keep-alive-timeout*—(Optional) Time to wait before expiring the registry to a Diameter server.

Value— Number of seconds

Default— 60

Editing Level—Basic

`registry-retry-interval` *registry-retry-interval*—(Optional) Time to wait before retrying a failed registry to a Diameter server.

Value— Number of seconds

Default— 30

Editing Level—Basic

`reply-timeout` *reply-timeout*—(Optional) Time to wait before expiring a request sent to a Diameter server.

Value— Number of seconds

Default— 20

Editing Level—Basic

`sequential-message-timeout` *sequential-message-timeout*—(Optional) Time to wait before expiring an expected message.

Value— Number of seconds

Default— 20

Editing Level—Basic

`thread-pool-size` *thread-pool-size*—(Optional) Number of working threads that process requests.

Value— Thread pool size

Default— 50

Editing Level—Basic

`thread-idle-timeout` *thread-idle-timeout*—(Optional) Time to wait before stopping working threads after they become idle.

Value— Number of seconds

Default— 60

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration driver junos-ise session-store

Syntax

```
shared sae configuration driver junos-ise session-store {
    maximum-queue-age maximum-queue-age;
    maximum-queued-operations maximum-queued-operations;
    maximum-queue-size maximum-queue-size;
    maximum-file-size maximum-file-size;
    minimum-disk-space-usage minimum-disk-space-usage;
    rotation-batch-size rotation-batch-size;
    maximum-session-size maximum-session-size;
    disk-load-buffer-size disk-load-buffer-size;
    network-buffer-size network-buffer-size;
    retry-interval retry-interval;
    communications-timeout communications-timeout;
    load-timeout load-timeout;
    idle-timeout idle-timeout;
    maximum-backlog-ratio maximum-backlog-ratio;
    minimum-backlog minimum-backlog;
}
```

Hierarchy Level

```
[edit shared sae configuration driver junos-ise session-store]
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the session store for the device driver.

maximum-queue-age maximum-queue-age—(Optional) Maximum age that a queue of buffered store operations (such as adding a session to the store or removing a session from the store) can reach before the queue is written to a session store file.

Value— Number of milliseconds in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 5000

Editing Level—Advanced

maximum-queued-operations maximum-queued-operations—(Optional) Number of buffered store operations that are queued before the queue is written to a session store file.

Value— Integer in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 50

Editing Level—Advanced

`maximum-queue-size` *maximum-queue-size*—(Optional) Maximum size that a queue of buffered store operations can reach before the queue is written to a session store file.

Value— Number of bytes in the range 0–2147483647

Default— 51050

Editing Level—Advanced

`maximum-file-size` *maximum-file-size*—(Optional) Maximum size of session store files. When a file reaches this size, a new file is created.

Value— Number of bytes in the range 0–2147483647

Default— 25000000

Editing Level—Advanced

`minimum-disk-space-usage` *minimum-disk-space-usage*—(Optional) Percentage of space in all session store files that is used by live sessions. When the percentage of space in the session store files that is used by live sessions decreases to this percentage, the oldest session store file is compacted and appended to the newest session store file, and then the oldest session store file is deleted.

Value— Percentage of disk space in the range 1–100. We recommend a range of 30-50

Default— 25

Editing Level—Advanced

`rotation-batch-size` *rotation-batch-size*—(Optional) When the oldest session store file is rotated, specifies the number of sessions that are rotated from the oldest file to the newest file at the same time. While a set of sessions is rotated, no other session store activity can take place.

Value— Integer in the range 0–2147483647

Default— 50

Editing Level—Advanced

`maximum-session-size` *maximum-session-size*—(Optional) Maximum size of a single subscriber or service session. Use this parameter to reserve memory for an internal buffer.

Value— Number of bytes in the range 0–2147483647

Default— 10000

Editing Level—Advanced

`disk-load-buffer-size` *disk-load-buffer-size*—(Optional) Size of the buffer that is used to load all of a session store's files from disk at startup.

Value— Number of bytes in the range 0–2147483647

Default— 1000000

Editing Level—Advanced

`network-buffer-size` *network-buffer-size*—(Optional) Size of the buffer that holds messages or message segments that are waiting to be sent to passive session stores

Value— Number of bytes in the range 21+ <size of maximum session size field>–2147483647

Default— 51050

Editing Level—Advanced

`retry-interval` *retry-interval*—(Optional) Time interval between attempts by the active session store to connect to missing passive session stores.

Value— Number of milliseconds in the range 0–2147483647

Default— 5000

Editing Level—Advanced

`communications-timeout` *communications-timeout*—(Optional) Amount of time in milliseconds that a session store waits before closing when it is blocked from reading or writing a message. This timeout does not apply when a session store is waiting for a remote session store to load its state from disk. (A non-positive number means wait forever. This is not recommended.)

Value— Number of milliseconds

Default— 60000

Editing Level—Advanced

`load-timeout` *load-timeout*—(Optional) Amount of time in milliseconds that an active session store waits for a passive session store or a passive session store waits for an active session store to load its data from disk before it closes the connection to the session store. (A non-positive number means wait forever. This is not recommended.)

Value— Number of milliseconds

Default— 420000

Editing Level—Advanced

`idle-timeout` *idle-timeout*—(Optional) Amount of time that a passive session store waits for activity from the active session store before it closes the connection to the active

session store. This timeout applies after the session store startup and initial update processes are complete.

Value— Number of milliseconds in the range 0–2147483647

Default— 3600000

Editing Level—Advanced

`maximum-backlog-ratio` *maximum-backlog-ratio*—(Optional) Along with the minimum backlog size, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the backlog of unsent operations (in bytes) divided by the total size (in bytes) of all live store operations is greater than this number, the connection is closed.

Value— Floating point number

Default— 1.5

Editing Level—Advanced

`minimum-backlog` *minimum-backlog*—(Optional) Along with the maximum backlog ratio, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent to the passive session store. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the maximum backlog ratio is met, the active session store does not close the connection unless the backlog of messages (in bytes) is greater than this number.

Value— Number of bytes in the range 0–2147483647

Default— 5000000

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Advanced

shared sae configuration driver junos-ptsp

Syntax

```
shared sae configuration driver junos-ptsp {
    sae-community-manager sae-community-manager;
    cached-driver-expiration cached-driver-expiration;
    keep-alive-timeout keep-alive-timeout;
    registry-retry-interval registry-retry-interval;
    reply-timeout reply-timeout;
    sequential-message-timeout sequential-message-timeout;
    thread-pool-size thread-pool-size;
    thread-idle-timeout thread-idle-timeout;
}
```

Hierarchy Level

```
[edit shared sae configuration driver junos-ptsp]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the SAE to manage PTSP devices.

Options

sae-community-manager sae-community-manager— Name of the community manager that manages PTSP device communities. Active SAEs are selected from this community.

Value— Community name
Default— PTSPCommunityManager
Editing Level—Expert

cached-driver-expiration cached-driver-expiration— Minimum amount of time to keep the state of a router driver after its Diameter connection is closed. You might want to change this value because the SAE can resynchronize more quickly if most of the state is still in memory and it does not need to be reread from the disk.

Value— Number of seconds in the range 0–2147483647
Default— 600
Editing Level—Advanced

`keep-alive-timeout` *keep-alive-timeout*—(Optional) Time to wait before expiring the registry to a Diameter server.

Value— Number of seconds
Default— 60
Editing Level—Basic

`registry-retry-interval` *registry-retry-interval*—(Optional) Time to wait before retrying a failed registry to a Diameter server.

Value— Number of seconds
Default— 30
Editing Level—Basic

`reply-timeout` *reply-timeout*—(Optional) Time to wait before expiring a request sent to a Diameter server.

Value— Number of seconds
Default— 20
Editing Level—Basic

`sequential-message-timeout` *sequential-message-timeout*—(Optional) Time to wait before expiring an expected message.

Value— Number of seconds
Default— 20
Editing Level—Basic

`thread-pool-size` *thread-pool-size*—(Optional) Number of working threads that process requests.

Value— Thread pool size
Default— 50
Editing Level—Basic

`thread-idle-timeout` *thread-idle-timeout*—(Optional) Time to wait before stopping working threads after they become idle.

Value— Number of seconds
Default— 60
Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration driver junos-ptsp session-store

Syntax

```
shared sae configuration driver junos-ptsp session-store {
    maximum-queue-age maximum-queue-age;
    maximum-queued-operations maximum-queued-operations;
    maximum-queue-size maximum-queue-size;
    maximum-file-size maximum-file-size;
    minimum-disk-space-usage minimum-disk-space-usage;
    rotation-batch-size rotation-batch-size;
    maximum-session-size maximum-session-size;
    disk-load-buffer-size disk-load-buffer-size;
    network-buffer-size network-buffer-size;
    retry-interval retry-interval;
    communications-timeout communications-timeout;
    load-timeout load-timeout;
    idle-timeout idle-timeout;
    maximum-backlog-ratio maximum-backlog-ratio;
    minimum-backlog minimum-backlog;
}
```

Hierarchy Level

```
[edit shared sae configuration driver junos-ptsp session-store]
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure the session store for the device driver.

maximum-queue-age *maximum-queue-age*—(Optional) Maximum age that a queue of buffered store operations (such as adding a session to the store or removing a session from the store) can reach before the queue is written to a session store file.

Value— Number of milliseconds in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 5000

Editing Level—Advanced

maximum-queued-operations *maximum-queued-operations*—(Optional) Number of buffered store operations that are queued before the queue is written to a session store file.

Value— Integer in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 50

Editing Level—Advanced

`maximum-queue-size` *maximum-queue-size*—(Optional) Maximum size that a queue of buffered store operations can reach before the queue is written to a session store file.

Value— Number of bytes in the range 0–2147483647

Default— 51050

Editing Level—Advanced

`maximum-file-size` *maximum-file-size*—(Optional) Maximum size of session store files. When a file reaches this size, a new file is created.

Value— Number of bytes in the range 0–2147483647

Default— 25000000

Editing Level—Advanced

`minimum-disk-space-usage` *minimum-disk-space-usage*—(Optional) Percentage of space in all session store files that is used by live sessions. When the percentage of space in the session store files that is used by live sessions decreases to this percentage, the oldest session store file is compacted and appended to the newest session store file, and then the oldest session store file is deleted.

Value— Percentage of disk space in the range 1–100. We recommend a range of 30-50

Default— 25

Editing Level—Advanced

`rotation-batch-size` *rotation-batch-size*—(Optional) When the oldest session store file is rotated, specifies the number of sessions that are rotated from the oldest file to the newest file at the same time. While a set of sessions is rotated, no other session store activity can take place.

Value— Integer in the range 0–2147483647

Default— 50

Editing Level—Advanced

`maximum-session-size` *maximum-session-size*—(Optional) Maximum size of a single subscriber or service session. Use this parameter to reserve memory for an internal buffer.

Value— Number of bytes in the range 0–2147483647

Default— 10000

Editing Level—Advanced

`disk-load-buffer-size` *disk-load-buffer-size*—(Optional) Size of the buffer that is used to load all of a session store's files from disk at startup.

Value— Number of bytes in the range 0–2147483647

Default— 1000000

Editing Level—Advanced

`network-buffer-size` *network-buffer-size*—(Optional) Size of the buffer that holds messages or message segments that are waiting to be sent to passive session stores

Value— Number of bytes in the range 21+ <size of maximum session size field>–2147483647

Default— 51050

Editing Level—Advanced

`retry-interval` *retry-interval*—(Optional) Time interval between attempts by the active session store to connect to missing passive session stores.

Value— Number of milliseconds in the range 0–2147483647

Default— 5000

Editing Level—Advanced

`communications-timeout` *communications-timeout*—(Optional) Amount of time in milliseconds that a session store waits before closing when it is blocked from reading or writing a message. This timeout does not apply when a session store is waiting for a remote session store to load its state from disk. (A non-positive number means wait forever. This is not recommended.)

Value— Number of milliseconds

Default— 60000

Editing Level—Advanced

`load-timeout` *load-timeout*—(Optional) Amount of time in milliseconds that an active session store waits for a passive session store or a passive session store waits for an active session store to load its data from disk before it closes the connection to the session store. (A non-positive number means wait forever. This is not recommended.)

Value— Number of milliseconds

Default— 420000

Editing Level—Advanced

`idle-timeout` *idle-timeout*—(Optional) Amount of time that a passive session store waits for activity from the active session store before it closes the connection to the active

session store. This timeout applies after the session store startup and initial update processes are complete.

Value— Number of milliseconds in the range 0–2147483647

Default— 3600000

Editing Level—Advanced

`maximum-backlog-ratio` *maximum-backlog-ratio*—(Optional) Along with the minimum backlog size, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the backlog of unsent operations (in bytes) divided by the total size (in bytes) of all live store operations is greater than this number, the connection is closed.

Value— Floating point number

Default— 1.5

Editing Level—Advanced

`minimum-backlog` *minimum-backlog*—(Optional) Along with the maximum backlog ratio, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent to the passive session store. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the maximum backlog ratio is met, the active session store does not close the connection unless the backlog of messages (in bytes) is greater than this number.

Value— Number of bytes in the range 0–2147483647

Default— 5000000

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Advanced

shared sae configuration driver junose

Syntax

```
shared sae configuration driver junose {
    cops-server-port cops-server-port;
    backlog backlog;
    keepalive-interval keepalive-interval;
    message-timeout message-timeout;
    replication-message-timeout replication-message-timeout;
    cops-message-maximum-length cops-message-maximum-length;
    cops-message-read-buffer-size cops-message-read-buffer-size;
    cops-message-write-buffer-size cops-message-write-buffer-size;
    pending-address-timeout pending-address-timeout;
    cops-handler-threads cops-handler-threads;
    cached-driver-expiration cached-driver-expiration;
    drop-unmanaged-interfaces-xdr-driver;
    track-unmanaged-interfaces-xdr-driver;
}
```

Hierarchy Level

```
[edit shared sae configuration driver junose]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the SAE to manage JUNOSe routers. The router driver specifies the COPS connection between the SAE COPS server and the COPS client in the JUNOSe router.

cops-server-port *cops-server-port*— TCP port number of the COPS server used to communicate with the JUNOSe routers.

Value— Port number that matches the configuration of the SRC client in the JUNOSe router.

Default— 3288

Editing Level—Advanced

backlog *backlog*— Maximum number of outstanding connection attempts before connections are dropped.

Value— Integer

Default— 50

Editing Level—Advanced

`keepalive-interval` *keepalive-interval*— Interval between keepalive messages sent from the COPS client (the JUNOS router). The COPS client monitors the COPS connection by sending keepalive messages at random intervals between one-fourth and three-fourths of the specified interval. If the client does not receive the expected keepalive answer within the specified timeout, the client terminates the connection.

A short interval results in a high load on the COPS interface.

A long interval results in a long time before a COPS failure is detected.

Value— Number of seconds in the range 0-32768. A value of 0 means that timeout is disabled.

Default— 45

Editing Level—Advanced

`message-timeout` *message-timeout*— Timeout interval in which the COPS server waits for a response to COPS requests. Under a high load the router may not be able to respond fast enough to COPS requests. Change this value only if a high number of COPS timeout events appear in the error log.

Value— Number of milliseconds

Default— 120000

Editing Level—Advanced

`replication-message-timeout` *replication-message-timeout*— Timeout interval in which the active SAE waits for a response to synchronization requests. Under a high load the router may not be able to respond fast enough to COPS requests. Change this value if Reliable Replication Mode can't be triggered.

Value— Number of milliseconds

Default— 1000

Editing Level—Advanced

`cops-message-maximum-length` *cops-message-maximum-length*— Maximum length of a COPS message. We recommend that you use the default setting.

Value— Number of bytes in the range 4 bytes to 2 GB

Default— 200000

Editing Level—Advanced

`cops-message-read-buffer-size` *cops-message-read-buffer-size*— Buffer size for receiving COPS messages from the JUNOS client. We recommend that you use the default setting unless you are instructed to change it by Juniper Networks engineers.

Value— Number of bytes in the range 4 bytes to 2 GB

Default— 30000

Editing Level—Advanced

`cops-message-write-buffer-size` *cops-message-write-buffer-size*— Buffer size for sending COPS messages to the JUNOS client. We recommend that you use the default setting unless you are instructed to change it by Juniper Networks engineers.

Value— Number of bytes in the range 4 bytes to 2 GB

Default— 30000

Editing Level—Advanced

`pending-address-timeout` *pending-address-timeout*— Maximum time that a DHCP address request remains pending.

Value— Number of milliseconds. Typical values are in the range 1000-15000 (1 second to 15 seconds).

Default— 5000

Editing Level—Advanced

`cops-handler-threads` *cops-handler-threads*—(Optional) Size of the thread pool for handling unsolicited messages. These threads are shared among all JUNOS router drivers. You may want to set this value higher than the default if you wish to create greater throughput on platforms with multiple processing cores, and you are not achieving full processor resource utilization. Increasing the number of threads increases the ability to use multiple processing cores in parallel.

Value— Number of threads

Default— No value

Editing Level—Advanced

`cached-driver-expiration` *cached-driver-expiration*— Minimum amount of time to keep the state of a router driver after its COPS connection is closed. You might want to change this value because the SAE can resynchronize more quickly if most of the state is still in memory and it does not need to be reread from the disk.

Value— Number of seconds in the range 0–2147483647

Default— 600

Editing Level—Advanced

`drop-unmanaged-interfaces-xdr-driver`—(Optional) For JUNOS COPS-XDR drivers, enables or disables the driver to keep a record of unmanaged interfaces. You must enable this option if you have unmanaged dynamic interfaces in a virtual router that is managed by COPS-XDR. If the driver does not keep a record of unmanaged interfaces, next-interface actions in policies may not work properly in certain cases. To use RAM more efficiently, enable this option if you have a large number of unmanaged interfaces that are not the target of next-hop policies.

Default— Disabled
Editing Level—Expert

`track-unmanaged-interfaces-xdr-driver`—(Optional) Enables sending of interface tracking events for unmanaged interfaces of the XDR router driver. Because the COPS-XDR protocol does not include notifications (DRQs) when unmanaged interfaces are disabled, plug-ins will not receive an unmanaged interface's stop events.

Default— Disabled
Editing Level—Expert

Required Privilege Level

system

Required Editing Level

Advanced

shared sae configuration driver junose session-store

Syntax

```
shared sae configuration driver junose session-store {
    maximum-queue-age maximum-queue-age;
    maximum-queued-operations maximum-queued-operations;
    maximum-queue-size maximum-queue-size;
    maximum-file-size maximum-file-size;
    minimum-disk-space-usage minimum-disk-space-usage;
    rotation-batch-size rotation-batch-size;
    maximum-session-size maximum-session-size;
    disk-load-buffer-size disk-load-buffer-size;
    network-buffer-size network-buffer-size;
    retry-interval retry-interval;
    communications-timeout communications-timeout;
    load-timeout load-timeout;
    idle-timeout idle-timeout;
    maximum-backlog-ratio maximum-backlog-ratio;
    minimum-backlog minimum-backlog;
}
```

Hierarchy Level

```
[edit shared sae configuration driver junose session-store]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the session store for the JUNOSe driver.

maximum-queue-age *maximum-queue-age*—(Optional) Maximum age that a queue of buffered store operations (such as adding a session to the store or removing a session from the store) can reach before the queue is written to a session store file.

Value— Number of milliseconds in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 5000

Editing Level—Advanced

maximum-queued-operations *maximum-queued-operations*—(Optional) Number of buffered store operations that are queued before the queue is written to a session store file.

Value— Integer in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 50

Editing Level—Advanced

`maximum-queue-size` *maximum-queue-size*—(Optional) Maximum size that a queue of buffered store operations can reach before the queue is written to a session store file.

Value— Number of bytes in the range 0–2147483647

Default— 51050

Editing Level—Advanced

`maximum-file-size` *maximum-file-size*—(Optional) Maximum size of session store files. When a file reaches this size, a new file is created.

Value— Number of bytes in the range 0–2147483647

Default— 25000000

Editing Level—Advanced

`minimum-disk-space-usage` *minimum-disk-space-usage*—(Optional) Percentage of space in all session store files that is used by live sessions. When the percentage of space in the session store files that is used by live sessions decreases to this percentage, the oldest session store file is compacted and appended to the newest session store file, and then the oldest session store file is deleted.

Value— Percentage of disk space in the range 1–100. We recommend a range of 30-50

Default— 25

Editing Level—Advanced

`rotation-batch-size` *rotation-batch-size*—(Optional) When the oldest session store file is rotated, specifies the number of sessions that are rotated from the oldest file to the newest file at the same time. While a set of sessions is rotated, no other session store activity can take place.

Value— Integer in the range 0–2147483647

Default— 50

Editing Level—Advanced

`maximum-session-size` *maximum-session-size*—(Optional) Maximum size of a single subscriber or service session. Use this parameter to reserve memory for an internal buffer.

Value— Number of bytes in the range 0–2147483647

Default— 10000

Editing Level—Advanced

`disk-load-buffer-size` *disk-load-buffer-size*—(Optional) Size of the buffer that is used to load all of a session store's files from disk at startup.

Value— Number of bytes in the range 0–2147483647

Default— 1000000

Editing Level—Advanced

`network-buffer-size` *network-buffer-size*—(Optional) Size of the buffer that holds messages or message segments that are waiting to be sent to passive session stores

Value— Number of bytes in the range 21+ <size of maximum session size field>–2147483647

Default— 51050

Editing Level—Advanced

`retry-interval` *retry-interval*—(Optional) Time interval between attempts by the active session store to connect to missing passive session stores.

Value— Number of milliseconds in the range 0–2147483647

Default— 5000

Editing Level—Advanced

`communications-timeout` *communications-timeout*—(Optional) Amount of time in milliseconds that a session store waits before closing when it is blocked from reading or writing a message. This timeout does not apply when a session store is waiting for a remote session store to load its state from disk. (A non-positive number means wait forever. This is not recommended.)

Value— Number of milliseconds

Default— 60000

Editing Level—Advanced

`load-timeout` *load-timeout*—(Optional) Amount of time in milliseconds that an active session store waits for a passive session store or a passive session store waits for an active session store to load its data from disk before it closes the connection to the session store. (A non-positive number means wait forever. This is not recommended.)

Value— Number of milliseconds

Default— 420000

Editing Level—Advanced

`idle-timeout` *idle-timeout*—(Optional) Amount of time that a passive session store waits for activity from the active session store before it closes the connection to the active

session store. This timeout applies after the session store startup and initial update processes are complete.

Value— Number of milliseconds in the range 0–2147483647

Default— 3600000

Editing Level—Advanced

`maximum-backlog-ratio` *maximum-backlog-ratio*—(Optional) Along with the minimum backlog size, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the backlog of unsent operations (in bytes) divided by the total size (in bytes) of all live store operations is greater than this number, the connection is closed.

Value— Floating point number

Default— 1.5

Editing Level—Advanced

`minimum-backlog` *minimum-backlog*—(Optional) Along with the maximum backlog ratio, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent to the passive session store. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the maximum backlog ratio is met, the active session store does not close the connection unless the backlog of messages (in bytes) is greater than this number.

Value— Number of bytes in the range 0–2147483647

Default— 5000000

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Advanced

shared sae configuration driver pcmm

Syntax

```
shared sae configuration driver pcmm {
    keepalive-interval keepalive-interval;
    tcp-connection-timeout tcp-connection-timeout;
    application-manager-id application-manager-id;
    message-timeout message-timeout;
    cops-message-maximum-length cops-message-maximum-length;
    cops-message-read-buffer-size cops-message-read-buffer-size;
    cops-message-write-buffer-size cops-message-write-buffer-size;
    sae-community-manager sae-community-manager;
    disable-full-sync;
    disable-pcmm-i03-policy;
    session-recovery-retry-interval session-recovery-retry-interval;
    element-id element-id;
    default-rks-plugin-in default-rks-plugin-in;
}
```

Hierarchy Level

[edit shared sae configuration driver pcmm]

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the SAE to manage PCMM devices. The SAE connects to the PCMM device by using a COPS-over-TCP connection. The PCMM device driver controls this connection.

keepalive-interval *keepalive-interval*— Interval between keepalive messages sent from the COPS client (the PCMM device) to the COPS server (the SAE). The COPS client monitors the COPS connection by sending keepalive messages at random intervals between one-fourth and three-fourths of the specified interval. If the client or the server does not receive the expected keepalive answer within the specified timeout, the client closes the connection.

Value— Number of seconds in the range 0-2147483647. A value of 0 means that the timeout is disabled.

Default— 45

Editing Level—Advanced

tcp-connection-timeout *tcp-connection-timeout*— Timeout for opening a TCP

connection to the PCMM device.

Value— Number of seconds in the range 0–2147483647.

Default— 5

Editing Level—Advanced

`application-manager-id application-manager-id`— Identifier of the application manager when this SAE is configured as the application manager. The application manager includes this identifier in all messages that it sends to the policy server. The policy server passes this ID to the CMTS device in Gate Control messages. The CMTS device returns the ID associated with the gate to the policy server. The policy server uses this information to associate gate messages with a particular application manager.

Value— 4-byte unsigned integer that is unique in a service provider network.

Default— 1

Editing Level—Normal

`message-timeout message-timeout`— Amount of time that the COPS server (the SAE) waits for a response to COPS requests from the COPS client (the PCMM device). Under a high load the PCMM device may not be able to respond fast enough to COPS requests. Change this value only if a high number of COPS timeout events appear in the error log.

Value— Number of milliseconds in the range 0–2147483647

Default— 120000

Editing Level—Advanced

`cops-message-maximum-length cops-message-maximum-length`— Maximum length of a COPS message. We recommend that you use the default setting.

Value— Number of bytes in the range 4 bytes to 2 GB

Default— 204800

Editing Level—Advanced

`cops-message-read-buffer-size cops-message-read-buffer-size`— Buffer size for receiving COPS messages from the PCMM client. We recommend that you use the default setting unless you are instructed to change it by Juniper Networks engineers.

Value— Number of bytes in the range 4 bytes to 2 GB

Default— 30000

Editing Level—Advanced

`cops-message-write-buffer-size cops-message-write-buffer-size`— Buffer size for sending COPS messages to the PCMM client. We recommend that you use the default setting unless you are instructed to change it by Juniper Networks engineers.

Value— Number of bytes in the range 4 bytes to 2 GB

Default— 30000

Editing Level—Advanced

`sae-community-manager sae-community-manager`— Name of the community manager that manages PCMM driver communities. Active SAEs are selected from this community.

Value— Community name

Default— PCMMCommunityManager

Editing Level—Expert

`disable-full-sync`—(Optional) Disables state synchronization with PCMM policy servers. State synchronization is achieved when the SAE is required to communicate with the policy server over the COPS connection.

Default—false

Editing Level—Expert

`disable-pcmm-i03-policy`—(Optional) Disables the SAE to send classifiers to the router that comply with PCMM I03. Use this option if your network deployment has CMTS devices that do not support PCMM I03.

Default—true

Editing Level—Expert

`session-recovery-retry-interval session-recovery-retry-interval`— Time interval between attempts by the SAE to restore service sessions that are still being recovered in the background when state synchronization is completed with a state-data-incomplete error. The SAE attempts to restore a service session if it receives a service modification or deactivation request for an unrecovered service session before the next interval.

We recommend setting this value to 3600000 (1 hour) or longer.

Value— Number of milliseconds in the range 0–2147483647

Default— 3600000

Editing Level—Expert

`element-id element-id`—(Optional) Unique identifier that the SAE uses to identify itself when it originates RKS events.

Value— 8-byte unsigned integer in the range 0–99999; must be unique within a PCMM network

Default— 1

Editing Level—Advanced

`default-rks-plug-in default-rks-plug-in`—(Optional) RKS plug-in to which the SAE sends event messages if you do not configure a CMTS-specific plug-in.

- Value**— Name of an RKS plug-in
- Default**— No value
- Editing Level**—Advanced

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration driver pcmm cmts-specific-rks-plug-ins

Syntax

```
shared sae configuration driver pcmm cmts-specific-rks-plug-ins name {
    rks-plug-in rks-plug-in;
}
```

Hierarchy Level

```
[edit shared sae configuration driver pcmm cmts-specific-rks-plug-ins]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a CMTS-specific RKS plug-in.

Options

name name— Name of the RKS plug-in.

Value—Text

rks-plug-in rks-plug-in—(Optional) Name of the plug-in to which the SAE sends events for this CMTS device.

Value— Name of an RKS plug-in

Default— No value

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Advanced

shared sae configuration driver pcmm session-store

Syntax

```
shared sae configuration driver pcmm session-store {
    maximum-queue-age maximum-queue-age;
    maximum-queued-operations maximum-queued-operations;
    maximum-queue-size maximum-queue-size;
    maximum-file-size maximum-file-size;
    minimum-disk-space-usage minimum-disk-space-usage;
    rotation-batch-size rotation-batch-size;
    maximum-session-size maximum-session-size;
    disk-load-buffer-size disk-load-buffer-size;
    network-buffer-size network-buffer-size;
    retry-interval retry-interval;
    communications-timeout communications-timeout;
    load-timeout load-timeout;
    idle-timeout idle-timeout;
    maximum-backlog-ratio maximum-backlog-ratio;
    minimum-backlog minimum-backlog;
}
```

Hierarchy Level

```
[edit shared sae configuration driver pcmm session-store]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the session store for the PCMM driver.

maximum-queue-age maximum-queue-age—(Optional) Maximum age that a queue of buffered store operations (such as adding a session to the store or removing a session from the store) can reach before the queue is written to a session store file.

Value— Number of milliseconds in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 5000

Editing Level—Advanced

maximum-queued-operations maximum-queued-operations—(Optional) Number of buffered store operations that are queued before the queue is written to a session store file.

Value— Integer in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 50

Editing Level—Advanced

`maximum-queue-size` *maximum-queue-size*—(Optional) Maximum size that a queue of buffered store operations can reach before the queue is written to a session store file.

Value— Number of bytes in the range 0–2147483647

Default— 51050

Editing Level—Advanced

`maximum-file-size` *maximum-file-size*—(Optional) Maximum size of session store files. When a file reaches this size, a new file is created.

Value— Number of bytes in the range 0–2147483647

Default— 25000000

Editing Level—Advanced

`minimum-disk-space-usage` *minimum-disk-space-usage*—(Optional) Percentage of space in all session store files that is used by live sessions. When the percentage of space in the session store files that is used by live sessions decreases to this percentage, the oldest session store file is compacted and appended to the newest session store file, and then the oldest session store file is deleted.

Value— Percentage of disk space in the range 1–100. We recommend a range of 30-50

Default— 25

Editing Level—Advanced

`rotation-batch-size` *rotation-batch-size*—(Optional) When the oldest session store file is rotated, specifies the number of sessions that are rotated from the oldest file to the newest file at the same time. While a set of sessions is rotated, no other session store activity can take place.

Value— Integer in the range 0–2147483647

Default— 50

Editing Level—Advanced

`maximum-session-size` *maximum-session-size*—(Optional) Maximum size of a single subscriber or service session. Use this parameter to reserve memory for an internal buffer.

Value— Number of bytes in the range 0–2147483647

Default— 10000

Editing Level—Advanced

`disk-load-buffer-size` *disk-load-buffer-size*—(Optional) Size of the buffer that is used to load all of a session store's files from disk at startup.

Value— Number of bytes in the range 0–2147483647

Default— 1000000

Editing Level—Advanced

`network-buffer-size` *network-buffer-size*—(Optional) Size of the buffer that holds messages or message segments that are waiting to be sent to passive session stores

Value— Number of bytes in the range 21+ <size of maximum session size field>–2147483647

Default— 51050

Editing Level—Advanced

`retry-interval` *retry-interval*—(Optional) Time interval between attempts by the active session store to connect to missing passive session stores.

Value— Number of milliseconds in the range 0–2147483647

Default— 5000

Editing Level—Advanced

`communications-timeout` *communications-timeout*—(Optional) Amount of time in milliseconds that a session store waits before closing when it is blocked from reading or writing a message. This timeout does not apply when a session store is waiting for a remote session store to load its state from disk. (A non-positive number means wait forever. This is not recommended.)

Value— Number of milliseconds

Default— 60000

Editing Level—Advanced

`load-timeout` *load-timeout*—(Optional) Amount of time in milliseconds that an active session store waits for a passive session store or a passive session store waits for an active session store to load its data from disk before it closes the connection to the session store. (A non-positive number means wait forever. This is not recommended.)

Value— Number of milliseconds

Default— 420000

Editing Level—Advanced

`idle-timeout` *idle-timeout*—(Optional) Amount of time that a passive session store waits for activity from the active session store before it closes the connection to the active

session store. This timeout applies after the session store startup and initial update processes are complete.

Value— Number of milliseconds in the range 0–2147483647

Default— 3600000

Editing Level—Advanced

`maximum-backlog-ratio` *maximum-backlog-ratio*—(Optional) Along with the minimum backlog size, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the backlog of unsent operations (in bytes) divided by the total size (in bytes) of all live store operations is greater than this number, the connection is closed.

Value— Floating point number

Default— 1.5

Editing Level—Advanced

`minimum-backlog` *minimum-backlog*—(Optional) Along with the maximum backlog ratio, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent to the passive session store. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the maximum backlog ratio is met, the active session store does not close the connection unless the backlog of messages (in bytes) is greater than this number.

Value— Number of bytes in the range 0–2147483647

Default— 5000000

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Advanced

shared sae configuration driver scripts

Syntax

```
shared sae configuration driver scripts {
    extension-path extension-path;
    general general;
    junos junos;
    junose junose;
    junose-xdr junose-xdr;
    pcmm pcmm;
    third-party third-party;
    junos-ise junos-ise;
    junos-ptsp junos-ptsp;
}
```

Hierarchy Level

```
[edit shared sae configuration driver scripts]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure device scripts. When the SAE establishes a connection with a router, PCMM device, or other network device, it can run a script to customize the setup of the connection. These scripts are run when the connection is established and again when the connection is dropped.

Options

extension-path extension-path—(Optional) Path to scripts that are not in the default location, */opt/UMC/sae/lib* .

Value— List of paths separated by semicolons (;)

Default— No value

Editing Level—Normal

general general—(Optional) Script that can be used for all types of routers, PCMM devices, and other network devices that the SRC software supports. The script is run when the connection between a router or other network device and the SAE is established and again when the connection is dropped.

Value— Name of a script

Default— No value

Editing Level—Basic

`junos junos`—(Optional) Initialization script for JUNOS routing platforms. The script is run when the connection between a router and the SAE is established and again when the connection is dropped.

Value— Name of a script

Default— No value

Editing Level—Basic

`junose junose`—(Optional) [Alias: `junose-pr`] Initialization script for JUNOSe routers when the JUNOSe driver uses COPS-PR mode when connecting to the SAE. The script is run when the connection between a router and the SAE is established and again when the connection is dropped.

Value— Name of the file that contains the script without including the .py extension.

Default— No value

Editing Level—Basic

`junose-xdr junose-xdr`—(Optional) Initialization script for JUNOSe routers when the JUNOSe driver uses XDR mode when connecting to the SAE. The script is run when the connection between a router and the SAE is established and again when the connection is dropped.

In COPS XDR mode, the router does not send the network access server (NAS) IP address to the SAE. If your configuration requires this value, add the following line to a JUNOSe script:

```
import ERXnasip
```

When you add the `import ERXnasip` entry, the script obtains the NAS-IP address from the router through SNMP. This mechanism can affect performance, especially when the SAE manages a large number of virtual routers.

Value— Name of a script. For example, `iorPublisher`, `poolPublisher`.

Default— No value

Editing Level—Basic

`pcmm pcmm`—(Optional) Initialization script for the Juniper Policy Server in a PCMM environment. The script is run when the connection between a policy server and the SAE is established and again when the connection is dropped.

Value— Name of a script

Default— No value

Editing Level—Basic

`third-party` *third-party*—(Optional) Initialization script for third-party device drivers. The script is run when the third-party device driver is activated or deactivated.

Value— Name of a script. For example, `iorPublisher`.

Default— No value

Editing Level—Basic

`junos-ise` *junos-ise*—(Optional) [Alias: `intelligent-service-edge`] Initialization script for intelligent-service-edge device drivers. The script is run when the intelligent-service-edge device driver is activated or deactivated.

Value— Name of a script. For example, `iorPublisher`.

Default— No value

Editing Level—Basic

`junos-ptsp` *junos-ptsp*—(Optional) Initialization script for junos-ptsp device drivers. The script is run when the junos-ptsp device driver is activated or deactivated.

Value— Name of a script. For example, `iorPublisher`.

Default— No value

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration driver session-store

Syntax

```
shared sae configuration driver session-store {
    ip-address ip-address;
    port port;
    root-directory root-directory;
}
```

Hierarchy Level

```
[edit shared sae configuration driver session-store]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure global session store parameters that are shared by all session store instances (active or passive) on the SAE. You can also configure session store parameters within a router or other device driver configuration.

Options

ip-address ip-address—(Optional) IP address that the session store infrastructure on this SAE uses to listen for incoming TCP connections from active session stores.

Value— IP address. The address must be an IP address configured for the SAE host. If you do not enter an address or if you disable this field, active session stores cannot create passive session stores on this SAE. We recommend that you enter an address that is configured in a list of connected SAEs.

Default— No value

Editing Level—Advanced

port port—(Optional) TCP port number on which the session store infrastructure on this SAE listens for incoming connections from active session stores. This option has no effect if you have not configured a session store IP address.

Value— Port number in the range 1027–65535

Default— No value

Editing Level—Advanced

root-directory root-directory—(Optional) Root directory in which the session store

creates files. This option has no effect if you have not configured a session store IP address.

- Value**— Directory name
- Default**— *No value*
- Editing Level**—Advanced

Required Privilege Level

system

Required Editing Level

Advanced

shared sae configuration driver simulated

Syntax

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

Hierarchy Level

```
[edit shared sae configuration driver simulated]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure 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.

Options

name *name*— Name of the simulated router driver.

Value—Text

driver-type (junos | junose | pcmm)— Type of device that the simulated driver simulates

Value— One of the following:

- junos
- junose
- pcmm

Default— JUNOS

Editing Level—Basic

router-version *router-version*—(Optional) Version of the device software to

simulate.

Value— Valid software version for the device that is being simulated.

Default— No value

Editing Level—Basic

router-address router-address— Address of the router that is available for router initialization scripts.

Value— IP address

Default—10.0.0.1

Editing Level—Basic

transport-router transport-router—(Optional) 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 JUNOS routing platforms.

Value— Name of a virtual router

Default— No value

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration driver simulated *name* session-store

Syntax

```
shared sae configuration driver simulated name session-store {
    maximum-queue-age maximum-queue-age;
    maximum-queued-operations maximum-queued-operations;
    maximum-queue-size maximum-queue-size;
    maximum-file-size maximum-file-size;
    minimum-disk-space-usage minimum-disk-space-usage;
    rotation-batch-size rotation-batch-size;
    maximum-session-size maximum-session-size;
    disk-load-buffer-size disk-load-buffer-size;
    network-buffer-size network-buffer-size;
    retry-interval retry-interval;
    communications-timeout communications-timeout;
    load-timeout load-timeout;
    idle-timeout idle-timeout;
    maximum-backlog-ratio maximum-backlog-ratio;
    minimum-backlog minimum-backlog;
}
```

Hierarchy Level

```
[edit shared sae configuration driver simulated name session-store]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the session store for the simulated driver.

maximum-queue-age *maximum-queue-age*—(Optional) Maximum age that a queue of buffered store operations (such as adding a session to the store or removing a session from the store) can reach before the queue is written to a session store file.

Value— Number of milliseconds in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 5000

Editing Level—Advanced

maximum-queued-operations *maximum-queued-operations*—(Optional) Number of buffered store operations that are queued before the queue is written to a session store file.

Value— Integer in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 50

Editing Level—Advanced

`maximum-queue-size` *maximum-queue-size*—(Optional) Maximum size that a queue of buffered store operations can reach before the queue is written to a session store file.

Value— Number of bytes in the range 0–2147483647

Default— 51050

Editing Level—Advanced

`maximum-file-size` *maximum-file-size*—(Optional) Maximum size of session store files. When a file reaches this size, a new file is created.

Value— Number of bytes in the range 0–2147483647

Default— 25000000

Editing Level—Advanced

`minimum-disk-space-usage` *minimum-disk-space-usage*—(Optional) Percentage of space in all session store files that is used by live sessions. When the percentage of space in the session store files that is used by live sessions decreases to this percentage, the oldest session store file is compacted and appended to the newest session store file, and then the oldest session store file is deleted.

Value— Percentage of disk space in the range 1–100. We recommend a range of 30-50

Default— 25

Editing Level—Advanced

`rotation-batch-size` *rotation-batch-size*—(Optional) When the oldest session store file is rotated, specifies the number of sessions that are rotated from the oldest file to the newest file at the same time. While a set of sessions is rotated, no other session store activity can take place.

Value— Integer in the range 0–2147483647

Default— 50

Editing Level—Advanced

`maximum-session-size` *maximum-session-size*—(Optional) Maximum size of a single subscriber or service session. Use this parameter to reserve memory for an internal buffer.

Value— Number of bytes in the range 0–2147483647

Default— 10000
Editing Level—Advanced

`disk-load-buffer-size` *disk-load-buffer-size*—(Optional) Size of the buffer that is used to load all of a session store's files from disk at startup.

Value— Number of bytes in the range 0–2147483647
Default— 1000000
Editing Level—Advanced

`network-buffer-size` *network-buffer-size*—(Optional) Size of the buffer that holds messages or message segments that are waiting to be sent to passive session stores

Value— Number of bytes in the range 21+ <size of maximum session size field>–2147483647
Default— 51050
Editing Level—Advanced

`retry-interval` *retry-interval*—(Optional) Time interval between attempts by the active session store to connect to missing passive session stores.

Value— Number of milliseconds in the range 0–2147483647
Default— 5000
Editing Level—Advanced

`communications-timeout` *communications-timeout*—(Optional) Amount of time in milliseconds that a session store waits before closing when it is blocked from reading or writing a message. This timeout does not apply when a session store is waiting for a remote session store to load its state from disk. (A non-positive number means wait forever. This is not recommended.)

Value— Number of milliseconds
Default— 60000
Editing Level—Advanced

`load-timeout` *load-timeout*—(Optional) Amount of time in milliseconds that an active session store waits for a passive session store or a passive session store waits for an active session store to load its data from disk before it closes the connection to the session store. (A non-positive number means wait forever. This is not recommended.)

Value— Number of milliseconds
Default— 420000
Editing Level—Advanced

`idle-timeout` *idle-timeout*—(Optional) Amount of time that a passive session store

waits for activity from the active session store before it closes the connection to the active session store. This timeout applies after the session store startup and initial update processes are complete.

Value— Number of milliseconds in the range 0–2147483647

Default— 3600000

Editing Level—Advanced

`maximum-backlog-ratio` *maximum-backlog-ratio*—(Optional) Along with the minimum backlog size, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the backlog of unsent operations (in bytes) divided by the total size (in bytes) of all live store operations is greater than this number, the connection is closed.

Value— Floating point number

Default— 1.5

Editing Level—Advanced

`minimum-backlog` *minimum-backlog*—(Optional) Along with the maximum backlog ratio, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent to the passive session store. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the maximum backlog ratio is met, the active session store does not close the connection unless the backlog of messages (in bytes) is greater than this number.

Value— Number of bytes in the range 0–2147483647

Default— 5000000

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Advanced

shared sae configuration driver snmp

Syntax

```
shared sae configuration driver snmp {
    read-only-community-string read-only-community-string;
    read-write-community-string read-write-community-string;
}
```

Hierarchy Level

```
[edit shared sae configuration driver snmp]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure global default SNMP communities for use with JUNOSe routers and JUNOS routing platforms. Global default SNMP communities are used if a virtual router does not exist on the router or the community strings have not been configured for the VR.

Options

read-only-community-string read-only-community-string— Default SNMP community string used for read access to the router.

Value— SNMP community string that matches a read-only community string configured on the router.

Default— public

Editing Level—Normal

read-write-community-string read-write-community-string— Default SNMP community string used for write access to the router.

Value— SNMP community string that matches a read-write community string configured on the router.

Default— private

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration driver third-party

Syntax

```
shared sae configuration driver third-party {
    sae-community-manager sae-community-manager;
}
```

Hierarchy Level

```
[edit shared sae configuration driver third-party]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the community manager for third-party devices that the SAE manages.

sae-community-manager sae-community-manager— Name of the community manager that manages network device communities. Active SAEs are selected from this community.

Value— Community name

Default— PROXYCommunityManager

Editing Level—Expert

Required Privilege Level

system

Required Editing Level

Advanced

shared sae configuration driver third-party session-store

Syntax

```
shared sae configuration driver third-party session-store {
    maximum-queue-age maximum-queue-age;
    maximum-queued-operations maximum-queued-operations;
    maximum-queue-size maximum-queue-size;
    maximum-file-size maximum-file-size;
    minimum-disk-space-usage minimum-disk-space-usage;
    rotation-batch-size rotation-batch-size;
    maximum-session-size maximum-session-size;
    disk-load-buffer-size disk-load-buffer-size;
    network-buffer-size network-buffer-size;
    retry-interval retry-interval;
    communications-timeout communications-timeout;
    load-timeout load-timeout;
    idle-timeout idle-timeout;
    maximum-backlog-ratio maximum-backlog-ratio;
    minimum-backlog minimum-backlog;
}
```

Hierarchy Level

```
[edit shared sae configuration driver third-party session-store]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the session store for the third-party device driver.

maximum-queue-age maximum-queue-age—(Optional) Maximum age that a queue of buffered store operations (such as adding a session to the store or removing a session from the store) can reach before the queue is written to a session store file.

Value— Number of milliseconds in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 5000

Editing Level—Advanced

maximum-queued-operations maximum-queued-operations—(Optional) Number of buffered store operations that are queued before the queue is written to a session store file.

Value— Integer in the range 0–2147483647. A value of -1 indicates that there is no limit. A value of zero causes the session store to write each store operation to a session store file immediately.

Default— 50

Editing Level—Advanced

`maximum-queue-size` *maximum-queue-size*—(Optional) Maximum size that a queue of buffered store operations can reach before the queue is written to a session store file.

Value— Number of bytes in the range 0–2147483647

Default— 51050

Editing Level—Advanced

`maximum-file-size` *maximum-file-size*—(Optional) Maximum size of session store files. When a file reaches this size, a new file is created.

Value— Number of bytes in the range 0–2147483647

Default— 25000000

Editing Level—Advanced

`minimum-disk-space-usage` *minimum-disk-space-usage*—(Optional) Percentage of space in all session store files that is used by live sessions. When the percentage of space in the session store files that is used by live sessions decreases to this percentage, the oldest session store file is compacted and appended to the newest session store file, and then the oldest session store file is deleted.

Value— Percentage of disk space in the range 1–100. We recommend a range of 30-50

Default— 25

Editing Level—Advanced

`rotation-batch-size` *rotation-batch-size*—(Optional) When the oldest session store file is rotated, specifies the number of sessions that are rotated from the oldest file to the newest file at the same time. While a set of sessions is rotated, no other session store activity can take place.

Value— Integer in the range 0–2147483647

Default— 50

Editing Level—Advanced

`maximum-session-size` *maximum-session-size*—(Optional) Maximum size of a single subscriber or service session. Use this parameter to reserve memory for an internal buffer.

Value— Number of bytes in the range 0–2147483647

Default— 10000

Editing Level—Advanced

`disk-load-buffer-size` *disk-load-buffer-size*—(Optional) Size of the buffer that is used to load all of a session store's files from disk at startup.

Value— Number of bytes in the range 0–2147483647

Default— 1000000

Editing Level—Advanced

`network-buffer-size` *network-buffer-size*—(Optional) Size of the buffer that holds messages or message segments that are waiting to be sent to passive session stores

Value— Number of bytes in the range 21+ <size of maximum session size field>–2147483647

Default— 51050

Editing Level—Advanced

`retry-interval` *retry-interval*—(Optional) Time interval between attempts by the active session store to connect to missing passive session stores.

Value— Number of milliseconds in the range 0–2147483647

Default— 5000

Editing Level—Advanced

`communications-timeout` *communications-timeout*—(Optional) Amount of time in milliseconds that a session store waits before closing when it is blocked from reading or writing a message. This timeout does not apply when a session store is waiting for a remote session store to load its state from disk. (A non-positive number means wait forever. This is not recommended.)

Value— Number of milliseconds

Default— 60000

Editing Level—Advanced

`load-timeout` *load-timeout*—(Optional) Amount of time in milliseconds that an active session store waits for a passive session store or a passive session store waits for an active session store to load its data from disk before it closes the connection to the session store. (A non-positive number means wait forever. This is not recommended.)

Value— Number of milliseconds

Default— 420000

Editing Level—Advanced

`idle-timeout` *idle-timeout*—(Optional) Amount of time that a passive session store waits for activity from the active session store before it closes the connection to the active

session store. This timeout applies after the session store startup and initial update processes are complete.

Value— Number of milliseconds in the range 0–2147483647

Default— 3600000

Editing Level—Advanced

`maximum-backlog-ratio` *maximum-backlog-ratio*—(Optional) Along with the minimum backlog size, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the backlog of unsent operations (in bytes) divided by the total size (in bytes) of all live store operations is greater than this number, the connection is closed.

Value— Floating point number

Default— 1.5

Editing Level—Advanced

`minimum-backlog` *minimum-backlog*—(Optional) Along with the maximum backlog ratio, specifies when the active session store closes the connection to a passive session store because of a backlog of messages waiting to be sent to the passive session store. After the startup and initial update processes are complete, if the backlog becomes too large, the connection to the passive session store is closed. After the retry interval ends, a new connection is opened.

If the maximum backlog ratio is met, the active session store does not close the connection unless the backlog of messages (in bytes) is greater than this number.

Value— Number of bytes in the range 0–2147483647

Default— 5000000

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Advanced

shared sae configuration dynamic-radius-server

Syntax

```
shared sae configuration dynamic-radius-server {
    maximum-cached-peer maximum-cached-peer;
}
```

Hierarchy Level

```
[edit shared sae configuration dynamic-radius-server]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the number of peers that the dynamic RADIUS server can maintain.

Options

maximum-cached-peer maximum-cached-peer— Maximum number of peers maintained by the dynamic RADIUS server.

Value— Integer

Default— 100

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration external-interface-features

Syntax

```
shared sae configuration external-interface-features name ...
```

Hierarchy Level

```
[edit shared sae configuration external-interface-features]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Create an external interface configuration.

Options

name name— Name of the external interface configuration.

Value—Text

Required Privilege Level

system

Required Editing Level

Advanced

shared sae configuration external-interface-features *name* CommunityManager

Syntax

```
shared sae configuration external-interface-features name CommunityManager {
    keepalive-interval keepalive-interval;
    threads threads;
    acquire-timeout acquire-timeout;
    blackout-time blackout-time;
}
```

Hierarchy Level

```
[edit shared sae configuration external-interface-features name CommunityManager]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the SAE community manager that manages PCMM and third-party device communities.

keepalive-interval keepalive-interval— Interval between keepalive messages sent from the active SAE to the passive members of the community.

Value— Number of seconds in the range 0–2147483647

Default— 30

Editing Level—Basic

threads threads— Number of threads that are allocated to manage the community. You generally do not need to change this property.

Value— Integer in the range 1–50

Default— 5

Editing Level—Basic

acquire-timeout acquire-timeout— Amount of time an SAE waits for a remote member of the community when it is acquiring a distributed lock. To avoid race conditions when the SAE community is determining which SAE is the active SAE, the community manager has a distributed lock. When an SAE attempts to become the active SAE, it needs to acquire the distributed lock. You generally do not need to change this property.

Value— Number of seconds in the range 0–2147483647

Default— 15

Editing Level—Advanced

`blackout-time` *blackout-time*— Amount of time that an active SAE must wait after it shuts down before it can try to become the active SAE of the community again.

Value— Number of seconds in the range 0–2147483647

Default— 30

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration external-interface-features *name* EventAPI

Syntax

```
shared sae configuration external-interface-features name EventAPI {
    retry-time retry-time;
    retry-limit retry-limit;
    threads threads;
}
```

Hierarchy Level

```
[edit shared sae configuration external-interface-features name EventAPI]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure properties for the Event Notification API.

`retry-time retry-time`— Amount of time between attempts to send router events that could not be delivered.

Value— Number of seconds in the range 0–2147483647

Default— 300

Editing Level—Basic

`retry-limit retry-limit`— Maximum number of times an event fails to be delivered before it is discarded.

Value— Integer in the range 0–2147483647

Default— 5

Editing Level—Basic

`threads threads`— Number of threads allocated to process events.

Value— Integer in the range 0–2147483647

Default— 5

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration external-interface-features *name* JavaScriptProcessor

Syntax

```
shared sae configuration external-interface-features name JavaScriptProcessor {
    script-directory script-directory;
    scan-interval scan-interval;
    compiler-classpath compiler-classpath;
    character-encoding character-encoding;
    compiler-debug;
    java-compiler java-compiler;
}
```

Hierarchy Level

```
[edit shared sae configuration external-interface-features name JavaScriptProcessor]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the SAE properties that activate and configure the Java script interface module.

script-directory script-directory—(Optional) Storage location for Java scripts; defined relative to the SAE installation directory. If you store the scripts in the /opt/UMC/sae/var/javaScripts directory on the SRC system, you do not need to specify this property.

Do not specify a directory that is part of the class path of the JVM running the SAE. If you do so, unloading of Java scripts will fail.

Value— Path that can be read by a URL class loader, in one of the following formats:

- file: //<path><filename>
- http: //<hostName>.<portNumber><path><filename>
- path—List of directories separated by forward slashes
- filename—Name of the JAR file
- hostName—Name of the host on which the script is stored
- portNumber—Number of the TCP/IP port

Default— *var/javaScripts*

Editing Level—Advanced

`scan-interval` *scan-interval*— Time interval between scans in the script directory for new or modified .java source files. At each scan, the interface module compiles new and modified files. If the scripts conform to Java script requirements, the interface module installs them on the SAE as Java scripts. It also removes deleted scripts from the SAE.

Value— Number of seconds in the range 0–2147483647; 0 (zero) means that the interface module does not scan the directories.

Default— 0

Editing Level—Advanced

`compiler-classpath` *compiler-classpath*— Class path that the compiler uses to load source files.

Value— Path that can be read by a URL class loader, in one of the following formats:

- file: `//<path><filename>`
- http: `//<hostName>.<portNumber><path><filename>`
- path—List of directories separated by forward slashes
- filename—Name of the JAR file
- hostName—Name of the host on which the script is stored
- portNumber—Number of the TCP/IP port

If you clear this value, the value defaults to the Java script directory specified by the script-directory option.

Default— `var/javaScripts/lib/sae.jar`

Editing Level—Advanced

`character-encoding` *character-encoding*—(Optional) Character encoding that the compiler uses when it loads Java source files.

Value— See <http://java.sun.com/j2se/1.4/docs/guide/intl/encoding.doc.html>

Default— Default encoding for the platform on which you are working

Editing Level—Advanced

`compiler-debug`—(Optional) Enables or disables whether the compiler places debug information into .class files

Default— Disabled

Editing Level—Advanced

`java-compiler` *java-compiler*—(Optional)

If you do not specify an external compiler, the interface module compiles the scripts-in-process with the `com.sun.tools.javac.Main` compiler from Sun Microsystems's `tools.jar`. The information specified in the Character Encoding, Compiler Classpath, and Compiler Debug fields is passed to the compiler.

If you specify an external compiler, an external process is created to perform the compilation using the specified command, and the information specified in the Character Encoding, Compiler Classpath, and Compiler Debug fields is ignored. Assumptions:

- The specified shell command will invoke an appropriate Java compiler without error.
- The specified shell command uses a class path that includes both the Java script directory specified in the Script Directory field and the SAE's public APIs.
- The compiler outputs its `.class` files to the directory specified in the Script Directory field.

Value— Command string with the class path that identifies both the Java script directory and the public APIs for the SAE.

Default— `javac -classpath var/javaScripts:lib/sae.jar -d var/javaScripts`

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration external-interface-features *name* PythonScriptProcessor

Syntax

```
shared sae configuration external-interface-features name PythonScriptProcessor {  
}
```

Hierarchy Level

```
[edit shared sae configuration external-interface-features name PythonScriptProcessor]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Create an instance of the Python script processor.

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration external-interface-features *name* SAEAccess

Syntax

```
shared sae configuration external-interface-features name SAEAccess {
    cache-size cache-size;
    cache-timeout cache-timeout;
    cache-clean cache-clean;
}
```

Hierarchy Level

```
[edit shared sae configuration external-interface-features name SAEAccess]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure properties for the SAE access interface module.

`cache-size cache-size`— Maximum number of subscriber objects kept in the cache.

Value— Integer in the range 0–2147483647

Default— 1024

Editing Level—Normal

`cache-timeout cache-timeout`— Maximum time that idle subscriber objects are kept in the cache.

Value— Number of seconds in the range 0–2147483647

Default— 30

Editing Level—Normal

`cache-clean cache-clean`— Number of subscriber objects removed from the cache when the maximum number is reached.

Value— Integer in the range 1–<cache size>

Default— 1

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration external-interface-features *name* SAEFeature

Syntax

```
shared sae configuration external-interface-features name SAEFeature {
    java-class java-class;
    additional-classpath additional-classpath;
}
```

Hierarchy Level

```
[edit shared sae configuration external-interface-features name SAEFeature]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure SAE properties for customized interface modules.

java-class java-class— Name of the Java class that implements the interface module.

Value— Fully qualified Java class name. For example, net.juniper.smgmt.sae.saeimpl.SAEAccessImpl.

Default— No value

Editing Level—Normal

additional-classpath additional-classpath—(Optional) Path to the location where libraries are stored. If you store the libraries in the /opt/UMC/sae/lib directory on the host where you installed the SAE software, you do not need to specify a class path.

Value— Comma-separated list of URLs that can be read by a URL class loader in one of the following formats:

- file://<path><filename>
- http://<hostName><portNumber><path><filename>

where

- path is a list of directories separated by backslashes
- filename is the name of the JAR file
- hostName is the name of the host on which the script is stored
- portNumber is the number of the TCP/IP port

Default— No value
Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration external-interface-features *name* SAEFeature properties

Syntax

```
shared sae configuration external-interface-features name SAEFeature properties name {  
    value;  
}
```

Hierarchy Level

```
[edit shared sae configuration external-interface-features name SAEFeature properties]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Define properties for an SAE customized interface module.

Options

name name— Name of the property for which you want to define a value.

Value—Text

value— Value for the property.

- Value**— Value for the property.
- Default**— No value
- Editing Level**—Basic

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration file-accounting-template

Syntax

```
shared sae configuration file-accounting-template name ...
```

Hierarchy Level

```
[edit shared sae configuration file-accounting-template]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a template that defines header names for attributes listed in accounting files. When the SAE writes data to a flat file, it writes into the first line the headers that identify the attributes in the file. For example, in the following accounting file, the first line lists headers for all attribute fields in the file, and the following lines list the actual data in each field:

Accounting Status,NAS ID,SAE Host,Router Name,Interface Name,Interface Alias

start,SSP.uelmo,uelmo,default@erx7_ssp57,FastEthernet1/1.1.

You can assign your own names to the headers that appear in the file. To do so, you define the header names in a template and then set up file accounting plug-ins to use the template. The default template, FileAccounting.std, defines header names for all possible attributes. You can use the default template or create your own templates.

Options

name name— Name of the file-accounting template.

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration file-accounting-template *name* attributes

Syntax

```
shared sae configuration file-accounting-template name attributes (status | nas-
id | host | router-name | interface-name | interface-alias | interface-descr |
port-id | user-ip-address | login-name | accounting-id | auth-user-id | if-radius-
class | if-session-id | service-name | radius-class | event-time | session-id |
terminate-cause | session-time | in-octets | out-octets | in-packets | out-
packets | nas-ip | user-mac-address | service-session-name | service-session-tag
| user-type | user-radius-class | user-session-id | primary-user-name |
subscription-name | login-id | if-index | event-time-millisecond | nas-port |
operational | user-inet-address | nas-inet-address | router-type | interface-
speed | service-bundle | user-dn | uid | domain | retailer-dn | password |
service-scope | session-timeout | downstream-bandwidth | upstream-bandwidth |
dhcp-packet | aggr-session-id | aggr-login-name | aggr-user-dn | aggr-user-inet-
address | aggr-accounting-id | aggr-auth-user-id | user-session-handle | calling-
station-id) {
    value;
}
```

Hierarchy Level

```
[edit shared sae configuration file-accounting-template name attributes]
```

Description

Configure the values for the attribute headers that will appear in accounting files.

Options

Name of the accounting attribute for which you want to define a header.

Value

- status
- nas-id
- host
- router-name
- interface-name
- interface-alias
- interface-descr
- port-id
- user-ip-address
- login-name
- accounting-id
- auth-user-id
- if-radius-class

- . if-session-id
- . service-name
- . radius-class
- . event-time
- . session-id
- . terminate-cause
- . session-time
- . in-octets
- . out-octets
- . in-packets
- . out-packets
- . nas-ip
- . user-mac-address
- . service-session-name
- . service-session-tag
- . user-type
- . user-radius-class
- . user-session-id
- . primary-user-name
- . subscription-name
- . login-id
- . if-index
- . event-time-millisecond
- . nas-port
- . operational
- . user-inet-address
- . nas-inet-address
- . router-type
- . interface-speed
- . service-bundle
- . user-dn
- . uid
- . domain
- . retailer-dn
- . password
- . service-scope
- . session-timeout
- . downstream-bandwidth
- . upstream-bandwidth
- . dhcp-packet
- . aggr-session-id
- . aggr-login-name
- . aggr-user-dn
- . aggr-user-inet-address
- . aggr-accounting-id
- . aggr-auth-user-id
- . user-session-handle
- . calling-station-id

value— Header text that appears in the accounting file.

Value— Text that you want to appear as the header in the property file. If the header contains spaces, enclose the header in quotation marks.

Default— No value

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration global-radius-udp-port

Syntax

```
shared sae configuration global-radius-udp-port {
    udp-port;
}
```

Hierarchy Level

```
[edit shared sae configuration global-radius-udp-port]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a global source UDP port or a pool of ports that RADIUS plug-ins use to communicate with RADIUS servers.

In RADIUS packets that RADIUS plug-ins send to a RADIUS server, the plug-in uses an identifier field to match requests to replies. This field provides for a maximum of 256 identifiers. Once all identifiers are used, the plug-in cannot send any more requests until it receives replies that match the requests already sent. In high-load systems, this limit can slow performance.

To overcome this limitation, you can configure a pool of UDP ports for RADIUS plug-ins. Having a pool of ports allows RADIUS plug-ins to create one queue per port to wait for RADIUS replies. Each queue can wait for 256 RADIUS packets. The RADIUS plug-ins send RADIUS packets through the pool of ports in a round-robin mode.

Options

udp-port— Global source UDP port or a pool of ports that RADIUS plug-ins use to communicate with RADIUS servers. You can also configure UDP ports for each plug-in instance. If you do not configure a UDP port for a plug-in instance, the plug-in uses the global UDP port.

Value— You can enter a single port number, a pool of port numbers, or a list of port numbers and port ranges:

- Port number in the range 1–65535
- A range of ports in the format port-port; for example, 7000-7003

Default— 18130

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Advanced

shared sae configuration idle-timeout

Syntax

```
shared sae configuration idle-timeout {
    adjust-session-time;
}
```

Hierarchy Level

```
[edit shared sae configuration idle-timeout]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify whether or not the SAE reduces the session time reported in the accounting stop message by the idle time. This way the session time is accurately reported to avoid overcharges for the session.

Options

`adjust-session-time`—(Optional) If enabled, when an idle timeout terminates a session, the session time reported in the accounting stop message is reduced by the idle time.

Default— No value
Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Advanced

shared sae configuration interim-accounting

Syntax

```
shared sae configuration interim-accounting {
    service-interim-accounting;
    service-interim-interval service-interim-interval;
    subscriber-interim-accounting;
    subscriber-interim-interval subscriber-interim-interval;
}
```

Hierarchy Level

```
[edit shared sae configuration interim-accounting]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Enable interim accounting and set intervals between interim accounting messages for services and subscribers. These settings apply to all subscriber sessions and service sessions. You can override these settings for specific services by configuring an accounting interim interval in the service configuration.

Options

service-interim-accounting—(Optional) Enable interim accounting for services. You can override this setting for specific services by configuring an accounting interim interval in the service configuration.

Default— Enabled
Editing Level—Basic

service-interim-interval *service-interim-interval*— Interval between service interim accounting messages. A short interval causes the SAE to send many messages to the router and to the RADIUS servers. A long interval can result in a large loss of accounting information in the event of a system failure.

Value— Number of seconds in the range 900–86400
Default— 900
Editing Level—Basic

subscriber-interim-accounting—(Optional) Enable interim accounting for subscribers. If enabled, the SAE continually generates Interim-Update accounting requests

for all active subscribers at the interval specified with the **subscriber-interim-interval** option.

Default— Enabled

Editing Level—Basic

`subscriber-interim-interval` *subscriber-interim-interval*— Interval between subscriber interim accounting messages. A short interval causes the SAE to send many messages to any configured accounting servers. A long interval can result in a large loss of accounting information in the event of a system failure.

Value— Number of seconds in the range 900–86400

Default— 900

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration interim-session-job-manager

Syntax

```
shared sae configuration interim-session-job-manager {
    number-of-threads number-of-threads;
}
```

Hierarchy Level

```
[edit shared sae configuration interim-session-job-manager]
```

Release Information

Statement introduced in SRC Release 3.1.0

Description

Configure the number of threads used for interim-session-related activity; for example, subscriber and service session interim accounting.

Options

`number-of-threads number-of-threads`— Number of threads used for interim-session-related activity.

Value— Integer in the range 1–1000

Default— 32

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Expert

shared sae configuration ldap

Syntax

```
shared sae configuration ldap {
    network-dn network-dn;
    enable-directory-eventing;
}
```

Hierarchy Level

```
[edit shared sae configuration ldap]
```

Description

Configure the LDAP connection from the SAE to the directory in which network device data is stored.

Options

`network-dn network-dn`— Subtree in the directory in which network device data is stored.

Value— <DN>. You can use the special value <base> to refer to the globally configured base DN. The string <base> is replaced with the directory base DN.

Default— `o=Network,<base>`

Editing Level—Expert

`enable-directory-eventing`—(Optional) Enables or disables automatic discovery of changes in the SAE configuration data.

Default— Enabled

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration ldap directory-eventing

Syntax

```
shared sae configuration ldap directory-eventing {
    timeout timeout;
    dispatcher-pool-size dispatcher-pool-size;
}
```

Hierarchy Level

```
[edit shared sae configuration ldap directory-eventing]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a timeout for SAE directory eventing, and specify the number of events that the SAE can receive from the directory simultaneously.

Options

`timeout timeout`— Maximum time that the directory eventing system waits for the directory to respond.

Value— Number of seconds in the range 1–2147483647

Default— No value

Editing Level—Basic

`dispatcher-pool-size dispatcher-pool-size`— Number of events that the SAE can receive from the directory simultaneously.

Value— Integer in the range 1–2147483647

Default— No value

Editing Level—Expert

Required Privilege Level

system

Required Editing Level

Expert

shared sae configuration ldap persistent-login-cache

Syntax

```
shared sae configuration ldap persistent-login-cache {
    dn dn;
    server-address [server-address...];
    port-number port-number;
    authentication-dn authentication-dn;
    password password;
    directory-eventing;
    polling-interval polling-interval;
    blacklist;
    (ldaps);
}
```

Hierarchy Level

```
[edit shared sae configuration ldap persistent-login-cache]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the LDAP connection from the SAE to the directory in which persistent login cache data is stored.

Options

dn dn— Subtree in the directory in which persistent login cache data is stored.

Value— <DN>. You can use the special value <base> to refer to the globally configured base DN. The string <base> is replaced with the directory base DN.

Default— o=authCache,<base>

Editing Level—Normal

server-address [server-address...]—(Optional) Directory server that stores information.

Value— IP address or hostname. For multiple directory servers, enclose the addresses or hostnames in quotes and separate addresses or names with a space. For example: "127.153.27.1 192.168.0.1".

Default— No value

Editing Level—Normal

`port-number` *port-number*—(Optional) Directory port number

Value—Integer in the range -2147483648–2147483647

Default— 389

Editing Level—Normal

`authentication-dn` *authentication-dn*—(Optional) DN that the SAE uses to authenticate access to the directory server. The specified directory entry must exist and have read access to all attributes.

For subscriber data, the entry must have write access if subscribers are allowed to customize their subscription profiles.

Value— <DN>. You can use the special value <base> to refer to the globally configured base DN. The string <base> is replaced with the directory base DN.

Default— No value

Editing Level—Normal

`password` *password*—(Optional) Password used to authenticate access to the directory server. You must configure the password in the directory to authenticate read access to the directory.

Value— Text string or base64 string.

For authentication to access subscriber data, the password must match the value of the `userPassword` attribute of the authentication DN.

Default— No value

Editing Level—Normal

`directory-eventing`—(Optional) Enables or disables automatic discovery of changes to directory data.

For subscriber data:

- If enabled, changes in the subscriber profile or subscriptions take effect automatically while the subscriber is logged in.
- If disabled, changes in the subscriber profile or subscriptions do not take effect until the next time the subscriber logs in.

For service data:

- If enabled, changes in service definitions take effect automatically. If a changed

service is in use, all service instances are deactivated and then reactivated with the modified settings. Consequently, service may be affected for subscribers who are logged in at the time of the modification.

- If disabled, changes in service definitions do not take effect until you restart the SAE.

Default— Disabled

Editing Level—Advanced

`polling-interval` *polling-interval*— Frequency for checking the directory for changes.

Value— Number of seconds in the range 15–86400

Default— 30

Editing Level—Advanced

`blacklist`—(Optional) Specifies whether the directory monitoring system prevents connection to a directory if the directory fails to respond during 10 polling intervals.

Value— true or false

Default— true

Editing Level—Advanced

`ldaps`—Enables LDAPS as the secure protocol for connections to the directory server.

Value— `ldaps`—Enable LDAPS

Default— Disabled

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration ldap policy-data

Syntax

```
shared sae configuration ldap policy-data {
    policy-dn policy-dn;
    parameter-dn parameter-dn;
    directory-eventing;
    polling-interval polling-interval;
}
```

Hierarchy Level

```
[edit shared sae configuration ldap policy-data]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the LDAP connection from the SAE to the directory in which service data is stored.

Options

policy-dn policy-dn— Subtree in the directory in which policy data is stored.

Value— <DN>. You can use the special value <base> to refer to the globally configured base DN. The string <base> is replaced with the directory base DN.

Default— *o=Policies,<base>*

Editing Level—Normal

parameter-dn parameter-dn— Subtree in the directory in which policy parameter data is stored.

Value— <DN>. You can use the special value <base> to refer to the globally configured base DN. The string <base> is replaced with the directory base DN.

Default— *o=Parameters,<base>*

Editing Level—Normal

directory-eventing—(Optional) Enables or disables automatic discovery of changes to directory data.

- If enabled, changes in policy definitions take effect automatically. If a changed policy is in use, all policy instances are deactivated and then reactivated with the modified settings. Consequently, service may be affected for subscribers who are logged in when the change is made.
- If disabled, changes in policy definitions do not take effect until you restart the SAE.

Default— Disabled

Editing Level—Advanced

`polling-interval` *polling-interval*— Frequency for checking the directory for changes.

Value— Number of seconds in the range 15–86400

Default— 30

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration ldap service-data

Syntax

```
shared sae configuration ldap service-data {
    dn dn;
    server-address [server-address...];
    port-number port-number;
    authentication-dn authentication-dn;
    password password;
    directory-eventing;
    polling-interval polling-interval;
    blacklist;
    (ldaps);
}
```

Hierarchy Level

```
[edit shared sae configuration ldap service-data]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the LDAP connection from the SAE to the directory in which service data is stored.

Options

dn dn— Subtree in the directory in which service data is stored.

The SAE loads service definitions on startup and when service reloading is requested.

Value— <DN>. You can use the special value <base> to refer to the globally configured base DN. The string <base> is replaced with the directory base DN.

Default— <base>

Editing Level—Normal

server-address [server-address...]—(Optional) Directory server that stores information.

Value— IP address or hostname. For multiple directory servers, enclose the addresses or hostnames in quotes and separate addresses or names

with a space. For example: "127.153.27.1 192.168.0.1".

Default— No value

Editing Level—Normal

`port-number` *port-number*—(Optional) Directory port number

Value—Integer in the range -2147483648–2147483647

Default— 389

Editing Level—Normal

`authentication-dn` *authentication-dn*—(Optional) DN that the SAE uses to authenticate access to the directory server. The specified directory entry must exist and have read access to all attributes.

For subscriber data, the entry must have write access if subscribers are allowed to customize their subscription profiles.

Value— <DN>. You can use the special value <base> to refer to the globally configured base DN. The string <base> is replaced with the directory base DN.

Default— No value

Editing Level—Normal

`password` *password*—(Optional) Password used to authenticate access to the directory server. You must configure the password in the directory to authenticate read access to the directory.

Value— Text string or base64 string.

For authentication to access subscriber data, the password must match the value of the `userPassword` attribute of the authentication DN.

Default— No value

Editing Level—Normal

`directory-eventing`—(Optional) Enables or disables automatic discovery of changes to directory data.

For subscriber data:

- If enabled, changes in the subscriber profile or subscriptions take effect automatically while the subscriber is logged in.
- If disabled, changes in the subscriber profile or subscriptions do not take effect until the next time the subscriber logs in.

For service data:

- If enabled, changes in service definitions take effect automatically. If a changed service is in use, all service instances are deactivated and then reactivated with the modified settings. Consequently, service may be affected for subscribers who are logged in at the time of the modification.
- If disabled, changes in service definitions do not take effect until you restart the SAE.

Default— Disabled

Editing Level—Advanced

`polling-interval` *polling-interval*— Frequency for checking the directory for changes.

Value— Number of seconds in the range 15–86400

Default— 30

Editing Level—Advanced

`blacklist`—(Optional) Specifies whether the directory monitoring system prevents connection to a directory if the directory fails to respond during 10 polling intervals.

Value— true or false

Default— true

Editing Level—Advanced

`ldaps`—Enables LDAPS as the secure protocol for connections to the directory server.

Value— `ldaps`—Enable LDAPS

Default— Disabled

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration ldap subscriber-data

Syntax

```
shared sae configuration ldap subscriber-data {
    subscription-loading-filter (subscriberRefFilter | objectClassFilter);
    load-subscriber-schedules;
    persistent-sessions;
    login-cache-dn login-cache-dn;
    session-cache-dn session-cache-dn;
    dn dn;
    server-address [server-address...];
    port-number port-number;
    authentication-dn authentication-dn;
    password password;
    directory-eventing;
    polling-interval polling-interval;
    blacklist;
    (ldaps);
}
```

Hierarchy Level

```
[edit shared sae configuration ldap subscriber-data]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the LDAP connection from the SAE to the directory in which subscriber data is stored.

Options

`subscription-loading-filter (subscriberRefFilter | objectClassFilter)`
 — Filter that the SAE uses to search for subscriptions in the directory when the SAE loads a subscription.

Value— One of the following:

- `subscriberRefFilter`—Subscriber reference filter. The SAE runs a search based on the `subscriberRef` attribute in the `umcServiceProfile` object, which is the base object class of the service profile hierarchy. The `subscriberRef` attribute contains a DN that points to the parent of the subscriber object.
- `objectClassFilter`—Subscription Objectclass filter. The SAE performs a one-level search with the directory entry, which

represents the subscriber folder as the base DN. The search filter is (objectClass=sspServiceProfile). This method can be slow if you have a large number of subscription entries within the subscriber folder subtree.

Default— objectClassFilter

Editing Level—Normal

`load-subscriber-schedules`—(Optional) Enable or disable loading of subscriber schedules.

Default— Enabled

Editing Level—Normal

`persistent-sessions`—(Optional) Load existing persistent sessions and schedules when starting or recovering a user session.

Default—false

Editing Level—Normal

`login-cache-dn` *login-cache-dn*— Subtree in the directory where subscriber login information is cached. When a subscriber logs in to a residential portal, the SAE searches subscriber profiles by mapping the realm of the login name to a retailer object found below the search base.

Value— <DN>. You can use the special value <base> to refer to the globally configured base DN. The string <base> is replaced with the directory base DN.

Default— *o=userProfileCache,<base>*

Editing Level—Normal

`session-cache-dn` *session-cache-dn*— Subtree in the directory where persistent session data is cached.

Value— <DN>. You can use the special value <base> to refer to the globally configured base DN. The string <base> is replaced with the directory base DN.

Default— *o=PersistentSessions,<base>*

Editing Level—Normal

`dn` *dn*— Subtree in the directory in which subscriber data is stored.

When a subscriber logs in to a residential portal, the SAE searches subscriber profiles by mapping the realm of the login name to a retailer object found below the DN.

Value— <DN>. You can use the special value <base> to refer to the globally configured base DN. The string <base> is replaced with the directory base DN.

Default— o=Users,<base>

Editing Level—Normal

`server-address` [*server-address...*]—(Optional) Directory server that stores information.

Value— IP address or hostname. For multiple directory servers, enclose the addresses or hostnames in quotes and separate addresses or names with a space. For example: "127.153.27.1 192.168.0.1".

Default— No value

Editing Level—Normal

`port-number` *port-number*—(Optional) Directory port number

Value—Integer in the range -2147483648–2147483647

Default— 389

Editing Level—Normal

`authentication-dn` *authentication-dn*—(Optional) DN that the SAE uses to authenticate access to the directory server. The specified directory entry must exist and have read access to all attributes.

For subscriber data, the entry must have write access if subscribers are allowed to customize their subscription profiles.

Value— <DN>. You can use the special value <base> to refer to the globally configured base DN. The string <base> is replaced with the directory base DN.

Default— No value

Editing Level—Normal

`password` *password*—(Optional) Password used to authenticate access to the directory server. You must configure the password in the directory to authenticate read access to the directory.

Value— Text string or base64 string.

For authentication to access subscriber data, the password must match the value of the userPassword attribute of the authentication DN.

Default— No value

Editing Level—Normal

`directory-eventing`—(Optional) Enables or disables automatic discovery of changes to directory data.

For subscriber data:

- If enabled, changes in the subscriber profile or subscriptions take effect automatically while the subscriber is logged in.
- If disabled, changes in the subscriber profile or subscriptions do not take effect until the next time the subscriber logs in.

For service data:

- If enabled, changes in service definitions take effect automatically. If a changed service is in use, all service instances are deactivated and then reactivated with the modified settings. Consequently, service may be affected for subscribers who are logged in at the time of the modification.
- If disabled, changes in service definitions do not take effect until you restart the SAE.

Default— Disabled

Editing Level—Advanced

`polling-interval` *polling-interval*— Frequency for checking the directory for changes.

Value— Number of seconds in the range 15–86400

Default— 30

Editing Level—Advanced

`blacklist`—(Optional) Specifies whether the directory monitoring system prevents connection to a directory if the directory fails to respond during 10 polling intervals.

Value— true or false

Default— true

Editing Level—Advanced

`ldaps`—Enables LDAPS as the secure protocol for connections to the directory server.

Value— ldaps—Enable LDAPS

Default— Disabled

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration license-manager client

Syntax

```
shared sae configuration license-manager client {
    type type;
    cache cache;
}
```

Hierarchy Level

```
[edit shared sae configuration license-manager client]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the license manager client.

Options

`type type`— Type of the license client.

Value— SDX is currently the only valid value

Default— SDX

Editing Level—Expert

`cache cache`— Path to a cache file.

Value— Valid path

Default— var/run/lic_cache

Editing Level—Expert

Required Privilege Level

system

Required Editing Level

Expert

shared sae configuration license-manager directory-access

Syntax

```
shared sae configuration license-manager directory-access {
    server-address server-address;
    server-port server-port;
    license-dn license-dn;
    authentication-dn authentication-dn;
    password password;
    (ldaps);
    connection-manager-id connection-manager-id;
    event-base-dn event-base-dn;
    signature-dn signature-dn;
    snmp-agent;
}
```

Hierarchy Level

```
[edit shared sae configuration license-manager directory-access]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure directory access to the license manager.

Options

server-address server-address—(Optional) IP addresses or hostnames of the directory server that stores licensing data.

Value— IP address or hostname. For multiple directory servers, enclose the addresses or hostnames in quotes and separate addresses or names with a space.

Default— No value

Editing Level—Normal

server-port server-port—(Optional) Port number of the LDAP connection to the directory server that stores licensing data.

Value— Port number in the range 0–65535

Default— 389

Editing Level—Normal

`license-dn` *license-dn*—(Optional) Subtree in the directory where licensing information is stored. The SAE searches for the license key below this path.

Value— <DN>. The string <base> is replaced with the directory base DN

Default— ou=Licenses, o=Management, <base>

Editing Level—Normal

`authentication-dn` *authentication-dn*—(Optional) DN the SAE uses to authenticate access to the directory server.

Value— <DN>. The string <base> is replaced with the directory base DN

Default— No value

Editing Level—Normal

`password` *password*—(Optional) Password used to authenticate access to the directory.

Value— Text string or Base64 string

Default— No value

Editing Level—Normal

Enables or disables LDAPS as the secure protocol for connections to the directory server that stores license data.

Value

• `ldaps`—

Default— Disabled

Editing Level—Normal

`connection-manager-id` *connection-manager-id*— DES connection manager within the Java Naming and Directory Interface (JNDI) framework.

Value— Text

Default— LICENSE_MANAGER

Editing Level—Expert

`event-base-dn` *event-base-dn*—(Optional) Directory eventing base DN for the license manager data.

Value— <DN>. The string <base> is replaced with the directory base DN

Default— No value

Editing Level—Expert

`signature-dn signature-dn`—(Optional) DN of the entry that specifies the LDAP schema attribute usedDirectory. This attribute identifies the type of directory, such as openLDAP or DirX, on which the license data is stored.

Value— <DN>. The string <base> is replaced with the directory base DN

Default— No value

Editing Level—Expert

`snmp-agent`—(Optional) Specifies whether the SRC SNMP agent exports MIBs for this directory connection.

Default— Disabled

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration logger

Syntax

```
shared sae configuration logger name ...
```

Hierarchy Level

```
[edit shared sae configuration logger]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Create a logging configuration for the SAE.

Options

name name— Name of the logging configuration.

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration logger *name* file

Syntax

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

Hierarchy Level

```
[edit shared sae configuration logger name file]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure logging of messages to a file.

filter filter—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

Editing Level—Basic

filename filename— Absolute path of the filename that contains the current logs.

Note: 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.

Value— Filename

Default— No value

Editing Level—Basic

rollover-filename rollover-filename—(Optional) 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— Path of filename

Example—/opt/UMC/sae/var/log/sae.alt

Default— The default value is different for each type of component.

Editing Level—Normal

`maximum-file-size` *maximum-file-size*—(Optional) Maximum size of the log file and the rollover file.

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

Value—Integer in the range 0–2147483647 kbytes

Default— 1000000

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration logger *name* syslog

Syntax

```
shared sae configuration logger name syslog {
    filter filter;
    host host;
    facility facility;
    format format;
}
```

Hierarchy Level

```
[edit shared sae configuration logger name syslog]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure logging of messages to system logging.

filter filter—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default—/error-

Editing Level—Basic

host host— IP address or name of a host that collects event messages by means of a standard system logging daemon.

Value— IP address or hostname

Default—loghost

Editing Level—Basic

facility facility—(Optional) Type of system log in accordance with the system logging protocol.

Value—Integer in the range 0–23

Default— 3

Editing Level—Advanced

format format—(Optional) MessageFormat string that specifies how the information in an event message is printed. (The strings {#} are replaced with the log information [...]).

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

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration login-registration

Syntax

```
shared sae configuration login-registration {  
    registration-authentication;  
}
```

Hierarchy Level

```
[edit shared sae configuration login-registration]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Enable the authentication of registered username/password pairs.

Options

`registration-authentication`—(Optional) Enables the authentication of registered username/password pairs. Enable this option if your authentication server does not allow authentication while a session for the authenticated username is active.

Default—
Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration nic-proxy-configuration

Syntax

```
shared sae configuration nic-proxy-configuration name {  
}
```

Hierarchy Level

```
[edit shared sae configuration nic-proxy-configuration]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a NIC proxy.

Options

name name— Name of the NIC proxy configuration.

Value—Text

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration nic-proxy-configuration *name* cache

Syntax

```
shared sae configuration nic-proxy-configuration name cache {
    cache-size cache-size;
    cache-cleanup-interval cache-cleanup-interval;
    cache-entry-age cache-entry-age;
}
```

Hierarchy Level

```
[edit shared sae configuration nic-proxy-configuration name cache]
```

Description

Configure the NIC proxy cache properties. You can modify cache properties for the NIC proxy to optimize the resolution performance for your network configuration and system resources. Typically, you can use the default settings for the cache properties.

cache-size cache-size—(Optional) Maximum size of the cache in which the NIC proxy retains data. If you decrease the cache size or disable the cache while the NIC proxy is running, the NIC proxy removes entries in order of descending age until the cache size meets the new limit.

Value— Integer in the range 0–2147483647

Default—10000

Editing Level—Advanced

cache-cleanup-interval cache-cleanup-interval— Time interval at which the NIC proxy removes expired entries from its cache.

Value— Number of seconds in the range 5–2147483

Default—15

Editing Level—Advanced

cache-entry-age cache-entry-age—(Optional) Maximum time that the NIC proxy can cache an entry. The NIC proxy compares this property with the life expectancy of each entry and uses the lower value to determine when to remove the entry.

Value— Number of seconds in the range 0–4294967295

- 0 or unspecified—Life expectancy of the data, which determines expiration of data
- Other values—Actual time that the NIC proxy caches entries

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Advanced

shared sae configuration nic-proxy-configuration *name* nic-host-selection

Syntax

```
shared sae configuration nic-proxy-configuration name nic-host-selection {
    groups [groups...];
    selection-criteria (roundRobin | randomPick | priorityList);
}
```

Hierarchy Level

```
[edit shared sae configuration nic-proxy-configuration name nic-host-selection]
```

Description

Configure the mechanism that a NIC proxy uses to select NIC system if multiple systems are available. You use NIC host selection when you use NIC replication.

groups [*groups...*]—(Optional) List of groups of NIC hosts that the NIC proxy can contact for resolution requests.

Value— Names of groups.

Default— No value

Editing Level—Advanced

selection-criteria (roundRobin | randomPick | priorityList)— Selection criteria that the NIC proxy uses to determine which NIC host to contact. Configure selection criteria if you configure more than one group.

Value— One of the following criteria:

- roundRobin—NIC proxy selects NIC hosts in a fixed, cyclic order. The NIC proxy always selects the next host in the list.
- randomPick—NIC proxy selects NIC hosts randomly from the list.
- priorityList—NIC proxy selects NIC hosts according to their assigned priorities in the list. If the host with the highest priority in the list is not available, the NIC proxy tries the host with the next-highest priority, and so on.

Use round-robin or random pick to distribute resolution requests among NIC hosts. Use priority list if you prefer to use a particular NIC host; for example, you may reduce operating cost by using a local NIC host.

Default— roundRobin

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Advanced

shared sae configuration nic-proxy-configuration *name* nic-host-selection blacklisting

Syntax

```
shared sae configuration nic-proxy-configuration name nic-host-
selection blacklisting {
    try-next-system-on-error;
    number-of-retries-before-blacklisting number-of-retries-before-blacklisting;
    blacklist-retry-interval blacklist-retry-interval;
}
```

Hierarchy Level

```
[edit shared sae configuration nic-proxy-configuration name nic-host-
selection blacklisting]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure how to handle nonresponsive NIC hosts. When a NIC host does not respond, it is blacklisted which means that other NIC hosts are contacted until the blacklisted host becomes available again.

Options

try-next-system-on-error—(Optional) Specifies whether or not the NIC proxy should contact the next specified NIC host if a NIC host is determined to be unavailable. Configure this property only if you configure more than one group.

Default—true

Editing Level—Advanced

number-of-retries-before-blacklisting *number-of-retries-before-blacklisting*— Number of times the NIC proxy tries to communicate with a NIC host before the NIC proxy stops communicating with the NIC host for a period of time.

Value—Integer in the range 0–2147483647

Default—3

Editing Level—Advanced

blacklist-retry-interval *blacklist-retry-interval*— Interval at which the

NIC proxy attempts to connect to an unavailable NIC host.

Value—Integer in the range 15–2147483647 s

Default—15

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration nic-proxy-configuration *name* resolution

Syntax

```
shared sae configuration nic-proxy-configuration name resolution {
    resolver-name resolver-name;
    key-type key-type;
    value-type value-type;
    expect-multiple-values;
    constraints constraints;
}
```

Hierarchy Level

```
[edit shared sae configuration nic-proxy-configuration name resolution]
```

Description

Configure properties for a NIC proxy (NIC locator), the NIC component that requests information on behalf of an application.

resolver-name resolver-name— NIC resolver that the NIC proxy uses. This resolver must be the same as one that is configured on the NIC host.

Value— Path to the NIC resolver.

Example—/realms/ip/A1,/realms/dn/A1.

Default— No value

Editing Level—Basic

key-type key-type— Type of data used that the key provides for the NIC resolution. You can provide a qualifier to a data type to distinguish between different instances of a data type in a resolution scenario, or to provide information about a data type to clarify the use of that data type in a resolution.

Value— One of the following types:

- Ip —Subscriber's IP address
- Vr—Virtual router
- Interface—Name of router's interface
- InterfaceId—Identifier of an interface on the router
- Dn—LDAP distinguished name for subscriber
- LoginName—Subscriber login ID
- AnyString—Other information

To qualify data types, enter a qualifier within parentheses.

Example—LoginName(username).

Default— No value

Editing Level—Basic

value-type value-type— Type of value to be returned in the resolution. The value type varies according to the application that uses the NIC proxy.

Value— One of the following types:

- SaelId—SAE server ID
- LoginName—Subscriber login ID
- AnyString—Other information

To qualify data types, enter a qualifier within parentheses.

Example—LoginName(username).

Default— No value

Editing Level—Basic

expect-multiple-values—(Optional) Specifies whether or not the key can have multiple corresponding values.

Editing Level—Basic

constraints constraints—(Optional) Data type that a resolver uses during the resolution process. A constraint represents a condition that must or may be satisfied before the next stage of the resolution process can proceed.

Configure a constraint only if the constraint will be provided by the application in the resolution request. Typically, you do not need to configure constraints.

Value— Data types of constraints specified for the NIC resolution.

Separate data types with commas.

Default— No value

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration nic-proxy-configuration *name* test-nic-bindings

Syntax

```
shared sae configuration nic-proxy-configuration name test-nic-bindings {
    use-test-bindings;
}
```

Hierarchy Level

```
[edit shared sae configuration nic-proxy-configuration name test-nic-bindings]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure key-value mappings to be used to test a NIC resolution.

Options

`use-test-bindings`—(Optional) Test the NIC resolutions without having to configure or run a NIC host. The values returned are those configured in the key-values property.

Default—false

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration nic-proxy-configuration *name* test-nic-bindings key-values

Syntax

```
shared sae configuration nic-proxy-configuration name test-nic-bindings key-  
values name {  
    value;  
}
```

Hierarchy Level

```
[edit shared sae configuration nic-proxy-configuration name test-nic-bindings key-  
values]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure keys and associated values to use for testing. Define all of values to be returned for specified keys.

Options

name name—

Value—Text

value—

Value—Text
Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Advanced

shared sae configuration plug-ins

Syntax

```
shared sae configuration plug-ins {
    plugin-publisher-auth-queue plugin-publisher-auth-queue;
    plugin-publisher-tracking-queue plugin-publisher-tracking-queue;
}
```

Hierarchy Level

[edit shared sae configuration plug-ins]

Options

plugin-publisher-auth-queue plugin-publisher-auth-queue—

Value—Integer in the range -2147483648–2147483647

Default—20

Editing Level—Advanced

plugin-publisher-tracking-queue plugin-publisher-tracking-queue—

Value—Integer in the range -2147483648–2147483647

Default—20

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration plug-ins event-publishers

Syntax

```
shared sae configuration plug-ins event-publishers {
    subscriber-authorization [subscriber-authorization...];
    default-retailer-authentication [default-retailer-authentication...];
    default-vr-authentication [default-vr-authentication...];
    default-retailer-dhcp-authentication [default-retailer-dhcp-
authentication...];
    dhcp-authorization [dhcp-authorization...];
    service-authorization [service-authorization...];
    subscription-authorization [subscription-authorization...];
    subscriber-tracking [subscriber-tracking...];
    service-tracking [service-tracking...];
    interface-tracking [interface-tracking...];
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins event-publishers]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure event publishers. Event publishers tell the SAE which events to send to which plug-in.

Options

subscriber-authorization [*subscriber-authorization...*]—(Optional)
 Authorize all subscriber sessions. These plug-in instances are called after a subscriber profile is loaded but before a subscriber session is started. The SAE calls these plug-ins for each subscriber who logs in to a portal.

These plug-in instances cannot perform authentication because passwords are not available at this point in the login process. Therefore if you specify plug-ins that perform authentication, the login process will fail.

Value— List of plug-ins

Default— No value

Introduced in—1.0.0

Editing Level—Normal

`default-retailer-authentication [default-retailer-authentication...]`

—(Optional) Authenticate subscribers who are assigned to retailer objects that do not specify a an authentication plug-in. These plug-ins are called when the subscriber logs in to a domain. The authentication process for portal logins maps the supplied domain name to a retailer object.

If you do not specify default retailer authentication plug-ins or retailer-specific plug-ins, subscribers are admitted without authentication.

Value— List of plug-ins

Default— No value

Editing Level—Normal

`default-vr-authentication [default-vr-authentication...]`—(Optional)

Authenticate subscribers who are assigned to a VR that do not specify a an authentication plug-in. These plug-ins are called when the subscriber logs in to a domain.

If you do not specify default vr authentication plug-ins or retailer-specific plug-ins, subscribers are admitted without authentication.

Value— List of plug-ins

Default— No value

Editing Level—Normal

`default-retailer-dhcp-authentication [default-retailer-dhcp-`

`authentication...]`—(Optional) Authenticate DHCP address requests for subscribers who are assigned to retailer objects that do not specify a DHCP authentication plug-in. These plug-ins are called when the SAE receives a DHCP discover request from a client that has its username and password cached in the SAE. The username and password can either be cached persistently in the directory or temporarily in memory during a switch from an unauthenticated to an authenticated address.

Value— List of plug-ins

Default— No value

Editing Level—Normal

`dhcp-authorization [dhcp-authorization...]`—(Optional) Authorize all DHCP address requests for all DHCP subscribers who log in to a portal. These plug-ins are called for both authenticated and unauthenticated address requests.

Value— List of plug-ins

Default— No value

Editing Level—Normal

`service-authorization [service-authorization...]`—(Optional) Authorize all service sessions. These plug-ins are called before a service session is started, and are called for every service session started by any subscriber.

Value— List of plug-ins**Default**— No value**Editing Level**—Normal`subscription-authorization [subscription-authorization...]`—(Optional)

Authorize subscribers to change their subscriptions. These plug-ins are called when a subscriber tries to modify, subscribe to, or unsubscribe from a subscription.

Value— List of plug-ins**Default**— No value**Editing Level**—Normal

`subscriber-tracking [subscriber-tracking...]`—(Optional) Collect accounting data for all subscriber sessions. These plug-ins are called for every subscriber session that is started and stopped. They are called after a subscriber session has started and when the session is stopped.

Value— List of plug-ins**Default**— No value**Editing Level**—Normal

`service-tracking [service-tracking...]`—(Optional) Collect accounting data for all service sessions. These plug-ins are called for every service session that is started and stopped. They are called after a service session starts, when the service session stops, and during interim updates.

Value— List of plug-ins**Default**— No value**Editing Level**—Normal

`interface-tracking [interface-tracking...]`—(Optional) Collect accounting data for all interfaces that the SAE manages. These plug-ins are called for every managed interface that is started and stopped. They are called after an interface comes up, when new policies are installed on the interface, and when the interface goes down. You can include NIC SAE plug-ins, which cause the SAE to send interface tracking events to the NIC SAE plug-in agent.

Value— List of plug-ins**Default**— No value**Editing Level**—Normal

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration plug-ins event-publishers device-type-authentication

Syntax

```
shared sae configuration plug-ins event-publishers device-type-authentication {
    junos [junos...];
    junos-ptsp [junos-ptsp...];
    junos-ise [junos-ise...];
    junose [junose...];
    pcmm [pcmm...];
    third-party [third-party...];
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins event-publishers device-type-authentication]
```

Release Information

Statement introduced in SRC Release 1.0.0

Options

`junos [junos...]`—(Optional) Authenticate subscriber sessions logging in through a JUNOS(BEEP) device.

Value—Text
Editing Level—Normal

`junos-ptsp [junos-ptsp...]`—(Optional) Authenticate subscriber sessions logging in through a JUNOS-PTSP device.

Value—Text
Editing Level—Normal

`junos-ise [junos-ise...]`—(Optional) [Alias: intelligent-service-edge] Authenticate subscriber sessions logging in through a JUNOS-JSRC device.

Value—Text
Editing Level—Normal

`junose [junose...]`—(Optional) Authenticate subscriber sessions logging in through a JUNOSe (COPS-PR) device.

Value—Text

Editing Level—Normal

`pcmm [pcmm...]`—(Optional) Authenticate subscriber sessions logging in through a PCMM device.

Value—Text

Editing Level—Normal

`third-party [third-party...]`—(Optional) Authenticate subscriber sessions logging in through a JUNOS(BEEP) device.

Value—Text

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins manager

Syntax

```
shared sae configuration plug-ins manager {
    threads threads;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins manager]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the number of threads used for plug-in synchronization.

Options

`threads threads`— Number of threads that the SAE maintains for plug-in synchronization.

Value— Integer in the range 0–100

Default— 5

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Expert

shared sae configuration plug-ins name

Syntax

```
shared sae configuration plug-ins name name ...
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a plug-in. A plug-in configuration describes a particular plug-in that can handle events that it receives from the SAE.

- An authorization plug-in configuration might perform RADIUS authentication when it receives a subscriber login event.
- A tracking plug-in might write accounting information to a file when it receives service session events.

For each type of plug-in you can create multiple instances that contain different configurations of the plug-in.

Alias

pool

Options

name name— Name of the plug-in configuration.

Value—Text

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration plug-ins name *name* acp-interface-listener

Syntax

```
shared sae configuration plug-ins name name acp-interface-listener {
    ldap-server ldap-server;
    bind-dn bind-dn;
    bind-password bind-password;
    (ldaps);
    congestion-points-base-dn congestion-points-base-dn;
    admission-control-base-dn admission-control-base-dn;
    timeout timeout;
    acp-remote-corba-ior acp-remote-corba-ior;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name acp-interface-listener]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a hosted internal plug-in for SRC-ACP that the SAE uses to monitor the state of interfaces on a VR for backbone congestion points.

ldap-server ldap-server— IP address or name of the host that supports the directory that contains backbone service definitions and network interfaces.

Value— IP address or name of the host optionally followed by a port number. Use the format <host>:<port number>. For example, 10.227.0.0:389

Default— No value

Editing Level—Normal

bind-dn bind-dn— DN of the directory entry that defines the username with which the plug-in accesses the directory.

Value— <DN>. You can use the special value <base> to refer to the globally configured base DN. The string <base> is replaced with the directory base DN.

Default— No value

Editing Level—Normal

`bind-password` *bind-password*— Password with which the plug-in accesses the directory.

Value— Text string
Default— No value
Editing Level—Normal

`ldaps`—Enables LDAPS as the secure protocol for connections to the directory server.

Value— `ldaps`—Enable LDAPS
Default— Disabled
Editing Level—Advanced

`congestion-points-base-dn` *congestion-points-base-dn*— DN at which SRC-ACP stores backbone congestion points.

Value— <DN>. You can use the special value <base> to refer to the globally configured base DN. The string <base> is replaced with the directory base DN.
Default— No value
Editing Level—Normal

`admission-control-base-dn` *admission-control-base-dn*— DN at which SRC-ACP stores edge congestion points.

Value— <DN>. You can use the special value <base> to refer to the globally configured base DN. The string <base> is replaced with the directory base DN.
Default— No value
Editing Level—Normal

`timeout` *timeout*—(Optional) Maximum time that the plug-in waits for the router to respond.

Value— Number of milliseconds in the range 0–2147483647. A zero means there is no timeout.
Default— 5000
Editing Level—Advanced

`acp-remote-corba-ior` *acp-remote-corba-ior*— Object reference for the ACP plug-in.

Value— ACP CORBA reference that is defined with the **edit shared acp configuration corba acp-ior** statement.
Default— No value

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* custom-radius-accounting

Syntax

```
shared sae configuration plug-ins name name custom-radius-accounting {
    java-class-radius-packet-handler java-class-radius-packet-handler;
    class-path-radius-packet-handler class-path-radius-packet-handler;
    append-acct-status-type-attribute;
    require-mandatory-attributes;
    load-balancing-mode (failover | roundRobin);
    fallback-timer fallback-timer;
    timeout timeout;
    retry-interval retry-interval;
    maximum-queue-length maximum-queue-length;
    bind-address bind-address;
    udp-port udp-port;
    default-peer default-peer;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name custom-radius-accounting]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a custom RADIUS accounting plug-in.

java-class-radius-packet-handler java-class-radius-packet-handler—
Name of the Java class that implements the RadiusPacketHandler interface in the RADIUS client library.

Value— Java class name. For example, net.juniper.smgmt.radius.
RadiusPacketHandlerImpl

Default— No value

Editing Level—Basic

class-path-radius-packet-handler class-path-radius-packet-handler—
(Optional) List of URLs that identify a location from which Java classes are loaded when the plug-in is initialized.

Value— Comma-separated list of URLs

Default— No value

Editing Level—Basic

`append-acct-status-type-attribute`—(Optional) Enable or disable whether or not the plug-in includes the Acct-Status-Type attribute in a RADIUS accounting request packet.

Default— Enabled

Editing Level—Normal

`require-mandatory-attributes`—(Optional) Enable or disable whether or not a RADIUS authentication or accounting request must contain all mandatory RADIUS attributes before sending the request packet.

Default— Enabled

Editing Level—Normal

`load-balancing-mode (failover | roundRobin)`— Mode for load-balancing RADIUS servers. You can set up the plug-in to switch between RADIUS servers in case of failure or to load-balance every request.

Value— One of the following:

- Failover—The SAE sends requests to the RADIUS server that is configured as the default peer. If the default peer fails, the SAE uses the next server configured in the peer group. The SAE cycles through the configured RADIUS servers as needed.
- Round-robin—The SAE alternates requests between all RADIUS servers configured in the peer group.

Default— Failover

Editing Level—Normal

`failback-timer failback-timer`— Controls if and when the SAE attempts to fail back to the default peer.

Value— One of the following:

- Number of seconds after a failover that the SAE attempts to fail back; range is -1–2147483647
- 0—SAE always attempts to fail back
- -1—SAE never attempts to fail back

Default— -1

Editing Level—Normal

`timeout timeout`— Maximum time the SAE waits for a response from a RADIUS server. If the RADIUS server does not respond to the request, the request fails and the SAE logs an error message. Note: configure this attribute to be five times (or more) greater than the `retry-interval` attribute to make sure the fail-over mechanism works without losing any packet.

Value— Number of milliseconds in the range -1–9223372036854775807. -1 means that there is no timeout.
Default— 15000
Editing Level—Normal

`retry-interval retry-interval`— Time the SAE waits for a response from a RADIUS server before it resends the RADIUS packet. The SAE keeps sending RADIUS packets until either the server acknowledges the packet or the maximum timeout is reached. Note: configure the timeout attribute to be five times (or more) greater than this attribute to make sure the fail-over mechanism works without losing any packet.

Value— Number of milliseconds in the range 0–9223372036854775807.
Default— 3000
Editing Level—Normal

`maximum-queue-length maximum-queue-length`— Maximum number of unacknowledged RADIUS messages that the plug-in receives from the RADIUS server before it discards new messages.

Value— Integer in the range 0–2147483647
Default— 10000
Editing Level—Normal

`bind-address bind-address`—(Optional) Source IP address that the plug-in uses to communicate with the RADIUS server. If you do not specify an address, the global default address is used. You configure the global default address with the **slot number sae radius local-address** command.

Value— IP address
Default— No value
Editing Level—Advanced

`udp-port udp-port`—(Optional) Source UDP port used for communication with the RADIUS server. If not specified, the global default is used.

Value— One of the following:

- Port number in the range 1–65535
- A range of ports in the format `port-port`; for example, 7000-7003
- A comma-separated list of port numbers and port ranges enclosed in double quotation marks. For example, "7000-7003,

7006, 7007-7009".

Default— No value

Editing Level—Advanced

`default-peer` *default-peer*— Name of the RADIUS server to which the SAE sends packets for this plug-in.

Value— Name of the server as defined with the **shared sae configuration plug-ins pool *name* custom-radius-accounting peer-group** command.

Default— No value

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* custom-radius-accounting peer-group

Syntax

```
shared sae configuration plug-ins name name custom-radius-accounting peer-
group name {
    server-address server-address;
    server-port server-port;
    secret secret;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name custom-radius-accounting peer-
group]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a RADIUS peer, which is an instance of a RADIUS server. If you define multiple servers, the SAE uses them in cases of failover or as alternate servers for load-balancing purposes.

Note that if you configure more than one RADIUS peer in a plug-in instance that has the same properties, the SNMP counters for the plug-in will not update correctly. The reason is that the software does not know which RADIUS peer to send updates to.

Options

name name— Name of the RADIUS peer.

Value—Text

server-address server-address— IP address of the RADIUS server to which the SAE sends accounting data or that the SAE uses for authentication and authorization.

Value— IP address

Default— No value

Editing Level—Normal

`server-port` *server-port*— Port used for RADIUS packets.

Value— Port number in the range 0–65535.

- RADIUS accounting servers typically use ports 1813 or 1646.
- RADIUS authentication servers typically use ports 1812 or 1645.

Default—1812

Editing Level—Normal

`secret` *secret*— Password that is shared with the RADIUS server. You must configure the same secret on the RADIUS server.

Value— Shared secret; the software encodes the secret using BASE-64.

Default— No value

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* custom-radius-authentication

Syntax

```
shared sae configuration plug-ins name name custom-radius-authentication {
    java-class-radius-packet-handler java-class-radius-packet-handler;
    class-path-radius-packet-handler class-path-radius-packet-handler;
    require-mandatory-attributes;
    load-balancing-mode (failover | roundRobin);
    fallback-timer fallback-timer;
    timeout timeout;
    retry-interval retry-interval;
    maximum-queue-length maximum-queue-length;
    bind-address bind-address;
    udp-port udp-port;
    default-peer default-peer;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name custom-radius-authentication]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a custom RADIUS authentication plug-in.

java-class-radius-packet-handler java-class-radius-packet-handler—
Name of the Java class that implements the RadiusPacketHandler interface in the RADIUS client library.

Value— Java class name. For example, net.juniper.smgmt.radius.

RadiusPacketHandlerImpl

Default— No value

Editing Level—Basic

class-path-radius-packet-handler class-path-radius-packet-handler—
(Optional) List of URLs that identify a location from which Java classes are loaded when the plug-in is initialized.

Value— Comma-separated list of URLs

Default— No value
Editing Level—Basic

`require-mandatory-attributes`—(Optional) Specifies whether or not a RADIUS authentication or accounting request must contain all mandatory RADIUS attributes before sending the request packet.

Value— true or false
Default— true
Editing Level—Normal

`load-balancing-mode` (`failover` | `roundRobin`)— Mode for load-balancing RADIUS servers. You can set up the plug-in to switch between RADIUS servers in case of failure or to load-balance every request.

Value— One of the following:

- **Failover**—The SAE sends requests to the RADIUS server that is configured as the default peer. If the default peer fails, the SAE uses the next server configured in the peer group. The SAE cycles through the configured RADIUS servers as needed.
- **Round-robin**—The SAE alternates requests between all RADIUS servers configured in the peer group.

Default— Failover
Editing Level—Normal

`failback-timer` *failback-timer*— Controls if and when the SAE attempts to fail back to the default peer.

Value— One of the following:

- Number of seconds after a failover that the SAE attempts to fail back; range is -1–2147483647
- 0—SAE always attempts to fail back
- -1—SAE never attempts to fail back

Default— -1
Editing Level—Normal

`timeout` *timeout*— Maximum time the SAE waits for a response from a RADIUS server. If the RADIUS server does not respond to the request, the request fails and the SAE logs an error message. Note: configure this attribute to be five times (or more) greater than the `retry-interval` attribute to make sure the fail-over mechanism works without losing any packet.

Value— Number of milliseconds in the range -1–9223372036854775807. -1 means that there is no timeout.
Default— 15000
Editing Level—Normal

`retry-interval` *retry-interval*— Time the SAE waits for a response from a RADIUS server before it resends the RADIUS packet. The SAE keeps sending RADIUS packets until either the server acknowledges the packet or the maximum timeout is reached. Note: configure the timeout attribute to be five times (or more) greater than this attribute to make sure the fail-over mechanism works without losing any packet.

Value— Number of milliseconds in the range 0–9223372036854775807
Default— 3000
Editing Level—Normal

`maximum-queue-length` *maximum-queue-length*— Maximum number of unacknowledged RADIUS messages that the plug-in receives from the RADIUS server before it discards new messages.

Value— Integer in the range 0–2147483647
Default— 10000
Editing Level—Normal

`bind-address` *bind-address*—(Optional) Source IP address that the plug-in uses to communicate with the RADIUS server. If you do not specify an address, the global default address is used. You configure the global default address with the **slot number sae radius local-address** command.

Value— IP address
Default— No value
Editing Level—Advanced

`udp-port` *udp-port*—(Optional) Source UDP port or a range of source UDP ports used for communication with the RADIUS server. If you do not specify a UDP port, the global UDP port is used. You configure the global UDP port with the **shared sae configuration global-radius-udp-port** command.

Value— One of the following:

- Port number in the range 1–65535
- A range of ports in the format port-port; for example, 7000-7003
- A comma-separated list of port numbers and port ranges enclosed in double quotation marks. For example, 7000-7003, 7006, 7007-7009

Default— No value
Editing Level—Advanced

`default-peer` *default-peer*— Name of the RADIUS server to which the SAE sends packets for this plug-in.

Value— Name of the server as defined with the **shared sae configuration plug-ins pool *name* custom-radius-authentication peer-group** command.

Default— No value

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* custom-radius-authentication peer-group

Syntax

```
shared sae configuration plug-ins name name custom-radius-authentication peer-
group name {
    server-address server-address;
    server-port server-port;
    secret secret;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name custom-radius-
authentication peer-group]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a RADIUS peer, which is an instance of a RADIUS server. If you define multiple servers, the SAE uses them in cases of failover or as alternate servers for load-balancing purposes.

Note that if you configure more than one RADIUS peer in a plug-in instance that has the same properties, the SNMP counters for the plug-in will not update correctly. The reason is that the software does not know which RADIUS peer to send updates to.

Options

name name— Name of the RADIUS peer.

Value—Text

server-address server-address— IP address of the RADIUS server to which the SAE sends accounting data or that the SAE uses for authentication and authorization.

Value— IP address

Default— No value

Editing Level—Normal

`server-port` *server-port*— Port used for RADIUS packets.

Value— Port number in the range 0–65535.

- RADIUS accounting servers typically use ports 1813 or 1646.
- RADIUS authentication servers typically use ports 1812 or 1645.

Default—1812

Editing Level—Normal

`secret` *secret*— Password that is shared with the RADIUS server. You must configure the same secret on the RADIUS server.

Value— Shared secret; the software encodes the secret using BASE-64.

Default— No value

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* ejb-adaptor

Syntax

```
shared sae configuration plug-ins name name ejb-adaptor {
    classpath classpath;
    jndi-service-provider jndi-service-provider;
    application-server-url application-server-url;
    jndi-sae-event-listener jndi-sae-event-listener;
    event-admitter event-admitter;
    use-ejb-cluster;
    ejb-clustering-strategy (EJBObjectClustering | EJBHomeClustering |
JNDIClustering);
    attributes [attributes...];
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name ejb-adaptor]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Note that the EJB adapter plug-in works only with the SRC-VTA, which is not yet supported on the C-series platform.

Configure an EJB adapter plug-in that the SRC-VTA uses to communicate with the SAE. The plug-in performs the following functions:

- Filters SAE plug-in events for the SRC-VTA.
- Adapts internal SAE events to EJB-compatible methods.
- Sends SAE tracking events to the SRC-VTA.

classpath classpath— Classpath used to load EJB adapter plug-in and JBoss client libraries.

Value—Text

Default—file:///opt/UMC/sae/lib/plugins/ejb/plugin.ejb.adapter.jar,file:///opt/UMC/sae/lib/plugins/ejb/jbossall-client.jar,file:///opt/UMC/sae/lib/plugins/ejb/jboss-common-client.jar,file:///opt/UMC/sae/lib/plugins/ejb/jboss-j2ee.jar,file:///opt/UMC/sae/lib/plugins/ejb/jnp-client.jar,file:///opt/UMC/sae/lib/plugins/ejb/jboss-client.jar,file:///opt/UMC/sae/lib/plugins/ejb/jbossha-client.jar,file:///opt/UMC/sae/lib/plugins/ejb/jbosssx-client.jar,file:///opt/UMC/sae/lib/plugins/ejb/log4j.jar

Editing Level—Expert

`jndi-service-provider` *jndi-service-provider*— Class name of the J2EE application server's JNDI service provider

Value— Depends on the type of J2EE application server. Consult documentation for the J2EE application server.

Default— `org.jnp.interfaces.NamingContextFactory`

Editing Level—Advanced

`application-server-url` *application-server-url*— URL of J2EE application server that is running the JNDI service.

Value— Depends on the type of J2EE application server. Consult the documentation for the J2EE application server.

Default— `jnp://127.0.0.1:1099`

Editing Level—Normal

`jndi-sae-event-listener` *jndi-sae-event-listener*— JNDI name of SAAEventListener EJB of the peer SRC-VTA.

Value— JNDI name. For example, `Quota/SAAEventListenerBean`.

Default— No value

Editing Level—Normal

`event-admitter` *event-admitter*—(Optional) LDAP filter that determines the subscriber and service events that the EJB adapter plug-in sends to the SRC-VTA.

Value— See *Installing and Initially Configuring the SRC-VTA* in the *SRC Application Library Guide*.

Default— No value

Editing Level—Normal

`use-ejb-cluster`—(Optional) Property that specifies whether or not the J2EE application server uses EJB cluster.

Default— Disabled

Editing Level—Advanced

`ejb-clustering-strategy` (`EJBObjectClustering` | `EJBHomeClustering` | `JNDIClustering`)— Load-balancing scheme of the J2EE application server that hosts the SRC-VTA. See the documentation for the J2EE application server to determine which load-balancing scheme it supports.

Value— One of the following:

- EJBObjectClustering—load balancing by means of object stubs.
- EJBHomeClustering—load balancing by means of home interface.
- JNDIClustering—Load balancing by means of JNDI

Default— EJBObjectClustering

Editing Level—Advanced

`attributes [attributes...]`—(Optional) Attributes that are sent to the plug-in. We recommend that you configure only the required attributes. If you do not specify attributes, all attributes are sent. Specifying fewer attributes improves the performance of the SRC network.

Value—Text

Default— All attributes

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* external

Syntax

```
shared sae configuration plug-ins name name external {
    corba-object-reference corba-object-reference;
    state-synchronization;
    attributes [attributes...];
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name external]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure SAE external plug-ins. You need to configure external plug-ins for SAE plug-in agents for the NIC, for Admission Control Plug-Ins, and for custom plug-ins developed in Common Object Request Broker Architecture (CORBA).

corba-object-reference corba-object-reference— Object reference of the external plug-in that is exported to the SAE. When the SAE sends the first event to a registered plug-in, it resolves the object reference.

Value— Object reference in one of the following formats:

- The absolute path to the interoperable object reference (IOR) file in the format: "file://<absolute path>"
- The corbaloc URL in the format corbaloc::<host>:<portNumber>/<path> where:
 - host is the name or IP address of the host that supports the plug-in
 - portNumber is the port number of the host
 - path is the absolute path to the plug-in
- Common Object Services (COS) in the format corbaname::<host>[:<port>][/*serviceName*][#<key> where the key is provided by the publisher of the IOR to the COS naming service.
- The actual IOR in the form IOR:<objectReference>

Default— No value

Editing Level—Normal

`state-synchronization`—(Optional) Plug-in implements state synchronization interface

Editing Level—Normal

`attributes` [*attributes...*]—(Optional) Attributes that are sent to the plug-in. We recommend that you configure only the required attributes. If you do not specify attributes, all attributes are sent. Specifying fewer attributes improves the performance of the SRC network.

Value—Text

Default— All attributes

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* file-accounting

Syntax

```
shared sae configuration plug-ins name name file-accounting {
    filename filename;
    template template;
    interval interval;
    fields [(status | nas-id | host | router-name | interface-name | interface-
alias | interface-descr | port-id | user-ip-address | login-name | accounting-id
| auth-user-id | if-radius-class | if-session-id | service-name | radius-class |
event-time | session-id | terminate-cause | session-time | in-octets | out-octets
| in-packets | out-packets | nas-ip | user-mac-address | service-session-name |
service-session-tag | user-type | user-radius-class | user-session-id | primary-
user-name | subscription-name | login-id | if-index | event-time-millisecond |
nas-port | operational | user-inet-address | nas-inet-address | router-type |
interface-speed | calling-station-id)...];
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name file-accounting]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a file accounting plug-in, which writes information to a file in a comma-separated format.

filename filename— Name and location of the file to which the SAE writes accounting information. The SAE names accounting files by appending the timestamp for the start of the accounting period.

Value— Path and name of file

Default— */var/acct/log*

Editing Level—Normal

template template— Name of the template that defines header names for the attributes written to the accounting file.

Value— Template name

Default— *std*

Editing Level—Normal

`interval interval`— Number of hours of information stored in each accounting file. When the interval expires, the SAE closes the file, renames it to the archive name, and creates a new file.

Accounting files are aligned with midnight of the day the SAE process starts. If the interval is 24 hours, the SAE starts a new file at midnight every day beginning on the day the SAE process starts.

- If the interval is a divisor of 24 hours (for example, 15 minutes, 30 minutes, 1 hour), there is a repeatable pattern of file starts. For example, if the interval is set to 6 hours, the SAE creates a new file at midnight, 6 am, 12 pm, and 6 pm every day.
- If the interval is not a divisor of 24 hours, then the file start times shift each day to different times of the day.

If the SAE is restarted, the schedule for creating accounting files is reset to start at midnight.

Value— Interval in the format hour:minutes

Default— 24

Editing Level—Normal

`fields [(status | nas-id | host | router-name | interface-name | interface-alias | interface-descr | port-id | user-ip-address | login-name | accounting-id | auth-user-id | if-radius-class | if-session-id | service-name | radius-class | event-time | session-id | terminate-cause | session-time | in-octets | out-octets | in-packets | out-packets | nas-ip | user-mac-address | service-session-name | service-session-tag | user-type | user-radius-class | user-session-id | primary-user-name | subscription-name | login-id | if-index | event-time-millisecond | nas-port | operational | user-inet-address | nas-inet-address | router-type | interface-speed | calling-station-id) ...]`—(Optional) List of accounting attributes that are written to the accounting file.

Value

- `status`—Accounting status
- `nas-id`—NAS identifier
- `host`—Hostname of the SAE
- `router-name`—Router name
- `interface-name`—Interface name
- `interface-alias`—Interface alias
- `interface-descr`—Interface description
- `port-id`—NAS port ID
- `user-ip-address`—Subscriber IP address
- `login-name`—Login name
- `accounting-id`—Accounting ID
- `auth-user-id`—User authentication ID
- `if-radius-class`—Interface RADIUS class
- `if-session-id`—Interface session ID
- `service-name`—Service name
- `radius-class`—RADIUS class

- event-time—Event time (s)
- session-id—Session ID
- terminate-cause—Terminate cause
- session-time—Session time
- in-octets—Number of input octets
- out-octets—Number of output octets
- in-packets—Number of input packets
- out-packets—Number of output packets
- nas-ip—NAS IP address
- user-mac-address—Subscriber MAC address
- service-session-name—Service session name
- service-session-tag—Service session tag
- user-type—Subscriber session type
- user-radius-class—Subscriber session RADIUS class
- user-session-id—Subscriber session ID
- primary-user-name—Primary subscriber name
- subscription-name—Subscription name
- login-id—Login ID
- if-index—Interface index
- event-time-millisecond—Event time (ms)
- nas-port—NAS port
- operational—Operational flag
- user-inet-address—Subscriber INET address
- nas-inet-address—NAS INET address
- router-type—Router type
- interface-speed—Interface speed
- calling-station-id—Calling Station ID

Default— status,nas-id,host,router-name,interface-name,interface-alias, interface-descr,port-id,user-ip-address, login-name,accounting-id,auth-user-id,if-radius-class,if-session-id,service-name,radius-class,event-time, session-id, terminate-cause,session-time,in-octets,out-octets,in-packets, out-packets,nas-ip,user-mac-address,service-session-name, service-session-tag,user-type,user-radius-class,user-session-id,user-session-handle,calling-station-id

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* flex-radius-accounting

Syntax

```
shared sae configuration plug-ins name name flex-radius-accounting {
    load-balancing-mode (failover | roundRobin);
    failback-timer failback-timer;
    timeout timeout;
    retry-interval retry-interval;
    maximum-queue-length maximum-queue-length;
    bind-address bind-address;
    udp-port udp-port;
    error-handling (0 | 1);
    default-peer default-peer;
    template template;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name flex-radius-accounting]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a flexible RADIUS accounting plug-in.

`load-balancing-mode (failover | roundRobin)`— Mode for load-balancing RADIUS servers. You can set up the plug-in to switch between RADIUS servers in case of failure or to load-balance every request.

Value— One of the following:

- **Failover**—The SAE sends requests to the RADIUS server that is configured as the default peer. If the default peer fails, the SAE uses the next server configured in the peer group. The SAE cycles through the configured RADIUS servers as needed.
- **Round-robin**—The SAE alternates requests between all RADIUS servers configured in the peer group.

Default— Failover

Editing Level—Normal

`failback-timer` *failback-timer*— Controls if and when the SAE attempts to fail back to the default peer.

Value— One of the following:

- Number of seconds after a failover that the SAE attempts to fail back; range is -1–2147483647
- 0—SAE always attempts to fail back
- -1—SAE never attempts to fail back

Default— -1

Editing Level—Normal

`timeout` *timeout*— Maximum time the SAE waits for a response from a RADIUS server. If the RADIUS server does not respond to the request, the request fails and the SAE logs an error message. Note: configure this attribute to be five times (or more) greater than the retry-interval attribute to make sure the fail-over mechanism works without losing any packet.

Value— Number of milliseconds in the range -1–9223372036854775807. -1 means that there is no timeout.

Default— 15000

Editing Level—Normal

`retry-interval` *retry-interval*— Time the SAE waits for a response from a RADIUS server before it resends the RADIUS packet. The SAE keeps sending RADIUS packets until either the server acknowledges the packet or the maximum timeout is reached. Note: configure the timeout attribute to be five times (or more) greater than this attribute to make sure the fail-over mechanism works without losing any packet.

Value— Number of milliseconds in the range 0–9223372036854775807

Default— 3000

Editing Level—Normal

`maximum-queue-length` *maximum-queue-length*— Maximum number of unacknowledged RADIUS messages that the plug-in receives from the RADIUS server before it discards new messages.

Value— Integer in the range 0–2147483647

Default— 10000

Editing Level—Normal

`bind-address` *bind-address*—(Optional) Source IP address that the plug-in uses to communicate with the RADIUS server. If you do not specify an address, the global default address is used. You configure the global default address with the **slot number sae radius local-address** command.

Value— IP address
Default— No value
Editing Level—Advanced

`udp-port udp-port`—(Optional) Source UDP port or a range of source UDP ports used for communication with the RADIUS server. If you do not specify a UDP port, the global UDP port is used. You configure the global UDP port with the **shared sae configuration global-radius-udp-port** command.

Value— One of the following:

- Port number in the range 1–65535
- A range of ports in the format port-port; for example, 7000-7003
- A comma-separated list of port numbers and port ranges enclosed in double quotation marks. For example, "7000-7003, 7006, 7007-7009".

Default— No value
Editing Level—Advanced

`error-handling (0 | 1)`— Configures the way the SAE handles errors.

Value— One of the following:

- 0—Ignores incorrect definitions and logs them for debugging purposes
- 1—Logs errors and discards the affected RADIUS packet

Default— 0 (Ignore)
Editing Level—Normal

`default-peer default-peer`— Name of the RADIUS server to which the SAE sends packets for this plug-in.

Value— Name of the server as defined with the **shared sae configuration plug-ins pool *name* flex-radius-accounting peer-group** command.
Default— No value
Editing Level—Normal

`template template`— Name of RADIUS packet template.

Value— Name of template
Default— No value
Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* flex-radius-accounting peer-group

Syntax

```
shared sae configuration plug-ins name name flex-radius-accounting peer-
group name {
    server-address server-address;
    server-port server-port;
    secret secret;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name flex-radius-accounting peer-
group]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a RADIUS peer, which is an instance of a RADIUS server. If you define multiple servers, the SAE uses them in cases of failover or as alternate servers for load-balancing purposes.

Note that if you configure more than one RADIUS peer in a plug-in instance that has the same properties, the SNMP counters for the plug-in will not update correctly. The reason is that the software does not know which RADIUS peer to send updates to.

Options

name name— Name of the RADIUS peer.

Value—Text

server-address server-address— IP address of the RADIUS server to which the SAE sends accounting data or that the SAE uses for authentication and authorization.

Value— IP address

Default— No value

Editing Level—Normal

`server-port` *server-port*— Port used for RADIUS packets.

Value— Port number in the range 0–65535.

- RADIUS accounting servers typically use ports 1813 or 1646.
- RADIUS authentication servers typically use ports 1812 or 1645.

Default—1812

Editing Level—Normal

`secret` *secret*— Password that is shared with the RADIUS server. You must configure the same secret on the RADIUS server.

Value— Shared secret; the software encodes the secret using BASE-64.

Default— No value

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* flex-radius-accounting radius-packet-definition

Syntax

```
shared sae configuration plug-ins name name flex-radius-accounting radius-packet-  
definition name ...
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name flex-radius-accounting radius-  
packet-definition]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a RADIUS packet definition for the plug-in.

Options

name name— Name of the RADIUS attribute instance.

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* flex-radius-accounting radius-packet-definition *name* attributes

Syntax

```
shared sae configuration plug-ins name name flex-radius-accounting radius-packet-
definition name attributes name {
    value;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name flex-radius-accounting radius-
packet-definition name attributes]
```

Description

Configure RADIUS attributes within a plug-in.

Options

name *name*— Name of the RADIUS attribute.

Value—Text

value— Value of the RADIUS attribute.

Value— Value can be a standard value or an expression. For a list of standard values, see *Configuring Accounting and Authentication Plug-Ins (SRC CLI)* in the *SRC PE Subscribers and Subscriptions Guide*.

Default— No value

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* flex-radius-accounting radius-packet-definition *name* vendor-specific

Syntax

```
shared sae configuration plug-ins name name flex-radius-accounting radius-packet-
definition name vendor-specific name ...
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name flex-radius-accounting radius-
packet-definition name vendor-specific]
```

Description

Configure Juniper Networks vendor-specific attributes (VSAs).

Options

name *name*—

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* flex-radius-accounting radius-packet-definition *name* vendor-specific *name* attributes

Syntax

```
shared sae configuration plug-ins name name flex-radius-accounting radius-packet-  
definition name vendor-specific name attributes name {  
    value;  
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name flex-radius-accounting radius-  
packet-definition name vendor-specific name attributes]
```

Options

name *name*— RADIUS attribute definition.

Value—Text

value—

Value—Text
Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* flex-radius-accounting radius-packet-definition *name* vendor-specific *name* type

Syntax

```
shared sae configuration plug-ins name name flex-radius-accounting radius-packet-definition name vendor-specific name type name ...
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name flex-radius-accounting radius-packet-definition name vendor-specific name type]
```

Options

name *name*— Data type of the attribute value.

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* flex-radius-accounting radius-packet-definition *name* vendor-specific *name* type *name* attributes

Syntax

```
shared sae configuration plug-ins name name flex-radius-accounting radius-packet-
definition name vendor-specific name type name attributes name {
    value;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name flex-radius-accounting radius-
packet-definition name vendor-specific name type name attributes]
```

Options

name *name*— RADIUS attribute definition.

Value—Text

value—

Value—Text

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* flex-radius-accounting radius-packet-definition *name* vendor-specific-26

Syntax

```
shared sae configuration plug-ins name name flex-radius-accounting radius-packet-
definition name vendor-specific-26 name ...
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name flex-radius-accounting radius-
packet-definition name vendor-specific-26]
```

Description

Configure Juniper Networks vendor-specific attributes (VSAs).

Options

name *name*—

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* flex-radius-accounting radius-packet-definition *name* vendor-specific-26 *name* attributes

Syntax

```
shared sae configuration plug-ins name name flex-radius-accounting radius-packet-
definition name vendor-specific-26 name attributes name {
    value;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name flex-radius-accounting radius-
packet-definition name vendor-specific-26 name attributes]
```

Options

name *name*— RADIUS attribute definition.

Value—Text

value—

Value—Text

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* flex-radius-accounting radius-packet-definition *name* vendor-specific-26 *name* type

Syntax

```
shared sae configuration plug-ins name name flex-radius-accounting radius-packet-definition name vendor-specific-26 name type name ...
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name flex-radius-accounting radius-packet-definition name vendor-specific-26 name type]
```

Options

name *name*—

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* flex-radius-accounting radius-packet-definition *name* vendor-specific-26 *name* type *name* attributes

Syntax

```
shared sae configuration plug-ins name name flex-radius-accounting radius-packet-
definition name vendor-specific-26 name type name attributes name {
    value;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name flex-radius-accounting radius-
packet-definition name vendor-specific-26 name type name attributes]
```

Options

name *name*— RADIUS attribute definition.

Value—Text

value—

Value—Text
Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* flex-radius-authentication

Syntax

```
shared sae configuration plug-ins name name flex-radius-authentication {
    load-balancing-mode (failover | roundRobin);
    failback-timer failback-timer;
    timeout timeout;
    retry-interval retry-interval;
    maximum-queue-length maximum-queue-length;
    bind-address bind-address;
    udp-port udp-port;
    error-handling (0 | 1);
    default-peer default-peer;
    template template;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name flex-radius-authentication]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a flexible RADIUS authentication plug-in.

`load-balancing-mode (failover | roundRobin)`— Mode for load-balancing RADIUS servers. You can set up the plug-in to switch between RADIUS servers in case of failure or to load-balance every request.

Value— One of the following:

- **Failover**—The SAE sends requests to the RADIUS server that is configured as the default peer. If the default peer fails, the SAE uses the next server configured in the peer group. The SAE cycles through the configured RADIUS servers as needed.
- **Round-robin**—The SAE alternates requests between all RADIUS servers configured in the peer group.

Default— Failover

Editing Level—Normal

`failback-timer` *failback-timer*— Controls if and when the SAE attempts to fail back to the default peer.

Value— One of the following:

- Number of seconds after a failover that the SAE attempts to fail back; range is -1–2147483647
- 0—SAE always attempts to fail back
- -1—SAE never attempts to fail back

Default— -1

Editing Level—Normal

`timeout` *timeout*— Maximum time the SAE waits for a response from a RADIUS server. If the RADIUS server does not respond to the request, the request fails and the SAE logs an error message. Note: configure this attribute to be five times (or more) greater than the retry-interval attribute to make sure the fail-over mechanism works without losing any packet.

Value— Number of milliseconds in the range -1–9223372036854775807. -1 means that there is no timeout.

Default— 15000

Editing Level—Normal

`retry-interval` *retry-interval*— Time the SAE waits for a response from a RADIUS server before it resends the RADIUS packet. The SAE keeps sending RADIUS packets until either the server acknowledges the packet or the maximum timeout is reached. Note: configure the timeout attribute to be five times (or more) greater than this attribute to make sure the fail-over mechanism works without losing any packet.

Value— Number of milliseconds in the range 0–9223372036854775807

Default— 3000

Editing Level—Normal

`maximum-queue-length` *maximum-queue-length*— Maximum number of unacknowledged RADIUS messages that the plug-in receives from the RADIUS server before it discards new messages.

Value— Integer in the range 0–2147483647

Default— 10000

Editing Level—Normal

`bind-address` *bind-address*—(Optional) Source IP address that the plug-in uses to communicate with the RADIUS server. If you do not specify an address, the global default address is used. You configure the global default address with the **slot number sae radius local-address** command.

Value— IP address

Default— No value

Editing Level—Advanced

`udp-port udp-port`—(Optional) Source UDP port or a range of source UDP ports used for communication with the RADIUS server. If you do not specify a UDP port, the global UDP port is used. You configure the global UDP port with the **shared sae configuration global-radius-udp-port** command.

Value— One of the following:

- Port number in the range 1–65535
- A range of ports in the format port-port; for example, 7000-7003
- A comma-separated list of port numbers and port ranges enclosed in double quotation marks. For example, "7000-7003, 7006, 7007-7009".

Default— No value

Editing Level—Advanced

`error-handling (0 | 1)`— Configure the way the SAE handles errors.

Value— One of the following:

- 0—Ignores incorrect definitions and logs them for debugging purposes
- 1—Logs errors and discards the affected RADIUS packet

Default— 0 (Ignore)

Editing Level—Normal

`default-peer default-peer`— Name of the RADIUS server to which the SAE sends packets for this plug-in.

Value— Name of the server as defined with the **shared sae configuration plug-ins pool *name* flex-radius-authentication peer-group** command.

Default— No value

Editing Level—Normal

`template template`— Name of RADIUS packet template.

Value— Name of template

Default— No value

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* flex-radius-authentication peer-group

Syntax

```
shared sae configuration plug-ins name name flex-radius-authentication peer-
group name {
    server-address server-address;
    server-port server-port;
    secret secret;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name flex-radius-authentication peer-
group]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a RADIUS peer, which is an instance of a RADIUS server. If you define multiple servers, the SAE uses them in cases of failover or as alternate servers for load-balancing purposes.

Note that if you configure more than one RADIUS peer in a plug-in instance that has the same properties, the SNMP counters for the plug-in will not update correctly. The reason is that the software does not know which RADIUS peer to send updates to.

Options

name name— Name of the RADIUS peer.

Value—Text

server-address server-address— IP address of the RADIUS server to which the SAE sends accounting data or that the SAE uses for authentication and authorization.

Value— IP address

Default— No value

Editing Level—Normal

`server-port` *server-port*— Port used for RADIUS packets.

Value— Port number in the range 0–65535.

- RADIUS accounting servers typically use ports 1813 or 1646.
- RADIUS authentication servers typically use ports 1812 or 1645.

Default—1812

Editing Level—Normal

`secret` *secret*— Password that is shared with the RADIUS server. You must configure the same secret on the RADIUS server.

Value— Shared secret; the software encodes the secret using BASE-64.

Default— No value

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* flex-radius-authentication radius-packet-definition

Syntax

```
shared sae configuration plug-ins name name flex-radius-authentication radius-
packet-definition name ...
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name flex-radius-
authentication radius-packet-definition]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a RADIUS packet definition for the plug-in.

Options

name name— Name of the RADIUS attribute instance.

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* flex-radius-authentication radius-packet-definition *name* attributes

Syntax

```
shared sae configuration plug-ins name name flex-radius-authentication radius-
packet-definition name attributes name {
    value;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name flex-radius-
authentication radius-packet-definition name attributes]
```

Description

Configure RADIUS attributes within a plug-in.

Options

name *name*— Name of the RADIUS attribute.

Value—Text

value— Value of the RADIUS attribute.

Value— Value can be a standard value or an expression. For a list of standard values, see *Configuring Accounting and Authentication Plug-Ins (SRC CLI)* in the *SRC PE Subscribers and Subscriptions Guide*.

Default— No value

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* flex-radius-authentication radius-packet-definition *name* vendor-specific

Syntax

```
shared sae configuration plug-ins name name flex-radius-authentication radius-
packet-definition name vendor-specific name ...
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name flex-radius-
authentication radius-packet-definition name vendor-specific]
```

Description

Configure Juniper Networks vendor-specific attributes (VSAs).

Options

name *name*—

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* flex-radius-authentication radius-packet-definition *name* vendor-specific *name* attributes

Syntax

```
shared sae configuration plug-ins name name flex-radius-authentication radius-  
packet-definition name vendor-specific name attributes name {  
    value;  
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name flex-radius-  
authentication radius-packet-definition name vendor-specific name attributes]
```

Options

name *name*— RADIUS attribute definition.

Value—Text

value—

Value—Text
Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* flex-radius-authentication radius-packet-definition *name* vendor-specific *name* type

Syntax

```
shared sae configuration plug-ins name name flex-radius-authentication radius-packet-definition name vendor-specific name type name ...
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name flex-radius-authentication radius-packet-definition name vendor-specific name type]
```

Options

name *name*— Data type of the attribute value.

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* flex-radius-authentication radius-packet-definition *name* vendor-specific *name* type *name* attributes

Syntax

```
shared sae configuration plug-ins name name flex-radius-authentication radius-
packet-definition name vendor-specific name type name attributes name {
    value;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name flex-radius-
authentication radius-packet-definition name vendor-
specific name type name attributes]
```

Options

name *name*— RADIUS attribute definition.

Value—Text

value—

Value—Text

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* flex-radius-authentication radius-packet-definition *name* vendor-specific-26

Syntax

```
shared sae configuration plug-ins name name flex-radius-authentication radius-
packet-definition name vendor-specific-26 name ...
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name flex-radius-
authentication radius-packet-definition name vendor-specific-26]
```

Description

Configure Juniper Networks vendor-specific attributes (VSAs).

Options

name *name*—

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* flex-radius-authentication radius-packet-definition *name* vendor-specific-26 *name* attributes

Syntax

```
shared sae configuration plug-ins name name flex-radius-authentication radius-  
packet-definition name vendor-specific-26 name attributes name {  
    value;  
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name flex-radius-  
authentication radius-packet-definition name vendor-specific-26 name attributes]
```

Options

name *name*— RADIUS attribute definition.

Value—Text

value—

Value—Text
Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* flex-radius-authentication radius-packet-definition *name* vendor-specific-26 *name* type

Syntax

```
shared sae configuration plug-ins name name flex-radius-authentication radius-packet-definition name vendor-specific-26 name type name ...
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name flex-radius-authentication radius-packet-definition name vendor-specific-26 name type]
```

Options

name *name*—

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* flex-radius-authentication radius-packet-definition *name* vendor-specific-26 *name* type *name* attributes

Syntax

```
shared sae configuration plug-ins name name flex-radius-authentication radius-
packet-definition name vendor-specific-26 name type name attributes name {
    value;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name flex-radius-
authentication radius-packet-definition name vendor-specific-
26 name type name attributes]
```

Options

name *name*— RADIUS attribute definition.

Value—Text

value—

Value—Text

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* interface-subscriber-limit

Syntax

```
shared sae configuration plug-ins name name interface-subscriber-limit {
    concurrent-subscribers concurrent-subscribers;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name interface-subscriber-limit]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a plug-in that limits the number of authenticated subscribers who connect to an IP interface on the router.

concurrent-subscribers *concurrent-subscribers*— Number of authenticated subscribers who can connect to an IP interface on the router simultaneously.

Value— Integer in the range 0–2147483647

Default— 1

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* internal

Syntax

```
shared sae configuration plug-ins name name internal {
    plug-in-class plug-in-class;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name internal]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an internal plug-in.

plug-in-class plug-in-class— Class name of the plug-in.

Value— Fully qualified name of the Java class

Default— No value

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* internal properties

Syntax

```
shared sae configuration plug-ins name name internal properties name {
    value;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name internal properties]
```

Description

Configure the property name and value pairs that make up the plug-in.

Options

name name— Name of the property for which you want to define a value.

Value—Text

value— Value for the property.

Value— Value for the property.

Default— No value

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration plug-ins name *name* jms-adaptor

Syntax

```
shared sae configuration plug-ins name name jms-adaptor {
    shared-dsa-configuration shared-dsa-configuration;
    subject-id-attribute-name [subject-id-attribute-name...];
    fail-queue-resend-interval fail-queue-resend-interval;
    fail-queues-max-size fail-queues-max-size;
    jms-blacklist-time jms-blacklist-time;
    jms-time-to-live jms-time-to-live;
    jms-connection-factory jms-connection-factory;
    dsa-application-server-urls [dsa-application-server-urls...];
    timeout timeout;
    socket-timeout socket-timeout;
    factory-initial factory-initial;
    factory-packages factory-packages;
    principal principal;
    credentials credentials;
    protocol protocol;
    authentication authentication;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name jms-adaptor]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the SAE plug-in to send events to Dynamic Service Activator through the Java Message Service (JMS). Dynamic Service Activator then publishes the events to listening external SOAP applications.

shared-dsa-configuration shared-dsa-configuration— Grouped configuration used by all Dynamic Service Activator instances to which this plug-in forwards SAE events.

Value—
Default—
Editing Level—Basic

subject-id-attribute-name [subject-id-attribute-name...]—(Optional) SAE plug-in event attributes whose values are used to find SOAP event subscriptions. The values

from these attributes are the event's subject ID, which specifies a user or interface. The value can be set by the SAE's subscriber classification script. If the values match any subject ID configured in a Dynamic Service Activator event subscription, then the plug-in forwards the event to Dynamic Service Activator, which in turn publishes it to the external SOAP application that owns the event subscription. Note that this attribute is multivalued. If any of the event attributes contains a value that matches an event subscription's subject-id configuration attribute, then the event is forwarded as specified in that event subscription.

Value—

Default— PA_ACCOUNTING_ID

Editing Level—Basic

`fail-queue-resend-interval` *fail-queue-resend-interval*—(Optional) Time between attempts to resend the events in the fail queue for each configured external SOAP application. When an event cannot be sent to any Dynamic Service Activator instance, it is stored in a fail queue.

Value—Integer in the range 1–2147483647

Default— 10 seconds

Editing Level—Advanced

`fail-queues-max-size` *fail-queues-max-size*—(Optional) Maximum size of all the fail queues combined. When an event cannot be sent to any Dynamic Service Activator instance, it is stored in a fail queue. Zero means all undeliverable events are discarded immediately, instead of being placed in a fail queue.

Value—Integer in the range 0–9223372036854775807

Default— 200 MB

Editing Level—Advanced

`jms-blacklist-time` *jms-blacklist-time*—(Optional) Time between connection attempts after a failure to establish a connection to a JMS queue on Dynamic Service Activator.

Value—

Default— 60 seconds

Editing Level—Advanced

`jms-time-to-live` *jms-time-to-live*—(Optional) Time before undelivered JMS messages can be silently discarded. Zero means forever.

Value—Integer in the range 0–2147483647

Default— 60 seconds

Editing Level—Advanced

`jms-connection-factory` *jms-connection-factory*—(Optional) JNDI name used to find JMS on the application server.

Value—
Default— ConnectionFactory
Editing Level—Expert

`dsa-application-server-urls` [*dsa-application-server-urls...*]— Dynamic Service Activator application servers to which SAE plug-in events are published. Dynamic Service Activator forwards the events as SOAP calls to external SOAP applications. The URLs point at the JNDI name servers on the Dynamic Service Activator application servers.

Value— The URLs are of the form `jnp://127.0.0.1:1099/`. The protocol and port sections of the URL are optional. An IP address or DNS name alone may be sufficient, assuming default application server configuration.
Default— `jnp://127.0.0.1:1099`
Editing Level—Basic

`timeout` *timeout*—(Optional) Connection timeout, in milliseconds, used when attempting to contact the JNDI name servers on application servers. Zero means the connection attempt will block until the TCP/IP layer times out.

Value—
Default— 3000
Editing Level—Advanced

`socket-timeout` *socket-timeout*—(Optional) Connected socket read timeout, in milliseconds, used when reading from sockets connected to the JNDI name servers on application servers. Zero means reading will block.

Value—
Default— 0
Editing Level—Advanced

`factory-initial` *factory-initial*—(Optional) Fully qualified class name of the factory class that creates the JNDI initial context.

Value—
Default— `org.jnp.interfaces.NamingContextFactory`
Editing Level—Expert

`factory-packages` *factory-packages*—(Optional) List of Java package prefixes for the class name of the factory class that creates a URL context factory.

Value— Colon-separated list of Java package prefixes
Default— `org.jboss.naming:org.jnp.interfaces`
Editing Level—Expert

`principal principal`—(Optional) Security principal used for authentication. This option may be relevant if you use a non-default value for the factory-initial option.

Value—

Default— Undefined.

Editing Level—Expert

`credentials credentials`—(Optional) Security credentials. This option may be relevant if you use a non-default value for the factory-initial option.

Value—

Default— Undefined.

Editing Level—Expert

`protocol protocol`—(Optional) Security protocol. This option may be relevant if you use a non-default value for the factory-initial option.

Value—

Default— Undefined.

Editing Level—Expert

`authentication authentication`—(Optional) Security authentication. This option may be relevant if you use a non-default value for the factory-initial option.

Value—

Default— Undefined.

Editing Level—Expert

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* ldap-authentication

Syntax

```
shared sae configuration plug-ins name name ldap-authentication {
    method (search | bind);
    server server;
    bind-dn bind-dn;
    bind-password bind-password;
    search-filter search-filter;
    (ldaps);
    search-base-dn search-base-dn;
    name-attribute name-attribute;
    password-attribute password-attribute;
    service-bundle-attribute service-bundle-attribute;
    session-volume-quota session-volume-quota;
    timeout timeout;
    signature-dn signature-dn;
    blacklist;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name ldap-authentication]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an LDAP authentication plug-in. This plug-in performs authentication against different directories using different authentication methods.

`method (search | bind)`— LDAP authentication method that the SAE uses. Both search and bind have different implications for system security and performance. When you design the system, consider:

- Search—Because the SAE retrieves passwords from the directory, the directory must allow read access to the password. Allowing read access can be a security risk because an attacker may be able to read passwords in subscriber profiles. However, to lower the risk of password exposure, you can store passwords in encrypted (hashed) form.
- Bind—The SAE sends the password to the directory for authentication. The advantage is that passwords never need to be read from the directory. However, passwords are sent in clear text, and an attacker could intercept them. Bind is a relatively expensive operation that can affect system performance.

Value— One of the following:

- **Search**—The SAE searches the directory for the username that the subscriber enters, retrieves the found object, and compares the password stored in the object with the provided password. You can store passwords in clear text or encrypted (hashed) format by using the crypt (UNIX `/etc/passwd`), SHA, or MD5 algorithms. The format for a hashed password is: `{crypt}hashed password`, `{sha}base64 SHA password`, or `{md5}base64 MD5 password`.
- **Bind**—The SAE performs a directory search, retrieves the DN of the found object, and tries to bind this DN and the password that the subscriber provides. If you specify the bind method, the plug-in uses the provided username and password to authenticate the directory (bind). You can store passwords in clear text or encrypted (hashed) format by using the crypt (UNIX `/etc/passwd`), SHA, or MD5 algorithms. You must use an encryption method that the directory supports.

Default— Search

Editing Level—Normal

`server server`—(Optional) List of IP addresses of the LDAP authentication server(s).

Value— Comma-separated list of IP addresses

Default— 127.0.0.1

Editing Level—Normal

`bind-dn bind-dn`—(Optional) DN used to authenticate access to the directory.

Value— DN

Default— `cn=ssp, ou=Components, o=Operators, <base>`

Editing Level—Normal

`bind-password bind-password`—(Optional) Password that the SAE uses to authenticate its access to the directory to search for the subscriber profile. If you do not specify a bind DN or bind password, the SAE uses anonymous access.

Value— Characters that make up the password. The SRC software encodes the secret using base64.

Default— `ssp`

Editing Level—Normal

`search-filter search-filter`—(Optional) Additional LDAP search filter that the SAE uses to search the directory for the subscriber profile. The initial search uses a search filter in the form `(&(nameAttribute=username) filter)`. The search is successful when the username and the filter match.

Value— Search filter syntax defined in RFC 2254—The String

Representation of LDAP Search Filters (December 1997)

Default— (objectClass=umcSubscriber)

Editing Level—Normal

ldaps—Enables LDAPS as the secure protocol used for LDAP connections with the directory. Enabling LDAPS causes communication with the directory to be encrypted with Secure Sockets Layer (SSL).

Value— ldaps—Enable LDAPS

Default— Disabled

Editing Level—Advanced

search-base-dn *search-base-dn*—(Optional) Base DN for searching entries in the directory. If you do not specify a base DN, the SAE uses the DN of the associated retailer object.

Also, if you do not specify the base DN, the SAE takes a username in the form subscriber@domain and maps domain to a retailer object by comparing domain with the domain names stored in the retailer object. There are two special cases:

- If domain is empty, first the virtual router name and then the name default are tried.
- If a retailer defines * (asterisk) as a domain name, it is used to map all domains that cannot be mapped directly.

Value— DN

Default— No value

Editing Level—Normal

name-attribute *name-attribute*—(Optional) Name of the directory attribute that holds the username.

Value— Attribute name

Default— uniqueID

Editing Level—Normal

password-attribute *password-attribute*—(Optional) Name of the directory attribute that stores the password.

Value— Directory attribute name

Default— userPassword

Editing Level—Normal

service-bundle-attribute *service-bundle-attribute*—(Optional) Name of the directory attribute that contains the name of the service bundle that is used for subscriber authentication. This value is made available to the subscriber classification process and can be used to select the subscriber profile to load.

Value— Directory attribute name

Default— No value

Editing Level—Normal

`session-volume-quota` *session-volume-quota*—(Optional) Name of the LDAP attribute that contains the value of the session volume quota. The LDAP plug-in sets the session volume quota to this value.

Value— Name of LDAP attribute

Default— No value

Editing Level—Normal

`timeout` *timeout*—(Optional) Maximum time the SAE waits for a response from a directory server. If the directory server does not respond to the request, the request fails and the SAE logs an error message.

Value— Number of milliseconds in the range 0–2147483647

Default— 5000

Editing Level—Advanced

`signature-dn` *signature-dn*—DES Signature DN

Value—Text

Default—<base>

Editing Level—Expert

`blacklist`—(Optional) Directory blacklisting

Default—true

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* pcmm-rks

Syntax

```
shared sae configuration plug-ins name name pcmm-rks {
    load-balancing-mode (failover | roundRobin);
    failback-timer failback-timer;
    timeout timeout;
    retry-interval retry-interval;
    maximum-queue-length maximum-queue-length;
    bind-address bind-address;
    udp-port udp-port;
    feid-mso-data feid-mso-data;
    feid-mso-domain-name feid-mso-domain-name;
    trusted-element;
    default-peer default-peer;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name pcmm-rks]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a PCMM record-keeping server plug-in.

load-balancing-mode (failover | roundRobin)— Mode for load-balancing RADIUS servers. You can set up the plug-in to switch between RADIUS servers in case of failure or to load-balance every request.

Value— One of the following:

- **Failover**—The SAE sends requests to the RADIUS server that is configured as the default peer. If the default peer fails, the SAE uses the next server configured in the peer group. The SAE cycles through the configured RADIUS servers as needed.
- **Round-robin**—The SAE alternates requests between all RADIUS servers configured in the peer group.

Default— Failover

Editing Level—Normal

`failback-timer` *failback-timer*— Controls if and when the SAE attempts to fail back to the default peer.

Value— One of the following:

- Number of seconds after a failover that the SAE attempts to fail back; range is -1–2147483647
- 0—SAE always attempts to fail back
- -1—SAE never attempts to fail back

Default— -1

Editing Level—Normal

`timeout` *timeout*— Maximum time the SAE waits for a response from a RADIUS server. If the RADIUS server does not respond to the request, the request fails and the SAE logs an error message. Note: configure this attribute to be five times (or more) greater than the retry-interval attribute to make sure the fail-over mechanism works without losing any packet.

Value— Number of milliseconds in the range -1–9223372036854775807. -1 means that there is no timeout.

Default— 15000

Editing Level—Normal

`retry-interval` *retry-interval*— Time the SAE waits for a response from a RADIUS server before it resends the RADIUS packet. The SAE keeps sending RADIUS packets until either the server acknowledges the packet or the maximum timeout is reached. Note: configure the timeout attribute to be five times (or more) greater than this attribute to make sure the fail-over mechanism works without losing any packet.

Value— Number of milliseconds in the range 0–9223372036854775807

Default— 3000

Editing Level—Normal

`maximum-queue-length` *maximum-queue-length*— Maximum number of unacknowledged RADIUS messages that the plug-in receives from the RADIUS server before it discards new messages.

Value— Integer in the range 0–2147483647

Default— 10000

Editing Level—Normal

`bind-address` *bind-address*—(Optional) Source IP address that the plug-in uses to communicate with the RADIUS server. If you do not specify an address, the global default address is used. You configure the global default address with the **slot number sae radius local-address** command.

Value— IP address

Default— No value

Editing Level—Advanced

`udp-port udp-port`—(Optional) Source UDP port or a range of source UDP ports used for communication with the RADIUS server. If you do not specify a UDP port, the global UDP port is used. You configure the global UDP port with the **shared sae configuration global-radius-udp-port** command.

Value— One of the following:

- Port number in the range 1–65535
- A range of ports in the format `port-port`; for example, 7000-7003
- A comma-separated list of port numbers and port ranges enclosed in double quotation marks. For example, "7000-7003, 7006, 7007-7009".

Default— No value

Editing Level—Advanced

`feid-mso-data feid-mso-data`—(Optional) MSO-defined data in the financial entity ID (FEID) attribute, which is included in event messages.

Value— First eight bytes of the FEID attribute

Default— The first eight bytes are filled with zeros.

Editing Level—Normal

`feid-mso-domain-name feid-mso-domain-name`— The MSO domain name that uniquely identifies the MSO for billing and settlement purposes.

Value— Domain name up to 239 bytes; begins at the ninth byte of the FEID attribute

Default— No value

Editing Level—Normal

`trusted-element`—(Optional) When the SAE is running as a policy server—which means that the SAE sends event messages directly to the RKS—enables the SAE as a trusted network element.

Default— Enabled

Editing Level—Normal

`default-peer default-peer`— Configure an RKS peer, which is an instance of an RKS. You must configure at least one RKS peer.

Value— Name of the server as defined with the **shared sae configuration plug-ins pool PccmRKSPugin peer-group** command.

Default— No value

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* pcmm-rks peer-group

Syntax

```
shared sae configuration plug-ins name name pcmm-rks peer-group name {
    server-address server-address;
    server-port server-port;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name pcmm-rks peer-group]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a RADIUS peer, which is an instance of a RADIUS server. If you define multiple servers, the SAE uses them in cases of failover or as alternate servers for load-balancing purposes.

Note that if you configure more than one RADIUS peer in a plug-in instance that has the same properties, the SNMP counters for the plug-in will not update correctly. The reason is that the software does not know which RADIUS peer to send updates to.

Options

name name— Name of the RADIUS peer.

Value—Text

server-address server-address— IP address of the RKS server to which the SAE sends accounting data

Value— IP address

Default— No value

Editing Level—Normal

server-port server-port— Port used for sending accounting packets.

Value— Port number in the range 0–65535

Default— 1813

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* qos-profile-tracking

Syntax

```
shared sae configuration plug-ins name name qos-profile-tracking {
    threads threads;
    default-qos-profile default-qos-profile;
    separator separator;
    qos-profile-prefix qos-profile-prefix;
    service-selection-attribute service-selection-attribute;
    search-filter search-filter;
    invisible-qos-service invisible-qos-service;
    qos-profile-parameter-name qos-profile-parameter-name;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name qos-profile-tracking]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a QoS-tracking plug-in that you can use to ensure that, as a subscriber activates and deactivates services, the required QoS profile is attached to the subscriber interface.

threads threads— Number of working threads that all QTP instances share when they process QTP events.

Value— Integer in the range 1–100.

Default— 1

Editing Level—Advanced

default-qos-profile default-qos-profile—(Optional) Name of the QoS profile that is attached to the interface when QoS services have been deactivated.

Value— Name of QoS profile

Default— No value

Editing Level—Normal

separator separator— Character that is placed between QoS profile input values when the system concatenates the values during the process of creating QoS profile names.

Value— Any character that is valid in QoS profile names on the router.

Default— A single hyphen (-)

Editing Level—Advanced

`qos-profile-prefix` *qos-profile-prefix*— Prefix added to the QoS service name as part of the process to determine the name of the QoS profile that needs to be attached to an interface for a particular service.

Value— Prefix that, when combined with QoS profile input values, matches a QoS profile on the router.

Default— qos-profile

Editing Level—Normal

`service-selection-attribute` *service-selection-attribute*— Name of the attribute in the service definition that you want the QTP to use as QoS profile input values. The QTP uses these values to determine the name of the QoS profile that needs to be attached to an interface for a group of QoS services.

Value— Name of any attribute in the service object; for example, serviceCategory, sspDesignAndGraphics. For a list of attribute names for the sspService object class, see the documentation for the LDAP schema in the SRC software distribution in the folder *SDK/doc/ldap* or on the Juniper Networks Web site at

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

Default— serviceName

Editing Level—Normal

`search-filter` *search-filter*— Search filter that the SAE uses to search service objects in the directory to find QoS services. You can set up the filter to search the values of any attribute in the service object, such as service name, category, or tracking plug-in. The search is successful when a value matches the filter.

Value— Search filter in a format similar to the LDAP search filter. See *Managing Tiered and Premium Services with QoS on JUNOSe Routers* in the *SRC Solutions Guide* for a list of the values that you can use for filters.

Default— (attribute.trackPlugin=) Note that you must add a search value after the equal sign.

Editing Level—Normal

`invisible-qos-service` *invisible-qos-service*— Name of the hidden QoS profile attachment service that the QTP uses to attach QoS profiles to and remove QoS profiles from a router interface.

Value— Name of the configured service

Default— svc-qos-attach
Editing Level—Normal

`qos-profile-parameter-name` *qos-profile-parameter-name*— Name of the variable parameter used in the QoS profile name field in the QoS profile attachment action of the policy group that is assigned to the hidden QoS service. When the QTP obtains the name of the required QoS profile, it substitutes that value for the variable parameter.

Value— Valid parameter name
Default— qpName
Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* radius-accounting

Syntax

```
shared sae configuration plug-ins name name radius-accounting {
    load-balancing-mode (failover | roundRobin);
    failback-timer failback-timer;
    nas-ip (SspIp | ErxIp);
    timeout timeout;
    retry-interval retry-interval;
    maximum-queue-length maximum-queue-length;
    bind-address bind-address;
    udp-port udp-port;
    username (login-name | accounting-id | auth-user-name | manager-id);
    calling-station-id (mac | no);
    default-peer default-peer;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name radius-accounting]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a basic RADIUS accounting plug-in. This plug-in sends accounting information to an external RADIUS accounting server or a group of accounting servers.

`load-balancing-mode (failover | roundRobin)`— Mode for load-balancing RADIUS servers. You can set up the plug-in to switch between RADIUS servers in case of failure or to load-balance every request.

Value— One of the following:

- **Failover**—The SAE sends requests to the RADIUS server that is configured as the default peer. If the default peer fails, the SAE uses the next server configured in the peer group. The SAE cycles through the configured RADIUS servers as needed.
- **Round-robin**—The SAE alternates requests between all RADIUS servers configured in the peer group.

Default— Failover

Editing Level—Normal

`failback-timer` *failback-timer*— Controls if and when the SAE attempts to fail back to the default peer.

Value— One of the following:

- Number of seconds after a failover that the SAE attempts to fail back; range is -1–2147483647
- 0—SAE always attempts to fail back
- -1—SAE never attempts to fail back

Default— -1

Editing Level—Normal

`nas-ip` (`SspIp` | `ErxCip`)—(Optional) Value of the NAS-Ip attribute.

Value— One of the following:

- SSP local IP—IP address of the SAE
- RADIUS client IP—IP address of the virtual router

Default— No value

Editing Level—Normal

`timeout` *timeout*— Maximum time the SAE waits for a response from a RADIUS server. If the RADIUS server does not respond to the request, the request fails and the SAE logs an error message. Note: configure this attribute to be five times (or more) greater than the retry-interval attribute to make sure the fail-over mechanism works without losing any packet.

Value— Number of milliseconds in the range -1–9223372036854775807. -1 means that there is no timeout.

Default— 15000

Editing Level—Normal

`retry-interval` *retry-interval*— Time the SAE waits for a response from a RADIUS server before it resends the RADIUS packet. The SAE keeps sending RADIUS packets until either the server acknowledges the packet or the maximum timeout is reached. Note: configure the timeout attribute to be five times (or more) greater than this attribute to make sure the fail-over mechanism works without losing any packet.

Value— Number of milliseconds in the range 0–9223372036854775807

Default— 3000

Editing Level—Normal

`maximum-queue-length` *maximum-queue-length*—Maximum number of unacknowledged RADIUS messages that the plug-in receives from the RADIUS server before it discards new messages.

Value— Integer in the range 0–2147483647

Default— 10000

Editing Level—Normal

`bind-address` *bind-address*—(Optional) Source IP address that the plug-in uses to communicate with the RADIUS server. If you do not specify an address, the global default address is used. You configure the global default address with the **slot number sae radius local-address** command.

Value— IP address

Default— No value

Editing Level—Advanced

`udp-port` *udp-port*—(Optional) Source UDP port or a range of source UDP ports used for communication with the RADIUS server. If you do not specify a UDP port, the global UDP port is used. You configure the global UDP port with the **shared sae configuration global-radius-udp-port** command.

Value— One of the following:

- Port number in the range 1–65535
- A range of ports in the format port-port; for example, 7000-7003
- A comma-separated list of port numbers and port ranges enclosed in quotation marks. For example, "7000-7003, 7006, 7007-7009".

Default— No value

Editing Level—Advanced

`username` (`login-name` | `accounting-id` | `auth-user-name` | `manager-id`)—Value of the User-Name attribute (RADIUS attribute [1]).

Value— One of the following:

- `login-name`—Name used for login
- `accounting-id`—Value stored in the subscriber profile
- `auth-user-name`—Name used to authenticate a service
- `manager-id`—Value of the manager ID in the service subscription; use this setting to identify subscribers to enterprise services. Manager ID is the value of `modifiersName` (DN of the administrator who last modified the entry in the directory) in the subscription. If `modifiersName` does not exist, manager ID is the value of `creatorsName` (DN of the administrator who created the entry in the directory).

Default— login-name
Editing Level—Normal

`calling-station-id (mac | no)`— Specifies whether the SAE sends the MAC address of the subscriber in the Calling-Station-Id attribute.

Value— One of the following:

- `mac`—Sends the MAC address in the Calling-Station-Id attribute
- `no`—Does not send the MAC address in the Calling-Station-Id attribute

Default— no
Editing Level—Normal

`default-peer default-peer`— Name of the RADIUS server to which the SAE sends packets for this plug-in.

Value— Name of the server as defined with the **shared sae configuration plug-ins pool RadiusAcctPlugin peer-group** command.
Default— No value
Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* radius-accounting peer-group

Syntax

```
shared sae configuration plug-ins name name radius-accounting peer-group name {
    server-address server-address;
    server-port server-port;
    secret secret;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name radius-accounting peer-group]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a RADIUS peer, which is an instance of a RADIUS server. If you define multiple servers, the SAE uses them in cases of failover or as alternate servers for load-balancing purposes.

Note that if you configure more than one RADIUS peer in a plug-in instance that has the same properties, the SNMP counters for the plug-in will not update correctly. The reason is that the software does not know which RADIUS peer to send updates to.

Options

name name— Name of the RADIUS peer.

Value—Text

server-address server-address— IP address of the RADIUS server to which the SAE sends accounting data or that the SAE uses for authentication and authorization.

Value— IP address

Default— No value

Editing Level—Normal

server-port server-port— Port used for RADIUS packets.

Value— Port number in the range 0–65535.

- RADIUS accounting servers typically use ports 1813 or 1646.
- RADIUS authentication servers typically use ports 1812 or 1645.

Default—1812

Editing Level—Normal

secret secret— Password that is shared with the RADIUS server. You must configure the same secret on the RADIUS server.

Value— Shared secret; the software encodes the secret using BASE-64.

Default— No value

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* radius-authentication

Syntax

```
shared sae configuration plug-ins name name radius-authentication {
    load-balancing-mode (failover | roundRobin);
    failback-timer failback-timer;
    nas-ip (SspIp | ErxIp);
    timeout timeout;
    retry-interval retry-interval;
    maximum-queue-length maximum-queue-length;
    bind-address bind-address;
    udp-port udp-port;
    default-peer default-peer;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name radius-authentication]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a basic RADIUS accounting plug-in. This plug-in sends authentication information to an external RADIUS authentication server or a group of redundant servers.

`load-balancing-mode (failover | roundRobin)`— Mode for load-balancing RADIUS servers. You can set up the plug-in to switch between RADIUS servers in case of failure or to load-balance every request.

Value— One of the following:

- **Failover**—The SAE sends requests to the RADIUS server that is configured as the default peer. If the default peer fails, the SAE uses the next server configured in the peer group. The SAE cycles through the configured RADIUS servers as needed.
- **Round-robin**—The SAE alternates requests between all RADIUS servers configured in the peer group.

Default— Failover

Editing Level—Normal

`failback-timer` *failback-timer*— Controls if and when the SAE attempts to fail back to the default peer.

Value— One of the following:

- Number of seconds after a failover that the SAE attempts to fail back; range is -1–2147483647
- 0—SAE always attempts to fail back
- -1—SAE never attempts to fail back

Default— -1

Editing Level—Normal

`nas-ip` (`SspIp` | `ErxIp`)—(Optional) Value of the NAS-Ip attribute.

Value— One of the following:

- SSP local IP—IP address of the SAE
- RADIUS client IP—IP address of the virtual router

Default— No value

Editing Level—Normal

`timeout` *timeout*— Maximum time the SAE waits for a response from a RADIUS server. If the RADIUS server does not respond to the request, the request fails and the SAE logs an error message. Note: configure this attribute to be five times (or more) greater than the retry-interval attribute to make sure the fail-over mechanism works without losing any packet.

Value— Number of milliseconds in the range -1–9223372036854775807. -1 means that there is no timeout.

Default— 15000

Editing Level—Normal

`retry-interval` *retry-interval*— Time the SAE waits for a response from a RADIUS server before it resends the RADIUS packet. The SAE keeps sending RADIUS packets until either the server acknowledges the packet or the maximum timeout is reached. Note: configure the timeout attribute to be five times (or more) greater than this attribute to make sure the fail-over mechanism works without losing any packet.

Value— Number of milliseconds in the range 0–9223372036854775807

Default— 3000

Editing Level—Normal

`maximum-queue-length` *maximum-queue-length*— Maximum number of unacknowledged RADIUS messages that the plug-in receives from the RADIUS server

before it discards new messages.

Value— Integer in the range 0–2147483647

Default— 10000

Editing Level—Normal

`bind-address bind-address`—(Optional) Source IP address that the plug-in uses to communicate with the RADIUS server. If you do not specify an address, the global default address is used. You configure the global default address with the **slot number sae radius local-address** command.

Value— IP address

Default— No value

Editing Level—Advanced

`udp-port udp-port`—(Optional) Source UDP port or a range of source UDP ports used for communication with the RADIUS server. If you do not specify a UDP port, the global UDP port is used. You configure the global UDP port with the **shared sae configuration global-radius-udp-port** command.

Value— One of the following:

- Port number in the range 1–65535
- A range of ports in the format port-port; for example, 7000-7003
- A comma-separated list of port numbers and port ranges enclosed in double quotation marks. For example, "7000-7003, 7006, 7007-7009".

Default— No value

Editing Level—Advanced

`default-peer default-peer`— Name of the RADIUS server to which the SAE sends packets for this plug-in.

Value— Name of the server as defined with the **shared sae configuration plug-ins pool RadiusAuthPlugin peer-group** command.

Default— No value

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* radius-authentication peer-group

Syntax

```
shared sae configuration plug-ins name name radius-authentication peer-group name
{
    server-address server-address;
    server-port server-port;
    secret secret;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name radius-authentication peer-group]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a RADIUS peer, which is an instance of a RADIUS server. If you define multiple servers, the SAE uses them in cases of failover or as alternate servers for load-balancing purposes.

Note that if you configure more than one RADIUS peer in a plug-in instance that has the same properties, the SNMP counters for the plug-in will not update correctly. The reason is that the software does not know which RADIUS peer to send updates to.

Options

name name— Name of the RADIUS peer.

Value—Text

server-address server-address— IP address of the RADIUS server to which the SAE sends accounting data or that the SAE uses for authentication and authorization.

Value— IP address

Default— No value

Editing Level—Normal

`server-port` *server-port*— Port used for RADIUS packets.

Value— Port number in the range 0–65535.

- RADIUS accounting servers typically use ports 1813 or 1646.
- RADIUS authentication servers typically use ports 1812 or 1645.

Default—1812

Editing Level—Normal

`secret` *secret*— Password that is shared with the RADIUS server. You must configure the same secret on the RADIUS server.

Value— Shared secret; the software encodes the secret using BASE-64.

Default— No value

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* schedule-authorization

Syntax

```
shared sae configuration plug-ins name name schedule-authorization {  
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name schedule-authorization]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Create an authorization plug-in that authorizes a scheduled service.

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins name *name* ssr-reader

Syntax

```
shared sae configuration plug-ins name name ssr-reader {
    read-attributes [read-attributes...];
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins name name ssr-reader]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an SSR reader plug-in.

`read-attributes [read-attributes...]`—(Optional) Plug-in attribute to set based on the values read from the SSR subscriber session table.

Value—Text
Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration plug-ins state-synchronization

Syntax

```
shared sae configuration plug-ins state-synchronization {
    fail-queue-size fail-queue-size;
    fail-queue-age fail-queue-age;
    batch-time batch-time;
    keepalive-time keepalive-time;
}
```

Hierarchy Level

```
[edit shared sae configuration plug-ins state-synchronization]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a state synchronization plug-in. Some plug-ins, such as the ACP plug-in and the SAE plug-in agent for the NIC, support state synchronization with the SAE. The state synchronization plug-in allows external plug-ins to maintain the state of active subscriber, service, and interface sessions without having to store intermediate versions of the state locally.

Options

fail-queue-size fail-queue-size— Maximum number of plug-in events that are stored while the communication with a state synchronization plug-in is interrupted.

Value— Integer in the range -1–2147483647. -1 means unlimited.

Default— 5000

Editing Level—Basic

fail-queue-age fail-queue-age— Mximum time for which plug-in events are stored while the communication with a state synchronization plug-in is interrupted.

Value— Integer in the range -1–2147483647. -1 means unlimited.

Default— -1

Editing Level—Basic

batch-time batch-time— Time the SAE waits for other plug-ins to become ready before starting a synchronization sequence.

Value— Number of seconds in the range 0–2147483647

Default— 60

Editing Level—Basic

`keepalive-time` *keepalive-time*— Time the SAE waits after an event before sending a ping to the remote plug-in.

Value— Number of seconds in the range 0–2147483647

Default— 60

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration policy-management-configuration

Syntax

```
shared sae configuration policy-management-configuration {  
    enable-junose-classifier-expansion;  
}
```

Hierarchy Level

```
[edit shared sae configuration policy-management-configuration]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify whether or not the SAE expands the JUNOSe classify-traffic conditions into multiple classifiers before it installs the policy on the router.

Options

`enable-junose-classifier-expansion`—(Optional) Enables or disables the expansion of JUNOSe classify-traffic conditions into multiple classifiers before it installs the policy on the router.

You would use this feature in policies that are used in IP multimedia subsystem (IMS) environments. You can also use it to simplify the configuration of JUNOSe policies.

Because classifier expansion uses processing resources when the policy is created, you should set this property to true only if you are going to use the feature.

Default— Disabled
Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration radius-packet-template

Syntax

```
shared sae configuration radius-packet-template name ...
```

Hierarchy Level

```
[edit shared sae configuration radius-packet-template]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a RADIUS packet template that contains the definition of RADIUS packets. You can use the template to define the content of RADIUS packets that the SAE sends to RADIUS servers. You can then apply the template to flexible RADIUS plug-ins.

Options

name name— Name of the RADIUS packet template.

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration radius-packet-template *name* radius-attributes

Syntax

```
shared sae configuration radius-packet-template name radius-attributes name ...
```

Hierarchy Level

```
[edit shared sae configuration radius-packet-template name radius-attributes]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Create a RADIUS attribute instance.

Options

name name— Name of the file-accounting template. RADIUS attribute instance. The name you assign to the RADIUS attribute instance must match a RADIUS attribute instance name listed in *Configuring Accounting and Authentication Plug-Ins (SRC CLI)* in the *SRC PE Subscribers and Subscriptions Guide*.

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration radius-packet-template *name* radius-attributes *name* attributes

Syntax

```
shared sae configuration radius-packet-template name radius-
attributes name attributes name {
    value;
}
```

Hierarchy Level

```
[edit shared sae configuration radius-packet-template name radius-
attributes name attributes]
```

Description

Configure RADIUS attributes within a plug-in.

Options

name *name*— Name of the RADIUS attribute.

Value—Text

value— Value of the RADIUS attribute.

Value— Value can be a standard value or an expression. For a list of standard values, see *Configuring Accounting and Authentication Plug-Ins (SRC CLI)* in the *SRC PE Subscribers and Subscriptions Guide*.

Default— No value

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration radius-packet-template *name* radius-attributes *name* vendor-specific

Syntax

```
shared sae configuration radius-packet-template name radius-attributes name vendor-specific name ...
```

Hierarchy Level

```
[edit shared sae configuration radius-packet-template name radius-attributes name vendor-specific]
```

Description

Configure Juniper Networks vendor-specific attributes (VSAs).

Options

name name—

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration radius-packet-template *name* radius-attributes *name* vendor-specific *name* attributes

Syntax

```
shared sae configuration radius-packet-template name radius-
attributes name vendor-specific name attributes name {
    value;
}
```

Hierarchy Level

```
[edit shared sae configuration radius-packet-template name radius-
attributes name vendor-specific name attributes]
```

Options

name *name*— RADIUS attribute definition.

Value—Text

value—

Value—Text

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration radius-packet-template *name* radius-attributes *name* vendor-specific *name* type *name*

Syntax

```
shared sae configuration radius-packet-template name radius-attributes name vendor-specific name type name ...
```

Hierarchy Level

```
[edit shared sae configuration radius-packet-template name radius-attributes name vendor-specific name type]
```

Options

name *name*— Data type of the attribute value.

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration radius-packet-template *name* radius-attributes *name* vendor-specific *name* type *name* attributes

Syntax

```
shared sae configuration radius-packet-template name radius-
attributes name vendor-specific name type name attributes name {
    value;
}
```

Hierarchy Level

```
[edit shared sae configuration radius-packet-template name radius-
attributes name vendor-specific name type name attributes]
```

Options

name name— RADIUS attribute definition.

Value—Text

value—

Value—Text

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration radius-packet-template *name* radius-attributes *name* vendor-specific-26

Syntax

```
shared sae configuration radius-packet-template name radius-attributes name vendor-specific-26 name ...
```

Hierarchy Level

```
[edit shared sae configuration radius-packet-template name radius-attributes name vendor-specific-26]
```

Description

Configure Juniper Networks vendor-specific attributes (VSAs).

Options

name *name*—

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration radius-packet-template *name* radius-attributes *name* vendor-specific-26 *name* attributes

Syntax

```
shared sae configuration radius-packet-template name radius-
attributes name vendor-specific-26 name attributes name {
    value;
}
```

Hierarchy Level

```
[edit shared sae configuration radius-packet-template name radius-
attributes name vendor-specific-26 name attributes]
```

Options

name *name*— RADIUS attribute definition.

Value—Text

value—

Value—Text

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration radius-packet-template *name* radius-attributes *name* vendor-specific-26 *name* type

Syntax

```
shared sae configuration radius-packet-template name radius-attributes name vendor-specific-26 name type name ...
```

Hierarchy Level

```
[edit shared sae configuration radius-packet-template name radius-attributes name vendor-specific-26 name type]
```

Options

name *name*—

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration radius-packet-template *name* radius-attributes *name* vendor-specific-26 *name* type *name* attributes

Syntax

```
shared sae configuration radius-packet-template name radius-
attributes name vendor-specific-26 name type name attributes name {
    value;
}
```

Hierarchy Level

```
[edit shared sae configuration radius-packet-template name radius-
attributes name vendor-specific-26 name type name attributes]
```

Options

name *name*— RADIUS attribute definition.

Value—Text

value—

Value—Text

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae configuration script-extension

Syntax

```
shared sae configuration script-extension {
    flexible-radius-script flexible-radius-script;
    dynamic-radius-script dynamic-radius-script;
}
```

Hierarchy Level

```
[edit shared sae configuration script-extension]
```

Release Information

Statement introduced in SRC Release 1.0.0

Options

`flexible-radius-script flexible-radius-script`— Python script name of flexible radius plug-in

Value—

Default— flexRadius

Editing Level—Basic

`dynamic-radius-script dynamic-radius-script`— Python script name of local dynamic radius server

Value—

Default— dynRadius

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Expert

shared sae configuration service-activation

Syntax

```
shared sae configuration service-activation {
    retry-time retry-time;
    retry-limit retry-limit;
    activate-on-modification;
}
```

Hierarchy Level

```
[edit shared sae configuration service-activation]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure session reactivation behavior. If a service session fails unexpectedly, the SAE tries to start the session again in the background. You can change how many times the SAE tries to activate the session and the interval between these attempts. In most instances, the default values do not need to be changed.

Options

retry-time retry-time— Time between attempts to activate a service session if activation fails or to deactivate a service session if deactivation fails. This process takes place in the background.

Value— Number of seconds in the range -1–9223372036854775807; -1 indicates no limit

Default— 60

Editing Level—Basic

retry-limit retry-limit— Number of times the SAE tries to activate a service session if activation fails or to deactivate a service session if deactivation fails. This process takes place in the background. Limit number of times to retry service failed background activation.

Value— Integer in the range -1-2147483647; -1 indicates no limit

Default— -1

Editing Level—Basic

activate-on-modification—(Optional) When a service subscription is modified, normally only services that are currently active are updated. If this flag is set, any activate-on-

login service that is currently not active is automatically activated. This flag can be used to force service activations that failed e.g. due to an invalid definition at activation time.

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Expert

shared sae configuration service-schedule

Syntax

```
shared sae configuration service-schedule {
    years-in-future years-in-future;
    years-in-past years-in-past;
}
```

Hierarchy Level

```
[edit shared sae configuration service-schedule]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure parameters related to service schedules.

Options

years-in-future years-in-future—(Optional) Amount of time in the future from the year that the SRC system is started, that the scheduler can see.

Value— Integer in the range 1–100

Default— No value

Editing Level—Basic

years-in-past years-in-past—(Optional) Amount of time in the past, from the year that the SRC system is started, that the scheduler can see.

Value— Integer in the range 1–100

Default— No value

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Advanced

shared sae configuration session-job-manager

Syntax

```
shared sae configuration session-job-manager {
    number-of-threads number-of-threads;
}
```

Hierarchy Level

```
[edit shared sae configuration session-job-manager]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the number of threads used for session-related activity; for example, aggregate service keepalives, and remote session monitoring.

Options

`number-of-threads` *number-of-threads*— Number of threads used for session-related activity.

Value— Integer in the range 1–1000

Default— 16

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Expert

shared sae configuration subscriber-sessions

Syntax

```
shared sae configuration subscriber-sessions {
    assigned-ip-idle-timeout assigned-ip-idle-timeout;
    allow-same-ip-login;
}
```

Hierarchy Level

```
[edit shared sae configuration subscriber-sessions]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an idle timeout for sessions of assigned IP subscribers, and specify whether or not the SAE allows multiple logins from the same IP address.

Options

assigned-ip-idle-timeout assigned-ip-idle-timeout— Interval after which assigned IP subscriber sessions are deactivated if no service session is active.

Value— Number of seconds in the range 0–2147483647

Default— 900

Editing Level—Basic

allow-same-ip-login—(Optional) Enables or disables whether the SAE allows a login from the same IP address without requiring that the previous session logs out first.

- If enabled, the SAE logs in the new subscriber session and automatically logs out the previous session.
- If disabled, the SAE denies login requests if a subscriber session for an IP address is active.

Default— Disabled

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration time-based-policies

Syntax

```
shared sae configuration time-based-policies {
    action-threshold action-threshold;
    preparation-time preparation-time;
    max-worker-threads max-worker-threads;
}
```

Hierarchy Level

```
[edit shared sae configuration time-based-policies]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the action threshold and preparation time for all schedules. You cannot set these values for individual schedules.

Options

action-threshold action-threshold— Maximum delay that the service allows for a time-related change to occur.

Value— Number of milliseconds in the range 0–9223372036854775807.

The recommended range is 60000-300000 milliseconds

Default— 300000 (5 minutes)

Editing Level—Basic

preparation-time preparation-time— Preparation time allowed for a state transition. When you set the preparation time, take into consideration system load and performance. Factors such as the number of subscribers, the number of active services, the number of schedule services, the speed of the processor on the system, as well as other conditions might affect the amount of time to process all the scheduled actions at a specified scheduled time.

Value— Number of milliseconds in the range 0–9223372036854775807

Default— 300000 (5 minutes)

Editing Level—Basic

max-worker-threads max-worker-threads—(Optional) The maximum number of

worker threads for service scheduling.

Value— Integer in the range 0–2147483647

Default—

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Normal

shared sae configuration timeout-session-job-manager

Syntax

```
shared sae configuration timeout-session-job-manager {
    number-of-threads number-of-threads;
}
```

Hierarchy Level

```
[edit shared sae configuration timeout-session-job-manager]
```

Release Information

Statement introduced in SRC Release 3.1.0

Description

Configure the number of threads used for timeout-session-related activity; for example, subscriber and service session timeout, idle timeouts.

Options

number-of-threads number-of-threads— Number of threads used for timeout-session-related activity.

Value— Integer in the range 1–1000

Default— 16

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Expert

shared sae dhcp-classifier rule

Syntax

```
shared sae dhcp-classifier rule name {
    target target;
}
```

Hierarchy Level

```
[edit shared sae dhcp-classifier rule]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a rule in a classifier script.

Options

name name— Name of a classification script.

Value—Text

target target—(Optional) Result of the classification script that is returned to the SAE.

Value— The result depends on the type of classification script:

- Subscriber classification script—An LDAP query that uniquely identifies a subscriber entry in the directory.
- DHCP classification script—DHCP profile.

Default— Not applicable

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae dhcp-classifier rule *name* condition

Syntax

```
shared sae dhcp-classifier rule name condition name ...
```

Hierarchy Level

```
[edit shared sae dhcp-classifier rule name condition]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure match conditions used to find a target. You can configure multiple conditions for each classifier rule.

Options

name name— Match conditions used to find a target. For information about configuring match conditions, see *Classifying Interfaces and Subscribers with the SRC CLI* in *SRC PE Subscribers and Subscriptions Guide*.

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared sae dhcp-classifier rule *name* script

Syntax

```
shared sae dhcp-classifier rule name script {
    script-value;
    include include;
}
```

Hierarchy Level

```
[edit shared sae dhcp-classifier rule name script]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a subscriber classifier. For more information about subscriber classifiers, see the *SRC PE Subscribers and Subscriptions Guide*.

Options

script-value—(Optional) Script target. A script that can contain definitions of custom functions that can be called during the matching process. The complete content of the script is interpreted when the classifier is initially loaded. Because you can insert code into a script target, you can use the classification script to perform various tasks.

Value— Script enclosed in quotation marks.

Default— No value

Editing Level—Basic

include include—(Optional) Name of an existing script to include in the script you are configuring.

Value— *script-name*

Default— No value

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae group

Syntax

```
shared sae group name ...
```

Hierarchy Level

```
[edit shared sae group]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a group of SAE configuration properties.

Options

name name— Name of a shared SAE configuration.

Value— Text

Required Privilege Level

system

Required Editing Level

Basic

shared sae subscriber-classifier rule

Syntax

```
shared sae subscriber-classifier rule name {
    target target;
}
```

Hierarchy Level

```
[edit shared sae subscriber-classifier rule]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a rule in a classifier script.

Options

name name— Name of a classification script.

Value—Text

target target—(Optional) Result of the classification script that is returned to the SAE.

Value— The result depends on the type of classification script:

- Subscriber classification script—An LDAP query that uniquely identifies a subscriber entry in the directory.
- DHCP classification script—DHCP profile.

Default— Not applicable

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared sae subscriber-classifier rule *name* condition

Syntax

```
shared sae subscriber-classifier rule name condition name ...
```

Hierarchy Level

```
[edit shared sae subscriber-classifier rule name condition]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure match conditions used to find a target. You can configure multiple conditions for each classifier rule.

Options

name name— Match conditions used to find a target. For information about configuring match conditions, see *Classifying Interfaces and Subscribers with the SRC CLI* in *SRC PE Subscribers and Subscriptions Guide*.

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared sae subscriber-classifier rule *name* script

Syntax

```
shared sae subscriber-classifier rule name script {
    script-value;
    include include;
}
```

Hierarchy Level

```
[edit shared sae subscriber-classifier rule name script]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a subscriber classifier. For more information about subscriber classifiers, see the *SRC PE Subscribers and Subscriptions Guide*.

Options

script-value—(Optional) Script target. A script that can contain definitions of custom functions that can be called during the matching process. The complete content of the script is interpreted when the classifier is initially loaded. Because you can insert code into a script target, you can use the classification script to perform various tasks.

Value— Script enclosed in quotation marks.

Default— No value

Editing Level—Basic

include include—(Optional) Name of an existing script to include in the script you are configuring.

Value— *script-name*

Default— No value

Editing Level—Basic

Required Privilege Level

system

Required Editing Level**Basic**

slot *number* sae

Syntax

```
slot number sae {
    base-dn base-dn;
    real-portal-address real-portal-address;
    java-runtime-environment java-runtime-environment;
    java-min-heap-size java-min-heap-size;
    java-heap-size java-heap-size;
    java-min-new-size java-min-new-size;
    java-new-size java-new-size;
    java-garbage-collection-options java-garbage-collection-options;
    port-offset port-offset;
    snmp-agent;
    shared shared;
}
```

Hierarchy Level

```
[edit slot number sae]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure local properties for the SAE, including the base DN, interface the SAE uses to communicate with the router, path to the JRE, Java heap size, Java garbage collection options, and port offset. The statement also specifies the shared configuration object that holds the shared SAE configuration, and it enables or disables SNMP.

Options

base-dn base-dn— Distinguished name (DN) of the root directory for the SAE. You must set this attribute if you use a directory-naming scheme different from the default.

Value— DN of the root directory for the SAE.

Default— *o=umc*

Editing Level—Advanced

real-portal-address real-portal-address— Interface on the SAE that the SAE uses for communication with the router. If you clear this field, the interface is assumed to be the interface that was used to connect the router driver to the SAE. If the SAE has multiple network interfaces, you must specify the interfaces that are used to communicate with the

router.

Value— IP address of the interface

Default— One of the IP addresses configured on the host (except 127.0.0.1)

Editing Level—Basic

`java-runtime-environment` *java-runtime-environment*— Path to the Java runtime environment (JRE) The SRC software requires a JRE that conforms to the Java 2 specification. The SRC software has been tested with Sun's JRE. See the SRC Release Notes for information about which version of the Sun JRE is distributed with the SRC software. We expect other JREs to work, but have not verified whether they do.

Value— Absolute or relative directory path. This path is the default installation path for the JRE that is distributed with the SRC software and installed with the other SRC components.

Default— `../jre/bin/java`

Editing Level—Expert

`java-min-heap-size` *java-min-heap-size*— Minimum Java heap (memory) size available to the JRE.

Value— Number of bytes or add k for kilobytes, m for megabytes, or g for gigabytes. For example, 896m. The value must be less or equal java-heap-size.

Default— The default is set to 2g for C2000 and 4g for C4000.

Editing Level—Advanced

`java-heap-size` *java-heap-size*— Maximum Java heap (memory) size available to the JRE.

Value— Number of bytes or add k for kilobytes, m for megabytes, or g for gigabytes. For example, 896m. Change this value if you experience problems caused by lack of memory. Set the value lower than the available physical memory to avoid low performance caused by disk swapping. See the documentation for the JRE for valid values.

Default— The value is calculated dynamically to 70% of the available real memory.

Editing Level—Advanced

`java-min-new-size` *java-min-new-size*— Minimum Java new generation heap (memory) size available to the JRE when the SAE starts.

Value— Integer in the range 0-<Java new size>. Specify the value in bytes or add m for megabytes, k for kilobytes, or g for gigabytes. For example, 24m. See the documentation for the JRE for valid values.

Default— 256m

Editing Level—Advanced

`java-new-size` *java-new-size*— Maximum Java new generation heap (memory) size available to the JRE when the SAE starts.

Value— Integer in the range 0–<Java heap size>. Specify the value in bytes or add m for megabytes, k for kilobytes, or g for gigabytes. For example, 24m. See the documentation for the JRE for valid values.

Default— 1000m

Editing Level—Advanced

`java-garbage-collection-options` *java-garbage-collection-options*— Garbage collection functionality of the Java Virtual Machine.

Value— Options defined by the JVM

Default— -Xbatch -XX:+UseConcMarkSweepGC -XX:

CMSInitiatingOccupancyFraction=80 -XX:+UseParNewGC -XX:

SurvivorRatio=1 -XX:InitialTenuringThreshold=8 -XX:

MaxTenuringThreshold=10 -XX:TargetSurvivorRatio=90 -XX:

+UseCMSCompactAtFullCollection -XX:CMSFullGCsBeforeCompaction=0

-XX:+CMSClassUnloadingEnabled -XX:+CMSParallelRemarkEnabled

Editing Level—Advanced

`port-offset` *port-offset*— Port offset for SAE instances. The offset is added to the OA port, RADIUS socket, and administration HTTPS server ports.

Value— Integer in the range 0–65535. Set to 0 if you install multiple SAE instances on the same host.

Default— 0

Editing Level—Expert

`snmp-agent`—(Optional) Enables the SAE to communicate with the SNMP agent.

Editing Level—Basic

`shared` *shared*— Shared configuration object that holds most of the SAE specific configuration.

Value— Name of the object in the format "/SAE/<path>". The <path> is separated by / and can contain multiple levels. The effective configuration is combined by all configuration objects in the path, with more specific configuration in the lower levels of the path.

Default— /SAE/POP-ID;

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

slot *number* sae initial

Syntax

```
slot number sae initial {
    static-dn static-dn;
    dynamic-dn dynamic-dn;
}
```

Hierarchy Level

```
[edit slot number sae initial]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure initial properties for SRC components.

Options

static-dn static-dn—(Optional) Location of administrator-defined configuration data in the directory.

Value—Text

Default—ou=staticConfiguration,ou=Configuration,o=Management,o=umc

Editing Level—Expert

dynamic-dn dynamic-dn—(Optional) Location of programmatically-defined configuration data in the directory.

Value—Text

Default—ou=dynamicConfiguration,ou=Configuration,o=Management,
o=umc

Editing Level—Expert

Required Privilege Level

system

Required Editing Level

Basic

slot *number* sae initial directory-connection

Syntax

```
slot number sae initial directory-connection {
    url url;
    backup-urls [backup-urls...];
    principal principal;
    credentials credentials;
    protocol (ldaps);
    timeout timeout;
    check-interval check-interval;
    blacklist;
    snmp-agent;
}
```

Hierarchy Level

```
[edit slot number sae initial directory-connection]
```

Description

Configure properties for the directory connection.

Options

url url—(Optional) URL that identifies the location of the primary directory server.

Value— URL

Default—ldap://127.0.0.1:389

Editing Level—Basic

backup-urls [backup-urls...]—(Optional) URLs that identify the locations of backup directory servers. Backup servers are used if the primary directory server is not accessible.

Value— List of URLs

Editing Level—Basic

principal principal— DN that the SRC component uses for authentication to access the directory.

Value— DN.

When you specify the DN, you can use <base> to indicate the base DN.

Editing Level—Basic

`credentials credentials`— Password with which the SRC component accesses the directory.

Value— Password

Editing Level—Basic

`protocol (ldaps)`—(Optional) Security protocol used to connect to the directory. If you do not configure a security protocol, plain socket is used.

Value

- `ldaps`— LDAPS which uses SSL.

Editing Level—Expert

`timeout timeout`—(Optional) Maximum amount of time during which the directory must respond to a connection request.

Value—Integer in the range 1–2147483647 s

Default—10

Editing Level—Expert

`check-interval check-interval`—(Optional) Time interval at which the directory monitoring system verifies its connection to the directory. If the directory connection fails after this interval, the directory monitoring system initiates a connection to another directory.

Value—Integer in the range 15–2147483647 s

Default—60

Editing Level—Expert

`blacklist`—(Optional) Specifies whether the directory monitoring system prevents connection to a directory if the directory fails to respond during 10 polling intervals.

Default—false

Editing Level—Basic

`snmp-agent`—(Optional) Specifies whether the SDX SNMP agent exports MIBs for this directory connection.

Default—false
Editing Level—Expert

Required Privilege Level

system

Required Editing Level

Basic

slot *number* sae initial directory-eventing

Syntax

```
slot number sae initial directory-eventing {
    eventing;
    signature-dn signature-dn;
    polling-interval polling-interval;
    event-base-dn event-base-dn;
    dispatcher-pool-size dispatcher-pool-size;
}
```

Hierarchy Level

```
[edit slot number sae initial directory-eventing]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Change configuration for directory eventing properties. In most cases, you can use the default configuration for these properties.

Options

eventing—(Optional) Enable an SRC component to poll the directory for changes.

Default—true

Editing Level—Normal

signature-dn *signature-dn*—(Optional) DN of the directory entry that specifies the usedDirectory attribute for the SRC CLI. The usedDirectory attribute identifies the vendor of the directory server.

Value— DN

Default—o=umc

Editing Level—Expert

polling-interval *polling-interval*—(Optional) Interval at which an SRC component polls the directory to check for directory changes.

Value—Integer in the range 15–2147483647 s

Default—30
Editing Level—Normal

`event-base-dn` *event-base-dn*—(Optional)

DN of an entry superior to the data associated with an SRC component in the directory.

If you are storing non-SRC data in the directory, and that data changes frequently whereas the SRC data does not, you may need to adjust the default value to improve performance. For optimal performance, set the value to the DN of an entry superior to both the SRC data and the changing non-SRC data.

Value— DN
Default—o=UMC
Editing Level—Expert

`dispatcher-pool-size` *dispatcher-pool-size*—(Optional) Number of directory change notifications that can be sent simultaneously to the SRC component.

Value—Integer in the range 0–2147483647
Default—1
Editing Level—Expert

Required Privilege Level

system

Required Editing Level

Basic

slot *number* sae radius

Syntax

```
slot number sae radius {
    local-address local-address;
    local-nas-id local-nas-id;
}
```

Hierarchy Level

```
[edit slot number sae radius]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the local address that the SAE uses to communicate with RADIUS servers, the network access server (NAS) ID that identifies the SAE when it sends RADIUS messages, and the real portal address that the SAE uses to communicate with the router.

Options

local-address local-address— Local IP address on the SAE host used for communication with RADIUS servers.

Value— IP address; should be a unique NAS IP address.

In an installation in which the SAE is equipped with multiple network interfaces, you must specify the interface that communicates with external RADIUS servers. Typically, you must configure the RADIUS server to accept requests from a client; use this IP address for the RADIUS client configuration. Even if the RADIUS server is running on the same server as the SAE, do not use 127.0.0.1 as the local address, because this address is typically the loopback address for a server.

Editing Level—Basic

local-nas-id local-nas-id— String that identifies the SAE when it sends RADIUS authentication and accounting messages.

Value— Text string that identifies the SAE. Typically, the string is the name

of the SAE host.

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

clear sae directory-blacklist

Syntax

```
clear sae directory-blacklist
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Delete directory blacklist or remove a server from the directory blacklist. A server is added to the blacklist if it repeatedly fails to respond while the server is running and accepting requests.

Required Privilege Level

clear

clear sae registered equipment

Syntax

```
clear sae registered equipment <mac-address mac-address> <force> <persistent>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Delete entries in the equipment registration cache.

Options

mac-address mac-address—(Optional) MAC address of equipment registrations.

Value— MAC address in the format xx:xx:xx:xx:xx:x

Default— No value

force—(Optional) Flag indicating that no confirmation is requested before the software clears the equipment registration.

Default— Disabled

persistent—(Optional) Flag indicating that equipment registration is also removed from the directory. If you do not set this flag, the equipment registration is removed only from the memory. Disabled

Default—false

Required Privilege Level

clear

clear sae registered login

Syntax

```
clear sae registered login <mac-address mac-address> <force> <persistent>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Delete entries in the login registration cache.

Options

mac-address mac-address—(Optional) MAC address of login registrations.

Value— MAC address in the format xx:xx:xx:xx:xx:xx

Default— No value

force—(Optional) Flag indicating that no confirmation is requested before the software clears the login registration.

Default— Disabled

persistent—(Optional) Flag indicating that login registration is also removed from the directory. If you do not set this flag, the login registration is removed only from the memory.

Default— Disabled

Required Privilege Level

clear

monitor sae statistics sessions

Syntax

```
monitor sae statistics sessions
```

Release Information

Command introduced in SRC Release 3.1.0

Description

Display real-time SNMP statistics for subscriber and service sessions.

Required Privilege Level

view

request sae load configuration

Syntax

```
request sae load configuration
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Reload SAE configuration data from the directory. The new configuration takes effect immediately.

Required Privilege Level

maintenance

request sae load domain-map

Syntax

```
request sae load domain-map
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Reload the mapping of domain names to retailer entries. This mapping is made available to the SAE's subscriber classification script.

Required Privilege Level

maintenance

request sae load interface-classification

Syntax

```
request sae load interface-classification
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Reload the interface classification scripts from the directory, and apply the result of the interface classification changes to the router as follows:

- For every unmanaged interface that becomes managed, new default policies are downloaded to the router.
- For every managed interface whose default policy group has changed, the old default policies are replaced by the new ones.
- For every managed interface that becomes unmanaged, an error message in the error log is displayed and no changes are applied until the interface goes down.

Required Privilege Level

maintenance

request sae load services

Syntax

```
request sae load services
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Reload the following objects from the directory: services, scopes, virtual routers, policies, service mutex groups, and service schedules. Related service sessions are activated, deactivated, or reactivated, as needed.

Required Privilege Level

maintenance

request sae load subscriptions

Syntax

```
request sae load subscriptions
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Reload all subscriptions from the directory. Related service sessions are activated, deactivated, or reactivated as needed.

Required Privilege Level

maintenance

request sae login ip authenticated-dhcp

Syntax

```
request sae login ip authenticated-dhcp virtual-router virtual-router address
address login-name login-name mac-address mac-address interface-type (ipv4 |
ipv6) <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>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Log in a simulated subscriber that is an authenticated DHCP subscriber. Logging in simulated subscribers allows you to test your SRC application without the need for a router or other device.

Options

virtual-router virtual-router— Name of a simulated virtual router that you want to appear in the simulated subscriber session.

Value— Text

Default— No value

address address— IP address from which you log in simulated subscribers.

Value— IP address

Default— No value

login-name login-name— Fully qualified name used to log in simulated subscribers.

Value— Fully qualified name

Default— No value

mac-address mac-address— MAC address used to log in simulated subscribers.

Value— MAC address in the format xx:xx:xx:xx:xx:xx

Default— 00:00:00:00:00:01

`interface-type (ipv4 | ipv6)` — Selects between IPv4 or IPv6 subscribers

Value

- `ipv4`—IPv4
- `ipv6`—IPv6

`service-bundle service-bundle`—(Optional) Service bundle used when logging in simulated subscribers.

Value— Service bundle name

Default— No value

`radius-class radius-class`—(Optional) RADIUS class used when logging in simulated subscribers.

Value— RADIUS class

Default— No value

`interface-name interface-name`—(Optional) Virtual interface used when logging in simulated subscribers.

Value— Virtual router name

Default— No value

`interface-alias interface-alias`—(Optional) Interface description used when logging in simulated subscribers. If you are simulating JUNOS routers, interface alias is the description that is configured on JUNOS routers with the **interface description** command.

Value— Text

Default— No value

`interface-description interface-description`—(Optional) Alternate interface name used when logging in simulated subscribers. This is the interface name that is used by SNMP.

Value— If you are simulating a:

- JUNOS router, the format of the description is `ip<slot>/<port>.<subinterface>`
- JUNOS routing platform, ifDesc is the same as interfaceName.

Default— No value

`nas-port-id` *nas-port-id*—(Optional) Port identifier of an interface used when logging in simulated subscribers.

Value— Includes interface name and additional layer 2 information. For example, fastEthernet 3/1.

Default— No value

Required Privilege Level

maintenance

request sae login ip authenticated-interface

Syntax

```
request sae login ip authenticated-interface virtual-router virtual-router
address address login-name login-name interface-type (ipv4 | ipv6) <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>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Log in a simulated subscriber that is an authenticated interface subscriber. Logging in simulated subscribers allows you to test your SRC application without the need for a router or other device.

Options

virtual-router virtual-router— Name of a simulated virtual router that you want to appear in the simulated subscriber session.

Value— Text

Default— No value

address address— IP address from which you log in simulated subscribers.

Value— IP address

Default— No value

login-name login-name— Fully qualified name used to log in simulated subscribers.

Value— Fully qualified name

Default— No value

interface-type (ipv4 | ipv6) — Selects between IPv4 or IPv6 subscribers

Value

- *ipv4*—IPv4

- `ipv6`—IPv6

`service-bundle` *service-bundle*—(Optional) Service bundle used when logging in simulated subscribers.

Value— Service bundle name

Default— No value

`radius-class` *radius-class*—(Optional) RADIUS class used when logging in simulated subscribers.

Value— RADIUS class

Default— No value

`interface-name` *interface-name*—(Optional) Virtual interface used when logging in simulated subscribers.

Value— Virtual router name

Default— No value

`interface-alias` *interface-alias*—(Optional) Interface description used when logging in simulated subscribers. If you are simulating JUNOS routers, interface alias is the description that is configured on JUNOS routers with the **interface description** command.

Value— Text

Default— No value

`interface-description` *interface-description*—(Optional) Alternate interface name used when logging in simulated subscribers. This is the interface name that is used by SNMP.

Value— If you are simulating a:

- JUNOS router, the format of the description is `ip<slot>/<port>.<subinterface>`
- JUNOS routing platform, ifDesc is the same as interfaceName.

Default— No value

`nas-port-id` *nas-port-id*—(Optional) Port identifier of an interface used when logging in simulated subscribers.

Value— Includes interface name and additional layer 2 information. For example, fastEthernet 3/1.

Default— No value

Required Privilege Level

maintenance

request sae login ip unauthenticated-dhcp

Syntax

```
request sae login ip unauthenticated-dhcp virtual-router virtual-router address
address mac-address mac-address interface-type (ipv4 | ipv6) <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>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Log in a simulated subscriber that is an unauthenticated DHCP subscriber. Logging in simulated subscribers allows you to test your SRC application without the need for a router or other device.

Options

virtual-router virtual-router— Name of a simulated virtual router that you want to appear in the simulated subscriber session.

Value— Text

Default— No value

address address— IP address from which you log in simulated subscribers.

Value— IP address

Default— No value

mac-address mac-address— MAC address used to log in simulated subscribers.

Value— MAC address in the format xx:xx:xx:xx:xx:xx

Default— 00:00:00:00:00:01

interface-type (ipv4 | ipv6) — Selects between IPv4 or IPv6 subscribers

Value

- *ipv4*—IPv4

- `ipv6`—IPv6

`login-name login-name`—(Optional) Fully qualified name used to log in simulated subscribers.

Value— Fully qualified name

Default— No value

`service-bundle service-bundle`—(Optional) Service bundle used when logging in simulated subscribers.

Value— Service bundle name

Default— No value

`radius-class radius-class`—(Optional) RADIUS class used when logging in simulated subscribers.

Value— RADIUS class

Default— No value

`interface-name interface-name`—(Optional) Virtual interface used when logging in simulated subscribers.

Value— Virtual router name

Default— No value

`interface-alias interface-alias`—(Optional) Interface description used when logging in simulated subscribers. If you are simulating JUNOS routers, interface alias is the description that is configured on JUNOS routers with the **interface description** command.

Value— Text

Default— No value

`interface-description interface-description`—(Optional) Alternate interface name used when logging in simulated subscribers. This is the interface name that is used by SNMP.

Value— If you are simulating a:

- JUNOS router, the format of the description is `ip<slot>/<port>.<subinterface>`
- JUNOS routing platform, ifDesc is the same as interfaceName.

Default— No value

`nas-port-id` *nas-port-id*—(Optional) Port identifier of an interface used when logging in simulated subscribers.

Value— Includes interface name and additional layer 2 information. For example, fastEthernet 3/1.

Default— No value

Required Privilege Level

maintenance

request sae login ip unauthenticated-interface

Syntax

```
request sae login ip unauthenticated-interface virtual-router virtual-router
interface-name interface-name interface-type (ipv4 | ipv6) <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>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Log in a simulated subscriber that is an unauthenticated interface subscriber. Logging in simulated subscribers allows you to test your SRC application without the need for a router or other device.

Options

virtual-router virtual-router— Name of a simulated virtual router that you want to appear in the simulated subscriber session.

Value— Text

Default— No value

interface-name interface-name— Virtual interface used when logging in simulated subscribers.

Value— Virtual interface name

Default— No value

interface-type (ipv4 | ipv6) — Selects between IPv4 or IPv6 subscribers

Value

- *ipv4*—IPv4
- *ipv6*—IPv6

address address—(Optional) IP address from which you log in simulated subscribers.

Value— IP address**Default**— No value

`login-name` *login-name*—(Optional) Fully qualified name used to log in simulated subscribers.

Value— Fully qualified name**Default**— No value

`service-bundle` *service-bundle*—(Optional) Service bundle used when logging in simulated subscribers.

Value— Service bundle name**Default**— No value

`radius-class` *radius-class*—(Optional) RADIUS class used when logging in simulated subscribers.

Value— RADIUS class**Default**— No value

`interface-alias` *interface-alias*—(Optional) Interface description used when logging in simulated subscribers. If you are simulating JUNOSe routers, interface alias is the description that is configured on JUNOSe routers with the **interface description** command.

Value— Text**Default**— No value

`interface-description` *interface-description*—(Optional) Alternate interface name used when logging in simulated subscribers. This is the interface name that is used by SNMP.

Value— If you are simulating a:

- JUNOSe router, the format of the description is ip<slot>/<port>.<subinterface>
- JUNOS routing platform, ifDesc is the same as interfaceName.

Default— No value

`nas-port-id` *nas-port-id*—(Optional) Port identifier of an interface used when logging in simulated subscribers.

Value— Includes interface name and additional layer 2 information. For example, fastEthernet 3/1.

Default— No value

Required Privilege Level

maintenance

request sae logout dn

Syntax

```
request sae logout dn <filter filter> <force>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Log out subscribers who are accessible by DN. All subscribers who have a subscriber profile in the directory are accessible by DN.

Options

filter filter—(Optional) DN or DN's of subscribers that you want to log out.

Value— All or part of the subscriber DN

Default— No value

force—(Optional) Flag indicating that no confirmation is requested before the software logs out subscribers.

Default— Disabled

Required Privilege Level

clear

request sae logout ip

Syntax

```
request sae logout ip <filter filter> <force>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Log out subscribers who are accessible by IP address. The following types of subscribers are accessible by IP address: DHCP subscribers, authenticated PPP subscribers, and static IP subscribers who have logged in through a portal.

Options

filter filter—(Optional) IP address or addresses of subscribers that you want to log out.

Value— All or part of the subscriber IP address

Default— No value

force—(Optional) Flag indicating that no confirmation is requested before the software logs out subscribers.

Default— Disabled

Required Privilege Level

clear

request sae logout login-name

Syntax

```
request sae logout login-name <filter filter> <force>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Log out subscribers who are accessible by login name. All authenticated subscribers are accessible by login name.

Options

filter filter—(Optional) Login name or names of subscribers that you want to log out.

Value— All or part of the login name

Default— No value

force—(Optional) Flag indicating that no confirmation is requested before the software logs out subscribers.

Default— Disabled

Required Privilege Level

clear

request sae logout session-id

Syntax

```
request sae logout session-id <filter filter> <force>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Log out subscribers who are accessible by session ID. All subscribers are accessible by session ID.

Options

filter filter—(Optional) Session ID or IDs of subscribers that you want to log out.

Value— All or part of the subscriber session ID

Default— No value

force—(Optional) Flag indicating that no confirmation is requested before the software logs out subscribers.

Default— Disabled

Required Privilege Level

clear

request sae modify device failover

Syntax

```
request sae modify device failover <ip-address ip-address> <tcp-port tcp-port>
<use-failover-server> virtual-router virtual-router <force>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Modify failover server parameters.

Options

ip-address ip-address—(Optional) IP address of an alternate SAE server to which a router or other device can reconnect when the device driver closes its connection. If the driver is configured to use this failover IP address, it sends this IP address to the router or other device when it closes its connection. The device then attempts to open a new connection to the failover IP address. This address is not applicable to the PCMM driver.

Value— IP address

Default— 0.0.0.0

tcp-port tcp-port—(Optional) Port of an alternate SAE server to which a router or other device can reconnect when the device driver closes its connection. If the driver is configured to use this failover port, it sends this failover port to the router or other device when it closes its connection. The device then attempts to open a new connection to this failover port. This TCP port is not applicable to the PCMM driver.

Value— Port number

Default— 0

use-failover-server—(Optional) If you set this flag, then the device driver sends its own failover IP address and port to the router or other device when it closes its connection. The device then attempts to open a new connection to the failover IP address and port. This flag is not applicable to the PCMM router driver.

Default— Disabled

virtual-router virtual-router— Virtual router name.

Value— Name of the virtual router.

- For JUNOSe router drivers, use the format `virtualRouterName@routerName`.
- For JUNOS router drivers and PCMM drivers, use the format `default@routerName`.

Default— No value

`force`—(Optional) Flag indicating that no confirmation is requested before the software proceeds with the modification.

Default— Disabled

Required Privilege Level

reset

request sae shutdown device

Syntax

```
request sae shutdown device <name name> <force>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Shut down the specified device driver.

Options

name name—(Optional) Device name or names that are managing the drivers that you want to shut down.

Value— All or part of the device name.

- For JUNOSe router drivers, use the format *virtualRouterName@routerName*.
- For JUNOS router drivers and PCMM drivers, use the format *default@routerName*.

Default— No value

force—(Optional) Flag indicating that no confirmation is requested before proceeding with the device driver shutdown.

Default— Disabled

Required Privilege Level

maintenance

request sae update ip-pools

Syntax

```
request sae update ip-pools virtual-router virtual-router <management-address  
management-address> <SNMP-community SNMP-community> <server server> <base-dn base-  
dn> <principal principal> <credentials credentials>
```

Release Information

Command introduced in SRC Release 3.2.0

Description

Options

virtual-router virtual-router— Name of the virtual router in the format *virtualRouterName@deviceName*.

Value— Text

Default— No value

management-address management-address—(Optional) The IP address of the virtual router.

Value— IP address

Default— -

SNMP-community SNMP-community—(Optional) SNMP community for a given virtual router.

Value— Text

Default— public

server server—(Optional) IP address or name of the host that supports the directory.

Value— IP address or name of the host

Default— 127.0.0.1

base-dn base-dn—(Optional) The base DN for the root of the tree to be used.

Value— DN

Default— o=Network,o=UMC

`principal principal`—(Optional) DN that defines the username with which an SRC component accesses the directory.

Value— DN

Default— No Value

`credentials credentials`—(Optional) Password used for authentication with the directory server.

Value— Text

Default— No value

Required Privilege Level

maintenance

request sae update qos-profiles

Syntax

```
request sae update qos-profiles virtual-router virtual-router <management-address  
management-address> <SNMP-community SNMP-community> <server server> <base-dn base-  
dn> <principal principal> <credentials credentials>
```

Release Information

Command introduced in SRC Release 3.2.0

Description

Options

virtual-router virtual-router— Name of the virtual router in the format *virtualRouterName@deviceName*.

Value— Text

Default— No value

management-address management-address—(Optional) The IP address of the virtual router.

Value— IP address

Default— -

SNMP-community SNMP-community—(Optional) SNMP community for a given virtual router.

Value— Text

Default— public

server server—(Optional) IP address or name of the host that supports the directory.

Value— IP address or name of the host

Default— 127.0.0.1

base-dn base-dn—(Optional) The base DN for the root of the tree to be used.

Value— DN

Default— o=Network,o=UMC

`principal` *principal*—(Optional) DN that defines the username with which an SRC component accesses the directory.

Value— DN

Default— No Value

`credentials` *credentials*—(Optional) Password used for authentication with the directory server.

Value— Text

Default— No value

Required Privilege Level

maintenance

show sae directory-blacklist

Syntax

```
show sae directory-blacklist
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display the directory blacklist.

Required Privilege Level

view

show sae drivers

Syntax

```
show sae drivers <device-name device-name> < (brief) > <maximum-results maximum-
results>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display the state of SAE device drivers. Each device driver manages one logical router instance. For example, a JUNOS routing platform, a JUNOSe virtual router, a PCMM device, or another third-party device.

Options

`device-name device-name`—(Optional) Name of a device.

Value— All or part of the device name.

- For JUNOSe router drivers, use the format `virtualRouterName@routerName`.
- For JUNOS router drivers and PCMM drivers, use the format `default@routerName`.

Default— No value

(Optional) Output style

Value

- `brief`— Display only virtual router names.

Default— Detail

`maximum-results maximum-results`—(Optional) Number of results to be displayed.

Value—Integer in the range 1–2147483647

Default— 25

Required Privilege Level

view

show sae interfaces

Syntax

```
show sae interfaces <interface-name interface-name> <virtual-router virtual-router> < (brief) > <maximum-results maximum-results>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display information about router interfaces that the SAE is managing.

Options

interface-name interface-name—(Optional) Name of router interface.

Value— All or part of the interface name

Default— No value

virtual-router virtual-router—(Optional) Name of virtual router.

Value— All or part of the virtual router name

Default— No value

(Optional) Output style.

Value

- *brief*— Display only interface names.

Default— Detail

maximum-results maximum-results—(Optional) Number of results to be displayed.

Value—Integer in the range 1–2147483647

Default— 25

Required Privilege Level

view

show sae policies

Syntax

```
show sae policies <group group> < (brief) > <maximum-results maximum-results>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display policy groups.

Options

group group—(Optional) Name of a policy group.

Value— All or part of the policy group name

Default— No value

(Optional) Output style.

Value

- *brief*— Display only policy group names.

Default—detail

maximum-results maximum-results—(Optional) Number of results to be displayed.

Value—Integer in the range 1–2147483647

Default— 25

Required Privilege Level

view

show sae registered equipment

Syntax

```
show sae registered equipment <mac-address mac-address> < (brief) > <maximum-  
results maximum-results>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display equipment registrations.

Options

`mac-address mac-address`—(Optional) MAC address of equipment registrations.

Value— MAC address in the format xx:xx:xx:xx:xx:xx

Default— No value

(Optional) Output style.

Value

- `brief`— Display only the MAC address of registered equipment.

Default— Detail

`maximum-results maximum-results`—(Optional) Number of results to be displayed.

Value—Integer in the range 1–2147483647

Default— 25

Required Privilege Level

view

show sae registered login

Syntax

```
show sae registered login <mac-address mac-address> < (brief) > <maximum-results
maximum-results>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display login registrations.

Options

`mac-address mac-address`—(Optional) MAC address of login registrations.

Value— MAC address in the format xx:xx:xx:xx:xx:xx

Default— No value

(Optional) Output style

Value

- `brief`— Display only the MAC address of login registrations.

Default— Detail

`maximum-results maximum-results`—(Optional) Number of results to be displayed.

Value—Integer in the range 1–2147483647

Default— 25

Required Privilege Level

view

show sae services

Syntax

```
show sae services <name name> <secret> < (brief) > <maximum-results maximum-
results>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display the state of services running on the SAE.

Options

`name name`—(Optional) Name of service.

Value— All or part of the service name

Default— No value

`secret`—(Optional) Display subscriber sessions and service sessions for hidden services.

Default— Disabled

(Optional) Output style

Value

- `brief`— Display only service names.

Default— Detail

`maximum-results maximum-results`—(Optional) Number of results to be displayed.

Value—Integer in the range 1–2147483647

Default— 25

Required Privilege Level

view

show sae statistics device

Syntax

```
show sae statistics device <name name> < (brief) >
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display SNMP information for routers and other devices that the SAE is managing. For example, Juniper Networks routers, PCMM devices, and other third-party devices.

Options

name name—(Optional) Name of a device.

Value— All or part of the device name.

- For JUNOSe router drivers, use the format `virtualRouterName@routerName`.
- For JUNOS router drivers and PCMM drivers, use the format `default@routerName`.

Default— No value

(Optional) Output style

Value

- `brief`— Display only device names.

Default— Detail

Required Privilege Level

view

show sae statistics device common

Syntax

```
show sae statistics device common < (junos | junose | packetcable-cops | proxy |  
aaa | junos-ise | junos-ptsp) >
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display SNMP statistics for all device drivers of a particular type.

Options

(Optional) Display SNMP statistics for a specified device driver type.

Value

- `junos`— JUNOS router drivers.
- `junose`— JUNOSe router drivers.
- `packetcable-cops`— PCMM device drivers.
- `proxy`— Third-party device drivers.
- `aaa`— AAA device drivers.
- `junos-ise`— ISE device drivers.
- `junos-ptsp`— PTSP device drivers.

Default— No value

Required Privilege Level

view

show sae statistics directory

Syntax

```
show sae statistics directory
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display SNMP statistics about the directory.

Required Privilege Level

view

show sae statistics directory connections

Syntax

```
show sae statistics directory connections <id id> < (brief) >
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display SNMP statistics for directory connections.

Options

id id—(Optional) Directory connection ID.

Value— All or part of the connection ID

Default— No value

(Optional) Output style

Value

- *brief*— Display only directory connection IDs.

Default— Detail

Required Privilege Level

view

show sae statistics license client

Syntax

```
show sae statistics license client
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display SNMP information about the state of client licenses.

Required Privilege Level

view

show sae statistics license device

Syntax

```
show sae statistics license device <name name> < (brief) >
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display SNMP information about the state of licenses on specified devices.

Options

name name—(Optional) Name of a device.

Value— All or part of the device name.

- For JUNOSe router drivers, use the format `virtualRouterName@routerName`.
- For JUNOS router drivers and PCMM drivers, use the format `default@routerName`.

Default— No value

(Optional) Output style

Value

- `brief`— Display only device names.

Default— Detail

Required Privilege Level

view

show sae statistics license local

Syntax

```
show sae statistics license local
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display SNMP information about the state of local licenses.

Required Privilege Level

view

show sae statistics policy-management

Syntax

```
show sae statistics policy-management
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display SNMP information about the policy engine, policy decision point, and the shared object repository where the policy objects are stored.

Required Privilege Level

view

show sae statistics process

Syntax

```
show sae statistics process
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display SNMP information about the SAE server process.

Required Privilege Level

view

show sae statistics radius

Syntax

```
show sae statistics radius
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display SNMP RADIUS information. Display SNMP statistics for RADIUS clients.

Required Privilege Level

view

show sae statistics radius client

Syntax

```
show sae statistics radius client (accounting | authentication) <ip-address ip-  
address> <udp-port udp-port> < (brief) >
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display SNMP information about RADIUS clients.

Options

Display SNMP information for either RADIUS accounting clients or RADIUS authentication clients.

Value

- *accounting*— Display SNMP information for RADIUS accounting clients.
- *authentication*— Display SNMP information for RADIUS authentication clients.

Default— No value

ip-address ip-address—(Optional) IP address or addresses of RADIUS clients.

Value— All or part of the client IP address

Default— No value

udp-port udp-port—(Optional) Port number for RADIUS clients.

Value— All or part of the client port number

Default— No value

(Optional) Output style.

Value

- **brief**— Display only a list of the clients that are accessible by IP address and port number.

Default— Detail

Required Privilege Level

view

show sae statistics sessions

Syntax

```
show sae statistics sessions
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display SNMP statistics for subscriber sessions and service sessions.

Required Privilege Level

view

show sae subscribers

Syntax

```
show sae subscribers <maximum-results maximum-results> <secret> < (brief | terse) >
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display information about subscriber sessions.

Options

maximum-results maximum-results—(Optional) Number of results to be displayed.

Value—Integer in the range 1–2147483647

Default— 25

secret—(Optional) Display subscriber sessions and service sessions for hidden services.

Default— Disabled

(Optional) Output style

Value

- *brief*— Display subscriber session information. Service sessions are not displayed.
- *terse*— Display subscriber session ID, login name, and IP address.

Default— Detail

Required Privilege Level

view

show sae subscribers dn

Syntax

```
show sae subscribers dn <filter filter>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display subscriber sessions accessible by DN. All subscribers who have a subscriber profile in the directory are accessible by DN.

Options

filter filter—(Optional) DN of the subscribers.

Value— All or part of the subscriber DN

Default— No value

Required Privilege Level

view

show sae subscribers ip

Syntax

```
show sae subscribers ip <address address>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display subscriber sessions that are accessible by IP address. The following subscribers are accessible by IP address: DHCP subscribers, authenticated PPP subscribers, and static IP subscribers who have logged in through a portal.

Options

address address—(Optional) IP address of subscriber sessions.

Value— All or part of the subscriber IP address

Default— No value

Required Privilege Level

view

show sae subscribers login-name

Syntax

```
show sae subscribers login-name <filter filter>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display subscriber sessions accessible by login name. All authenticated subscribers are accessible by login name.

Options

filter filter—(Optional) Login name of subscriber sessions.

Value— All or part of the subscriber login name

Default— No value

Required Privilege Level

view

show sae subscribers service-name

Syntax

```
show sae subscribers service-name <filter filter>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display all active subscriber sessions activated from a subscription to the specified service name.

Options

filter filter—(Optional) Service name of subscriber sessions.

Value— All or part of the service name

Default— No value

Required Privilege Level

view

show sae subscribers session-id

Syntax

```
show sae subscribers session-id <filter filter>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display subscriber sessions by session ID.

Options

filter filter—(Optional) ID of subscriber sessions.

Value— All or part of the subscriber session ID

Default— No value

Required Privilege Level

view

show sae threads

Syntax

```
show sae threads
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display information about threads and their priority on the SAE.

Required Privilege Level

view

Network Information Collector (NIC)

The following table summarizes the command-line interface (CLI) for the network information collector (NIC). Configuration statements and operational commands are listed in alphabetical order.

NIC
Configuration Statements
shared nic scenario
shared nic scenario name agents
shared nic scenario name agents name configuration consolidator
shared nic scenario name agents name configuration directory
shared nic scenario name agents name configuration properties
shared nic scenario name agents name configuration sae-client
shared nic scenario name agents name configuration sae-plug-in
shared nic scenario name agents name configuration xml
shared nic scenario name hosts
shared nic scenario name hosts logger
shared nic scenario name hosts logger name file
shared nic scenario name hosts logger name syslog
shared nic scenario name hosts name configuration
shared nic scenario name hosts name configuration logger
shared nic scenario name hosts name configuration logger name file
shared nic scenario name hosts name configuration logger name syslog
shared nic scenario name nic-locators
shared nic scenario name nic-locators name resolution
shared nic scenario name realms
shared nic scenario name realms name configuration custom-resolver classname
shared nic scenario name realms name configuration transitions

shared nic scenario name realms name resolvers
shared nic scenario name realms name resolvers name configuration
slot number network-publisher directory-connection
slot_number_network-publisher_logger
slot number network-publisher logger name file
slot number network-publisher logger name syslog
slot number network-publisher routers
slot number network-publisher routers authentication
slot number network-publisher routers router
slot number network-publisher routers router router-name authentication
slot number network-publisher routers router router-name test-mode
slot number network-publisher routers test-mode
slot number network publisher select
slot number nic
slot number nic initial
slot number nic initial directory-connection
slot number nic initial directory-eventing
Operational Commands
request network-publisher execute
request nic clear scenario-data
request nic restart agent
request nic restart resolver
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](#)[test nic resolve](#)

shared nic scenario

Syntax

```
shared nic scenario name ...
```

Hierarchy Level

```
[edit shared nic scenario]
```

Description

Configure a NIC configuration scenario to use. A configuration scenario defines the type of resolution to be performed.

Options

name name— Name of a NIC configuration scenario.

Value— Name of a configuration scenario that has been established for the NIC.

Required Privilege Level

system

Required Editing Level

Basic

shared nic scenario *name* agents

Syntax

```
shared nic scenario name agents name ...
```

Hierarchy Level

```
[edit shared nic scenario name agents]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a NIC agent in a NIC configuration scenario.

Options

name name— Name of a NIC agent in a configuration scenario.

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared nic scenario *name* agents *name* configuration consolidator

Syntax

```
shared nic scenario name agents name configuration consolidator {
    resolvers-list resolvers-list;
    roles-list roles-list;
    source-agent source-agent;
    agent-processor agent-processor;
    network-data-types network-data-types;
    publishingInterval publishingInterval;
    event-life-expectancy event-life-expectancy;
}
```

Hierarchy Level

```
[edit shared nic scenario name agents name configuration consolidator]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure properties for consolidator agents. When you use a configuration scenario, you typically change the source-agent option.

Before you change the value of this statement or the value of any of the options for this statement, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

resolvers-list resolvers-list—(Optional) Names of NIC resolvers to which this agent sends events. If you do not define a list of NIC resolvers, you must define a list of roles.

Value— List of paths to NIC resolvers; paths are relative to the static configuration object. Separate resolvers with commas.

Default— No value

Editing Level—Expert

roles-list roles-list—(Optional) Names of NIC roles to which this agent sends events. All resolvers that participate in a role receive events.

If you do not define the names of the NIC roles, you must define a list of resolvers.

Value— Names of NIC roles in the format *realmName* : *roleName* .
Use commas to separate one role from another in the list.

Default— No value
Editing Level—Expert

`source-agent` *source-agent*— Path to the agent for which this consolidator agent publishes data.

Value— Text

Example—/agents/InterfaceIdInterface

Default— No value
Editing Level—Basic

`agent-processor` *agent-processor*— Name of the Java class that the NIC agent uses to generate the data value object.

Value— Path to Java class
Default— No value
Editing Level—Expert

`network-data-types` *network-data-types*— Data types that the agent publishes.

For more information, see the documentation for the NIC resolution process.

If the agent publishes mappings, specify two data types in the format *key* , *value* . Use commas to separate entries.

Value— Data type in the format *key* or *key* , *value* , where

- *key* —Name of data key
- *value* — Name of data value

Example—IpPool, InterfaceId

Default— No value
Editing Level—Expert

`publishingInterval` *publishingInterval*—(Optional) Interval at which the NIC agent sends updates to the NIC resolvers.

Value— Number of seconds in the range 0–2147483647
Default—60
Editing Level—Expert

`event-life-expectancy event-life-expectancy`—(Optional) Length of time that data is valid after the NIC proxy receives data associated with events published by this agent.

Value— Number of seconds in the range 0–4294967295

- 0—Data does not expire
- Other values—Actual life expectancy of data

Default—0

Editing Level—Expert

Required Privilege Level

system

Required Editing Level

Basic

shared nic scenario *name* agents *name* configuration directory

Syntax

```
shared nic scenario name agents name configuration directory {
    principal principal;
    credentials credentials;
    key-attribute-processor key-attribute-processor;
    value-attribute-processor value-attribute-processor;
    mapping-attribute-processor mapping-attribute-processor;
    publishing-interval publishing-interval;
    resolvers-list resolvers-list;
    roles-list roles-list;
    search-base search-base;
    search-filter search-filter;
    search-scope (object | one-level | sub-tree);
    server-url server-url;
    directory-backup-urls directory-backup-urls;
    key-attribute-name key-attribute-name;
    value-attribute-name value-attribute-name;
    network-data-types network-data-types;
    event-life-expectancy event-life-expectancy;
    enable-directory-eventing;
    directory-connection-id directory-connection-id;
    snmp-agent;
    share-directory-connection;
    polling-interval polling-interval;
    retry-interval retry-interval;
}
```

Hierarchy Level

[edit shared nic scenario *name* agents *name* configuration directory]

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure properties for directory agents. When you use a configuration scenario provided in the SRC software, you typically change only the following options:

- search-base
- search-filter
- search-scope
- server-url

- `authentication-dn`
- `password`

`principal principal`— DN that the NIC agent uses for authentication to access the directory.

Value— *DN, base*

Example—*cn=nic,ou=Components,o=Operators,base*

Default— *cn=nic,ou=Components,o=Operators,<base>*

Editing Level—Basic

`credentials credentials`— Password with which the NIC agent accesses the directory.

Value— *password*

Default— *nic*

Editing Level—Basic

`key-attribute-processor key-attribute-processor`—(Optional) Java class that the NIC agent uses to generate the network data object named key.

The object includes a list of attributes from the directory. If no class is specified, there can be only one key attribute (in the `key.attrNames` property).

This value is ignored if a mapping processor is specified.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Path to Java class

Example—*net.juniper.smgmt.gateway.nic.agent.dir.DnAttributeProcessor*

Default— No value

Editing Level—Expert

`value-attribute-processor value-attribute-processor`—(Optional) Name of the Java class that the NIC agent uses to generate the data value object. Specify only if the agent publishes mappings.

If no class is specified, there can be only one value attribute (in the `value.attrNames` property).

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Path to Java class

Default— No value

Editing Level—Expert

`mapping-attribute-processor` *mapping-attribute-processor*—(Optional)

Name of the Java class that the NIC agent uses to process the key object and the value object, and to produce the mapping object DataPair. If no class is specified, NIC uses the key and value attribute processors.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Path to Java class

Default— No value

Editing Level—Expert

`publishing-interval` *publishing-interval*—(Optional) Interval at which the NIC agent sends updates to the NIC resolvers.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Number of seconds in the range 0–2147483647

Default— 60

Editing Level—Expert

`resolvers-list` *resolvers-list*—(Optional) Names of NIC resolvers to which this agent sends events. If you do not define a list of the NIC resolvers, you must define a list of roles.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— List of paths to NIC resolvers; paths are relative to the static configuration object. Separate resolvers with commas.

Example—`/realms/ip/B1, /realms/sharedIp/B1, /realms/login/D1`

Default— No value

Editing Level—Expert

`roles-list` *roles-list*—(Optional) Names of NIC roles to which this agent sends

events. All resolvers that participate in a role receive events. If you do not define the names of the NIC roles, you must define a list of resolvers.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Names of NIC roles in the format *realmName:roleName*. Use commas to separate one role from another in the list.

Default— No value

Editing Level—Expert

search-base search-base— DN of the location in the directory from which the agent should read information.

Value— *DN, base*

Default— No value

Editing Level—Basic

search-filter search-filter—(Optional) Directory search filter that the agent should use.

Value— LDAP search filter

Default— No value

Editing Level—Basic

search-scope (object | one-level | sub-tree)—(Optional) Location in the directory relative to the base DN from which the NIC agent can retrieve information.

Value— One of the following options:

- 0—Object; entry specified in the Search Base field only
- 1—One level; entry specified in the Search Base field and objects that are subordinate by one level
- 2—Subtree of entry specified in the Search Base field

Default— *sub-tree*

Editing Level—Basic

server-url server-url— URL that identifies the location of the primary directory server to which this NIC agent connects.

Value— Location of the directory that stores configuration information in URL string format *protocol:// host:portNumber* where:

- *protocol* —*ldap* or *ldaps*

- *host* —IP address or name of directory host
- *portNumber* —Number of TCP/IP port

Example—`ldap://127.0.0.1:389/`

Default— No value

Editing Level—Basic

`directory-backup-urls` *directory-backup-urls*—(Optional) URLs that identify the locations of backup directory servers. Backup servers are used if the primary directory server is not accessible.

Value— URLs of redundant directories separated by semicolons.

Example—`ldap://127.0.0.1:389/`

Default— No value

Editing Level—Basic

`key-attribute-name` *key-attribute-name*— Name of the directory attribute that the NIC agent uses for the network data object called key. You can define these attribute names if you use a customized key attribute processor.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Name of one or more attributes in the directory. Use commas to separate attribute names.

Example—`virtualRouterName`

Default— No value

Editing Level—Expert

`value-attribute-name` *value-attribute-name*—(Optional) Directory attribute that the NIC agent uses for the network data object called value. Specify only if the agent publishes mappings.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Name of an attribute in the directory.

Example—Saeld**Default—** No value**Editing Level—**Expert

`network-data-types network-data-types`— Names of the data types that this NIC agent publishes.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Data type in the form *key, value*. If there is more than one data type, separate entries with commas.

Example

- Agent to publish IP pools—`networkDataTypes=IpPool`
- Agent is to publish mappings between IP pools and VRs—`networkDataTypes=IpPool, Vr`

Default— No value**Editing Level—**Expert

`event-life-expectancy event-life-expectancy`—(Optional) Length of time that data is valid after the NIC proxy receives data associated with events published by this agent.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Number of seconds in the range 0–4294967295

- 0—Data does not expire
- Other values—Actual life expectancy of data

Default— 0**Editing Level—**Expert

`enable-directory-eventing`—(Optional) Specifies whether NIC polls the directory for changes.

Value—

- `true`—Enable polling.
- `false`—Disable polling

Default—true
Editing Level—Expert

`directory-connection-id` *directory-connection-id*— Name for directory connection in SNMP agent view.

Value— ID for connection manager.

Example—DIRAGENT_POOL_VR

Default— No value
Editing Level—Expert

`snmp-agent`—(Optional) Enable the SDX SNMP agent to export MIBs for this directory connection.

Editing Level—Expert

`share-directory-connection`—(Optional) Enable DES listeners of NIC agents to share a connection to the directory.

Do not change this value unless instructed to do so by Juniper Networks.

Editing Level—Expert

`polling-interval` *polling-interval*— Time interval at which the SRC component polls the directory.

Value—Integer in the range 30–2147483647
Default— 30
Editing Level—Expert

`retry-interval` *retry-interval*— Length of time that the directory monitoring system waits to initiate a directory connection after an unsuccessful attempt to connect to the directory.

Value—Integer in the range -2147483648–2147483647 s
Default— No value
Editing Level—Expert

Required Privilege Level

system

Required Editing Level

Basic

shared nic scenario *name* agents *name* configuration properties

Syntax

```
shared nic scenario name agents name configuration properties {
    resolvers-list resolvers-list;
    roles-list roles-list;
    data-sources data-sources;
    network-data-types network-data-types;
    publishing-interval publishing-interval;
    event-life-expectancy event-life-expectancy;
    reverse-values;
}
```

Hierarchy Level

```
[edit shared nic scenario name agents name configuration properties]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure properties agents. A properties agent retrieves information from one or more specified property files and makes event information based on the information in the file available to the NIC.

Although a properties agent may be used by an SRC application, typically you do not need to configure it. Before you change the value of this statement or the value of any of the options for this statement, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

resolvers-list resolvers-list—(Optional) Names of NIC resolvers to which this agent sends events. If you do not define a list of the NIC resolvers, you must define a list of roles.

Value— List of paths to NIC resolvers; paths are relative to the static configuration object. Separate resolvers with commas.

Default— No value

Editing Level—Expert

roles-list roles-list—(Optional) Names of NIC roles to which this agent sends events. All resolvers that participate in a role receive events.

If you do not define the names of the NIC roles, you must define a list of resolvers.

Value— Names of NIC roles in the format *realmName : roleName* .
 Use commas to separate one role from another in the list.
Default— No value
Editing Level—Expert

data-sources data-sources— List of URIs or filenames of property files that provides information about NIC events to the NIC system. You must provide at least one URI or filename.

At this time, the only supported format for the data source is a property file.

Value— URIs or filenames separated by commas
Default— No value
Editing Level—Basic

network-data-types network-data-types— Data types that the agent publishes.

For more information, see the documentation for the NIC resolution process.

If the agent publishes mappings, specify two data types in the format *key , value* . Use commas to separate entries.

Value— Data type in the format *key* or *key , value* , where

- *key* —Name of data key
- *value* — Name of data value

Example—IpPool, InterfaceId

Default— No value
Editing Level—Expert

publishing-interval publishing-interval—(Optional) Interval at which the NIC agent sends updates to the NIC resolvers.

Value— Number of seconds in the range 0–2147483647
Default—60
Editing Level—Expert

event-life-expectancy event-life-expectancy—(Optional) Length of time that data is valid after the NIC proxy receives data associated with events published by this agent.

Value— Number of seconds in the range 0–4294967295

- 0—Data does not expire
- Other values—Actual life expectancy of data

Default—0

Editing Level—Expert

`reverse-values`—(Optional) Specifies whether a property name is made available as a NIC key or a NIC value. If enabled, properties are published as keys.

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared nic scenario *name* agents *name* configuration sae-client

Syntax

```
shared nic scenario name agents name configuration sae-client {
    principal principal;
    credentials credentials;
    subscriber-id (user-ip-address | dn | login-name | interface-name | primary-
user-name);
    sae-connection-threads sae-connection-threads;
    sae-retry-interval sae-retry-interval;
    resolvers-list resolvers-list;
    roles-list roles-list;
    search-base search-base;
    search-filter search-filter;
    search-scope (object | one-level | sub-tree);
    server-url server-url;
    directory-backup-urls directory-backup-urls;
    key-attribute-name key-attribute-name;
    value-attribute-name value-attribute-name;
    network-data-types network-data-types;
    event-life-expectancy event-life-expectancy;
    enable-directory-eventing;
    directory-connection-id directory-connection-id;
    snmp-agent;
    share-directory-connection;
    polling-interval polling-interval;
    retry-interval retry-interval;
}
```

Hierarchy Level

```
[edit shared nic scenario name agents name configuration sae-client]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure properties for SAE client agents. When you use a configuration scenario provided in the SRC software, you typically change only the following options:

- search-base
- search-filter
- search-scope
- server-url

- `backup-servers-url`
- `principal`
- `credentials`

`principal principal`— DN that the NIC agent uses for authentication to access the directory.

Value— *DN, base*

Example—*cn=umcadmin, base*

Default— *cn=umcadmin, <base>*

Editing Level—Basic

`credentials credentials`— Password with which the NIC agent accesses the directory.

Value— *password*

Default—*admin123*

Editing Level—Basic

`subscriber-id (user-ip-address | dn | login-name | interface-name | primary-user-name)`— The SAE subscriber type. The NIC passes subscriber ID of the specified type to the SAE external interface of active SAEs to determine which SAE has a user session for the subscriber.

Value— One of the following options:

- *user-ip-address* —Subscriber's IP address
- *dn* —DN that identifies the subscriber in the directory
- *login-name* —Login name that identifies the subscriber
- *interface-name* —Name of the interface through which the subscriber traffic passes
- *primary-user-name* —User name that identifies the subscriber

Default— No value

Editing Level—Basic

`sae-connection-threads sae-connection-threads`—(Optional) Size of the thread pool for contacting SAEs during resolution. These threads are shared among all resolution requests and are spanned in parallel one thread per SAE per resolution request. You may want to set this value higher than the default if you have multiple SAEs in your network and a high resolution rate.

Value— Number of threads

Default— 5
Editing Level—Advanced

`sae-retry-interval` *sae-retry-interval*—(Optional) Min. length of time that the agent waits before it sends a resolution request to a particular SAE after an unsuccessful attempt to contact it.

Value— Retry interval in seconds
Default— 30
Editing Level—Advanced

`resolvers-list` *resolvers-list*—(Optional) Names of NIC resolvers to which this agent sends events. If you do not define a list of the NIC resolvers, you must define a list of roles.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— List of paths to NIC resolvers; paths are relative to the static configuration object. Separate resolvers with commas.

Example—/realms/ip/B1,/realms/sharedIp/B1,/realms/login/D1

Default— No value
Editing Level—Expert

`roles-list` *roles-list*—(Optional) Names of NIC roles to which this agent sends events. All resolvers that participate in a role receive events. If you do not define the names of the NIC roles, you must define a list of resolvers.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Names of NIC roles in the format *realmName:roleName*. Use commas to separate one role from another in the list.
Default— No value
Editing Level—Expert

`search-base` *search-base*— DN of the location in the directory from which the agent should read information.

Value— *DN, base*
Default— No value
Editing Level—Basic

`search-filter` *search-filter*—(Optional) Directory search filter that the agent should use.

Value— LDAP search filter

Default— No value

Editing Level—Basic

`search-scope` (`object` | `one-level` | `sub-tree`)—(Optional) Location in the directory relative to the base DN from which the NIC agent can retrieve information.

Value— One of the following options:

- 0—Object; entry specified in the Search Base field only
- 1—One level; entry specified in the Search Base field and objects that are subordinate by one level
- 2—Subtree of entry specified in the Search Base field

Default— `sub-tree`

Editing Level—Basic

`server-url` *server-url*— URL that identifies the location of the primary directory server to which this NIC agent connects.

Value— Location of the directory that stores configuration information in URL string format `protocol:// host:portNumber` where:

- *protocol* —`ldap` or `ldaps`
- *host* —IP address or name of directory host
- *portNumber* —Number of TCP/IP port

Example—`ldap://127.0.0.1:389/`

Default— No value

Editing Level—Basic

`directory-backup-urls` *directory-backup-urls*—(Optional) URLs that identify the locations of backup directory servers. Backup servers are used if the primary directory server is not accessible.

Value— URLs of redundant directories separated by semicolons.

Example—`ldap://127.0.0.1:389/`

Default— No value
Editing Level—Basic

`key-attribute-name` *key-attribute-name*— Name of the directory attribute that the NIC agent uses for the network data object called key. You can define these attribute names if you use a customized key attribute processor.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Name of one or more attributes in the directory. Use commas to separate attribute names.

Example—virtualRouterName

Default— No value
Editing Level—Expert

`value-attribute-name` *value-attribute-name*—(Optional) Directory attribute that the NIC agent uses for the network data object called value. Specify only if the agent publishes mappings.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Name of an attribute in the directory.

Example—Saeld

Default— No value
Editing Level—Expert

`network-data-types` *network-data-types*— Names of the data types that this NIC agent publishes.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Data type in the form *key, value*. If there is more than one data type, separate entries with commas.

Example

- Agent to publish IP pools—`networkDataTypes=IpPool`

- Agent is to publish mappings between IP pools and VRs—
networkDataTypes=IpPool, Vr

Default— No value

Editing Level—Expert

`event-life-expectancy` *event-life-expectancy*—(Optional) Length of time that data is valid after the NIC proxy receives data associated with events published by this agent.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Number of seconds in the range 0–4294967295

- 0—Data does not expire
- Other values—Actual life expectancy of data

Default— 0

Editing Level—Expert

`enable-directory-eventing`—(Optional) Specifies whether NIC polls the directory for changes.

Value—

- true—Enable polling.
- false—Disable polling

Default—true

Editing Level—Expert

`directory-connection-id` *directory-connection-id*— Name for directory connection in SNMP agent view.

Value— ID for connection manager.

Example—DIRAGENT_POOL_VR

Default— No value

Editing Level—Expert

`snmp-agent`—(Optional) Enable the SDX SNMP agent to export MIBs for this directory

connection.

Editing Level—Expert

`share-directory-connection`—(Optional) Enable DES listeners of NIC agents to share a connection to the directory.

Do not change this value unless instructed to do so by Juniper Networks.

Editing Level—Expert

`polling-interval` *polling-interval*— Time interval at which the SRC component polls the directory.

Value—Integer in the range 30–2147483647

Default— 30

Editing Level—Expert

`retry-interval` *retry-interval*— Length of time that the directory monitoring system waits to initiate a directory connection after an unsuccessful attempt to connect to the directory.

Value—Integer in the range -2147483648–2147483647 s

Default— No value

Editing Level—Expert

Required Privilege Level

system

Required Editing Level

Basic

shared nic scenario *name* agents *name* configuration sae-plugin

Syntax

```
shared nic scenario name agents name configuration sae-plugin {
    resolvers-list resolvers-list;
    plug-in-event-type (Interface | User);
    key-attribute-name key-attribute-name;
    key-attribute-processor key-attribute-processor;
    value-attribute-name value-attribute-name;
    value-attribute-processor value-attribute-processor;
    naming-context naming-context;
    event-filter event-filter;
    share-the-event-system;
    number-of-events number-of-events;
    network-data-types network-data-types;
    event-life-expectancy event-life-expectancy;
}
```

Hierarchy Level

```
[edit shared nic scenario name agents name configuration sae-plugin]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure properties for SAE plug-in agents. When you use a configuration scenario provided in the SRC software, you typically change only the following options:

- `event-filter`
- `number-of-events`

`resolvers-list resolvers-list`—(Optional) Names of NIC resolvers to which this agent sends events. If you do not define a list of the NIC resolvers, you must define a list of roles.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— List of paths to NIC resolvers; paths are relative to the static configuration object. Separate resolvers with commas.

Example—`/realms/dB/E1`

Default— No value
Editing Level—Expert

`plug-in-event-type` (`Interface` | `User`)—(Optional) Types of plug-in events that the agent supports.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— One of the following:

- `User`—Agent supports user-tracking plug-in events.
- `Interface`—Agent supports interface-tracking plug-in events.

Default—User
Editing Level—Expert

`key-attribute-name` *key-attribute-name*— Names of the plug-in attributes that provide information for the data key. You can define these attribute names if you use a customized key attribute processor.

The list can contain one or more plug-in attributes. If the format of the single plug-in attribute is not a string or you specify multiple plug-in attributes, the agent passes the data to the key processor to construct the data value in string format. In this case, you must specify the processor in the Key Attribute Processor field.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Name of one or more attributes in the directory. Use commas to separate attribute names.

Example—PA_USER_DN,PA_ROUTER_NAME

Default— No value
Editing Level—Expert

`key-attribute-processor` *key-attribute-processor*—(Optional) Name of the Java class that the agent uses to generate the data key object. If no class is specified, there can be only one key event attribute.

Configure a key attribute processor if the agent acquires for the key value either a single plug-in attribute that is not in string format or multiple plug-in attributes.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Path to Java class

Example—net.juniper.smgmt.gateway.nic.agent. saeplugin.
InterfaceIdProcessor

Default— No value

Editing Level—Expert

`value-attribute-name value-attribute-name`— List of plug-in attributes that provide information for the data value.

The list can contain one or more plug-in attributes. If the format of the single plug-in attribute is not a string or you specify multiple plug-in attributes, the agent passes the data to the value processor to construct the data value in string format. In this case, you must specify the processor for the value attribute processor option.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— List of comma-separated plug-in attributes.

Example—PA_USER_DN, PA_ROUTER_NAME

Default— No value

Editing Level—Expert

`value-attribute-processor value-attribute-processor`—(Optional) Name of the Java class that the agent uses to generate the data value object. If no class is specified, there can be only one value event attribute.

Configure a value attribute processor if the agent acquires for the data value either a single plug-in attribute that is not in string format or multiple plug-in attributes.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Path to Java class

Example—net.juniper.smgmt.gateway.nic.agent. saeplugin.
InterfaceProcessor

Default— No value
Editing Level—Expert

`naming-context naming-context`— CORBA naming context in which the agent publishes references.

If you configure event sharing for multiple SAE plug-in agents, this setting must be identical for all those agents.

The incoming interface is bound under the specified context with the name `saePort`. The mirror interface has the name `mirrorPort`.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— String that must match the context name in the `objectref` property for this SAE plug-in. For more information, see the documentation for the NIC resolution process.

Example—`nicstaetestDNOttawa`

This example matches the context name of the following `objectref` property:

`corbaname::10.10.10.10:900/NameService#nicstaetestDNOttawa/saePort`

In this property:

- 10.10.10.10—Address of the machine running the CORBA naming server
- 900—TCP/IP port
- `saePort`—Name of plug-in (in this case, the agent eventing system)

Default— No value
Editing Level—Expert

`event-filter event-filter`— LDAP filter that restricts the events that the agent collects.

Value— `pluginAttribute = attributeValue`

where

- `pluginAttribute` — Plug-in attribute name
- `attributeValue` — Value of filter

Example—PA_USER_TYPE=INTF

Default— No value

Editing Level—Basic

`share-the-event-system`—(Optional) Enable an agent to share the event system with other agents in the same host. If you configure event sharing for multiple SAE plug-in agents, this setting must be identical for all those agents.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Editing Level—Expert

`number-of-events` *number-of-events*—(Optional) Number of events that the SAE sends to the agent at one time during state synchronization. This value is used if state synchronization is enabled.

Value— Integer in the range 1–2147483647

Default—50

Editing Level—Basic

`network-data-types` *network-data-types*— Data types that the agent publishes.

For more information, see the documentation for the NIC resolution process.

If the agent publishes mappings, specify two data types in the format *key*, *value* . Use commas to separate entries.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Data type in the format *key* or *key* , *value* , where

- *key* —Name of data key
- *value* — Name of data value

Example—Dn, Vr

Default— No value

Editing Level—Expert

`event-life-expectancy` *event-life-expectancy*—(Optional) Length of time that

data is valid after the NIC proxy receives data associated with events published by this agent.

Before you change the value of this option, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Value— Number of seconds in the range 0–4294967295

- 0—Data does not expire
- Other values—Actual life expectancy of data

Default— 0

Editing Level—Expert

Required Privilege Level

system

Required Editing Level

Basic

shared nic scenario *name* agents *name* configuration xml

Syntax

```
shared nic scenario name agents name configuration xml {
    resolvers-list resolvers-list;
    roles-list roles-list;
    data-source data-source;
    search-base search-base;
    search-filter search-filter;
    search-scope (0 | 1 | 2);
    mapping-file mapping-file;
    root-tag-name root-tag-name;
    key-attribute-name key-attribute-name;
    key-attribute-processor key-attribute-processor;
    value-attribute-name value-attribute-name;
    value-attribute-processor value-attribute-processor;
    network-data-types network-data-types;
    publishing-interval publishing-interval;
    event-life-expectancy event-life-expectancy;
    enable-eventing;
}
```

Hierarchy Level

```
[edit shared nic scenario name agents name configuration xml]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an XML agent. An XML agent retrieves information from a specified XML document and makes information available to the NIC based on specified tags in the file. An XML agent provides information about one type of data or mappings.

Although an XML agent may be used by an SRC application, typically you do not need to configure it. Before you change the value of this statement or the value of any of the options for this statement, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

resolvers-list resolvers-list—(Optional) Names of NIC resolvers to which this agent sends events. If you do not define a list of the NIC resolvers, you must define a list of roles.

Value— List of paths to NIC resolvers; paths are relative to the static configuration object. Separate resolvers with commas.

Default— No value
Editing Level—Expert

`roles-list` *roles-list*—(Optional) Names of NIC roles to which this agent sends events. All resolvers that participate in a role receive events.

If you do not define the names of the NIC roles, you must define a list of resolvers.

Value— Names of NIC roles in the format *realmName* : *roleName* .
 Use commas to separate one role from another in the list.
Default— No value
Editing Level—Expert

`data-source` *data-source*— URI of the XML document that provides information about NIC events to the NIC system. You must provide a URI for the XML document.

At this time, the only supported schema is a file.

Value— URI
Default— No value
Editing Level—Basic

`search-base` *search-base*—(Optional) Root XML element in the specified XML document at which the agent starts to search the XML document. If you do not specify an element for the search base, the agent starts searching at the top of the file.

Value— XML element
Default— No value
Editing Level—Normal

`search-filter` *search-filter*—(Optional) Search filter that the agent uses to read entries in an XML document.

Value— Search filter syntax defined in RFC 2254— The String Representation of LDAP Search Filters (December 1997)
Default— No value
Editing Level—Normal

`search-scope` (0 | 1 | 2)—(Optional) Level at which the agent searches the XML document.

Value— Search level:

- Object—Searches the object defined by the search base entry.
- One level—Specifies objects at the same level as the object

defined by the search base entry.

- Subtree—Searches objects subordinate to the object defined by the search base entry.

Default— No value

Editing Level—Basic

`mapping-file` *mapping-file*—(Optional) Name of the property file that maps XML tag names to corresponding Java class names. Enter a value if the XML document does not conform to the SDX XML schema.

Value— Filename

Default— No value

Editing Level—Normal

`root-tag-name` *root-tag-name*—(Optional) Tag name of the root XML element in the data source. Enter a value if the XML document does not follow the SDX XML schema.

Value— Tag name

Default— No value

Editing Level—Normal

`key-attribute-name` *key-attribute-name*— List of XML attribute names to be used in constructing the key network data object for a custom processor.

Value—Text

Editing Level—Expert

`key-attribute-processor` *key-attribute-processor*—(Optional) The name of the Java class for processing the key object.

If specified, it will be used to produce the key network data object by using the list of attributes read from the directory. If no class is specified, there must be only one key LDAP attribute (in the `key.attrNames` property), and the attribute value must be in the proper format expected by the data type.

Value—Text

Editing Level—Expert

`value-attribute-name` *value-attribute-name*—(Optional) List of LDAP attribute names to be used in constructing a value for the network data object. Specified attribute names if the agent publishes mappings or if you use a custom processor.

Value— List of attribute names. Use commas to separate entries.

Editing Level—Expert

`value-attribute-processor` *value-attribute-processor*—(Optional) The name of the Java class for processing the value object.

If specified, it will be used to produce the value network data object by using the list of attributes read from the directory. If no class is specified, there must be only one value attribute (in the `value.attrNames` property), and the attribute value must be in the proper format expected by the data type.

Value—Text
Editing Level—Expert

`network-data-types` *network-data-types*— Data types that the agent publishes.

For more information, see the documentation for the NIC resolution process.

If the agent publishes mappings, specify two data types in the format *key* , *value* . Use commas to separate entries.

Value— Data type in the format *key* or *key* , *value* , where

- *key* —Name of data key
- *value* — Name of data value

Example—IpPool, InterfaceId

Default— No value
Editing Level—Expert

`publishing-interval` *publishing-interval*—(Optional) Interval at which the NIC agent sends updates to the NIC resolvers.

Value— Number of seconds in the range 0–2147483647
Default—60
Editing Level—Expert

`event-life-expectancy` *event-life-expectancy*—(Optional) Length of time that data is valid after the NIC proxy receives data associated with events published by this agent.

Value— Number of seconds in the range 0–4294967295

- 0—Data does not expire
- Other values—Actual life expectancy of data

Default—0
Editing Level—Expert

`enable-eventing`—(Optional) Enable Eventing

Default—true
Editing Level—Expert

Required Privilege Level

system

Required Editing Level

Basic

shared nic scenario *name* hosts

Syntax

```
shared nic scenario name hosts name ...
```

Hierarchy Level

```
[edit shared nic scenario name hosts]
```

Description

Configure a NIC host for a specified NIC configuration scenario.

Options

name name— Name of the NIC host.

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared nic scenario *name* hosts logger

Syntax

```
shared nic scenario name hosts logger name ...
```

Hierarchy Level

```
[edit shared nic scenario name hosts logger]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a logging component for NIC. Logging can be to a file or to the system logging utility.

Options

name name— Name of a NIC logging component.

Value—Text

Required Privilege Level

system

Required Editing Level

Normal

shared nic scenario *name* hosts logger *name* file

Syntax

```
shared nic scenario name hosts logger name file {
    filter filter;
    filename filename;
    rollover-filename rollover-filename;
    maximum-file-size maximum-file-size;
}
```

Hierarchy Level

```
[edit shared nic scenario name hosts logger name file]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure logging of messages to a file.

filter filter—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

Editing Level—Basic

filename filename— Absolute path of the filename that contains the current logs.

Note: 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.

Value— Filename

Default— No value

Editing Level—Basic

rollover-filename rollover-filename—(Optional) 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— Path of filename

Example—/opt/UMC/sae/var/log/sae.alt

Default— The default value is different for each type of component.

Editing Level—Normal

`maximum-file-size` *maximum-file-size*—(Optional) Maximum size of the log file and the rollover file.

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

Value—Integer in the range 0–2147483647 kbytes

Default— 1000000

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared nic scenario *name* hosts logger *name* syslog

Syntax

```
shared nic scenario name hosts logger name syslog {
    filter filter;
    host host;
    facility facility;
    format format;
}
```

Hierarchy Level

```
[edit shared nic scenario name hosts logger name syslog]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure logging of messages to system logging.

filter filter—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default—/error-

Editing Level—Basic

host host— IP address or name of a host that collects event messages by means of a standard system logging daemon.

Value— IP address or hostname

Default—loghost

Editing Level—Basic

facility facility—(Optional) Type of system log in accordance with the system logging protocol.

Value—Integer in the range 0–23

Default— 3

Editing Level—Advanced

format format—(Optional) MessageFormat string that specifies how the information in an event message is printed. (The strings {#} are replaced with the log information [...]).

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

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Basic

shared nic scenario *name* hosts *name* configuration

Syntax

```
shared nic scenario name hosts name configuration {
    hosted-resolvers hosted-resolvers;
    hosted-agents hosted-agents;
}
```

Hierarchy Level

```
[edit shared nic scenario name hosts name configuration]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure NIC hosts.

Options

hosted-resolvers *hosted-resolvers*— List of resolvers that should run on this host.

Value— Names of NIC resolvers which include the path of the locations of the NIC resolvers relative to the static configuration object. A forward slash (/) separates components in a path.

Example—/realms/sharedIp/A1,/realms/sharedIp/B1,/realms/sharedIp/C1,/realms/ip/A1,/realms/ip/B1,/realms/ip/C1,/realms/dn/A1,/realms/dn/B1,/realms/dn/C1,/realms/login/A1,/realms/login/B1,/realms/login/C1,/realms/login/D1

Default— No value

Editing Level—Basic

hosted-agents *hosted-agents*— List of paths to NIC agents that this host supports.

Value— Names of NIC agents that include the path of the locations of the NIC agents relative to the static configuration object. A forward slash (/) separates components in a path.

Example—/agents/VrSaeld,/agents/Router,/agents/PoolInterfaceId,/agents/

InterfaceIdInterface

Default— No value
Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared nic scenario *name* hosts *name* configuration logger

Syntax

shared nic scenario *name* hosts *name* configuration logger *name* ...

Hierarchy Level

[edit shared nic scenario *name* hosts *name* configuration logger]

Release Information

Statement introduced in SRC Release 1.0.0

Options

name *name*—

Value—Text

Required Privilege Level

system

Required Editing Level

Normal

shared nic scenario *name* hosts *name* configuration logger *name* file

Syntax

```
shared nic scenario name hosts name configuration logger name file {
    filter filter;
    filename filename;
    rollover-filename rollover-filename;
    maximum-file-size maximum-file-size;
}
```

Hierarchy Level

```
[edit shared nic scenario name hosts name configuration logger name file]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure logging of messages to a file.

filter filter—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

Editing Level—Basic

filename filename— Absolute path of the filename that contains the current logs.

Note: 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.

Value— Filename

Default— No value

Editing Level—Basic

rollover-filename rollover-filename—(Optional) 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— Path of filename

Example—/opt/UMC/sae/var/log/sae.alt

Default— The default value is different for each type of component.

Editing Level—Normal

`maximum-file-size` *maximum-file-size*—(Optional) Maximum size of the log file and the rollover file.

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

Value—Integer in the range 0–2147483647 kbytes

Default— 1000000

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared nic scenario *name* hosts *name* configuration logger *name* syslog

Syntax

```
shared nic scenario name hosts name configuration logger name syslog {
    filter filter;
    host host;
    facility facility;
    format format;
}
```

Hierarchy Level

```
[edit shared nic scenario name hosts name configuration logger name syslog]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure logging of messages to system logging.

filter filter—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default—/error-

Editing Level—Basic

host host— IP address or name of a host that collects event messages by means of a standard system logging daemon.

Value— IP address or hostname

Default—loghost

Editing Level—Basic

facility facility—(Optional) Type of system log in accordance with the system logging protocol.

Value—Integer in the range 0–23

Default— 3

Editing Level—Advanced

format format—(Optional) MessageFormat string that specifies how the information in an event message is printed. (The strings {#} are replaced with the log information [...]).

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

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Basic

shared nic scenario *name* nic-locators

Syntax

```
shared nic scenario name nic-locators name ...
```

Hierarchy Level

```
[edit shared nic scenario name nic-locators]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a NIC locator or NIC proxy, a NIC component that requests data resolution.

Options

name *name*— Name of the NIC locator.

Value—Text

Required Privilege Level

system

Required Editing Level

Normal

shared nic scenario *name* nic-locators *name* resolution

Syntax

```
shared nic scenario name nic-locators name resolution {
    resolver-name resolver-name;
    key-type key-type;
    value-type value-type;
    expect-multiple-values;
    constraints constraints;
}
```

Hierarchy Level

```
[edit shared nic scenario name nic-locators name resolution]
```

Description

Configure properties for a NIC proxy (NIC locator), the NIC component that requests information on behalf of an application.

resolver-name resolver-name— NIC resolver that the NIC proxy uses. This resolver must be the same as one that is configured on the NIC host.

Value— Path to the NIC resolver.

Example—/realms/ip/A1,/realms/dn/A1.

Default— No value

Editing Level—Basic

key-type key-type— Type of data used that the key provides for the NIC resolution. You can provide a qualifier to a data type to distinguish between different instances of a data type in a resolution scenario, or to provide information about a data type to clarify the use of that data type in a resolution.

Value— One of the following types:

- Ip —Subscriber's IP address
- Vr—Virtual router
- Interface—Name of router's interface
- InterfaceId—Identifier of an interface on the router
- Dn—LDAP distinguished name for subscriber
- LoginName—Subscriber login ID
- AnyString—Other information

To qualify data types, enter a qualifier within parentheses.

Example—LoginName(username).

Default— No value

Editing Level—Basic

value-type value-type— Type of value to be returned in the resolution. The value type varies according to the application that uses the NIC proxy.

Value— One of the following types:

- SaelId—SAE server ID
- LoginName—Subscriber login ID
- AnyString—Other information

To qualify data types, enter a qualifier within parentheses.

Example—LoginName(username).

Default— No value

Editing Level—Basic

expect-multiple-values—(Optional) Specifies whether or not the key can have multiple corresponding values.

Editing Level—Basic

constraints constraints—(Optional) Data type that a resolver uses during the resolution process. A constraint represents a condition that must or may be satisfied before the next stage of the resolution process can proceed.

Configure a constraint only if the constraint will be provided by the application in the resolution request. Typically, you do not need to configure constraints.

Value— Data types of constraints specified for the NIC resolution.

Separate data types with commas.

Default— No value

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Normal

shared nic scenario *name* realms

Syntax

```
shared nic scenario name realms name ...
```

Hierarchy Level

```
[edit shared nic scenario name realms]
```

Description

Configure a NIC realm, the NIC component that consists of a group of resolvers that perform a series of resolution tasks to provide a mapping from a specified key to a specified data type.

Typically, you use the default realm configuration for the NIC configuration scenarios in the SRC software.

Options

name name— Name of the NIC realm.

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared nic scenario *name* realms *name* configuration custom-resolver classname

Syntax

```
shared nic scenario name realms name configuration custom-resolver classname name
{
    value;
}
```

Hierarchy Level

```
[edit shared nic scenario name realms name configuration custom-resolver classname]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure an identifier to distinguish between different instances of the same data type in a resolution sequence. For the value enter the nmae of the data type.

Options

name name— Identifier to append to data type

Value—Text

value—

Value—Text
Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Advanced

shared nic scenario *name* realms *name* configuration transitions

Syntax

```
shared nic scenario name realms name configuration transitions name {
    value;
}
```

Hierarchy Level

```
[edit shared nic scenario name realms name configuration transitions]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a set of resolution sequences that map a property to a value.

Options

name name— Identifier for a resolution that represents one transition, or step, in the resolution process. Use ? to view the list of transitions for this realm, a group of resolvers that perform a series of resolution tasks to provide a mapping from a specified key to a specified data type.

Value—Text

value—

Value—Text

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Normal

shared nic scenario *name* realms *name* resolvers

Syntax

```
shared nic scenario name realms name resolvers name ...
```

Hierarchy Level

```
[edit shared nic scenario name realms name resolvers]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure NIC resolvers— the components that process NIC resolution requests.

Before you change the value of this statement or the value of any of the options for this statement, contact Juniper Networks Professional Services or Juniper Networks Customer Support.

Options

name *name*— Name of the NIC resolver.

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared nic scenario *name* realms *name* resolvers *name* configuration

Syntax

```
shared nic scenario name realms name resolvers name configuration {
    resolver-role resolver-role;
    resolvers-list resolvers-list;
    roles-list roles-list;
}
```

Hierarchy Level

```
[edit shared nic scenario name realms name resolvers name configuration]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure resolution from a NIC key to a NIC value.

Options

`resolver-role resolver-role`— Configure a transition that defines a key to value mapping.

Value—Text

Editing Level—Normal

`resolvers-list resolvers-list`—(Optional) Names of NIC resolvers to which this agent sends events. If you do not define a list of the NIC resolvers, you must define a list of roles.

Value— List of paths to NIC resolvers; paths are relative to the static configuration object. Separate resolvers with commas.

Example—/realms/ip/A1, /realms/ip/B1

Default— No value

Editing Level—Normal

`roles-list roles-list`—(Optional) Names of NIC roles to which this agent sends

events. All resolvers that participate in a role receive events.

If you do not define the names of the NIC roles, you must define a list of resolvers.

- Value**— Names of NIC roles in the format *realmName* : *roleName* .
Use commas to separate one role from another in the list.
- Default**— No value
- Editing Level**—Normal

Required Privilege Level

system

Required Editing Level

Basic

slot *number* network-publisher directory-connection

Syntax

```
slot number network-publisher directory-connection {
    url url;
    base-dn base-dn;
    principal principal;
    credentials credentials;
}
```

Hierarchy Level

```
[edit slot number network-publisher directory-connection]
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure directory connection properties that the network publisher uses to connect to the Juniper Networks database.

Options

url url—(Optional) URL that the network publisher uses to connect to the Juniper Networks database.

Value— URL

Default—`ldap://127.0.0.1:389`

Editing Level—Basic

base-dn base-dn—(Optional) Specify the distinguished name (DN) of the subtree in the Juniper Networks database that stores data collected from JUNOS routing platforms.

Value— DN

Default—`o=Network,<base>`

Editing Level—Basic

principal principal—(Optional) Specify the DN that defines the username with which the network publisher accesses the Juniper Networks database.

Value— DN

Default—cn=cli,ou=Components,o=Operators,<base>

Editing Level—Basic

`credentials credentials`—(Optional) Specify the password with which the network publisher accesses the Juniper Networks database.

Value— *password*

Default—cli

Editing Level—Basic

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

slot *number* network-publisher logger

Syntax

```
slot number network-publisher logger name ...
```

Hierarchy Level

```
[edit slot number network-publisher logger]
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure logging to a file or to a system log server.

Options

name name— Configure logging to a file or to a system log server.

Value—Text

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

slot *number* network-publisher logger *name* file

Syntax

```
slot number network-publisher logger name file {
    filter filter;
    filename filename;
    rollover-filename rollover-filename;
    maximum-file-size maximum-file-size;
}
```

Hierarchy Level

```
[edit slot number network-publisher logger name file]
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure logging to save messages in a file.

filter filter—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

Editing Level—Basic

filename filename— Absolute path of the filename that contains the current logs.

Note: 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.

Value— Filename

Default— By default, SRC components and applications write log files in the folder in which the component or application is started.

Editing Level—Basic

`rollover-filename rollover-filename`—(Optional) 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— Path of filename

Example—`/opt/UMC/sae/var/log/sae.alt`

Default— The default value is different for each type of component.

Editing Level—Normal

`maximum-file-size maximum-file-size`—(Optional) Maximum size of the log file and the rollover file.

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

Value—Integer in the range 0–2147483647 kbytes

Default— 1000000

Editing Level—Normal

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

slot *number* network-publisher logger *name* syslog

Syntax

```
slot number network-publisher logger name syslog {
    filter filter;
    host host;
    facility facility;
    format format;
}
```

Hierarchy Level

```
[edit slot number network-publisher logger name syslog]
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure logging to send messages to the system log server.

filter filter—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

Editing Level—Basic

host host— IP address or name of a host that collects event messages by means of a standard system logging daemon.

Value— IP address or hostname

Default—loghost

Editing Level—Basic

facility facility—(Optional) Type of system log in accordance with the system logging protocol.

Value—Integer in the range 0–23

Default— 3

Editing Level—Advanced

`format format`—(Optional) MessageFormat string that specifies how the information in an event message is printed. (The strings {#} are replaced with the log information [...]).

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

Editing Level—Advanced

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

slot *number* network-publisher routers

Syntax

```
slot number network-publisher routers {
    router-release-number router-release-number;
    router-script-version router-script-version;
}
```

Hierarchy Level

```
[edit slot number network-publisher routers]
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure connections between JUNOS routing platforms and the network publisher. The network publisher connects to the JUNOScript server on a JUNOS routing platform. Properties defined at this hierarchy level are applied by all the configured JUNOS routing platforms unless you specify different properties for a particular device.

`router-release-number router-release-number`—(Optional) Release number of the JUNOS software running on the JUNOS routing platforms.

Value—Text

Default—No value

Editing Level—Basic

`router-script-version router-script-version`—(Optional) Version of JUNOScript running on the JUNOS routing platforms.

Value—Text

Default—1.0

Editing Level—Expert

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

slot *number* network-publisher routers authentication

Syntax

```
slot number network-publisher routers authentication {
    login-name login-name;
    credentials credentials;
    protocol (telnet | ssh);
}
```

Hierarchy Level

```
[edit slot number network-publisher routers authentication]
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure authentication properties for the JUNOS routing platforms to which the network publisher connects. Properties defined at this hierarchy level are applied to all the configured JUNOS routing platforms unless you specify different properties for a particular device.

Options

`login-name login-name`—(Optional) Username to log in to the JUNOS software.

Value—Text

Default— No value

Editing Level—Basic

`credentials credentials`—(Optional) Password to log in to the JUNOS software.

Value— *password*

Default— No value

Editing Level—Basic

`protocol (telnet | ssh)`—(Optional) Authentication protocol that network publisher uses to access a JUNOS routing platform.

Value

- `telnet`— Use JUNOScript over a Telnet connection.
- `ssh`— (Recommended) Use JUNOScript over an SSH connection.

Default—`ssh`

Editing Level—Basic

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

slot *number* network-publisher routers router

Syntax

```
slot number network-publisher routers router router-name {
    address address;
    router-release-number router-release-number;
    router-script-version router-script-version;
}
```

Hierarchy Level

```
[edit slot number network-publisher routers router]
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure connections between a particular JUNOS routing platform and the network publisher. The network publisher connects to the JUNOScript server on a JUNOS routing platform. Properties defined at this hierarchy level take precedence over those defined at the `slot 0 network-publisher routers` hierarchy level.

Options

`router-name router-name`— Name of a specific JUNOS routing platform.

Value—Text

`address address`— IP address of a JUNOS routing platform.

Value—IP address

Editing Level—Basic

`router-release-number router-release-number`—(Optional) Release number of the JUNOS software running on the JUNOS routing platforms.

Value—Text

Default— No value

Editing Level—Basic

`router-script-version` *router-script-version*—(Optional) Version of JUNOScript running on the JUNOS routing platforms.

Value—Text

Default—1.0

Editing Level—Expert

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

slot *number* network-publisher routers router *router-name* authentication

Syntax

```
slot number network-publisher routers router router-name authentication {
    login-name login-name;
    credentials credentials;
    protocol (telnet | ssh);
}
```

Hierarchy Level

```
[edit slot number network-publisher routers router router-name authentication]
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure authentication properties for the JUNOS routing platforms to which the network publisher connects. Properties defined at this hierarchy level are applied to all the configured JUNOS routing platforms unless you specify different properties for a particular device.

Options

`login-name login-name`—(Optional) Username to log in to the JUNOS software.

Value—Text

Default— No value

Editing Level—Basic

`credentials credentials`—(Optional) Password to log in to the JUNOS software.

Value— *password*

Default— No value

Editing Level—Basic

`protocol (telnet | ssh)`—(Optional) Authentication protocol that network publisher uses to access a JUNOS routing platform.

Value

- `telnet`— Use JUNOScript over a Telnet connection.
- `ssh`— (Recommended) Use JUNOScript over an SSH connection.

Default—ssh

Editing Level—Basic

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

slot *number* network-publisher routers router *router-name* test-mode

Syntax

```
slot number network-publisher routers router router-name test-mode {
    enable-file-input;
    enable-file-output;
    input-location input-location;
    output-location output-location;
}
```

Hierarchy Level

```
[edit slot number network-publisher routers router router-name test-mode]
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure information to test the network publisher.

Use an input file to test a configuration before routes to the NIC are available or before VPNs are configured. You can also use an input file to set up a test configuration for demonstration purposes.

Use an output file to review the information that the network publisher has gathered.

Options

`enable-file-input`—(Optional) Configure the network publisher to use data in a file, rather than in the directory, when you run the network publisher.

Editing Level—Basic

`enable-file-output`—(Optional) Configure the network publisher to collect data from JUNOS routing platforms and store that information in a file, rather than in the directory.

Editing Level—Basic

`input-location input-location`—(Optional) Location in the directory where input files are located. In most cases, you do not need to change the value of this option.

Note: Input filenames should be in the format `router_name_1.xml`. where `router_name` is the hostname of the JUNOS routing platform.

Value—Text

Default—`sample/junos/rt`

Editing Level—Advanced

`output-location` *output-location*—(Optional) Location in the directory where output files are located. In most cases, you do not need to change the value of this option.

Note: Output filenames should be in the format `router_name_1.xml` where `router_name` is the hostname of the JUNOS routing platform.

Value—Text

Default—`var/junos/rt`

Editing Level—Advanced

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

slot *number* network-publisher routers test-mode

Syntax

```
slot number network-publisher routers test-mode {
    enable-file-input;
    enable-file-output;
    input-location input-location;
    output-location output-location;
}
```

Hierarchy Level

```
[edit slot number network-publisher routers test-mode]
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure information to test the network publisher.

Use an input file to test a configuration before routes to the NIC are available or before VPNs are configured. You can also use an input file to set up a test configuration for demonstration purposes.

Use an output file to review the information that the network publisher has gathered.

Options

`enable-file-input`—(Optional) Configure the network publisher to use data in a file, rather than in the directory, when you run the network publisher.

Editing Level—Basic

`enable-file-output`—(Optional) Configure the network publisher to collect data from JUNOS routing platforms and store that information in a file, rather than in the directory.

Editing Level—Basic

`input-location input-location`—(Optional) Location in the directory where input files are located. In most cases, you do not need to change the value of this option.

Note: Input filenames should be in the format `router_name_1.xml`. where `router_name` is the hostname of the JUNOS routing platform.

Value—Text

Default—`sample/junos/rt`

Editing Level—Advanced

`output-location` *output-location*—(Optional) Location in the directory where output files are located. In most cases, you do not need to change the value of this option.

Note: Output filenames should be in the format `router_name_1.xml` where `router_name` is the hostname of the JUNOS routing platform.

Value—Text

Default—`var/junos/rt`

Editing Level—Advanced

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

slot *number* network-publisher select

Syntax

```
slot number network-publisher select {
    route-table-filter route-table-filter;
    route-entry-filter route-entry-filter;
}
```

Hierarchy Level

```
[edit slot number network-publisher select]
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Specify the routing tables and the entries in the routing tables from which the network publisher collects routing information.

The network publisher can collect information from JUNOS IPv4 and IPv6 routing tables. By default, it collects information from all IPv4 routing tables, including tables for VPNs, and entries for all protocols. Based on your network configuration, consider which protocols to exclude from the configuration for network publisher.

The network publisher saves the information collected in the Juniper Networks database.

Options

`route-table-filter route-table-filter`—(Optional) Routing table from which the network publisher collects information.

Value— Routing table name

Editing Level—Advanced

`route-entry-filter route-entry-filter`—(Optional) Routing table entry from which the network publisher collects information.

Value— Name of routing table entry

Editing Level—Advanced

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

slot *number* nic

Syntax

```
slot number nic {
    base-dn base-dn;
    java-runtime-environment java-runtime-environment;
    java-heap-size java-heap-size;
    java-new-size java-new-size;
    java-garbage-collection-options java-garbage-collection-options;
    java-64bit;
    snmp-agent;
    hostname hostname;
    scenario-name scenario-name;
    runtime-group runtime-group;
}
```

Hierarchy Level

```
[edit slot number nic]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure NIC local operating properties.

Options

base-dn base-dn— Distinguished name (DN) of the root directory for the NIC.

Value— DN

Default— o=umc

Editing Level—Basic

java-runtime-environment java-runtime-environment— Path to the Java runtime environment (JRE).

Value— Directory path

Default— ../jre/bin/java

Editing Level—Expert

`java-heap-size` *java-heap-size*— Maximum Java heap (memory) size available to the JRE. The value is inserted when the JRE starts. See documentation for the Java runtime environment for valid values.

Value— Number of megabytes in the format `###m`

Default— 128m

Editing Level—Advanced

`java-new-size` *java-new-size*— Maximum Java new generation heap (memory) size available to the JRE when the NIC starts.

Value— Integer in the range 0–<Java heap size>. Specify the value in bytes or add m for megabytes, k for kilobytes, or g for gigabytes. For example, 64m. See the documentation for the JRE for valid values.

Default— 24m

Editing Level—Advanced

`java-garbage-collection-options` *java-garbage-collection-options*— Garbage collection functionality of the Java Virtual Machine.

Value— Options defined by the JVM

Default— `-Xbatch -XX:CMSInitiatingOccupancyFraction=80 -XX: +UseParNewGC -XX:SurvivorRatio=1 -XX:InitialTenuringThreshold=8 -XX: MaxTenuringThreshold=10 -XX:+UseCMSCompactAtFullCollection -XX: CMSFullGCsBeforeCompaction=0 -XX:+CMSClassUnloadingEnabled -XX: +CMSParallelRemarkEnabled -XX:+UseConcMarkSweepGC`

Editing Level—Advanced

`java-64bit`—(Optional) Start the java virtual machine in 64 bit mode

Editing Level—Basic

`snmp-agent`—(Optional) Enable the NIC to communicate with the SNMP agent. By using SNMP, you can view SNMP counters with an SNMP browser.

Default—false

Editing Level—Basic

`hostname` *hostname*— Name of the NIC host. In most cases, use the name DemoHost because this is the hostname used in most NIC configuration scenarios. Refer to the documentation to verify that the NIC configuration scenario you use includes DemoHost as the NIC host.

Value— NIC hostname

Default— DemoHost for most configuration scenarios

Editing Level—Basic

`scenario-name` *scenario-name*— Name of the NIC scenario under the static configuration namespace.

Value— NIC hostname
Default— DemoHost for most configuration scenarios
Editing Level—Basic

`runtime-group` *runtime-group*—(Optional) Group to which this NIC host belongs for use with NIC replication. NIC hosts that run in the same system must specify the same runtime group. If you do not specify a value for the group, the NIC host creates the configuration.

Value— Group name
Default— No value
Editing Level—Basic

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

slot *number* nic initial

Syntax

```
slot number nic initial {
    static-dn static-dn;
    dynamic-dn dynamic-dn;
}
```

Hierarchy Level

```
[edit slot number nic initial]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure initial properties for the NIC.

Options

static-dn static-dn—(Optional) Location of administrator-defined configuration data in the directory.

Value—Text

Default—`l=NIC,ou=staticConfiguration,ou=Configuration,o=Management,o=umc`

Editing Level—Expert

dynamic-dn dynamic-dn—(Optional) Location of programmatically defined configuration data in the directory.

Value—DN

Default—`ou=dynamicConfiguration, ou=Configuration, o=Management, <base>`

Editing Level—Expert

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

slot *number* nic initial directory-connection

Syntax

```
slot number nic initial directory-connection {
    url url;
    backup-urls [backup-urls...];
    principal principal;
    credentials credentials;
    protocol (ldaps);
    timeout timeout;
    check-interval check-interval;
    blacklist;
    snmp-agent;
}
```

Hierarchy Level

```
[edit slot number nic initial directory-connection]
```

Description

Configure properties for the directory connection.

Options

`url url`—(Optional) URL that identifies the location of the primary directory server.

Value— URL

Default—ldap://127.0.0.1:389

Editing Level—Basic

`backup-urls [backup-urls...]`—(Optional) URLs that identify the locations of backup directory servers. Backup servers are used if the primary directory server is not accessible.

Value— List of URLs

Editing Level—Basic

`principal principal`— DN that the SRC component uses for authentication to access the directory.

Value— DN.

When you specify the DN, you can use <base> to indicate the base DN.

Editing Level—Basic

`credentials credentials`— Password with which the SRC component accesses the directory.

Value— Password

Editing Level—Basic

`protocol (ldaps)`—(Optional) Security protocol used to connect to the directory. If you do not configure a security protocol, plain socket is used.

Value

- `ldaps`— LDAPS which uses SSL.

Editing Level—Expert

`timeout timeout`—(Optional) Maximum amount of time during which the directory must respond to a connection request.

Value— Integer in the range 1–2147483647 s

Default—10

Editing Level—Expert

`check-interval check-interval`—(Optional) Time interval at which the directory monitoring system verifies its connection to the directory. If the directory connection fails after this interval, the directory monitoring system initiates a connection to another directory.

Value— Integer in the range 15–2147483647 s

Default—60

Editing Level—Expert

`blacklist`—(Optional) Specifies whether the directory monitoring system prevents connection to a directory if the directory fails to respond during 10 polling intervals.

Default—false

Editing Level—Basic

`snmp-agent`—(Optional) Specifies whether the SDX SNMP agent exports MIBs for this directory connection.

Default—false
Editing Level—Expert

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

slot *number* nic initial directory-eventing

Syntax

```
slot number nic initial directory-eventing {
    eventing;
    signature-dn signature-dn;
    polling-interval polling-interval;
    event-base-dn event-base-dn;
    dispatcher-pool-size dispatcher-pool-size;
}
```

Hierarchy Level

```
[edit slot number nic initial directory-eventing]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Change configuration for directory eventing properties. In most cases, you can use the default configuration for these properties.

Options

eventing—(Optional) Enable an SRC component to poll the directory for changes.

Default—true

Editing Level—Normal

signature-dn *signature-dn*—(Optional) DN of the directory entry that specifies the usedDirectory attribute for the SRC CLI. The usedDirectory attribute identifies the vendor of the directory server.

Value— DN

Default—o=umc

Editing Level—Expert

polling-interval *polling-interval*—(Optional) Interval at which an SRC component polls the directory to check for directory changes.

Value—Integer in the range 15–2147483647 s

Default—30
Editing Level—Normal

`event-base-dn` *event-base-dn*—(Optional)

DN of an entry superior to the data associated with an SRC component in the directory.

If you are storing non-SRC data in the directory, and that data changes frequently whereas the SRC data does not, you may need to adjust the default value to improve performance. For optimal performance, set the value to the DN of an entry superior to both the SRC data and the changing non-SRC data.

Value—DN
Default—o=UMC
Editing Level—Expert

`dispatcher-pool-size` *dispatcher-pool-size*—(Optional) Number of directory change notifications that can be sent simultaneously to the SRC component.

Value—Integer in the range 0–2147483647
Default—1
Editing Level—Expert

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

request network-publisher execute

Syntax

```
request network-publisher execute
```

Release Information

Command introduced in SRC Release 3.0.0

Description

Run the network publisher. The network publisher is a NIC component that connects to JUNOS routing platforms and collects information, such as information about system interfaces and VPNs, from IPv4 and IPv6 routing tables. After collecting the information, the network publisher stores this information in the Juniper Networks database for access by the NIC.

Before you run this command, make sure that the network publisher is configured and that the NIC is enabled.

Required Privilege Level

maintenance

request nic clear scenario-data

Syntax

```
request nic clear scenario-data
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Remove data stored for NIC scenarios. Run this command when you switch from one NIC configuration scenario to another.

Before you run this command, disable NIC by using the `disable component nic` command.

Required Privilege Level

maintenance

request nic restart agent

Syntax

```
request nic restart agent <name name>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Restart NIC agents. If you do not specify an agent name, the software restarts all NIC agents.

You can restart a NIC agent to have the agent read all data in the directory again. Restart a NIC agent if the agent is not synchronized with the directory, or if you switch from one directory to another.

Options

name name—(Optional) Name of the NIC agent to restart.

Value— Agent name. The agents included with the SRC software are:

- AcctIdIp
- DnVr
- Enterprise
- IpAcctId
- IpLoginName
- IpVr
- LoginNameVr
- PoolVr
- UserNameVr
- VrSaeld

Default— No value

Required Privilege Level

maintenance

request nic restart resolver

Syntax

```
request nic restart resolver <name name>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Restart NIC resolvers. If you do not specify a resolver name, the software restarts all resolvers.

In rare instances, such as when you are troubleshooting a NIC configuration, you may want to restart a NIC resolver.

Options

`name name`—(Optional) Name of the NIC resolver to restart.

Value— Resolver name

Default— No value

Required Privilege Level

maintenance

show nic data

Syntax

```
show nic data <maximum-results maximum-results>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display data that NIC uses during resolutions.

Options

maximum-results maximum-results—(Optional) Number of results to be displayed.

Value—Integer in the range 1–2147483647

Default—25

Required Privilege Level

view

show nic data agent

Syntax

```
show nic data agent <name name>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display the data that NIC agents store.

Options

name name—(Optional) Name of a NIC agent.

Value— Agent name. The agents included with the SRC software are:

- AcctIdIp
- DnVr
- Enterprise
- IpAcctId
- IpLoginName
- IpVr
- LoginNameVr
- PoolVr
- UserNameVr
- VrSaeld

Default— No value

Required Privilege Level

view

show nic data resolver

Syntax

```
show nic data resolver <name name>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display data that NIC resolvers store.

Options

name name—(Optional) Name of a NIC resolver.

Value— Resolver name

Default— No value

Required Privilege Level

view

show nic statistics

Syntax

```
show nic statistics
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display statistics for NIC.

Required Privilege Level

view

show nic statistics agent

Syntax

```
show nic statistics agent <name name>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display statistics for NIC agents. If you do not specify an agent name, the command displays statistics for all NIC agents.

Options

name name—(Optional) Name of a NIC agent.

Value— Agent name. The agents included with the SRC software are:

- AcctIdIp
- DnVr
- Enterprise
- IpAcctId
- IpLoginName
- IpVr
- LoginNameVr
- PoolVr
- UserNameVr
- VrSaeld

Default— No value

Required Privilege Level

view

show nic statistics host

Syntax

```
show nic statistics host
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display statistics for the NIC host.

Required Privilege Level

view

show nic statistics process

Syntax

```
show nic statistics process
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display process information for the NIC.

Required Privilege Level

view

show nic statistics resolver

Syntax

```
show nic statistics resolver <name name>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display statistics for NIC resolvers. If you do not specify a resolver name, the software displays statistics for all resolvers.

Options

name name—(Optional) Name of a NIC resolver.

Value— Resolver name

Default— No value

Required Privilege Level

view

test nic resolve

Syntax

```
test nic resolve locator locator key key <constraints constraints>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Issue a resolution request to the NIC host to test NIC resolution for a specified key.

Options

locator locator— Name of a NIC locator. A NIC locator can resolve the value of one or more NIC keys. Each NIC configuration scenario provides configuration for an associated NIC locator.

Value— Name of a NIC locator

key key— The NIC key to resolve.

Value— NIC key in the form `NIC data type:key string`; for example:
`Ip:10.10.10.10`.

constraints constraints—(Optional) List of values for NIC constraints. Constraints are NIC data types that a resolver uses when it executes a role (also referred to as a transition) in the resolution process. A role resolves a NIC key to a NIC value.

Value— Constraints in the form: `[constraint (,constraint)*]`. For each constraint, use the format: `NIC data type:key string`. For example,
`[AnyString(conn):false, domain:virneo]`

Required Privilege Level

maintenance

Session State Registrar (SSR)

The following table summarizes the SRC command-line interface (SRC CLI) for supporting the Session State Registrar (SSR). Configuration statements and operational commands are listed in alphabetical order.

Session State Registrar
Configuration Statements
shared_database_cluster
shared_database_cluster (primary) attribute-associations_entity
shared_database_cluster (primary) attribute-associations_entity_name_field
shared_database_cluster (primary) nodes
shared_database_cluster (primary) nodes_node
shared_database_cluster (primary) nodes_node_address_client-node
shared_database_cluster (primary) schema
shared_database_cluster (primary) schema_entity
shared_database_cluster (primary) schema_entity (subscriber-sessions) field
Operational Commands
request_database_create_database
request_database_delete_database
request_database_delete_subscriber-sessions_all
request_database_delete_subscriber-sessions_by-address
request_database_enter
show_database_mode
show_database_running-configuration
show_database_status
show_database_subscriber-sessions
show_database_subscriber-sessions_by-address
show_database_subscriber-sessions_by-indexed-field

[show_database_subscriber-sessions_count](#)

shared database cluster

Syntax

```
shared database cluster (primary) ...
```

Hierarchy Level

```
[edit shared database cluster]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the name of the database cluster.

Options

Name of an SSR database cluster. Only one cluster (primary) is supported.

Value

- `primary`— Name of database cluster. Only one cluster is supported. The name is fixed to primary.

Default—primary

Required Privilege Level

system

Required Editing Level

Basic

shared database cluster (primary) attribute-associations entity

Syntax

```
shared database cluster (primary) attribute-associations entity name ...
```

Hierarchy Level

```
[edit shared database cluster (primary) attribute-associations entity]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the name of the SSR database entity to which the attribute association is to be made. The only database entity that is configurable is the subscriber sessions table.

Options

name name— Name of the database entity to which the attribute association is to be made.
The only database entity supported is the subscriber sessions table.

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared database cluster (primary) attribute-associations entity *name* field

Syntax

```
shared database cluster (primary) attribute-associations entity name field name {
    sae-plugin-attribute sae-plugin-attribute;
}
```

Hierarchy Level

```
[edit shared database cluster (primary) attribute-associations entity name field]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the name of the field (attribute) in the subscriber sessions table. SSR client components such as the SAE, NIC, DSA and SIC, need to read and write information to the subscriber sessions table. They do this using SAE plugin attributes. You need to specify how these attributes are translated to subscriber sessions table attributes by defining the mapping between the two attributes. You need to define the mapping between the field in the subscriber sessions table and the SAE plugin attribute.

Options

name name— Name of the field (attribute) in the subscriber sessions table you want mapped to the SAE plugin attribute.

Value—Text

sae-plugin-attribute sae-plugin-attribute—(Optional) Name of an SAE plugin attribute you want mapped to the subscriber sessions table field (attribute).

Value—Text

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared database cluster (primary) nodes

Syntax

```
shared database cluster (primary) nodes {
    geometry (all-in-one | two-data-node | four-data-node);
}
```

Hierarchy Level

```
[edit shared database cluster (primary) nodes]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Define the SSR database cluster topology. The topology of all SSR clusters begins with four C Series Controllers. Two C Series Controllers configured as client nodes, each hosting a management server and SSR client components, and two C Series Controllers each hosting a data node. The cluster topology may be expanded to include up to twenty-four client nodes and a maximum of four data nodes.

All data nodes must have equal processor power, memory space, and available bandwidth because they are tightly coupled and share data. If the overall throughput of the data nodes varies from node to node, performance degrades. Therefore, all data nodes must be of the same C Series Controller model, either all C2000 or all C4000.

Options

`geometry (all-in-one | two-data-node | four-data-node)`— Database geometry type attribute.

Value

- `all-in-one`— Database cluster is a single C Series Controller acting as an entire cluster. If this value is selected, a single machine runs all node types (one data node and one client node hosting a management server). This configuration does not meet redundancy requirements and supports limited entries only and should only be used for demonstration purposes.

This option requires the node type to be configured as a data-client-node.

- `two-data-node`— Database cluster contains two data nodes. This is the minimum number of data nodes supported in a cluster.

- `four-data-node`— Database cluster contains four data nodes.
This is the maximum number of data nodes allowed in a cluster.

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared database cluster (primary) nodes node

Syntax

```
shared database cluster (primary) nodes node address {
    platform (C2000 | C4000);
    type (data-node | client-node | data-client-node);
}
```

Hierarchy Level

```
[edit shared database cluster (primary) nodes node]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the node properties and platform type (C Series Controller model) hosting the node. The node configuration is a list of all nodes in the cluster. Each entry in the list declares either a data node or a client node. For client nodes, an optional keyword specifies that a management server is enabled on the node.

The database cluster contains a node collection. Each node is identified its IP address. The type of node can be either data-node, client-node or data-client-node, which can only be used in all-in-one geometry. If the node type is set to client-node or data-client-node, a client-node object appears under the node for setting the client node related configurations. You can configure up to four data nodes and a maximum of twenty-four client nodes.

Options

`address address`— IP address of the node.

Value—IP address

`platform (C2000 | C4000)`— Platform type (model) of C Series Controller hosting the node.

Value

- C2000— Platform hosting node is a C2000.
- C4000— Platform hosting node is a C4000.

Editing Level—Basic

`type (data-node | client-node | data-client-node)`— Type of database cluster node.

Value

- `data-node`— Node is a data node. Data nodes are always configured in pairs and your cluster can contain either two or four data nodes. All data nodes must be of the same C Series Controller model, either all C2000 or all C4000.
- `client-node`— Node is a client node. Up to twenty-four client nodes can be configured. Client nodes can optionally host a management server.
- `data-client-node`— Node is a data-client-node. For demonstration purposes only. Configures the C Series Controller to host all node types (one data node, one client node and one management server). This setting is only used when the cluster geometry is set to all-in-one.

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared database cluster (primary) nodes node *address* client-node

Syntax

```
shared database cluster (primary) nodes node address client-node {
    management-server;
}
```

Hierarchy Level

```
[edit shared database cluster (primary) nodes node address client-node]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the client node to host a management server.

Options

management-server—(Optional) Client node is hosting a management server. The optimum number of management servers for the cluster is two (for redundancy), each running on a separate client node.

Default—false

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared database cluster (primary) schema

Syntax

```
shared database cluster (primary) schema {  
}
```

Hierarchy Level

```
[edit shared database cluster (primary) schema]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the SSR database schema. The SSR database schema includes multiple tables for storing subscriber identity information for session and service activation requests.

Required Privilege Level

system

Required Editing Level

Advanced

shared database cluster (primary) schema entity

Syntax

```
shared database cluster (primary) schema entity (subscriber-sessions) ...
```

Hierarchy Level

```
[edit shared database cluster (primary) schema entity]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Specify the entity in the SSR database schema you want to configure.

Options

Value

- `subscriber-sessions`— Name of the database entity you want to configure. The subscriber sessions table is the only configurable entity. The format of subscriber identity information stored for each session is managed by the subscriber sessions table.

Required Privilege Level

system

Required Editing Level

Advanced

shared database cluster (primary) schema entity (subscriber-sessions) field

Syntax

```
shared database cluster (primary) schema entity (subscriber-sessions) field name {
    type (int | string | binary);
    size size;
    require-value;
    indexed;
    default default;
    variable-length;
}
```

Hierarchy Level

```
[edit shared database cluster (primary) schema entity (subscriber-sessions) field]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Add a field to the subscriber sessions table. The subscriber sessions table controls the format of subscriber identity information stored for each session in the database. Configure the name and properties of the field.

The primary keys of the subscriber sessions table are the UserIpAddress and VpnID fields. The UserIpAddress field stores the subscribers IP address in binary format. The default schema uses 4 bytes, which is sufficient for IPv4 addresses. You can modify the length of the UserIpAddress field to 16 if you are using IPv6 addresses. The VpnID field stores the address realm where the user IP address is unique. For non-VPN sessions, the VpnID must be set to its default value, which is an empty string.

The subscriber sessions table is configurable with some restrictions. You can add new columns, remove existing columns, or modify column length, type or index. You cannot remove the UserIpAddress, VpnID, SessionStartTime or SessionState columns, however you can modify the length of the UserIpAddress and VpnID fields.

Options

name name— Name of field in subscriber sessions table to be added or modified.

Value—Text

type (int | string | binary)— Database field type

Value

- `int`— Signed integer data
- `string`— String data
- `binary`— Raw binary data

Editing Level—Advanced

`size size`— Database field storage size. For integer data type, the size can only be 1, 2, 3, 4 and 8.

Value—Integer in the range 1–65535
Editing Level—Advanced

`require-value`—(Optional) Value required for the database field. NULL is not allowed.

Default—false
Editing Level—Advanced

`indexed`—(Optional) If true, the field will be indexed.

Default—false
Editing Level—Advanced

`default default`—(Optional) Database field default value

Value—Text
Editing Level—Basic

`variable-length`—(Optional) Database field is variable-length

Default—false
Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Advanced

request database create database

Syntax

```
request database create database
```

Release Information

Command introduced in SRC Release 4.0.0

Description

Generate SSR database schema using the current configuration then create the SSR database and its tables. All SSR cluster components must have been enabled prior to creating the database. This command can only be executed when database is in maintenance mode.

Required Privilege Level

maintenance

request database delete database

Syntax

```
request database delete database
```

Release Information

Command introduced in SRC Release 4.0.0

Description

Destroys the SSR database and all its contents. This command should only be executed during a maintenance window. This command can only be executed when database is in maintenance mode.

Required Privilege Level

maintenance

request database delete subscriber-sessions all

Syntax

```
request database delete subscriber-sessions all
```

Release Information

Command introduced in SRC Release 4.0.0

Description

Delete all subscriber sessions in SSR database.

Required Privilege Level

maintenance

request database delete subscriber-sessions by-address

Syntax

```
request database delete subscriber-sessions by-address start-address start-  
address <end-address end-address> <vpn-id vpn-id>
```

Release Information

Command introduced in SRC Release 4.0.0

Description

Delete subscriber session IP address.

Options

start-address start-address— Start address of an IP range. If end address not specified, delete only the session with this address.

Value—Text

end-address end-address—(Optional) End address of an IP range. If not specified, delete only the session with the start address.

Value—Text

vpn-id vpn-id—(Optional) VPN ID that the sessions belong to. If not specified, delete sessions from public network and any VPN. To delete sessions from public network only, use single quotes (") as the VPN ID.

Value—Text

Required Privilege Level

maintenance

request database enter

Syntax

```
request database enter < (maintenance-mode | production-mode) >
```

Release Information

Command introduced in SRC Release 4.0.0

Description

Change SSR database running mode. This command can only be executed on a management node.

Options

(Optional) SSR database running mode.

Value

- `maintenance-mode`— Place SSR database in maintenance mode.
- `production-mode`— Place SSR database in production mode.

Required Privilege Level

maintenance

show database mode

Syntax

```
show database mode
```

Release Information

Command introduced in SRC Release 4.0.0

Description

Display the current mode of the SSR database.

Required Privilege Level

view

show database running-configuration

Syntax

```
show database running-configuration
```

Release Information

Command introduced in SRC Release 4.0.0

Description

Display the SSR database running configuration. When SSR database is in production mode, displays configuration running on SSR database. When SSR database is placed in maintenance mode, the running configuration is discarded and the SSR database running configuration is the configuration entered in CLI. This command can only be executed on management node.

Required Privilege Level

view

show database status

Syntax

```
show database status
```

Release Information

Command introduced in SRC Release 4.0.0

Description

Display the status of all nodes in the SSR cluster.

Required Privilege Level

view

show database subscriber-sessions

Syntax

```
show database subscriber-sessions <maximum-result maximum-result>
```

Release Information

Command introduced in SRC Release 4.0.0

Description

Display subscriber sessions in SSR database.

Options

`maximum-result maximum-result`—(Optional) Enter maximum number of subscriber sessions to display. Default is limited to 25 results

Value—Integer in the range -2147483648–2147483647

Default—25

Required Privilege Level

view

show database subscriber-sessions by-address

Syntax

```
show database subscriber-sessions by-address start-address start-address <end-  
address end-address> <vpn-id vpn-id>
```

Release Information

Command introduced in SRC Release 4.0.0

Description

Show subscriber sessions in SSR database by IP address.

Options

start-address start-address— Start address of an IP range. If end address is not specified, displays only session with this address.

Value—Text

end-address end-address—(Optional) End address of an IP range. If not specified, displays only session with the start address.

Value—Text

vpn-id vpn-id—(Optional) VPN ID that the subscriber sessions belong to. If not specified, display sessions from public network and any VPN. To display sessions from public network, use single quotes (") as the VPN ID.

Value—Text

Required Privilege Level

view

show database subscriber-sessions by-indexed-field

Syntax

```
show database subscriber-sessions by-indexed-field name name value value
```

Release Information

Command introduced in SRC Release 4.0.0

Description

Display subscriber sessions and associated service sessions stored in the SSR database by a specified indexed field in the subscriber sessions table. For string-type field, wildcard * can be used in value.

Options

name name— Name of indexed field in subscriber sessions table.

Value—Text

value value— Value of indexed field in subscriber sessions table.

Value—Text

Required Privilege Level

view

show database subscriber-sessions count

Syntax

```
show database subscriber-sessions count
```

Release Information

Command introduced in SRC Release 4.0.0

Description

Display the total number of subscriber sessions currently in SSR database.

Required Privilege Level

view

Subscriber Information Collector (SIC)

The following table summarizes the SRC command-line interface (SRC CLI) for the subscriber information collector (SIC). Configuration statements and operational commands are listed in alphabetical order.

SIC
Configuration Commands and Statements
load_radius_dictionary
shared_sic_group
shared_sic_group_identifier_accounting-method
shared_sic_group_identifier_accounting-method_accounting-method-name_database
shared_sic_group_identifier_accounting-method_accounting-method-name_database_plugin-attribute
shared_sic_group_identifier_accounting-method_accounting-method-name_proxy_radius
shared_sic_group_identifier_dictionary
shared_sic_group_identifier_dictionary_id_attribute
shared_sic_group_identifier_dictionary_id_attribute_id_radius
shared_sic_group_identifier_dictionary_id_attribute_id_radius_constant
shared_sic_group_identifier_editing
shared_sic_group_identifier_editing_editing-rule_default
shared_sic_group_identifier_editing_editing-rule_source_literal
shared_sic_group_identifier_editing_editing-rule_source_literal_identifier_condition_realm
shared_sic_group_identifier_editing_editing-rule_source_literal_identifier_condition_realm_does-not-equal
shared_sic_group_identifier_editing_editing-rule_source_literal_identifier_condition_realm_equals
shared_sic_group_identifier_editing_editing-rule_source_literal_identifier_condition_realm_has-prefix
shared_sic_group_identifier_editing_editing-rule_source_literal_identifier_condition_realm_has-suffix
shared_sic_group_identifier_editing_editing-rule_source_literal_identifier_condition_realm_range
shared_sic_group_identifier_editing_editing-rule_source_literal_identifier_condition_request
shared_sic_group_identifier_editing_editing-rule_source_literal_identifier_condition_request_attribute

[shared sic group identifier editing editing-rule source literal identifier condition request attribute attribute-name does-not-equal](#)

[shared sic group identifier editing editing-rule source literal identifier condition request attribute attribute-name equals](#)

[shared sic group identifier editing editing-rule source literal identifier condition request attribute attribute-name has-prefix](#)

[shared sic group identifier editing editing-rule source literal identifier condition request attribute attribute-name has-suffix](#)

[shared sic group identifier editing editing-rule source literal identifier condition request attribute attribute-name range](#)

[shared sic group identifier editing editing-rule source literal identifier condition user-identity](#)

[shared sic group identifier editing editing-rule source literal identifier condition user-identity does-not-equal](#)

[shared sic group identifier editing editing-rule source literal identifier condition user-identity equals](#)

[shared sic group identifier editing editing-rule source literal identifier condition user-identity has-prefix](#)

[shared sic group identifier editing editing-rule source literal identifier condition user-identity has-suffix](#)

[shared sic group identifier editing editing-rule source literal identifier condition user-identity range](#)

[shared sic group identifier editing editing-rule source request-attribute](#)

[shared sic group identifier editing editing-rule source request-attribute identifier condition realm](#)

[shared sic group identifier editing editing-rule source request-attribute identifier condition realm does-not-equal](#)

[shared sic group identifier editing editing-rule source request-attribute identifier condition realm equals](#)

[shared sic group identifier editing editing-rule source request-attribute identifier condition realm has-prefix](#)

[shared sic group identifier editing editing-rule source request-attribute identifier condition realm has-suffix](#)

[shared sic group identifier editing editing-rule source request-attribute identifier condition realm range](#)

[shared sic group identifier editing editing-rule source request-attribute identifier condition request](#)

[shared sic group identifier editing editing-rule source request-attribute identifier condition request attribute](#)

[shared sic group identifier editing editing-rule source request-attribute identifier condition request attribute attribute-name does-not-equal](#)

[shared_sic_group_identifier_editing_editing-rule_source_request-attribute_identifier_condition_request_attribute_attribute-name_equals](#)

[shared_sic_group_identifier_editing_editing-rule_source_request-attribute_identifier_condition_request_attribute_attribute-name_has-prefix](#)

[shared_sic_group_identifier_editing_editing-rule_source_request-attribute_identifier_condition_request_attribute_attribute-name_has-suffix](#)

[shared_sic_group_identifier_editing_editing-rule_source_request-attribute_identifier_condition_request_attribute_attribute-name_range](#)

[shared_sic_group_identifier_editing_editing-rule_source_request-attribute_identifier_condition_user-identity](#)

[shared_sic_group_identifier_editing_editing-rule_source_request-attribute_identifier_condition_user-identity_does-not-equal](#)

[shared_sic_group_identifier_editing_editing-rule_source_request-attribute_identifier_condition_user-identity_equals](#)

[shared_sic_group_identifier_editing_editing-rule_source_request-attribute_identifier_condition_user-identity_has-prefix](#)

[shared_sic_group_identifier_editing_editing-rule_source_request-attribute_identifier_condition_user-identity_has-suffix](#)

[shared_sic_group_identifier_editing_editing-rule_source_request-attribute_identifier_condition_user-identity_range](#)

[shared_sic_group_identifier_editing_editing-rule_source_variable](#)

[shared_sic_group_identifier_editing_editing-rule_source_variable_identifier_condition_realm](#)

[shared_sic_group_identifier_editing_editing-rule_source_variable_identifier_condition_realm_does-not-equal](#)

[shared_sic_group_identifier_editing_editing-rule_source_variable_identifier_condition_realm_equals](#)

[shared_sic_group_identifier_editing_editing-rule_source_variable_identifier_condition_realm_has-prefix](#)

[shared_sic_group_identifier_editing_editing-rule_source_variable_identifier_condition_realm_has-suffix](#)

[shared_sic_group_identifier_editing_editing-rule_source_variable_identifier_condition_realm_range](#)

[shared_sic_group_identifier_editing_editing-rule_source_variable_identifier_condition_request](#)

[shared_sic_group_identifier_editing_editing-rule_source_variable_identifier_condition_request_attribute](#)

[shared_sic_group_identifier_editing_editing-rule_source_variable_identifier_condition_request_attribute_attribute-name_does-not-equal](#)

[shared_sic_group_identifier_editing_editing-rule_source_variable_identifier_condition_request_attribute_attribute-name_equals](#)

<u>shared_sic_group_identifier_editing_editing-rule_source_variable_identifier_condition_request_attribute_attribute-name_has-prefix</u>
<u>shared_sic_group_identifier_editing_editing-rule_source_variable_identifier_condition_request_attribute_attribute-name_has-suffix</u>
<u>shared_sic_group_identifier_editing_editing-rule_source_variable_identifier_condition_request_attribute_attribute-name_range</u>
<u>shared_sic_group_identifier_editing_editing-rule_source_variable_identifier_condition_user-identity</u>
<u>shared_sic_group_identifier_editing_editing-rule_source_variable_identifier_condition_user-identity_does-not-equal</u>
<u>shared_sic_group_identifier_editing_editing-rule_source_variable_identifier_condition_user-identity_equals</u>
<u>shared_sic_group_identifier_editing_editing-rule_source_variable_identifier_condition_user-identity_has-prefix</u>
<u>shared_sic_group_identifier_editing_editing-rule_source_variable_identifier_condition_user-identity_has-suffix</u>
<u>shared_sic_group_identifier_editing_editing-rule_source_variable_identifier_condition_user-identity_range</u>
<u>shared_sic_group_identifier_editing_editing-rule_target</u>
<u>shared_sic_group_identifier_local-realm</u>
<u>shared_sic_group_identifier_model</u>
<u>shared_sic_group_identifier_radius_accounting-listener_limit</u>
<u>shared_sic_group_identifier_radius_accounting-listener_transport</u>
<u>shared_sic_group_identifier_radius_accounting-listener_transport_id</u>
<u>shared_sic_group_identifier_radius_network-element</u>
<u>shared_sic_group_identifier_radius_network-element_id_downstream failover-mode</u>
<u>shared_sic_group_identifier_radius_network-element_id_downstream model</u>
<u>shared_sic_group_identifier_radius_network-element_id_downstream_accounting-target</u>
<u>shared_sic_group_identifier_radius_network-element_id_downstream_accounting-target_name</u>
<u>shared_sic_group_identifier_radius_network-element_id_downstream_failover-policy</u>
<u>shared_sic_group_identifier_radius_network-element_id_downstream_failover-policy_fast-fail</u>
<u>shared_sic_group_identifier_radius_network-element_id_downstream_failover-policy_retry</u>

<u>shared_sic_group_identifier_radius_network-element_id_proxy</u>
<u>shared_sic_group_identifier_radius_network-element_id_proxy default-route-for-all-realms</u>
<u>shared_sic_group_identifier_radius_network-element_id_proxy_realm</u>
<u>shared_sic_group_identifier_radius_network-element_id_upstream</u>
<u>shared_sic_group_identifier_radius_network-element_id_upstream_accounting-client</u>
<u>shared_sic_group_identifier_radius_outbound-transport</u>
<u>shared_sic_group_identifier_radius_outbound-transport transport-name</u>
<u>shared_sic_group_identifier_server</u>
<u>shared_sic_group_identifier_server_identifier_accounting-route</u>
<u>shared_sic_group_identifier_server_identifier_accounting-route_id_condition_realm</u>
<u>shared_sic_group_identifier_server_identifier_accounting-route_id_condition_realm_does-not-equal</u>
<u>shared_sic_group_identifier_server_identifier_accounting-route_id_condition_realm_equals</u>
<u>shared_sic_group_identifier_server_identifier_accounting-route_id_condition_realm_has-prefix</u>
<u>shared_sic_group_identifier_server_identifier_accounting-route_id_condition_realm_has-suffix</u>
<u>shared_sic_group_identifier_server_identifier_accounting-route_id_condition_realm_range</u>
<u>shared_sic_group_identifier_server_identifier_accounting-route_id_condition_request</u>
<u>shared_sic_group_identifier_server_identifier_accounting-route_id_condition_request_attribute</u>
<u>shared_sic_group_identifier_server_identifier_accounting-route_id_condition_request_attribute_attribute-name_does-not-equal</u>
<u>shared_sic_group_identifier_server_identifier_accounting-route_id_condition_request_attribute_attribute-name_equals</u>
<u>shared_sic_group_identifier_server_identifier_accounting-route_id_condition_request_attribute_attribute-name_has-prefix</u>
<u>shared_sic_group_identifier_server_identifier_accounting-route_id_condition_request_attribute_attribute-name_has-suffix</u>
<u>shared_sic_group_identifier_server_identifier_accounting-route_id_condition_request_attribute_attribute-name_range</u>
<u>shared_sic_group_identifier_server_identifier_accounting-route_id_condition_user-identity</u>
<u>shared_sic_group_identifier_server_identifier_accounting-route_id_condition_user-identity_does-not-equal</u>

shared_sic_group_identifier_server_identifier_accounting-route_id_condition_user-identity_equals
shared_sic_group_identifier_server_identifier_accounting-route_id_condition_user-identity_has-prefix
shared_sic_group_identifier_server_identifier_accounting-route_id_condition_user-identity_has-suffix
shared_sic_group_identifier_server_identifier_accounting-route_id_condition_user-identity_range
shared_sic_group_identifier_server_identifier_accounting-route_id_editing
shared_sic_group_identifier_server_identifier_accounting-route_id_target
shared_sic_group_identifier_server_identifier_logger
shared_sic_group_identifier_server_identifier_logger_id_file
shared_sic_group_identifier_server_identifier_logger_id_group
shared_sic_group_identifier_server_identifier_outbound-transport
shared_sic_group_identifier_server_identifier_outbound-transport_transport-name
shared_sic_group_identifier_server_identifier_transport
shared_sic_group_identifier_server_identifier_transport_transport-name
shared_sic_group_identifier_snmp_event
shared_sic_group_identifier_transaction-manager
slot_number_sic_initial_directory-connection
slot_number_sic_server
Operational Commands
show_sic_statistics_radius_client_accounting
show_sic_statistics_radius_host_accounting
show_sic_statistics_radius_target_accounting
show_sic_statistics_route_accounting

load radius dictionary

Syntax

```
load radius dictionary dictionary-name <merge-option (merge | replace) >
```

Release Information

Command introduced in SRC Release 4.0.0

Description

Load a dictionary into the configuration. This command is valid only when entered relative to a particular group in the configuration hierarchy.

Options

dictionary-name— Name of the predefined dictionary. If a dictionary with the same name already exists, you can specify a merge option; otherwise, the configuration is not modified.

Value—Text

merge-option (merge | replace) —(Optional) Merge method for existing dictionaries. If a dictionary with the same name already exists and you do not specify a merge option, then the configuration is not modified.

Value

- *merge*— Merge the specified dictionary with the configured dictionary.
- *replace*— Remove and replace the configured dictionary with the specified dictionary.

Required Privilege Level

No specific privilege required.

shared sic group

Syntax

```
shared sic group identifier ...
```

Hierarchy Level

```
[edit shared sic group]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the shared SIC group properties. The SIC shared group configuration contains the configuration used by a group of servers. Each SIC server must belong to a group. The SIC group configuration contains the configuration properties for accounting methods, dictionaries, editing rules, and RADIUS options for the group. The identifier associated with the group is the name of the shared configuration. If you want a specific server to use a shared group configuration, you create a correlation between the server instance and the shared group configuration. Specify the name of the server you want to use the shared group configuration by using the `shared sic group identifier server` statement. The identifier associated with the server must match the name that you specified with the `slot number sic server` statement.

In addition, certain configuration options applicable to the individual server instances belonging to the group are also stored in the shared group configuration under the individual server name. These include the accounting route rules, the event logging configuration, and the inbound and outbound RADIUS transport configuration specific to the server instance.

Options

`identifier identifier`— Name of a shared SIC configuration.

Value— Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* accounting-method

Syntax

```
shared sic group identifier accounting-method accounting-method-name ...
```

Hierarchy Level

```
[edit shared sic group identifier accounting-method]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the type of accounting method used by the SIC group. An accounting method is an accounting target that is used for routing accounting requests. The types of accounting methods available for the SIC include storing accounting events in the session state registrar (SSR) database or proxy RADIUS, which forwards accounting events to a downstream authentication, authorization, and accounting (AAA) server. The proxy function must be assigned to the downstream network element.

Options

accounting-method-name *accounting-method-name*— Name of the accounting method. An accounting method is a named accounting target that can then be assigned to an accounting route.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* accounting-method *accounting-method-name* database

Syntax

```
shared sic group identifier accounting-method accounting-method-name database {  
}
```

Hierarchy Level

```
[edit shared sic group identifier accounting-method accounting-method-name database]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Use the SSR database as the accounting method. Accounting records will be stored in the SSR database. When you use the SSR database as the accounting method, you must also define the mapping between the SIC request attribute, variable, or literal, and the SAE plug-in attribute. The SAE plug-in attributes must also be mapped to the columns in the subscriber sessions table in the SSR database.

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* accounting-method *accounting-method-name* database plug-in-attribute

Syntax

```
shared sic group identifier accounting-method accounting-method-name database plug-in-attribute id {
    request-attribute request-attribute;
    variable variable;
    literal literal;
}
```

Hierarchy Level

```
[edit shared sic group identifier accounting-method accounting-method-name database plug-in-attribute]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the mapping between SIC variables or RADIUS attributes and the SAE plug-in attributes. When you use the SSR database as the accounting method, you must also define the mapping between SIC request attributes, variables, or literals, and the SAE plug-in attributes. The SAE plug-in attributes must also be mapped to the columns in the subscriber sessions table in the SSR database. This mapping must be configured to store accounting events in the SSR database. This mapping is combined with the mapping defined between SSR subscriber sessions table fields (columns) and SAE plug-in attributes. In addition, SIC uses internal variables to store intermediate results of transaction processing, such as request editing results. A variable from an editing rule can be used in the mapping to store the value of the internal variable (the result of the editing process) in the subscriber sessions table field.

Options

id id— Name of the SAE plug-in attribute to be mapped to the SIC request attribute, variable, or literal.

Value—Text

request-attribute request-attribute—(Optional) Name of the RADIUS request attribute to be mapped to the SAE plug-in attribute.

Value—Text

Editing Level—Basic

`variable variable`—(Optional) Name of transactional variable to be mapped to the SAE plug-in attribute.

Value—Text
Editing Level—Basic

`literal literal`—(Optional) Name of literal to be mapped to the SAE plug-in attribute.

Value—Text
Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* accounting-method *accounting-method-name* proxy radius

Syntax

```
shared sic group identifier accounting-method accounting-method-name proxy radius
{
    network-element network-element;
}
```

Hierarchy Level

```
[edit shared sic group identifier accounting-method accounting-method-name proxy radius]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Use a downstream RADIUS network element (AAA server) as the accounting target. The network element must be configured as a proxy server.

Options

network-element network-element— Name of a configured downstream RADIUS network element to which you want to forward (proxy) accounting requests. The network element must be configured as a RADIUS proxy server.

Value—Text
Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* dictionary

Syntax

```
shared sic group identifier dictionary id ...
```

Hierarchy Level

```
[edit shared sic group identifier dictionary]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure a dictionary used by the SIC group. The dictionary is a collection of related RADIUS attributes.

Options

id id— Name of the dictionary. Each dictionary must have a unique name.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* dictionary *id* attribute

Syntax

```
shared sic group identifier dictionary id attribute id ...
```

Hierarchy Level

```
[edit shared sic group identifier dictionary id attribute]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the name of the attribute you want to include in the dictionary.

Options

id id— Name of the attribute you want to define in the dictionary. Each attribute must have a unique name.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* dictionary *id* attribute *id* radius

Syntax

```
shared sic group identifier dictionary id attribute id radius {
    type type;
    format (one-byte-integer | integer | eight-byte-integer | string | ipv4-
address | ipv6-address | time | octets);
    vendor-id vendor-id;
    encrypt;
    salt-encrypt;
    tagged;
    sensitive;
}
```

Hierarchy Level

```
[edit shared sic group identifier dictionary id attribute id radius]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the properties of the RADIUS attribute you want included in the dictionary.

Options

type type— Type of RADIUS attribute specified as an integer value.

Value—Integer in the range 0–255

Editing Level—Basic

format (one-byte-integer | integer | eight-byte-integer | string | ipv4-address | ipv6-address | time | octets)— Format of the RADIUS attribute.

Value

- *one-byte-integer*— Attribute value is an 8 bit unsigned integer
- *integer*— Attribute value is a 32 bit unsigned integer
- *eight-byte-integer*— Attribute value is a 64 bit unsigned integer

- `string`— Attribute value is a string
- `ipv4-address`— Attribute value is an IPv4 address
- `ipv6-address`— Attribute value is an IPv6 address
- `time`— Attribute value is a 32 bit unsigned value, with the most significant octet appearing first. The value is equal to the number of seconds since 00:00:00 UTC, January 1, 1970
- `octets`— Attribute value consists of raw bytes

Editing Level—Basic

`vendor-id` *vendor-id*—(Optional) Attribute is vendor-specific, and this is the vendor ID.

Value—Integer in the range 0–2147483647

Editing Level—Basic

`encrypt`—(Optional) Attribute should be encrypted without a salt.

Default— false

Editing Level—Basic

`salt-encrypt`—(Optional) Attribute should be encrypted with a salt.

Default— false

Editing Level—Basic

`tagged`—(Optional) RADIUS attribute is tagged.

Default— false

Editing Level—Basic

`sensitive`—(Optional) RADIUS attribute carries sensitive data, so its value will not be logged.

Default— false

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* dictionary *id* attribute *id* radius constant

Syntax

```
shared sic group identifier dictionary id attribute id radius constant constant-  
name {  
    constant-value;  
}
```

Hierarchy Level

```
[edit shared sic group identifier dictionary id attribute id radius constant]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Define a constant you want to associate with the data contained in the RADIUS attribute. You must define a unique name and a value for the constant.

Options

constant-name *constant-name*— Name of the constant. Each constant must have a unique name.

Value—Text

constant-value—(Optional) Value mapped to the constant name.

Value—Integer in the range -2147483648–2147483647

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing

Syntax

```
shared sic group identifier editing editing-rule {  
    mode (replace | append);  
}
```

Hierarchy Level

```
[edit shared sic group identifier editing]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure editing rules. Editing rules allow you to modify values of RADIUS attributes or transaction variables based on an optional condition. Before the SIC sends the request to the specified accounting target, the request can optionally be edited based on the editing rules associated with the selected accounting routing rule. Editing rules are similar to accounting routing rules in that the request is examined for a matching condition and if one is found, the request is edited and then sent to the accounting target.

Editing rules provide power and flexibility to adapt request and response processing in different conditions to provide a standardized result. An example is the extraction of VPN-ID from a RADIUS request, which may be specified differently in incoming RADIUS requests depending on the device and the use case.

In addition to editing RADIUS attributes, the SIC can edit transactional variables. Editing rules can define new transactional variables in addition to certain built-in variables, such as the result of username parsing, NAS client lookup, and so on. Transactional variables are also referenced in the columns of the subscriber sessions table in the SSR database, which allows you to store the results of request processing and editing in the subscriber sessions table. There is a limit on the number of transactional variables; the default value is 255. Changing the limit requires restarting the SIC.

You configure editing rules by defining the source and its associated match conditions, the editing conditions applied to the source value, and the target in which to place the edited result. First the request is examined for the specified source (RValue) based on match conditions. The value of the source is read and then edited based on the defined editing rule. The result is then placed in the defined target. The edited request sent to the accounting target includes both the original source and the new target value.

Each editing rule is a simple assignment of a source (RValue) and a target (LValue). In any assignment the target can be either a transactional variable, a RADIUS attribute in the request, or a RADIUS attribute in the response.

The source can be either a literal, a transactional variable, or a RADIUS attribute in the request.

The match conditions that you can test for in the source include whether a specific realm, user identity, or request attribute is present, not present, equals, does not equal, has a certain suffix, has a certain prefix, or is within a specific range.

If a match condition is found in the source, you can append or replace the value of the source and put it in the target. Additionally, if the source is a request attribute, you can remove the prefix, remove the suffix, or remove the attribute before or after the @, and place the result in the target. Wildcards are supported for the remove before and remove after options.

Options

`editing-rule` *editing-rule*— Name of the editing rule.

Value—Text

`mode` (`replace` | `append`)—(Optional) Target (LValue) control mode. This setting controls how the target (LValue) is assigned. If a match condition is found on the source, you can append or replace the value of the source and put it in the target.

Value

- `replace`— Target (LValue) is replaced with new value from editing process
- `append`— Current target (LValue) value is concatenated with the new target value from the editing process

Default—`replace`

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* default

Syntax

```
shared sic group identifier editing editing-rule default {
    literal literal;
    request-attribute request-attribute;
    variable variable;
}
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule default]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the default RValue to use when no source is selected during the editing process. This default value is used only if none of the defined editing rule conditions are matched.

Options

literal literal—(Optional) String literal used by default when no source is selected during the editing process.

Value—Text
Editing Level—Basic

request-attribute request-attribute—(Optional) RADIUS request attribute used by default when no source is selected during the editing process.

Value—Text
Editing Level—Basic

variable variable—(Optional) Transactional variable used by default when no source is selected during the editing process.

Value—Text
Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source literal

Syntax

shared sic group *identifier* editing *editing-rule* source literal *identifier* ...

Hierarchy Level

[edit shared sic group *identifier* editing *editing-rule* source literal]

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure a string literal as the source of the editing rule.

Options

identifier identifier— String literal in editing rule.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source literal *identifier* condition realm

Syntax

```
shared sic group identifier editing editing-  
rule source literal identifier condition realm {  
    (present | not-present);  
}
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-  
rule source literal identifier condition realm]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure a realm match condition. If the condition is matched in the request, the route is selected.

Check for the presence of this value in the request.

Value

- `present`— Value must be present in request
- `not-present`— Value must not be present in request

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source literal *identifier* condition realm does-not-equal

Syntax

```
shared sic group identifier editing editing-rule source literal identifier condition realm does-not-equal value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source literal identifier condition realm does-not-equal]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must not match this value exactly.

Options

`value value`— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source literal *identifier* condition realm equals

Syntax

```
shared sic group identifier editing editing-  
rule source literal identifier condition realm equals value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-  
rule source literal identifier condition realm equals]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must match this value exactly.

Options

value *value*— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source literal *identifier* condition realm has-prefix

Syntax

```
shared sic group identifier editing editing-rule source literal identifier condition realm has-prefix value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source literal identifier condition realm has-prefix]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must have a prefix that matches this value exactly.

Options

`value value`— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source literal *identifier* condition realm has-suffix

Syntax

```
shared sic group identifier editing editing-rule source literal identifier condition realm has-suffix value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source literal identifier condition realm has-suffix]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must have a suffix that matches this value exactly.

Options

value *value*— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source literal *identifier* condition realm range

Syntax

```
shared sic group identifier editing editing-  
rule source literal identifier condition realm range {  
    low low;  
    high high;  
}
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-  
rule source literal identifier condition realm range]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the range of the match condition. Checked value in the realm must be within this range.

Options

low low—(Optional) Low range in text format.

Value—Text
Editing Level—Basic

high high—(Optional) High range in text format.

Value—Text
Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source literal *identifier* condition request

Syntax

```
shared sic group identifier editing editing-  
rule source literal identifier condition request {  
}
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-  
rule source literal identifier condition request]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the name of the request attribute in the match condition, and specify the presence option of the condition.

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source literal *identifier* condition request attribute

Syntax

```
shared sic group identifier editing editing-  
rule source literal identifier condition request attribute attribute-name {  
    (present | not-present);  
}
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-  
rule source literal identifier condition request attribute]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the request attribute match condition. If the request attribute condition is matched in the request, the route is selected.

Options

attribute-name attribute-name— Name of the request attribute.

Value—Text

Check for the presence of this value in the request.

Value

- *present*— Value must be present in request
- *not-present*— Value must not be present in request

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source literal *identifier* condition request attribute *attribute-name* does-not-equal

Syntax

```
shared sic group identifier editing editing-rule source literal identifier condition request attribute attribute-name does-not-equal value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source literal identifier condition request attribute attribute-name does-not-equal]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must not match this value exactly.

Options

`value value`— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source literal *identifier* condition request attribute *attribute-name* equals

Syntax

```
shared sic group identifier editing editing-rule source literal identifier condition request attribute attribute-name equals value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source literal identifier condition request attribute attribute-name equals]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must match this value exactly.

Options

value value— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source literal *identifier* condition request attribute *attribute-name* has-prefix

Syntax

```
shared sic group identifier editing editing-rule source literal identifier condition request attribute attribute-name has-prefix value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source literal identifier condition request attribute attribute-name has-prefix]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must have a prefix that matches this value exactly.

Options

value value— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source literal *identifier* condition request attribute *attribute-name* has-suffix

Syntax

```
shared sic group identifier editing editing-rule source literal identifier condition request attribute attribute-name has-suffix value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source literal identifier condition request attribute attribute-name has-suffix]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must have a suffix that matches this value exactly.

Options

value value— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source literal *identifier* condition request attribute *attribute-name* range

Syntax

```
shared sic group identifier editing editing-  
rule source literal identifier condition request attribute attribute-name range {  
    low low;  
    high high;  
}
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-  
rule source literal identifier condition request attribute attribute-name range]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the range of the match condition. Checked value in the attribute must be within this range.

Options

low low— Low range in text format.

Value—Text
Editing Level—Basic

high high— High range in text format.

Value—Text
Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source literal *identifier* condition user-identity

Syntax

```
shared sic group identifier editing editing-  
rule source literal identifier condition user-identity {  
    (present | not-present);  
}
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-  
rule source literal identifier condition user-identity]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure a user identity match condition. If the user identity condition is matched in the request, the route is selected. Possible match conditions are present, not present, does not equal, equals, has prefix, has suffix, or range.

Check for the presence of this value in the request.

Value

- `present`— Value must be present in request
- `not-present`— Value must not be present in request

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source literal *identifier* condition user-identity does-not-equal

Syntax

```
shared sic group identifier editing editing-rule source literal identifier condition user-identity does-not-equal value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source literal identifier condition user-identity does-not-equal]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must not match this value exactly.

Options

`value value`— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source literal *identifier* condition user-identity equals

Syntax

```
shared sic group identifier editing editing-rule source literal identifier condition user-identity equals value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source literal identifier condition user-identity equals]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must match this value exactly.

Options

value *value*— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source literal *identifier* condition user-identity has-prefix

Syntax

```
shared sic group identifier editing editing-rule source literal identifier condition user-identity has-prefix value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source literal identifier condition user-identity has-prefix]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must have a prefix that matches this value exactly.

Options

value *value*— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source literal *identifier* condition user-identity has-suffix

Syntax

```
shared sic group identifier editing editing-rule source literal identifier condition user-identity has-suffix value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source literal identifier condition user-identity has-suffix]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must have a suffix that matches this value exactly.

Options

value *value*— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source literal *identifier* condition user-identity range

Syntax

```
shared sic group identifier editing editing-  
rule source literal identifier condition user-identity range {  
    low low;  
    high high;  
}
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-  
rule source literal identifier condition user-identity range]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the range of the match condition. Checked value in the user identity must be within this range.

Options

low low—(Optional) Low range in text format.

Value—Text
Editing Level—Basic

high high—(Optional) High range in text format.

Value—Text
Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source request-attribute

Syntax

```
shared sic group identifier editing editing-rule source request-
attribute identifier {
    remove-prefix remove-prefix;
    remove-suffix remove-suffix;
    remove-before remove-before;
    remove-after remove-after;
}
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source request-attribute]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure a RADIUS attribute from the request to be the source of the editing rule. In addition, specify whether you want to remove the prefix, remove the suffix, or remove the attribute before or after the @ in the request.

Options

identifier identifier— RADIUS attribute from request to be used as the source in the editing rule.

Value—Text

remove-prefix remove-prefix—(Optional) Remove the specified prefix from the request.

Value—Text

Editing Level—Basic

remove-suffix remove-suffix—(Optional) Remove the specified suffix from the request.

Value—Text

Editing Level—Basic

`remove-before` *remove-before*—(Optional) Remove everything before the specified prefix from the request.

Value—Text
Editing Level—Basic

`remove-after` *remove-after*—(Optional) Remove everything after the specified suffix from the request.

Value—Text
Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source request-attribute *identifier* condition realm

Syntax

```
shared sic group identifier editing editing-rule source request-
attribute identifier condition realm {
    (present | not-present);
}
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source request-
attribute identifier condition realm]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure a realm match condition. If the condition is matched in the request, the route is selected.

Check for the presence of this value in the request.

Value

- `present`— Value must be present in request
- `not-present`— Value must not be present in request

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source request-attribute *identifier* condition realm does-not-equal

Syntax

```
shared sic group identifier editing editing-rule source request-attribute identifier condition realm does-not-equal value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source request-attribute identifier condition realm does-not-equal]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must not match this value exactly.

Options

value *value*— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source request-attribute *identifier* condition realm equals

Syntax

```
shared sic group identifier editing editing-rule source request-attribute identifier condition realm equals value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source request-attribute identifier condition realm equals]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must match this value exactly.

Options

value *value*— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source request-attribute *identifier* condition realm has-prefix

Syntax

```
shared sic group identifier editing editing-rule source request-
attribute identifier condition realm has-prefix value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source request-
attribute identifier condition realm has-prefix]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must have a prefix that matches this value exactly.

Options

value *value*— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source request-attribute *identifier* condition realm has-suffix

Syntax

```
shared sic group identifier editing editing-rule source request-attribute identifier condition realm has-suffix value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source request-attribute identifier condition realm has-suffix]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must have a suffix that matches this value exactly.

Options

value *value*— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source request-attribute *identifier* condition realm range

Syntax

```
shared sic group identifier editing editing-rule source request-
attribute identifier condition realm range {
    low low;
    high high;
}
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source request-
attribute identifier condition realm range]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the range of the match condition. Checked value in the realm must be within this range.

Options

low low—(Optional) Low range in text format.

Value—Text
Editing Level—Basic

high high—(Optional) High range in text format.

Value—Text
Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source request-attribute *identifier* condition request

Syntax

```
shared sic group identifier editing editing-rule source request-  
attribute identifier condition request {  
}
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source request-  
attribute identifier condition request]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the name of the request attribute in the match condition, and specify the presence option of the condition.

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source request-attribute *identifier* condition request attribute

Syntax

```
shared sic group identifier editing editing-rule source request-
attribute identifier condition request attribute attribute-name {
    (present | not-present);
}
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source request-
attribute identifier condition request attribute]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the request attribute match condition. If the request attribute condition is matched in the request, the route is selected.

Options

attribute-name attribute-name— Name of the request attribute.

Value—Text

Check for the presence of this value in the request.

Value

- *present*— Value must be present in request
- *not-present*— Value must not be present in request

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source request-attribute *identifier* condition request attribute *attribute-name* does-not-equal

Syntax

```
shared sic group identifier editing editing-rule source request-
attribute identifier condition request attribute attribute-name does-not-
equal value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source request-
attribute identifier condition request attribute attribute-name does-not-equal]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must not match this value exactly.

Options

value value— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source request-attribute *identifier* condition request attribute *attribute-name* equals

Syntax

```
shared sic group identifier editing editing-rule source request-
attribute identifier condition request attribute attribute-name equals value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source request-
attribute identifier condition request attribute attribute-name equals]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must match this value exactly.

Options

value *value*— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source request-attribute *identifier* condition request attribute *attribute-name* has-prefix

Syntax

```
shared sic group identifier editing editing-rule source request-
attribute identifier condition request attribute attribute-name has-
prefix value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source request-
attribute identifier condition request attribute attribute-name has-prefix]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must have a prefix that matches this value exactly.

Options

value value— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source request-attribute *identifier* condition request attribute *attribute-name* has-suffix

Syntax

```
shared sic group identifier editing editing-rule source request-
attribute identifier condition request attribute attribute-name has-
suffix value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source request-
attribute identifier condition request attribute attribute-name has-suffix]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must have a suffix that matches this value exactly.

Options

value value— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source request-attribute *identifier* condition request attribute *attribute-name* range

Syntax

```
shared sic group identifier editing editing-rule source request-
attribute identifier condition request attribute attribute-name range {
    low low;
    high high;
}
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source request-
attribute identifier condition request attribute attribute-name range]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the range of the match condition. Checked value in the attribute must be within this range.

Options

low low— Low range in text format.

Value—Text
Editing Level—Basic

high high— High range in text format.

Value—Text
Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source request-attribute *identifier* condition user-identity

Syntax

```
shared sic group identifier editing editing-rule source request-
attribute identifier condition user-identity {
    (present | not-present);
}
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source request-
attribute identifier condition user-identity]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure a user identity match condition. If the user identity condition is matched in the request, the route is selected. Possible match conditions are present, not present, does not equal, equals, has prefix, has suffix, or range.

Check for the presence of this value in the request.

Value

- `present`— Value must be present in request
- `not-present`— Value must not be present in request

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source request-attribute *identifier* condition user-identity does-not-equal

Syntax

```
shared sic group identifier editing editing-rule source request-
attribute identifier condition user-identity does-not-equal value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source request-
attribute identifier condition user-identity does-not-equal]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must not match this value exactly.

Options

value *value*— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source request-attribute *identifier* condition user-identity equals

Syntax

```
shared sic group identifier editing editing-rule source request-  
attribute identifier condition user-identity equals value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source request-  
attribute identifier condition user-identity equals]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must match this value exactly.

Options

value *value*— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source request-attribute *identifier* condition user-identity has-prefix

Syntax

```
shared sic group identifier editing editing-rule source request-
attribute identifier condition user-identity has-prefix value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source request-
attribute identifier condition user-identity has-prefix]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must have a prefix that matches this value exactly.

Options

value *value*— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source request-attribute *identifier* condition user-identity has-suffix

Syntax

```
shared sic group identifier editing editing-rule source request-attribute identifier condition user-identity has-suffix value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source request-attribute identifier condition user-identity has-suffix]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must have a suffix that matches this value exactly.

Options

value *value*— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source request-attribute *identifier* condition user-identity range

Syntax

```
shared sic group identifier editing editing-rule source request-
attribute identifier condition user-identity range {
    low low;
    high high;
}
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source request-
attribute identifier condition user-identity range]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the range of the match condition. Checked value in the user identity must be within this range.

Options

low low—(Optional) Low range in text format.

Value—Text
Editing Level—Basic

high high—(Optional) High range in text format.

Value—Text
Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source variable

Syntax

```
shared sic group identifier editing editing-rule source variable identifier ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source variable]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure a transactional variable as the source of the editing rule.

Options

identifier identifier— Transactional variable used as source of editing rule.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source variable *identifier* condition realm

Syntax

```
shared sic group identifier editing editing-  
rule source variable identifier condition realm {  
    (present | not-present);  
}
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-  
rule source variable identifier condition realm]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure a realm match condition. If the condition is matched in the request, the route is selected.

Check for the presence of this value in the request.

Value

- `present`— Value must be present in request
- `not-present`— Value must not be present in request

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source variable *identifier* condition realm does-not-equal

Syntax

```
shared sic group identifier editing editing-rule source variable identifier condition realm does-not-equal value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source variable identifier condition realm does-not-equal]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must not match this value exactly.

Options

value *value*— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source variable *identifier* condition realm equals

Syntax

```
shared sic group identifier editing editing-  
rule source variable identifier condition realm equals value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-  
rule source variable identifier condition realm equals]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must match this value exactly.

Options

value value— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source variable *identifier* condition realm has-prefix

Syntax

```
shared sic group identifier editing editing-  
rule source variable identifier condition realm has-prefix value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-  
rule source variable identifier condition realm has-prefix]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must have a prefix that matches this value exactly.

Options

`value value`— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source variable *identifier* condition realm has-suffix

Syntax

```
shared sic group identifier editing editing-rule source variable identifier condition realm has-suffix value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source variable identifier condition realm has-suffix]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must have a suffix that matches this value exactly.

Options

value value— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source variable *identifier* condition realm range

Syntax

```
shared sic group identifier editing editing-  
rule source variable identifier condition realm range {  
    low low;  
    high high;  
}
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-  
rule source variable identifier condition realm range]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the range of the match condition. Checked value in the realm must be within this range.

Options

low low—(Optional) Low range in text format.

Value—Text
Editing Level—Basic

high high—(Optional) High range in text format.

Value—Text
Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source variable *identifier* condition request

Syntax

```
shared sic group identifier editing editing-  
rule source variable identifier condition request {  
}
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-  
rule source variable identifier condition request]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the name of the request attribute in the match condition, and specify the presence option of the condition.

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source variable *identifier* condition request attribute

Syntax

```
shared sic group identifier editing editing-rule source variable identifier condition request attribute attribute-name {
    (present | not-present);
}
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source variable identifier condition request attribute]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the request attribute match condition. If the request attribute condition is matched in the request, the route is selected.

Options

attribute-name attribute-name— Name of the request attribute.

Value—Text

Check for the presence of this value in the request.

Value

- *present*— Value must be present in request
- *not-present*— Value must not be present in request

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source variable *identifier* condition request attribute *attribute-name* does-not-equal

Syntax

```
shared sic group identifier editing editing-rule source variable identifier condition request attribute attribute-name does-not-equal value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source variable identifier condition request attribute attribute-name does-not-equal]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must not match this value exactly.

Options

value value— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source variable *identifier* condition request attribute *attribute-name* equals

Syntax

```
shared sic group identifier editing editing-rule source variable identifier condition request attribute attribute-name equals value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source variable identifier condition request attribute attribute-name equals]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must match this value exactly.

Options

value *value*— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source variable *identifier* condition request attribute *attribute-name* has-prefix

Syntax

```
shared sic group identifier editing editing-rule source variable identifier condition request attribute attribute-name has-prefix value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source variable identifier condition request attribute attribute-name has-prefix]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must have a prefix that matches this value exactly.

Options

value value— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source variable *identifier* condition request attribute *attribute-name* has-suffix

Syntax

```
shared sic group identifier editing editing-rule source variable identifier condition request attribute attribute-name has-suffix value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source variable identifier condition request attribute attribute-name has-suffix]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must have a suffix that matches this value exactly.

Options

value value— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source variable *identifier* condition request attribute *attribute-name* range

Syntax

```
shared sic group identifier editing editing-
rule source variable identifier condition request attribute attribute-name range {
    low low;
    high high;
}
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-
rule source variable identifier condition request attribute attribute-name range]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the range of the match condition. Checked value in the attribute must be within this range.

Options

low low— Low range in text format.

Value—Text
Editing Level—Basic

high high— High range in text format.

Value—Text
Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source variable *identifier* condition user-identity

Syntax

```
shared sic group identifier editing editing-rule source variable identifier condition user-identity {
    (present | not-present);
}
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source variable identifier condition user-identity]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure a user identity match condition. If the user identity condition is matched in the request, the route is selected. Possible match conditions are present, not present, does not equal, equals, has prefix, has suffix, or range.

Check for the presence of this value in the request.

Value

- `present`— Value must be present in request
- `not-present`— Value must not be present in request

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source variable *identifier* condition user-identity does-not-equal

Syntax

```
shared sic group identifier editing editing-rule source variable identifier condition user-identity does-not-equal value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source variable identifier condition user-identity does-not-equal]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must not match this value exactly.

Options

`value value`— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source variable *identifier* condition user-identity equals

Syntax

```
shared sic group identifier editing editing-rule source variable identifier condition user-identity equals value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source variable identifier condition user-identity equals]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must match this value exactly.

Options

value value— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source variable *identifier* condition user-identity has-prefix

Syntax

```
shared sic group identifier editing editing-rule source variable identifier condition user-identity has-prefix value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source variable identifier condition user-identity has-prefix]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must have a prefix that matches this value exactly.

Options

value *value*— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source variable *identifier* condition user-identity has-suffix

Syntax

```
shared sic group identifier editing editing-rule source variable identifier condition user-identity has-suffix value ...
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule source variable identifier condition user-identity has-suffix]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must have a suffix that matches this value exactly.

Options

value value— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* source variable *identifier* condition user-identity range

Syntax

```
shared sic group identifier editing editing-  
rule source variable identifier condition user-identity range {  
    low low;  
    high high;  
}
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-  
rule source variable identifier condition user-identity range]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the range of the match condition. Checked value in the user identity must be within this range.

Options

low low—(Optional) Low range in text format.

Value—Text
Editing Level—Basic

high high—(Optional) High range in text format.

Value—Text
Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* editing *editing-rule* target

Syntax

```
shared sic group identifier editing editing-rule target {
    request-attribute request-attribute;
    response-attribute response-attribute;
    variable variable;
}
```

Hierarchy Level

```
[edit shared sic group identifier editing editing-rule target]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the target (LValue) in which to place the result of the editing process. The target can be a RADIUS request or response attribute or a transaction variable.

Options

request-attribute request-attribute—(Optional) Target of the editing rule is a RADIUS request attribute.

Value—Text
Editing Level—Basic

response-attribute response-attribute—(Optional) Target of the editing rule is a RADIUS response attribute.

Value—Text
Editing Level—Basic

variable variable—(Optional) Target of the editing rule is a transactional variable.

Value—Text
Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* local-realm

Syntax

```
shared sic group identifier local-realm name ...
```

Hierarchy Level

```
[edit shared sic group identifier local-realm]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Specify realms that are local to this server, meaning that any requests sent for these realms are treated as if there is no realm in the request.

For servers, the network access identifier (NAI) in the request identifies the intended realm. To properly interpret requests received from intermediate servers, the SIC server must know which realms it is responsible for servicing locally.

When a request is received, the server examines the NAI to determine the realm to which the request should be routed. If the realm name is specified here, the request is handled by this local SIC server. If no realm is present in the NAI, the request is considered to be local.

Options

name name— Name of local realm. If the realm to which the request is to be routed is listed in this field, the realm is ignored and the request is processed by this local server. If no realm is present in either the NAI, the request is considered to be local.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* model

Syntax

```
shared sic group identifier model id {
    dictionary dictionary;
}
```

Hierarchy Level

```
[edit shared sic group identifier model]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the device models supported by the group and their associated dictionaries.

Options

id id— Device model name. Each device must have an associated model name.

Value—Text

dictionary dictionary— Name of dictionary used by the device model.

Value—Text

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* radius accounting-listener limit

Syntax

```
shared sic group identifier radius accounting-listener limit {
    incoming-queue incoming-queue;
    transaction-queue transaction-queue;
}
```

Hierarchy Level

```
[edit shared sic group identifier radius accounting-listener limit]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure accounting listener queue limits.

Options

incoming-queue incoming-queue—(Optional) Limit of incoming queue for accounting listener. When the number of unprocessed received messages surpasses the incoming queue limit, the SIC server stops reading from the transport. Reading from the transport resumes as soon as the number of unprocessed received messages falls below this limit.

Value—Integer in the range 0–2147483647

Default— 1000

Editing Level—Basic

transaction-queue transaction-queue—(Optional) Limit of transaction queue for accounting listener. When the number of unscheduled transactions surpasses the transaction queue limit, the SIC server stops reading from the transport. Reading from the transport resumes as soon as the number of unscheduled transactions falls below this limit.

Value—Integer in the range 0–2147483647

Default— 1000

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* radius accounting-listener transport

Syntax

```
shared sic group identifier radius accounting-listener transport id ...
```

Hierarchy Level

```
[edit shared sic group identifier radius accounting-listener transport]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure RADIUS accounting listener transport. The accounting listener transport is used to listen for accounting requests from RADIUS clients over UDP.

Options

id id— Name of RADIUS accounting listener transport. Each RADIUS accounting transport must have a unique name.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* radius accounting-listener transport *id*

Syntax

```
shared sic group identifier radius accounting-listener transport id {
    port port;
    connections-per-thread connections-per-thread;
    connect-timeout connect-timeout;
    disconnect-timeout disconnect-timeout;
}
```

Hierarchy Level

```
[edit shared sic group identifier radius accounting-listener transport id]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure properties of the RADIUS transport used by accounting listener.

port port—UDP port number of the accounting listener. The server listens for RADIUS packets on this UDP port number.

Value—Integer in the range 0–2147483647

Editing Level—Basic

connections-per-thread connections-per-thread—(Optional) Number of UDP connections per thread. A single thread will handle these many UDP connections.

Value—Integer in the range 0–15

Default— 15

Editing Level—Basic

connect-timeout connect-timeout—(Optional) UDP connection timeout in milliseconds. The server will wait this long for a connection.

Value—Integer in the range 0–2147483647 ms

Default— 1000

Editing Level—Basic

`disconnect-timeout` *disconnect-timeout*—(Optional) UDP disconnection timeout in milliseconds. The server will wait this long for a disconnect.

Value—Integer in the range 0–2147483647 ms

Default— 1000

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* radius network-element

Syntax

```
shared sic group identifier radius network-element id ...
```

Hierarchy Level

```
[edit shared sic group identifier radius network-element]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure RADIUS network element. A network element is a logical network entity that hosts any number of SIC functions. Each RADIUS network element consists of a group of clients and targets that the SIC server may exchange messages with using the RADIUS protocol. An upstream network element is an accounting client that sends requests to the SIC server. A downstream network element is an accounting target to which the SIC forwards accounting requests.

Options

id id— Name of RADIUS network element. Each network element must have a unique name.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* radius network-element *id* downstream

Syntax

```
shared sic group identifier radius network-element id downstream {
    failover-mode (round-robin | primary-backup);
}
```

Hierarchy Level

```
[edit shared sic group identifier radius network-element id downstream]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the failover mode for the downstream network element. The failover mode manages how messages are sent over multiple paths to the network element.

Options

`failover-mode (round-robin | primary-backup)`— Failover mode used by SIC for this network element.

Value

- `round-robin`— Failover mode used by the server is the round robin method. When this failover mode is used, the server alternates the path it uses to send messages to the downstream RADIUS network element target.
- `primary-backup`— Failover mode used by the server is the primary backup method. When this failover mode is used, the server sends requests to the primary target unless it is unavailable, in which case it sends requests to the backup target.

Default—primary-backup

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* radius network-element *id* downstream

Syntax

```
shared sic group identifier radius network-element id downstream {
    model model;
}
```

Hierarchy Level

```
[edit shared sic group identifier radius network-element id downstream]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure device model of downstream RADIUS network element. A downstream RADIUS network element is an accounting target to which this server may send RADIUS accounting requests. The downstream target is a AAA server.

Options

`model model`—(Optional) Device model of the RADIUS network element target. Only device models that have previously been configured for the group may be specified.

Value—Text
Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* radius network-element *id* downstream accounting-target

Syntax

```
shared sic group identifier radius network-element id downstream accounting-
target name {
    address address;
}
```

Hierarchy Level

```
[edit shared sic group identifier radius network-element id downstream accounting-
target]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure a RADIUS accounting target in the downstream network element. The accounting target is a downstream AAA server that the SIC server may forward accounting requests to.

Options

name name— Name of the RADIUS accounting target. The accounting target must have a unique name to identify it among all accounting targets.

Value—Text

address address— IP address of the RADIUS accounting target.

Value—IP address

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* radius network-element *id* downstream accounting-target *name*

Syntax

```
shared sic group identifier radius network-element id downstream accounting-
target name {
    secret secret;
    outbound-transport outbound-transport;
    port port;
}
```

Hierarchy Level

```
[edit shared sic group identifier radius network-element id downstream accounting-
target name]
```

Release Information

Statement introduced in SRC Release 4.0.0

Options

secret secret— Configure the shared secret used by the RADIUS accounting target. A RADIUS shared secret is a case-sensitive password (text string) used to validate communications between two RADIUS devices, such as a RADIUS-based server and a RADIUS client or target. The shared secret must be configured to match on both devices. Configure shared secrets that are long enough and random enough to resist attack, and avoid using the same shared secret throughout your network.

Value—Text
Editing Level—Basic

outbound-transport outbound-transport—(Optional) Name of the local transport on the SIC server sending outbound requests to the downstream accounting target.

Value—Text
Editing Level—Basic

port port—(Optional) Specify the UDP port number on which the RADIUS accounting target listens for accounting requests.

Value—Integer in the range 0–2147483647
Default— 1813

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* radius network-element *id* downstream failover-policy

Syntax

```
shared sic group identifier radius network-element id downstream failover-policy {
    priority priority;
}
```

Hierarchy Level

```
[edit shared sic group identifier radius network-element id downstream failover-policy]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the failover policy for downstream RADIUS network element.

Options

priority priority—(Optional) Priority of the accounting target. The lowest priority targets are selected first in a failover policy.

Value—Integer in the range 0–2147483647

Default— 1

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* radius network-element *id* downstream failover-policy fast-fail

Syntax

```
shared sic group identifier radius network-element id downstream failover-
policy fast-fail {
    minimum-number minimum-number;
    timeout timeout;
    reset-delay reset-delay;
}
```

Hierarchy Level

```
[edit shared sic group identifier radius network-element id downstream failover-
policy fast-fail]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the fast fail options of the failover policy. The fast fail options control how the server handles unreachable targets. When the server sends a message to a target, it expects to receive a reply. If the server does not receive the reply within the timeframe specified by the fast fail policy, it goes into fast fail mode for that target and rejects the request.

Options

minimum-number minimum-number— Minimum number of attempts for failover policy. Specifies the minimum number of times the server will retransmit a message if an acknowledgment from the target is not received; if the minimum number is exhausted, the server places the target in fast fail.

Value—Integer in the range 0–2147483647

Default— 3

Editing Level—Basic

timeout timeout— Time in seconds before the server goes into fast fail mode for that target.

Value—Integer in the range 0–2147483647 s

Default— 3

Editing Level—Basic

`reset-delay` *reset-delay*— Time in seconds after which the server comes out of fast fail mode for that target.

Value—Integer in the range 0–2147483647 s
Default— 30
Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* radius network-element *id* downstream failover-policy retry

Syntax

```
shared sic group identifier radius network-element id downstream failover-
policy retry {
    number number;
    timeout timeout;
}
```

Hierarchy Level

```
[edit shared sic group identifier radius network-element id downstream failover-
policy retry]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the retry options for the target. The retry options control how the server retries failed requests.

Options

number number— Maximum number of attempts. Specifies the maximum number of times a message is retransmitted if an acknowledgment from the target is not received; if the maximum number is exhausted, the original request is rejected.

Value—Integer in the range 0–2147483647

Default— 3

Editing Level—Basic

timeout timeout— Number of seconds between retry attempts.

Value—Integer in the range 0–2147483647 s

Default— 4

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* radius network-element *id* proxy

Syntax

```
shared sic group identifier radius network-element id proxy {  
}
```

Hierarchy Level

```
[edit shared sic group identifier radius network-element id proxy]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Assign the proxy function to this downstream network element. This function instructs the SIC server to forward (proxy) accounting requests to this downstream network element (AAA server).

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* radius network-element *id* proxy

Syntax

```
shared sic group identifier radius network-element id proxy {
    default-route-for-all-realms;
}
```

Hierarchy Level

```
[edit shared sic group identifier radius network-element id proxy]
```

Description

Configure the default route for all realms. If this option is enabled, this will be the default route for messages received for all realms.

Options

`default-route-for-all-realms`—(Optional) Default route for all realms.

Default— false

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* radius network-element *id* proxy realm

Syntax

```
shared sic group identifier radius network-element id proxy realm realmValue {
    condition (exact | prefix);
}
```

Hierarchy Level

```
[edit shared sic group identifier radius network-element id proxy realm]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the realm names and match conditions for the network element. Any accounting requests received by the SIC server destined for these realms will be routed to this network element if there is a match on these realm conditions.

Options

realmValue realmValue— Realm name. Each realm name must be unique.

Value—Text

condition (exact | prefix)— Realm match condition. Route request to this network element if this condition is matched.

Value

- *exact*— *realmValue* must exactly match realm string in request.
- *prefix*— *realmValue* must match beginning of realm string in request.

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* radius network-element *id* upstream

Syntax

```
shared sic group identifier radius network-element id upstream {
    model model;
}
```

Hierarchy Level

```
[edit shared sic group identifier radius network-element id upstream]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Assign the upstream function to this network element and configure the device model of the client device. The upstream function is assigned to RADIUS clients that send RADIUS requests to this server.

Options

`model model`—(Optional) Device model of RADIUS client. This device model must have been previously configured for the SIC group.

Value—Text

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* radius network-element *id* upstream accounting-client

Syntax

```
shared sic group identifier radius network-element id upstream accounting-
client id {
    address address;
    accounting-secret accounting-secret;
}
```

Hierarchy Level

```
[edit shared sic group identifier radius network-element id upstream accounting-
client]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure settings for the RADIUS accounting client sending requests to the SIC server.

Options

id id— Name of RADIUS accounting client. Each accounting client must have a unique name among all accounting clients.

Value—Text

address address— IP address of RADIUS client sending accounting requests to SIC server.

Value—IP address
Editing Level—Basic

accounting-secret accounting-secret— Shared secret used by accounting client. If unspecified, no shared secret is used.

Value—Text
Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* radius outbound-transport

Syntax

```
shared sic group identifier radius outbound-transport transport-name ...
```

Hierarchy Level

```
[edit shared sic group identifier radius outbound-transport]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the name of the RADIUS transport used to send outbound requests to RADIUS targets over UDP.

Options

transport-name transport-name— Name of RADIUS outbound transport. Each RADIUS outbound transport must have a unique name.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* radius outbound-transport *transport-name*

Syntax

```
shared sic group identifier radius outbound-transport transport-name {
    connections-per-thread connections-per-thread;
    connect-timeout connect-timeout;
    disconnect-timeout disconnect-timeout;
    port port;
    port-range-size port-range-size;
}
```

Hierarchy Level

```
[edit shared sic group identifier radius outbound-transport transport-name]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure properties of the RADIUS transport used to send outbound requests to RADIUS targets over UDP.

connections-per-thread connections-per-thread—(Optional) Number of UDP connections per thread. A single thread will handle these many UDP connections.

Value—Integer in the range 0–15

Default— 15

Editing Level—Basic

connect-timeout connect-timeout—(Optional) UDP connection timeout in milliseconds. The server will wait this long for a connection.

Value—Integer in the range 0–2147483647 ms

Default— 1000

Editing Level—Basic

disconnect-timeout disconnect-timeout—(Optional) UDP disconnection timeout in milliseconds. The server will wait this long for a disconnect.

Value—Integer in the range 0–2147483647 ms

Default— 1000

Editing Level—Basic

`port port`— Outbound starting UDP port number. This server will send RADIUS packets from a port range starting with this UDP port number.

Value—Integer in the range 0–2147483647

Default—0

Editing Level—Basic

`port-range-size port-range-size`—(Optional) UDP source port range size. This value specifies the range of UDP ports that will be used to send RADIUS packets.

Value—Integer in the range 0–2147483647

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server

Syntax

```
shared sic group identifier server identifier ...
```

Hierarchy Level

```
[edit shared sic group identifier server]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the properties of the server belonging to the SIC group.

Options

identifier identifier— Name of SIC server using this group configuration. The server name must have previously been configured with the configuration statement-slot number sic server. This server name must match the name specified with the statement-slot number sic server.

Value— Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* accounting-route

Syntax

```
shared sic group identifier server identifier accounting-route id ...
```

Hierarchy Level

```
[edit shared sic group identifier server identifier accounting-route]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure an explicit accounting route and the criterion used by the server to select the accounting routing target.

Options

id id— Name of explicit accounting route. An accounting route must have a unique name.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* accounting-route *id* condition realm

Syntax

```
shared sic group identifier server identifier accounting-route id condition realm
{
    (present | not-present);
}
```

Hierarchy Level

```
[edit shared sic group identifier server identifier accounting-
route id condition realm]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure a realm match condition. If the condition is matched in the request, the route is selected.

Check for the presence of this value in the request.

Value

- `present`— Value must be present in request
- `not-present`— Value must not be present in request

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* accounting- route *id* condition realm does-not-equal

Syntax

```
shared sic group identifier server identifier accounting-  
route id condition realm does-not-equal value ...
```

Hierarchy Level

```
[edit shared sic group identifier server identifier accounting-  
route id condition realm does-not-equal]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must not match this value exactly.

Options

value value— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* accounting- route *id* condition realm equals

Syntax

```
shared sic group identifier server identifier accounting-  
route id condition realm equals value ...
```

Hierarchy Level

```
[edit shared sic group identifier server identifier accounting-  
route id condition realm equals]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must match this value exactly.

Options

value value— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* accounting- route *id* condition realm has-prefix

Syntax

```
shared sic group identifier server identifier accounting-  
route id condition realm has-prefix value ...
```

Hierarchy Level

```
[edit shared sic group identifier server identifier accounting-  
route id condition realm has-prefix]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must have a prefix that matches this value exactly.

Options

value value— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* accounting- route *id* condition realm has-suffix

Syntax

```
shared sic group identifier server identifier accounting-  
route id condition realm has-suffix value ...
```

Hierarchy Level

```
[edit shared sic group identifier server identifier accounting-  
route id condition realm has-suffix]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must have a suffix that matches this value exactly.

Options

value value— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* accounting- route *id* condition realm range

Syntax

```
shared sic group identifier server identifier accounting-
route id condition realm range {
    low low;
    high high;
}
```

Hierarchy Level

```
[edit shared sic group identifier server identifier accounting-
route id condition realm range]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the range of the match condition. Checked value in the realm must be within this range.

Options

low low—(Optional) Low range in text format.

Value—Text
Editing Level—Basic

high high—(Optional) High range in text format.

Value—Text
Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* accounting- route *id* condition request

Syntax

```
shared sic group identifier server identifier accounting-  
route id condition request {  
}
```

Hierarchy Level

```
[edit shared sic group identifier server identifier accounting-  
route id condition request]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the name of the request attribute in the match condition, and specify the presence option of the condition.

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* accounting- route *id* condition request attribute

Syntax

```
shared sic group identifier server identifier accounting-
route id condition request attribute attribute-name {
    (present | not-present);
}
```

Hierarchy Level

```
[edit shared sic group identifier server identifier accounting-
route id condition request attribute]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the request attribute match condition. If the request attribute condition is matched in the request, the route is selected.

Options

attribute-name attribute-name— Name of the request attribute.

Value—Text

Check for the presence of this value in the request.

Value

- *present*— Value must be present in request
- *not-present*— Value must not be present in request

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* accounting- route *id* condition request attribute *attribute-name* does-not-equal

Syntax

```
shared sic group identifier server identifier accounting-  
route id condition request attribute attribute-name does-not-equal value ...
```

Hierarchy Level

```
[edit shared sic group identifier server identifier accounting-  
route id condition request attribute attribute-name does-not-equal]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must not match this value exactly.

Options

value value— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* accounting- route *id* condition request attribute *attribute-name* equals

Syntax

```
shared sic group identifier server identifier accounting-  
route id condition request attribute attribute-name equals value ...
```

Hierarchy Level

```
[edit shared sic group identifier server identifier accounting-  
route id condition request attribute attribute-name equals]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must match this value exactly.

Options

value *value*— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* accounting- route *id* condition request attribute *attribute-name* has-prefix

Syntax

```
shared sic group identifier server identifier accounting-  
route id condition request attribute attribute-name has-prefix value ...
```

Hierarchy Level

```
[edit shared sic group identifier server identifier accounting-  
route id condition request attribute attribute-name has-prefix]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must have a prefix that matches this value exactly.

Options

value value— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* accounting- route *id* condition request attribute *attribute-name* has-suffix

Syntax

```
shared sic group identifier server identifier accounting-  
route id condition request attribute attribute-name has-suffix value ...
```

Hierarchy Level

```
[edit shared sic group identifier server identifier accounting-  
route id condition request attribute attribute-name has-suffix]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must have a suffix that matches this value exactly.

Options

value value— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* accounting- route *id* condition request attribute *attribute-name* range

Syntax

```
shared sic group identifier server identifier accounting-
route id condition request attribute attribute-name range {
    low low;
    high high;
}
```

Hierarchy Level

```
[edit shared sic group identifier server identifier accounting-
route id condition request attribute attribute-name range]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the range of the match condition. Checked value in the attribute must be within this range.

Options

low low— Low range in text format.

Value—Text
Editing Level—Basic

high high— High range in text format.

Value—Text
Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* accounting-route *id* condition user-identity

Syntax

```
shared sic group identifier server identifier accounting-route id condition user-identity {
    (present | not-present);
}
```

Hierarchy Level

```
[edit shared sic group identifier server identifier accounting-route id condition user-identity]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure a user identity match condition. If the user identity condition is matched in the request, the route is selected. Possible match conditions are present, not present, does not equal, equals, has prefix, has suffix, or range.

Check for the presence of this value in the request.

Value

- `present`— Value must be present in request
- `not-present`— Value must not be present in request

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* accounting-route *id* condition user-identity does-not-equal

Syntax

```
shared sic group identifier server identifier accounting-route id condition user-identity does-not-equal value ...
```

Hierarchy Level

```
[edit shared sic group identifier server identifier accounting-route id condition user-identity does-not-equal]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must not match this value exactly.

Options

value value— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* accounting-route *id* condition user-identity equals

Syntax

```
shared sic group identifier server identifier accounting-route id condition user-identity equals value ...
```

Hierarchy Level

```
[edit shared sic group identifier server identifier accounting-route id condition user-identity equals]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must match this value exactly.

Options

value value— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* accounting-route *id* condition user-identity has-prefix

Syntax

```
shared sic group identifier server identifier accounting-route id condition user-identity has-prefix value ...
```

Hierarchy Level

```
[edit shared sic group identifier server identifier accounting-route id condition user-identity has-prefix]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must have a prefix that matches this value exactly.

Options

value value— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* accounting-route *id* condition user-identity has-suffix

Syntax

```
shared sic group identifier server identifier accounting-route id condition user-identity has-suffix value ...
```

Hierarchy Level

```
[edit shared sic group identifier server identifier accounting-route id condition user-identity has-suffix]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the match condition. The value in the request must have a suffix that matches this value exactly.

Options

value value— Value of match condition.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* accounting-route *id* condition user-identity range

Syntax

```
shared sic group identifier server identifier accounting-route id condition user-identity range {
    low low;
    high high;
}
```

Hierarchy Level

```
[edit shared sic group identifier server identifier accounting-route id condition user-identity range]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the range of the match condition. Checked value in the user identity must be within this range.

Options

low low—(Optional) Low range in text format.

Value—Text
Editing Level—Basic

high high—(Optional) High range in text format.

Value—Text
Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* accounting-route *id* editing

Syntax

```
shared sic group identifier server identifier accounting-route id editing editing-rule ...
```

Hierarchy Level

```
[edit shared sic group identifier server identifier accounting-route id editing]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Specify an editing rule you want applied to the request before the server sends it to the accounting target. If the route is selected, the request will be edited according to this editing rule before the request is sent to the accounting target.

Options

editing-rule editing-rule— Name of the editing rule to be applied to the request if this route is selected.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* accounting-route *id* target

Syntax

```
shared sic group identifier server identifier accounting-route id target {
    accounting-method accounting-method;
}
```

Hierarchy Level

```
[edit shared sic group identifier server identifier accounting-route id target]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the target of the accounting route. If this route is selected, packets will be routed to this target.

Options

`accounting-method accounting-method`— Accounting method (accounting target) used if route is selected. If all match conditions are met and this route is selected, packets are routed to this accounting target.

Value—Text

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* logger

Syntax

```
shared sic group identifier server identifier logger id ...
```

Hierarchy Level

```
[edit shared sic group identifier server identifier logger]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the destination (log stream) for storing logging events. The SIC server uses log streams to store events. A log stream captures different groups of server-related events at various levels of granularity. You may configure the SIC server to capture any number of log streams. Each log stream saves events in a separate text file. Each text file is date stamped, and can be assigned a prefix for easy identification. The log group specifies the type of server-related events to be captured. You configure the level of granularity to be captured for the log group by setting the event level for the group.

Options

id id— Name used by the server to identify the log stream. If you configure multiple log streams, make sure to use unique names.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* logger *id* file

Syntax

```
shared sic group identifier server identifier logger id file {
    filter (/error | /debug-error);
    filename filename;
    maximum-file-size maximum-file-size;
    rollover-interval rollover-interval;
    rollover-on-startup;
    flush-after-writes;
    high-resolution-timestamps;
    header header;
    footer footer;
    prepend-message-header;
    work-id-label work-id-label;
    work-id-padding work-id-padding;
    utc;
}
```

Hierarchy Level

```
[edit shared sic group identifier server identifier logger id file]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the properties of the log stream file. Each log stream saves events in a separate text file. Each text file is date stamped, and can be assigned a prefix for easy identification.

Options

`filter (/error | /debug-error)`—(Optional) Filter to define which event messages are logged or ignored. The filter specifies the logging level, such as debug.

Value

- `/error`— Error events are captured for every log group
- `/debug-error`— Debug events are captured for every log group

Editing Level—Basic

`filename filename`—Prefix added to log file name. This string will be prepended to each log file name.

Value—Text
Editing Level—Basic

`maximum-file-size maximum-file-size`—(Optional) New log file created after these many bytes. When a log file reaches this size, logging will begin in a new log file.

Value—Integer in the range 0–2147483647 bytes
Default— 0 (no limit)
Editing Level—Basic

`rollover-interval rollover-interval`—(Optional) New log file is created after this amount of time elapses. Specified in seconds.

Value—Integer in the range 0–2147483647 s
Default— 86400
Editing Level—Basic

`rollover-on-startup`—(Optional) New log file is created every time the server starts.

Default— false
Editing Level—Basic

`flush-after-writes`—(Optional) Flush after every write. This setting is set to true for real-time logging and can be set to false for performance optimization when real-time logging is not needed.

Default— true
Editing Level—Basic

`high-resolution-timestamps`—(Optional) High resolution time reporting system functions are used.

Default— false
Editing Level—Basic

`header header`—(Optional) Header message added to the beginning of each log file.

Value—Text
Editing Level—Basic

`footer footer`—(Optional) Footer message added to the end of each log file.

Value—Text
Editing Level—Basic

`prepend-message-header`—(Optional) Prepend each log message with additional information. Add time, thread and transaction information to each log message. You can achieve additional fine tuning by using the `work-id-label`, `work-id-padding`, and `utc` options.

Default— true
Editing Level—Basic

`work-id-label work-id-label`—(Optional) Work data ID prefix added to each log message.

Value—Text
Editing Level—Basic

`work-id-padding work-id-padding`—(Optional) String added to each log message if work data is not available.

Value—Text
Editing Level—Basic

`utc`—(Optional) Time and date values reflect Universal Time Coordinates (UTC), formerly known as Greenwich Mean Time or (GMT). Otherwise, values reflect local time.

Default— false
Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* logger *id* group

Syntax

```
shared sic group identifier server identifier logger id group (administration |
configuration | system | packet | packet-trace | packet-trace-raw) {
    events (error | warning | standard | detail | debug);
}
```

Hierarchy Level

```
[edit shared sic group identifier server identifier logger id group]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the event level for the log group. The log group specifies the type of server-related events captured in the log stream. The event level specifies the level of detail captured for the log group. First specify the name of the log group, and, then specify the event level for it. Repeat for each log group.

Options

Log group for which to specify event level. Log messages are divided into several log groups according to the subject of the log information. You may configure a log stream to display only log messages from particular log groups. The log group specifies the type of server-related events to be captured. You configure the level of granularity captured for the log group by setting the event level for the group.

Value

- **administration**— Log group reports events related to server administration, such as changes made to the server configuration, including identity of the administrator. Use the Detail event level to capture these events
- **configuration**— Log group reports events related to server configuration
- **system**— Log group reports events related to the system, such as system start and system stop
- **packet**— Log group reports events related to transaction processing, such as incoming and outgoing packets
- **packet-trace**— Log group displays contents of a packet. The format is attribute name:attribute value
- **packet-trace-raw**— Log group displays raw data (octets) of incoming and outgoing packets

events (error | warning | standard | detail | debug)—(Optional) Highest event level for the log group. You may configure the log stream to display log items from levels at and below a particular event level. This is the highest event level displayed for this log group.

Be careful when using event logging because it consumes server resources while capturing events, and consumes disk space to store the log files. We recommend that event logging be used primarily for troubleshooting purposes. We recommend that you limit the amount of information captured in a log stream to control the consumption of server resources and disk space. This also makes it easier to interpret the information in the log files. For example, you might configure one log stream to capture only configuration-related events by setting the Configuration log group event level to Detail, and setting all other log group event levels to Error.

Value

- **error**— Messages in log shown at event level error. An error is defined as an event that may cause the system to operate incorrectly. Examples include exceptions being thrown, an inability to continue processing a transaction, or configuration errors that cause a component to fail to start
- **warning**— Messages in log shown at event levels error and warning. Warnings are less severe than errors, in that a warning should be logged when the system was able to handle an unexpected input or condition without any threat to the operation of the server. Examples of warnings include invalid packet contents or failures in contacting remote servers
- **standard**— Messages in log shown at event levels error, warning, and standard. Standard logging messages show events as a result of normal operation
- **detail**— Messages in log shown at event levels error, warning, standard, and detail. Detail logging is intended to inform why and how the particular result indicated by standard logging was reached. Server components that perform significant processing on the transaction, such as determining validity of the packet contents, log details about decisions they made. All server components that route the transaction through different processing based on the nature of the transaction log their routing activity at this level. The detail log is allowed to refer to the contents of messages logged at the standard level; that is, it will never be read without the standard messages
- **debug**— Messages in log shown at event levels error, warning, standard, detail, and debug. Debug logging is provided for the benefit of engineering only

Default— standard

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* outbound-transport

Syntax

```
shared sic group identifier server identifier outbound-transport transport-  
name ...
```

Hierarchy Level

```
[edit shared sic group identifier server identifier outbound-transport]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the RADIUS outbound transport properties used by the server to send outbound requests to RADIUS targets over UDP.

Options

transport-name transport-name— Name of RADIUS outbound transport used by the server. Each RADIUS outbound transport must have a unique name.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* outbound-transport *transport-name*

Syntax

```
shared sic group identifier server identifier outbound-transport transport-name {
    address address;
}
```

Hierarchy Level

```
[edit shared sic group identifier server identifier outbound-transport transport-name]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the RADIUS outbound transport properties used by the server to send outbound requests to RADIUS targets over UDP.

Options

address address—(Optional) IP address used by the server when sending outbound requests

Value—IP address
Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* transport

Syntax

```
shared sic group identifier server identifier transport transport-name ...
```

Hierarchy Level

```
[edit shared sic group identifier server identifier transport]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the RADIUS accounting transport for this server. RADIUS accounting transport is used to listen for accounting requests from RADIUS clients over UDP.

Options

transport-name transport-name— Name of RADIUS accounting transport for this server. Each RADIUS accounting transport must have a unique name.

Value—Text

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* server *identifier* transport *transport-name*

Syntax

```
shared sic group identifier server identifier transport transport-name {
    address address;
}
```

Hierarchy Level

```
[edit shared sic group identifier server identifier transport transport-name]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the RADIUS accounting transport for this server. RADIUS accounting transport is used to listen for accounting requests from RADIUS clients over UDP.

Options

address address—(Optional) IP address used by the server for receiving UDP packets.
The server listens for UDP RADIUS packets on this IP address.

Value—IP address

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* snmp event

Syntax

```
shared sic group identifier snmp event (sic-server-startup | sic-server-shutdown
| sic-server-unauthorized-administration-request | sic-server-internal-error |
sic-server-resource-failure | sic-server-log-file-failure) {
    dilution-factor dilution-factor;
}
```

Hierarchy Level

```
[edit shared sic group identifier snmp event]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure SNMP events for which a trap is sent when the event occurs, and configure the dilution factor.

Options

Name of the SNMP trap for which you want to configure dilution factor.

Value

- `sic-server-startup`— SNMP trap on server startup
- `sic-server-shutdown`— SNMP trap on server shutdown
- `sic-server-unauthorized-administration-request`—
SNMP trap on unauthorized administration request
- `sic-server-internal-error`— SNMP trap on server internal
error
- `sic-server-resource-failure`— SNMP trap on server
resource failure
- `sic-server-log-file-failure`— SNMP trap on server log
file failure

`dilution-factor dilution-factor`—(Optional) Dilution factor. Alert event dilution means that a particular alert is sent to the SNMP network management station once for every *n* occurrences of the condition that generated the alert. Dilution allows for a fine degree of control with respect to alert generation for certain warning and error conditions.

Value—Integer in the range 0–2147483647

Default— 1
Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

shared sic group *identifier* transaction-manager

Syntax

```
shared sic group identifier transaction-manager {
    maximum-number-of-variables maximum-number-of-variables;
}
```

Hierarchy Level

```
[edit shared sic group identifier transaction-manager]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure the number of transaction variables supported by the SIC group.

Options

maximum-number-of-variables maximum-number-of-variables—(Optional)
Maximum number of transactional variables supported by the SIC group.

Value—Integer in the range 0–2147483647

Default—255

Editing Level—Basic

Required Privilege Level

system system

Required Editing Level

Basic

slot *number* sic initial directory-connection

Syntax

```
slot number sic initial directory-connection {
    url url;
    port port;
    principal principal;
    credentials credentials;
    entry-dn entry-dn;
    filter filter;
}
```

Hierarchy Level

```
[edit slot number sic initial directory-connection]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure directory connection properties that the subscriber information collector uses to connect to the Juniper Networks database.

Options

url url—URL that identifies the location of the primary directory server.

Value—IP address

Default—127.0.0.1

Editing Level—Basic

port port—(Optional) Port the directory server listens on.

Value—Integer in the range 0–2147483647

Default—389

Editing Level—Basic

principal principal—(Optional) DN the SRC component uses for authentication to access the directory.

Value—Text

Default—cn=umcadmin,o=umc**Editing Level**—Basic

`credentials` *credentials*— Password with which the SRC component accesses the directory.

Value—Secret text**Editing Level**—Basic

`entry-dn` *entry-dn*—(Optional) Location of SIC configuration in directory.

Value—Text**Default**—l=SIC,ou=staticConfiguration,ou=Configuration,o=Management,o=umc**Editing Level**—Basic

`filter` *filter*—(Optional) Filter the SIC uses to query the directory for recent configuration changes. Do not change this setting.

Value—Text**Default**—(objectClass=*)**Editing Level**—Basic

Required Privilege Level

admin

Required Editing Level

Basic

slot *number* sic server

Syntax

```
slot number sic server {  
    name name;  
}
```

Hierarchy Level

```
[edit slot number sic server]
```

Release Information

Statement introduced in SRC Release 4.0.0

Description

Configure an instance of the SIC server.

Options

name name—(Optional) Name of SIC server referenced in SIC shared configuration.

Value—Text

Editing Level—Basic

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

show sic statistics radius client accounting

Syntax

```
show sic statistics radius client accounting
```

Release Information

Command introduced in SRC Release 4.0.0

Description

Display RADIUS client statistics for accounting requests. The statistics are presented for any client from which the server has received packets.

Required Privilege Level

view

show sic statistics radius host accounting

Syntax

```
show sic statistics radius host accounting
```

Release Information

Command introduced in SRC Release 4.0.0

Description

Display RADIUS host statistics for accounting transactions, as well as server runtime statistics and packet error statistics.

Required Privilege Level

view

show sic statistics radius target accounting

Syntax

```
show sic statistics radius target accounting
```

Release Information

Command introduced in SRC Release 4.0.0

Description

Display RADIUS target statistics for accounting requests. The statistics are available for RADIUS dynamic authorization and authentication targets that are defined in the server.

Required Privilege Level

view

show sic statistics route accounting

Syntax

```
show sic statistics route accounting
```

Release Information

Command introduced in SRC Release 4.0.0

Description

Display accounting route statistics. The server collects and displays statistics for each routing rule defined in the server (implicit, explicit, and default).

Required Privilege Level

view

SNMP Agent

The following table summarizes the SRC command-line interface (SRC CLI) for configuring the SNMP agent. Configuration statements are listed in alphabetical order.

SNMP Agent Configuration Statements
snmp
snmp agent
snmp agent initial
snmp agent initial directory-connection
snmp agent initial directory-eventing
snmp agent java
snmp agent logger
snmp agent logger name file
snmp agent logger name syslog
snmp community
snmp monitor
snmp monitor alarm
snmp monitor alarm name boolean-test
snmp monitor alarm name delta-discontinuity-check
snmp monitor alarm name existence-test
snmp monitor alarm name threshold-test
snmp monitor chassis-alarm
snmp monitor chassis-alarm cpu-temperature
snmp monitor chassis-alarm fan-speed
snmp monitor chassis-alarm system-temperature
snmp monitor chassis-alarm voltage-1.8v
snmp monitor chassis-alarm voltage-3.3v

<u>snmp monitor chassis-alarm voltage-5v</u>
<u>snmp monitor chassis-alarm voltage-12v</u>
<u>snmp monitor chassis-alarm voltage-battery</u>
<u>snmp monitor chassis-alarm voltage-cpu-core</u>
<u>snmp monitor chassis-alarm voltage-cpu-dimm</u>
<u>snmp monitor chassis-alarm voltage-negative12v</u>
<u>snmp monitor event</u>
<u>snmp monitor event name notification</u>
<u>snmp monitor event name snmp-set</u>
<u>snmp notify alarm category</u>
<u>snmp notify alarm category category-name alarm</u>
<u>snmp notify event category</u>
<u>snmp notify event category category-name event</u>
<u>snmp notify target</u>
<u>snmp v3 snmp-community</u>
<u>snmp v3 usm local-engine user</u>
<u>snmp v3 usm local-engine user username access</u>
<u>snmp v3 usm local-engine user username authentication-md5</u>
<u>snmp v3 usm local-engine user username authentication-sha</u>
<u>snmp v3 usm local-engine user username privacy-aes</u>
<u>snmp v3 usm local-engine user username privacy-des</u>
<u>snmp v3 vacm access group</u>
<u>snmp v3 vacm access group group-name default-context-prefix security-model</u>
<u>snmp v3 vacm access group group-name default-context-prefix security-model security-level</u>
<u>snmp v3 vacm security-to-group security-model</u>
<u>snmp v3 vacm security-to-group security-model security-name</u>
<u>snmp view</u>


```
snmp view view-name oid
```

snmp

Syntax

```
snmp {
    contact contact;
    name name;
    location location;
    description description;
    address [address...];
}
```

Hierarchy Level

```
[edit snmp]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure SNMP system information.

Options

`contact contact`—(Optional) Administrative contact for the system being managed by SNMP.

Value—Text
Editing Level—Basic

`name name`—(Optional) Name of the system being managed by SNMP.

Value—Text
Editing Level—Basic

`location location`—(Optional) Location of the system being managed by SNMP.

Value—Text
Editing Level—Basic

`description` *description*—(Optional) Description of the system being managed by SNMP.

Value—Text

Editing Level—Basic

`address` [*address...*]—(Optional) Listening address on which to receive incoming SNMP requests.

Value— IP address; list of addresses.

Default— The SNMP agent listens on all IPv4 interfaces.

Editing Level—Basic

Required Privilege Level

snmp

Required Editing Level

Basic

snmp agent

Syntax

```
snmp agent {
    trap-history-limit trap-history-limit;
    component-polling-interval component-polling-interval;
    protocol-log-level protocol-log-level;
}
```

Hierarchy Level

```
[edit snmp agent]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure SNMP agent.

Options

trap-history-limit trap-history-limit—(Optional) Maximum number of elements stored in the SNMP trap history table.

Value—Integer in the range 1–2147483647

Default—800

Editing Level—Basic

component-polling-interval component-polling-interval—(Optional) Interval at which the SRC component is polled to determine whether it is running and to generate up and down event traps.

Value—Integer in the range 10–2147483647 seconds

Default—60

Editing Level—Basic

protocol-log-level protocol-log-level—(Optional) The log level for SNMP requests received from the master agent and responses to the requests. To enable packet-level logging, set it to 9 or less.

Value—Integer in the range 0–100

Default—20
Editing Level—Expert

Required Privilege Level

snmp

Required Editing Level

Basic

snmp agent initial

Syntax

```
snmp agent initial {
    base-dn base-dn;
    host-id host-id;
}
```

Hierarchy Level

```
[edit snmp agent initial]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure initial properties for the SNMP agent.

Options

base-dn base-dn— DN of the directory used for the SNMP agent configuration data.

Value— DN

Default—\${system ldap client base-dn}

Editing Level—Basic

host-id host-id— Identifier of the system management configuration in the directory server that provides the remaining configuration for the SNMP agent. If the entry does not exist, the entry and the subentries for the components and traps is automatically created in the system management configuration.

Value— DN

Default—ou=POP-ID,ou=System Management,ou=Configuration,
o=Management,o=umc

Editing Level—Basic

Required Privilege Level

snmp

Required Editing Level

Basic

snmp agent initial directory-connection

Syntax

```
snmp agent initial directory-connection {
    url url;
    backup-urls [backup-urls...];
    principal principal;
    credentials credentials;
    protocol (ldaps);
    timeout timeout;
    check-interval check-interval;
    blacklist;
    snmp-agent;
}
```

Hierarchy Level

```
[edit snmp agent initial directory-connection]
```

Description

Configure properties for the directory connection.

Options

`url url`—(Optional) URL that identifies the location of the primary directory server.

Value— URL

Default—`ldap://127.0.0.1:389`

Editing Level—Basic

`backup-urls [backup-urls...]`—(Optional) URLs that identify the locations of backup directory servers. Backup servers are used if the primary directory server is not accessible.

Value— List of URLs

Editing Level—Basic

`principal principal`— DN that the SRC component uses for authentication to access the directory.

Value— DN.

When you specify the DN, you can use `<base>` to indicate the base DN.

Editing Level—Basic

`credentials credentials`— Password with which the SRC component accesses the directory.

Value— Password

Editing Level—Basic

`protocol (ldaps)`—(Optional) Security protocol used to connect to the directory. If you do not configure a security protocol, plain socket is used.

Value

- `ldaps`— LDAPS which uses SSL.

Editing Level—Expert

`timeout timeout`—(Optional) Maximum amount of time during which the directory must respond to a connection request.

Value—Integer in the range 1–2147483647 s

Default—10

Editing Level—Expert

`check-interval check-interval`—(Optional) Time interval at which the directory monitoring system verifies its connection to the directory. If the directory connection fails after this interval, the directory monitoring system initiates a connection to another directory.

Value—Integer in the range 15–2147483647 s

Default—60

Editing Level—Expert

`blacklist`—(Optional) Specifies whether the directory monitoring system prevents connection to a directory if the directory fails to respond during 10 polling intervals.

Default—false

Editing Level—Basic

`snmp-agent`—(Optional) Specifies whether the SDX SNMP agent exports MIBs for this directory connection.

Default—false
Editing Level—Expert

Required Privilege Level

snmp

Required Editing Level

Basic

snmp agent initial directory-eventing

Syntax

```
snmp agent initial directory-eventing {
    eventing;
    signature-dn signature-dn;
    polling-interval polling-interval;
    event-base-dn event-base-dn;
    dispatcher-pool-size dispatcher-pool-size;
}
```

Hierarchy Level

```
[edit snmp agent initial directory-eventing]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Change configuration for directory eventing properties. In most cases, you can use the default configuration for these properties.

Options

`eventing`—(Optional) Enable an SRC component to poll the directory for changes.

Default—true

Editing Level—Normal

`signature-dn signature-dn`—(Optional) DN of the directory entry that specifies the usedDirectory attribute for the SRC CLI. The usedDirectory attribute identifies the vendor of the directory server.

Value— DN

Default—o=umc

Editing Level—Expert

`polling-interval polling-interval`—(Optional) Interval at which an SRC component polls the directory to check for directory changes.

Value—Integer in the range 15–2147483647 s

Default—30
Editing Level—Normal

`event-base-dn` *event-base-dn*—(Optional)

DN of an entry superior to the data associated with an SRC component in the directory.

If you are storing non-SRC data in the directory, and that data changes frequently whereas the SRC data does not, you may need to adjust the default value to improve performance. For optimal performance, set the value to the DN of an entry superior to both the SRC data and the changing non-SRC data.

Value— DN
Default—o=UMC
Editing Level—Expert

`dispatcher-pool-size` *dispatcher-pool-size*—(Optional) Number of directory change notifications that can be sent simultaneously to the SRC component.

Value—Integer in the range 0–2147483647
Default—1
Editing Level—Expert

Required Privilege Level

snmp

Required Editing Level

Basic

snmp agent java

Syntax

```
snmp agent java {
    heap-size heap-size;
}
```

Hierarchy Level

```
[edit snmp agent java]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure local Java Runtime Environment (JRE) properties for the SNMP agent.

Options

heap-size heap-size—(Optional) Maximum amount of Java heap (memory) available to the JRE. Do not change this value unless instructed to do so by Juniper Networks.

Value— Number of megabytes in the format *integern*

Default—160m

Editing Level—Basic

Required Privilege Level

snmp

Required Editing Level

Basic

snmp agent logger

Syntax

```
snmp agent logger name ...
```

Hierarchy Level

```
[edit snmp agent logger]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the logging destination.

Options

name name— Name used to group parameters for the logging destination.

Value—Text

Required Privilege Level

snmp

Required Editing Level

Basic

snmp agent logger *name* file

Syntax

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

Hierarchy Level

```
[edit snmp agent logger name file]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the logging destination for file-based logging.

filter filter—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

Editing Level—Basic

filename filename— Absolute path of the filename that contains the current logs.

Note: 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.

Value— Filename

Default— By default, SRC components and applications write log files in the folder in which the component or application is started.

Editing Level—Basic

`rollover-filename rollover-filename`—(Optional) 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— Path of filename

Example—`/opt/UMC/sae/var/log/sae.alt`

Default— The default value is different for each type of component.

Editing Level—Normal

`maximum-file-size maximum-file-size`—(Optional) Maximum size of the log file and the rollover file.

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

Value—Integer in the range 0–2147483647 kbytes

Default— 1000000

Editing Level—Normal

Required Privilege Level

snmp

Required Editing Level

Basic

snmp agent logger *name* syslog

Syntax

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

Hierarchy Level

```
[edit snmp agent logger name syslog]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the logging destination for syslog-based logging.

filter filter—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

Editing Level—Basic

host host— IP address or name of a host that collects event messages by means of a standard system logging daemon.

Value— IP address or hostname

Default—loghost

Editing Level—Basic

facility facility—(Optional) Type of system log in accordance with the system logging protocol.

Value—Integer in the range 0–23

Default— 3

Editing Level—Advanced

format format—(Optional) MessageFormat string that specifies how the information in an event message is printed. (The strings {#} are replaced with the log information [...]).

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

Editing Level—Advanced

Required Privilege Level

snmp

Required Editing Level

Basic

snmp community

Syntax

```
snmp community community {
    authorization (read-only | read-write);
    clients clients;
    oid oid;
}
```

Hierarchy Level

```
[edit snmp community]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a community string, which defines the access control for client systems.

Options

`community community`— Community name.

Value—Text

`authorization (read-only | read-write)`—(Optional) Authorization type.

Value

- `read-only`— Allow read-only access
- `read-write`— Allow read and write access

Default—`read-only`

Editing Level—Basic

`clients clients`— IP address or subnet of the SNMP client hosts that are authorized to use this community. By default, all clients are allowed.

Value—Text

Default—0.0.0.0/0
Editing Level—Basic

`oid oid`—(Optional) Object identifier (OID) used to represent a subtree of MIB objects to which access is allowed.

Value—Text
Default— Access to the full OID tree
Editing Level—Basic

Required Privilege Level

snmp

Required Editing Level

Basic

snmp monitor

Syntax

```
snmp monitor {
    security-name security-name;
}
```

Hierarchy Level

```
[edit snmp monitor]
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Provide active monitoring of SRC MIB objects as configured. The software generates associated notification events when specified criteria are met.

Options

security-name security-name— SNMPv3 username to access a monitored MIB object. SNMPv3 provides security by controlling access to the objects.

Value— *username*

Default— No value

Editing Level—Normal

Required Privilege Level

snmp

Required Editing Level

Normal

snmp monitor alarm

Syntax

```
snmp monitor alarm name {
    interval interval;
    sample-type (absolute-value | delta-value);
    ignore-startup-alarm;
    event event;
    variable variable;
    strict-oid;
}
```

Hierarchy Level

```
[edit snmp monitor alarm]
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Monitor the value of a MIB object. You can configure how often to sample a value, the type of sampling to perform, the type of alarm or trigger to use the sampled value, and the event to generate in response to a specified condition.

Note: Configure one alarm condition at a time.

Options

`name name`— Name of the alarm (also referred to as a trigger).

Value—Text

`interval interval`— Interval between monitoring samples.

Value—Integer in the range seconds

Default—600

Editing Level—Normal

`sample-type (absolute-value | delta-value)`— Method of sampling to use for the specified variable.

Note: Existence tests disregard the sample type when set to `delta-value`.

Value

- `absolute-value`— Use actual value of the trigger to compare to the threshold value.
- `delta-value`— Use the delta (difference between two samples) to compare to the value.

Default— No value

Editing Level—Normal

`ignore-startup-alarm`—(Optional) Whether the alarm can be sent when it is first activated. If this option is set, the monitor expression is not evaluated when the alarm activates the first time. If not set, the first evaluation is done after the alarm is activated.

Default—false

Editing Level—Normal

`event event`—(Optional) The name of the event to be generated in response to the alarm condition. If you do not specify an event, the software uses one of the following DISMAN notification events: `mteTriggerFired` in existence or boolean tests, and `mteTriggerRising` or `mteTriggerFalling` in threshold tests.

Value— *event name*

Default— None

Editing Level—Normal

`variable variable`— Object identifier (OID) of the MIB variable to be monitored. The OID can be a an identifier in dotted decimal notation or the name of a MIB object.

Value— *OID or name*

Default— No value

Editing Level—Normal

`strict-oid`—(Optional) Monitor the SNMP object instance specified by the variable attribute. If you do not set this option, the software monitors all objects in the MIB branch specified by the variable option.

Default—false

Editing Level—Normal

Required Privilege Level

snmp

Required Editing Level

Normal

snmp monitor alarm *name* boolean-test

Syntax

```
snmp monitor alarm name boolean-test {
    comparison (equal | unequal | less | less-or-equal | greater | greater-or-
equal);
    value value;
}
```

Hierarchy Level

```
[edit snmp monitor alarm name boolean-test]
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Define a monitor test to compare a sample value to a specified value or range of values. If the condition specified for the test is met, the software generates the event. The software generates the event again after the status of the condition changes to false then to true again.

Note: Configure only one monitor test at a time.

Options

`comparison (equal | unequal | less | less-or-equal | greater | greater-or-equal)`— Type of boolean comparison to perform.

Value

- `equal`— True if the sample value equals object value.
- `unequal`— True if the sample value does not equal the object value.
- `less`— True if the sample is less than the object value.
- `less-or-equal`— True if the sample value is less than or equal to the object value.
- `greater`— True if the sample value is greater than the object value.
- `greater-or-equal`— True if the sample value is greater than or equal to the object value.

Default— No value

Editing Level—Normal

`value value`— Value against which to compare the sample value.

Value—Integer in the range -2147483648–2147483647
Default— No Value
Editing Level—Normal

Required Privilege Level

snmp

Required Editing Level

Normal

snmp monitor alarm *name* delta-discontinuity-check

Syntax

```
snmp monitor alarm name delta-discontinuity-check {
    variable variable;
    strict-oid;
}
```

Hierarchy Level

```
[edit snmp monitor alarm name delta-discontinuity-check]
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Configure SNMP to detect a discontinuity in values to prevent false alarms caused by the value of a MIB object being reset. Use this statement when the sample type is delta-value (a change in the value of a monitored MIB object is compared to a threshold value). You define a variable, called a discontinuity marker, which is a MIB object to use to validate the delta, or difference, between values. The marker object should be of type TimeTicks, DateAndTime, or Timestamp.

Before the SNMP agent calculates a delta, it checks the discontinuity marker for the trigger condition at the end of a polling interval. A change in the value of the discontinuity marker indicates that a discontinuity occurs. As a result, the agent does not perform the test for the associated trigger condition until the next polling interval.

Options

variable variable— Object identifier (OID) or name of a discontinuity marker.

Value— Marker object of type TimeTicks, DateAndTime or Timestamp

Default— No value

Editing Level—Normal

strict-oid—(Optional) Monitor the discontinuity marker instance specified by the variable attribute. If you do not set this option, the software monitors all discontinuity objects subordinate to the value set by the variable option.

Default—false

Editing Level—Normal

Required Privilege Level

snmp

Required Editing Level

Normal

snmp monitor alarm *name* existence-test

Syntax

```
snmp monitor alarm name existence-test {
    type (present | absent | changed);
}
```

Hierarchy Level

```
[edit snmp monitor alarm name existence-test]
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Define a monitor test to identify when an object appears, disappears, or changes value. If the test criteria are met, the test is successful.

Note: Configure only one monitor test at a time.

Options

`type (present | absent | changed)`— Type of monitor test to perform.

Value

- `present`— Test for appearance of object.
- `absent`— Test for disappearance of object.
- `changed`— Test for change in value of object.

Default— No value

Editing Level—Normal

Required Privilege Level

snmp

Required Editing Level

Normal

snmp monitor alarm *name* threshold-test

Syntax

```
snmp monitor alarm name threshold-test {
    rising-threshold rising-threshold;
    falling-threshold falling-threshold;
}
```

Hierarchy Level

```
[edit snmp monitor alarm name threshold-test]
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Define a threshold monitor test. A threshold test compares the sample value to a configured upper and lower threshold. The monitor generates a corresponding event when the value of the monitored object falls below the lower threshold or rises above the upper threshold.

After a rising threshold event is generated, it is generated again only after the sample value falls below the lower threshold. Similarly, a subsequent falling threshold event is generated when the sample value rises above the upper threshold.

Note: Configure only one monitor test at a time.

Options

rising-threshold rising-threshold— Upper threshold for the sample value. The software generates an event when the sample value is greater than or equal to the rising threshold, and the value at the last sampling interval is less than this threshold.

Value—Integer in the range -2147483648–2147483647

Default— No value

Editing Level—Normal

falling-threshold falling-threshold— Lower threshold for the sample value. The software generates an event when the sample value is less than or equal to the falling threshold, and the value at the last sampling interval is greater than this threshold.

Value—Integer in the range -2147483648–2147483647

Default— No value

Editing Level—Normal

Required Privilege Level

snmp

Required Editing Level

Normal

snmp monitor chassis-alarm

Syntax

```
snmp monitor chassis-alarm {
    disable;
    interval interval;
}
```

Hierarchy Level

```
[edit snmp monitor chassis-alarm]
```

Release Information

Statement introduced in SRC Release 3.2.0

Description

Configure built-in chassis alarms that monitor the sensors on C Series Controllers.

Options

`disable`—(Optional) Disables all chassis alarms.

Default—true

Editing Level—Basic

`interval interval`—(Optional) Time interval during which SNMP samples the value of an object.

Value—Integer in the range 15–2147483647 s

Default—15

Editing Level—Basic

Required Privilege Level

No specific privilege required.

Required Editing Level

Expert

snmp monitor chassis-alarm cpu-temperature

Syntax

```
snmp monitor chassis-alarm cpu-temperature {
    minor minor;
    major major;
    critical critical;
}
```

Hierarchy Level

```
[edit snmp monitor chassis-alarm cpu-temperature]
```

Release Information

Statement introduced in SRC Release 3.2.0

Description

Configure the SNMP alarm thresholds for CPU temperature sensors.

Options

`minor minor`—(Optional) Minor alarm upper threshold for CPU temperature.

Value—Integer in the range -2147483648–2147483647 degree C

Default—76

Editing Level—Basic

`major major`—(Optional) Major alarm upper threshold for CPU temperature.

Value—Integer in the range -2147483648–2147483647 degree C

Default—78

Editing Level—Basic

`critical critical`—(Optional) Critical alarm upper threshold for CPU temperature.

Value—Integer in the range -2147483648–2147483647 degree C

Default—80

Editing Level—Basic

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

snmp monitor chassis-alarm fan-speed

Syntax

```
snmp monitor chassis-alarm fan-speed {
    minor minor;
    major major;
    critical critical;
}
```

Hierarchy Level

```
[edit snmp monitor chassis-alarm fan-speed]
```

Release Information

Statement introduced in SRC Release 3.2.0

Description

Configure the SNMP alarm thresholds for fan speed sensors.

Options

`minor minor`—(Optional) Minor alarm lower threshold for fan speed (in RPM).

Value—Integer in the range -2147483648–2147483647 RPM

Default—540

Editing Level—Basic

`major major`—(Optional) Major alarm lower threshold for fan speed (in RPM).

Value—Integer in the range -2147483648–2147483647 RPM

Default—405

Editing Level—Basic

`critical critical`—(Optional) Critical alarm lower threshold for fan speed (in RPM).

Value—Integer in the range -2147483648–2147483647 RPM

Default—270

Editing Level—Basic

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

snmp monitor chassis-alarm system-temperature

Syntax

```
snmp monitor chassis-alarm system-temperature {
    minor minor;
    major major;
    critical critical;
}
```

Hierarchy Level

```
[edit snmp monitor chassis-alarm system-temperature]
```

Release Information

Statement introduced in SRC Release 3.2.0

Description

Configure the SNMP alarm thresholds for system temperature sensors.

Options

`minor minor`—(Optional) Minor alarm upper threshold for system temperature.

Value—Integer in the range -2147483648–2147483647 degree C

Default—76

Editing Level—Basic

`major major`—(Optional) Major alarm upper threshold for system temperature.

Value—Integer in the range -2147483648–2147483647 degree C

Default—78

Editing Level—Basic

`critical critical`—(Optional) Critical alarm upper threshold for system temperature.

Value—Integer in the range -2147483648–2147483647 degree C

Default—80

Editing Level—Basic

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

snmp monitor chassis-alarm voltage-1.8v

Syntax

```
snmp monitor chassis-alarm voltage-1.8v {
    below-minor below-minor;
    below-major below-major;
    below-critical below-critical;
    over-minor over-minor;
    over-major over-major;
    over-critical over-critical;
}
```

Hierarchy Level

```
[edit snmp monitor chassis-alarm voltage-1.8v]
```

Release Information

Statement introduced in SRC Release 3.2.0

Description

Configure the SNMP alarm thresholds for 1.8V sensors.

Options

`below-minor below-minor`—(Optional) Minor alarm lower threshold for 1.8V voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—1644

Editing Level—Basic

`below-major below-major`—(Optional) Major alarm lower threshold for 1.8V voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—1632

Editing Level—Basic

`below-critical below-critical`—(Optional) Critical alarm lower threshold for 1.8V voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—1620

Editing Level—Basic

`over-minor over-minor`—(Optional) Minor alarm upper threshold for 1.8V voltage.

Value—Integer in the range -2147483648–2147483647 mV
Default—2028
Editing Level—Basic

`over-major over-major`—(Optional) Major alarm upper threshold for 1.8V voltage.

Value—Integer in the range -2147483648–2147483647 mV
Default—2040
Editing Level—Basic

`over-critical over-critical`—(Optional) Critical alarm upper threshold for 1.8V voltage.

Value—Integer in the range -2147483648–2147483647 mV
Default—2052
Editing Level—Basic

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

snmp monitor chassis-alarm voltage-3.3v

Syntax

```
snmp monitor chassis-alarm voltage-3.3v {
    below-minor below-minor;
    below-major below-major;
    below-critical below-critical;
    over-minor over-minor;
    over-major over-major;
    over-critical over-critical;
}
```

Hierarchy Level

```
[edit snmp monitor chassis-alarm voltage-3.3v]
```

Release Information

Statement introduced in SRC Release 3.2.0

Description

Configure the SNMP alarm thresholds for 3.3V sensors.

Options

`below-minor below-minor`—(Optional) Minor alarm lower threshold for 3.3V voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—2890

Editing Level—Basic

`below-major below-major`—(Optional) Major alarm lower threshold for 3.3V voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—2873

Editing Level—Basic

`below-critical below-critical`—(Optional) Critical alarm lower threshold for 3.3V voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—2856

Editing Level—Basic

`over-minor over-minor`—(Optional) Minor alarm upper threshold for 3.3V voltage.

Value—Integer in the range -2147483648–2147483647 mV
Default—3587
Editing Level—Basic

`over-major over-major`—(Optional) Major alarm upper threshold for 3.3V voltage.

Value—Integer in the range -2147483648–2147483647 mV
Default—3604
Editing Level—Basic

`over-critical over-critical`—(Optional) Critical alarm upper threshold for 3.3V voltage.

Value—Integer in the range mV
Default—3621
Editing Level—Basic

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

snmp monitor chassis-alarm voltage-5v

Syntax

```
snmp monitor chassis-alarm voltage-5v {
    below-minor below-minor;
    below-major below-major;
    below-critical below-critical;
    over-minor over-minor;
    over-major over-major;
    over-critical over-critical;
}
```

Hierarchy Level

```
[edit snmp monitor chassis-alarm voltage-5v]
```

Release Information

Statement introduced in SRC Release 3.2.0

Description

Configure the SNMP alarm thresholds for 5V sensors.

Options

`below-minor below-minor`—(Optional) Minor alarm lower threshold for 5V voltage.

Value—Integer in the range mV

Default—4472

Editing Level—Basic

`below-major below-major`—(Optional) Major alarm lower threshold for 5V voltage.

Value—Integer in the range mV

Default—4446

Editing Level—Basic

`below-critical below-critical`—(Optional) Critical alarm lower threshold for 5V voltage.

Value—Integer in the range mV

Default—4420

Editing Level—Basic

`over-minor over-minor`—(Optional) Minor alarm upper threshold for 5V voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—5512

Editing Level—Basic

`over-major over-major`—(Optional) Major alarm upper threshold for 5V voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—5538

Editing Level—Basic

`over-critical over-critical`—(Optional) Critical alarm upper threshold for 5V voltage.

Value—Integer in the range -2147483648–2147483647

Default—5564

Editing Level—Basic

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

snmp monitor chassis-alarm voltage-12v

Syntax

```
snmp monitor chassis-alarm voltage-12v {
    below-minor below-minor;
    below-major below-major;
    below-critical below-critical;
    over-minor over-minor;
    over-major over-major;
    over-critical over-critical;
}
```

Hierarchy Level

```
[edit snmp monitor chassis-alarm voltage-12v]
```

Release Information

Statement introduced in SRC Release 3.2.0

Description

Configure the SNMP alarm thresholds for 12V sensors.

Options

`below-minor below-minor`—(Optional) Minor alarm lower threshold for 12V voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—10836

Editing Level—Basic

`below-major below-major`—(Optional) Major alarm lower threshold for 12V voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—10773

Editing Level—Basic

`below-critical below-critical`—(Optional) Critical alarm lower threshold for 12V voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—10710

Editing Level—Basic

`over-minor over-minor`—(Optional) Minor alarm upper threshold for 12V voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—13356

Editing Level—Basic

`over-major over-major`—(Optional) Major alarm upper threshold for 12V voltage.

Value—Integer in the range mV

Default—13419

Editing Level—Basic

`over-critical over-critical`—(Optional) Critical alarm upper threshold for 12V voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—13482

Editing Level—Basic

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

snmp monitor chassis-alarm voltage-battery

Syntax

```
snmp monitor chassis-alarm voltage-battery {
    below-minor below-minor;
    below-major below-major;
    below-critical below-critical;
    over-minor over-minor;
    over-major over-major;
    over-critical over-critical;
}
```

Hierarchy Level

```
[edit snmp monitor chassis-alarm voltage-battery]
```

Release Information

Statement introduced in SRC Release 3.2.0

Description

Configure the SNMP alarm thresholds for battery voltage sensors.

Options

`below-minor below-minor`—(Optional) Minor alarm lower threshold for battery voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—3024

Editing Level—Basic

`below-major below-major`—(Optional) Major alarm lower threshold for battery voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—3008

Editing Level—Basic

`below-critical below-critical`—(Optional) Critical alarm lower threshold for battery voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—2992

Editing Level—Basic

`over-minor over-minor`—(Optional) Minor alarm upper threshold for battery voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—3744

Editing Level—Basic

`over-major over-major`—(Optional) Major alarm upper threshold for battery voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—3760

Editing Level—Basic

`over-critical over-critical`—(Optional) Critical alarm upper threshold for battery voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—3776

Editing Level—Basic

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

snmp monitor chassis-alarm voltage-cpu-core

Syntax

```
snmp monitor chassis-alarm voltage-cpu-core {
    below-minor below-minor;
    below-major below-major;
    below-critical below-critical;
    over-minor over-minor;
    over-major over-major;
    over-critical over-critical;
}
```

Hierarchy Level

```
[edit snmp monitor chassis-alarm voltage-cpu-core]
```

Release Information

Statement introduced in SRC Release 3.2.0

Description

Configure the SNMP alarm thresholds for CPU core voltage sensors.

Options

`below-minor below-minor`—(Optional) Minor alarm lower threshold for CPU core voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—1030

Editing Level—Basic

`below-major below-major`—(Optional) Major alarm lower threshold for CPU core voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—1020

Editing Level—Basic

`below-critical below-critical`—(Optional) Critical alarm lower threshold for CPU core voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—1008

Editing Level—Basic

`over-minor over-minor`—(Optional) Minor alarm upper threshold for CPU core voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—1728

Editing Level—Basic

`over-major over-major`—(Optional) Major alarm upper threshold for CPU core voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—1740

Editing Level—Basic

`over-critical over-critical`—(Optional) Critical alarm upper threshold for CPU core voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—1752

Editing Level—Basic

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

snmp monitor chassis-alarm voltage-cpu-dimm

Syntax

```
snmp monitor chassis-alarm voltage-cpu-dimm {
    below-minor below-minor;
    below-major below-major;
    below-critical below-critical;
    over-minor over-minor;
    over-major over-major;
    over-critical over-critical;
}
```

Hierarchy Level

```
[edit snmp monitor chassis-alarm voltage-cpu-dimm]
```

Release Information

Statement introduced in SRC Release 3.2.0

Description

Configure the SNMP alarm thresholds for CPU DIMM voltage sensors.

Options

`below-minor below-minor`—(Optional) Minor alarm lower threshold for CPU DIMM voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—2292

Editing Level—Basic

`below-major below-major`—(Optional) Major alarm lower threshold for CPU DIMM voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—2280

Editing Level—Basic

`below-critical below-critical`—(Optional) Critical alarm lower threshold for CPU DIMM voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—2268

Editing Level—Basic

`over-minor` *over-minor*—(Optional) Minor alarm upper threshold for CPU DIMM voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—2832

Editing Level—Basic

`over-major` *over-major*—(Optional) Major alarm upper threshold for CPU DIMM voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—2844

Editing Level—Basic

`over-critical` *over-critical*—(Optional) Critical alarm upper threshold for CPU DIMM voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—2856

Editing Level—Basic

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

snmp monitor chassis-alarm voltage-negative12v

Syntax

```
snmp monitor chassis-alarm voltage-negative12v {
    below-minor below-minor;
    below-major below-major;
    below-critical below-critical;
    over-minor over-minor;
    over-major over-major;
    over-critical over-critical;
}
```

Hierarchy Level

```
[edit snmp monitor chassis-alarm voltage-negative12v]
```

Release Information

Statement introduced in SRC Release 3.2.0

Description

Configure the SNMP alarm thresholds for –12V sensors.

Options

`below-minor below-minor`—(Optional) Minor alarm lower threshold for –12V voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—13264

Editing Level—Basic

`below-major below-major`—(Optional) Major alarm lower threshold for –12V voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—13336

Editing Level—Basic

`below-critical below-critical`—(Optional) Critical alarm lower threshold for –12V voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—13408

Editing Level—Basic

`over-minor over-minor`—(Optional) Minor alarm upper threshold for –12V voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—10744

Editing Level—Basic

`over-major over-major`—(Optional) Major alarm upper threshold for –12V voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—10672

Editing Level—Basic

`over-critical over-critical`—(Optional) Critical alarm upper threshold for –12V voltage.

Value—Integer in the range -2147483648–2147483647 mV

Default—10600

Editing Level—Basic

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

snmp monitor event

Syntax

```
snmp monitor event name ...
```

Hierarchy Level

```
[edit snmp monitor event]
```

Release Information

Statement introduced in SRC Release 3.0.0

Options

name name— The name of the event to be invoked in response to a trigger or an alarm. When the event is invoked, SNMP sends a notification or an snmp-set.

Value—Text

Required Privilege Level

snmp

Required Editing Level

Normal

snmp monitor event *name* notification

Syntax

```
snmp monitor event name notification {
    oid oid;
    strict-object [strict-object...];
    wildcarded-object [wildcarded-object...];
}
```

Hierarchy Level

```
[edit snmp monitor event name notification]
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Define an event for which SNMP sends a notification.

Note: Do not define an event notification and an snmp-set for the same event.

Options

oid oid— Notification Object identifier (OID).

Value— *OID*

Default— No value

Editing Level—Normal

*strict-object [*strict-object...*]*—(Optional) OIDs of VARBIND objects to be used as specified

Value— *OID*

Default— No value

Editing Level—Normal

*wildcarded-object [*wildcarded-object...*]*—(Optional) OIDs of VARBIND objects include subidentifiers from the corresponding monitored object appended to the object.

Value— *OID*

Default— No value
Editing Level—Normal

Required Privilege Level

snmp

Required Editing Level

Normal

snmp monitor event *name* snmp-set

Syntax

```
snmp monitor event name snmp-set {
    variable variable;
    value value;
    strict-oid;
}
```

Hierarchy Level

```
[edit snmp monitor event name snmp-set]
```

Release Information

Statement introduced in SRC Release 3.0.0

Description

Define an event that sets a MIB variable. Do not define an event notification and an snmp-set for the same event.

Options

variable variable— Object identifier (OID) of MIB variable to be set

Value— *OID*

Default— No value

Editing Level—Normal

value value— Object value to set

Value—Integer in the range -2147483648–2147483647

Default— No value

Editing Level—Normal

strict-oid—(Optional) Monitor the OID exactly as specified by the variable option. If not set, the software adds any suffixes to any OID matches.

Default—false

Editing Level—Normal

Required Privilege Level

snmp

Required Editing Level

Normal

snmp notify alarm category

Syntax

```
snmp notify alarm category category-name ...
```

Hierarchy Level

```
[edit snmp notify alarm category]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure alarm category.

Options

category-name category-name— Category name for alarm.

Value— Category name from list of possible completions, including:

- acp
- jps
- nic-host
- policy-decision-point
- policy-engine
- radius-accounting-peer
- radius-authentication-peer
- sae
- sae-router-driver
- sdx-redirector
- system-management

Required Privilege Level

snmp

Required Editing Level

Basic

snmp notify alarm category *category-name* alarm

Syntax

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

Hierarchy Level

```
[edit snmp notify alarm category category-name alarm]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure alarm.

Options

alarm-name alarm-name— Alarm name.

Value— Alarm name from list of possible completions, depending on the specified alarm category

interval interval—(Optional) Interval at which the variable associated with the trap is polled.

Value—Integer in the range 1–2147483647

Default—60

Editing Level—Basic

critical critical— Threshold above which a critical alarm is generated.

Value—Integer in the range 0–2147483647

Editing Level—Basic

`major` *major*— Threshold above which a major alarm is generated.

Value—Integer in the range 0–2147483647

Editing Level—Basic

`minor` *minor*— Threshold above which a minor alarm is generated.

Value—Integer in the range 0–2147483647

Editing Level—Basic

Required Privilege Level

snmp

Required Editing Level

Basic

snmp notify event category

Syntax

```
snmp notify event category category-name ...
```

Hierarchy Level

```
[edit snmp notify event category]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure event category.

Options

category-name *category-name*— Category name for event trap.

Value— Category name from list of possible completions, including:

- acp
- directory-eventing-system
- jps
- nic-host
- sae
- sae-router-driver
- system-management

Required Privilege Level

snmp

Required Editing Level

Basic

snmp notify event category *category-name* event

Syntax

```
snmp notify event category category-name event event-name ...
```

Hierarchy Level

```
[edit snmp notify event category category-name event]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Enable event notification.

Options

event-name event-name— Event trap name.

Value— Event name from list of possible completions, depending on the specified event category

Required Privilege Level

snmp

Required Editing Level

Basic

snmp notify target

Syntax

```
snmp notify target target-name {
    address address;
    port port;
    community community;
    type (trapv1 | trapv2 | inform);
}
```

Hierarchy Level

```
[edit snmp notify target]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure notification target.

Options

target-name target-name— Notification target name.

Value—Text

address address— IPv4 or IPv6 address of the system to receive notifications.

Value—IP address

Editing Level—Basic

port port—(Optional) SNMP trap port number.

Value—Integer in the range 0–65535

Default—162

Editing Level—Basic

community community— Community string used when sending traps.

Value—Text
Editing Level—Basic

type (trapv1 | trapv2 | inform)— Type of notifications to receive.

Value

- trapv1—SNMPv1 trap
- trapv2—SNMPv2c trap
- inform—SNMPv2 inform

Editing Level—Basic

Required Privilege Level

snmp

Required Editing Level

Basic

snmp v3 snmp-community

Syntax

```
snmp v3 snmp-community community-index {
    community-name community-name;
    security-name security-name;
    address address;
}
```

Hierarchy Level

```
[edit snmp v3 snmp-community]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Map an SNMPv1 or SNMPv2c community string to a security name. Optionally, you can specify the IPv4 or IPv6 addresses of the SNMP client hosts that are authorized to use this community. By default, all SNMP clients using this community string are authorized to access the agent.

Options

community-index community-index— Unique index that identifies an SNMP community.

Value—Text

community-name community-name—(Optional) A community string for an SNMPv1 or SNMPv2c community. If unspecified, the community index is used.

Value—Text
Editing Level—Basic

security-name security-name— The view-based access control model (VACM) security name to associate with the community string.

Value—Text
Editing Level—Basic

`address address`— IP address or subnet of the SNMP client hosts that are authorized to use this community.

Value—Text
Default— 0.0.0.0/0
Editing Level—Basic

Required Privilege Level

snmp

Required Editing Level

Basic

snmp v3 usm local-engine user

Syntax

```
snmp v3 usm local-engine user username ...
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify a user associated with an SNMPv3 group. By default, no authentication or encryption is specified for the SNMPv3 user.

Options

`username username`—SNMPv3 user-based security model (USM) username

Value—Text

Required Privilege Level

snmp

Required Editing Level

Basic

snmp v3 usm local-engine user *username* access

Syntax

```
snmp v3 usm local-engine user username access {
    authorization (read-only | read-write);
    oid oid;
}
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user username access]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Define access privileges for SNMPv3 user

Note: You cannot assign this security name to SNMP group

Options

`authorization (read-only | read-write)`— Authorization type.

Value

- `read-only`— Allow read-only access
- `read-write`— Allow read and write access

Editing Level—Basic

`oid oid`—(Optional) Object identifier (OID) used to represent a subtree of MIB objects to which access is allowed.

Value—Text

Default— Access to the full OID tree

Editing Level—Basic

Required Privilege Level

snmp

Required Editing Level

Basic

snmp v3 usm local-engine user *username* authentication-md5

Syntax

```
snmp v3 usm local-engine user username authentication-md5 {
    authentication-password authentication-password;
}
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user username authentication-md5]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure Message Digest 5 (MD5) as the authentication type for the SNMPv3 user.

Options

`authentication-password authentication-password`— Password used for authentication.

Value— Password; must be at least eight characters

Editing Level—Basic

Required Privilege Level

snmp

Required Editing Level

Basic

snmp v3 usm local-engine user *username* authentication-sha

Syntax

```
snmp v3 usm local-engine user username authentication-sha {
    authentication-password authentication-password;
}
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user username authentication-sha]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure Secure Hash Algorithm (SHA) as the authentication type for the SNMPv3 user.

Options

`authentication-password authentication-password`— Password used for authentication.

Value— Password; must be at least eight characters

Editing Level—Basic

Required Privilege Level

snmp

Required Editing Level

Basic

snmp v3 usm local-engine user *username* privacy-aes

Syntax

```
snmp v3 usm local-engine user username privacy-aes {  
    privacy-password privacy-password;  
}
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user username privacy-aes]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure Advanced Encryption Standard (AES) for the SNMPv3 user.

Note: Before you configure encryption, you must configure MD5 or SHA authentication.

Options

`privacy-password privacy-password`— Privacy password for the SNMPv3 user.

Value— Password; must be at least eight characters

Editing Level—Basic

Required Privilege Level

snmp

Required Editing Level

Basic

snmp v3 usm local-engine user *username* privacy-des

Syntax

```
snmp v3 usm local-engine user username privacy-des {
    privacy-password privacy-password;
}
```

Hierarchy Level

```
[edit snmp v3 usm local-engine user username privacy-des]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure Data Encryption Standard (DES) for the SNMPv3 user.

Note: Before you configure encryption, you must configure MD5 or SHA authentication.

Options

`privacy-password privacy-password`— Privacy password for the SNMPv3 user.

Value— Password; must be at least eight characters

Editing Level—Basic

Required Privilege Level

snmp

Required Editing Level

Basic

snmp v3 vacm access group

Syntax

```
snmp v3 vacm access group group-name ...
```

Hierarchy Level

```
[edit snmp v3 vacm access group]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Define access privileges granted to a group.

Options

group-name group-name— Name for a collection of SNMP security names that belong to the same SNMP access policy.

Value—Text

Required Privilege Level

snmp

Required Editing Level

Basic

snmp v3 vacm access group *group-name* default-context-prefix security-model

Syntax

```
snmp v3 vacm access group group-name default-context-prefix security-model (any | v1 | v2c | usm) ...
```

Hierarchy Level

```
[edit snmp v3 vacm access group group-name default-context-prefix security-model]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure security model for access privileges.

Options

Type of security model used for access privileges.

Value

- *any*—Any security model
- *v1*—SNMPv1 model
- *v2c*—SNMPv2c model
- *usm*—SNMPv3 user-based security model

Required Privilege Level

snmp

Required Editing Level

Basic

snmp v3 vacm access group *group-name* default-context-prefix security-model (any | v1 | v2c | usm) security-level

Syntax

```
snmp v3 vacm access group group-name default-context-prefix security-model (any |
v1 | v2c | usm) security-level (authentication | none | privacy) {
    read-view read-view;
    write-view write-view;
}
```

Hierarchy Level

```
[edit snmp v3 vacm access group group-name default-context-prefix security-
model (any | v1 | v2c | usm) security-level]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure access privileges granted to a particular security model.

Options

Security level granted to a security model. If you are configuring the SNMPv1 or SNMPv2c security model, use `none` as the security level.

Value

- `authentication`— Provides authentication but no encryption
- `none`— Provides no authentication and no encryption
- `privacy`— Provides authentication and encryption

`read-view read-view`—(Optional) View used for SNMP Get requests.

Value—Text

Default—none

Editing Level—Basic

`write-view write-view`—(Optional) View used for SNMP Set requests.

Value—Text
Default—none
Editing Level—Basic

Required Privilege Level

snmp

Required Editing Level

Basic

snmp v3 vacm security-to-group security-model

Syntax

```
snmp v3 vacm security-to-group security-model (v1 | v2c | usm) ...
```

Hierarchy Level

```
[edit snmp v3 vacm security-to-group security-model]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure security model context for a group.

Options

Type of security model.

Value

- `v1`—SNMPv1 model
- `v2c`—SNMPv2c model
- `usm`—SNMPv3 user-based security model

Required Privilege Level

snmp

Required Editing Level

Basic

snmp v3 vacm security-to-group security-model (v1 | v2c | usm) security-name

Syntax

```
snmp v3 vacm security-to-group security-model (v1 | v2c | usm) security-
name security-name {
    group-name group-name;
}
```

Hierarchy Level

```
[edit snmp v3 vacm security-to-group security-model (v1 | v2c | usm) security-
name]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Map a security name in the specified security model to a named group.

Options

security-name security-name— Security name to assign to group. If the security model is usm, the security name is the username configured at the [edit snmp v3 usm local-engine user] hierarchy level.

Value—Text

group-name group-name— Group to which the security name is assigned.

Value—Text

Editing Level—Basic

Required Privilege Level

snmp

Required Editing Level

Basic

snmp view

Syntax

```
snmp view view-name ...
```

Hierarchy Level

```
[edit snmp view]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Define a MIB view.

Options

view-name view-name— MIB view name that identifies a group of MIB objects for which to define access. Each MIB object in a view has a common OID prefix. Each object identifier represents a subtree of the MIB object hierarchy.

Value—Text

Required Privilege Level

snmp

Required Editing Level

Basic

snmp view *view-name* oid

Syntax

```
snmp view view-name oid oid {
    (include | exclude);
}
```

Hierarchy Level

```
[edit snmp view view-name oid]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Specify an object identifier (OID) that represents a subtree of MIB objects for the view.

Options

oid oid— Object identifier (OID) that represents a subtree of MIB objects.

Value—Text

Specifies whether the OID is included in or excluded from the view.

Value

- *include*—Include this OID in the view
- *exclude*—Exclude this OID from the view

Editing Level—Basic

Required Privilege Level

snmp

Required Editing Level

Basic

SRC Admission Control Plug-In (SRC ACP)

The following table summarizes the SRC command-line interface (SRC CLI) for providing admission control. Configuration statements and operational commands are listed in alphabetical order.

SRC ACP
Configuration Statements
shared acp configuration acp-options
shared acp configuration corba
shared acp configuration ldap service-data
shared acp configuration ldap subscriber-data
shared acp configuration logger
shared acp configuration logger name file
shared acp configuration logger name syslog
shared acp configuration nic-proxy-configuration
shared acp configuration nic-proxy-configuration name cache
shared acp configuration nic-proxy-configuration name nic-host-selection
shared acp configuration nic-proxy-configuration name nic-host-selection blacklisting
shared acp configuration nic-proxy-configuration name resolution
shared acp configuration nic-proxy-configuration name test-nic-bindings
shared acp configuration nic-proxy-configuration name test-nic-bindings key-values
shared acp configuration redundancy
shared acp configuration scripts-and-classification
shared acp congestion-point-classifier rule
shared acp congestion-point-classifier rule name condition
shared acp congestion-point-classifier rule name script
shared acp group
shared admission-control device

shared admission-control device name interface
shared congestion-points congestion-point-profile
shared congestion-points profile
slot number acp
slot number acp initial
slot number acp initial directory-connection
slot number acp initial directory-eventing
Operational Commands
request acp reorganize-backup-database
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 device
show acp statistics directory
show acp statistics general

shared acp configuration acp-options

Syntax

```
shared acp configuration acp-options {
    backup-directory backup-directory;
    mode (edge | backbone | dual);
    event-cache-size event-cache-size;
    overload-method overload-method;
    reservation-timeout reservation-timeout;
    congestion-point-auto-completion;
    tuning-factor tuning-factor;
    subscriber-bandwidth-exceed-message subscriber-bandwidth-exceed-message;
    network-bandwidth-exceed-message network-bandwidth-exceed-message;
    backup-database-maximum-size backup-database-maximum-size;
    remote-update-database-index-keys remote-update-database-index-keys;
    interface-tracking-filter interface-tracking-filter;
    state-sync-bulk-size state-sync-bulk-size;
}
```

Hierarchy Level

[edit shared acp configuration acp-options]

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure SRC-ACP operation.

Options

backup-directory *backup-directory*— Folder that stores backup information about subscribers, services, and congestion points.

Value—Text

Default— var/backup

Editing Level—Expert

mode (edge | backbone | dual)— Regions of the network that SRC-ACP manages.

Value— One of the following regions:

- **edge**—SRC-ACP operates in the edge region of network only
- **backbone**—SRC-ACP operates in the backbone region of the network only
- **dual**—SRC-ACP operates in both the edge and backbone regions of network

Default— dual

Editing Level—Basic

`event-cache-size event-cache-size`— Number of plug-in events from the SAE that SRC-ACP can store in its cache. Specifying a large number increases the efficiency of SRC-ACP, and minimizes the use of CPU resources; however, the amount of memory available for the cache will depend on the host's resources.

Value—Integer in the range 0–2147483647

Default— 1000

Editing Level—Expert

`overload-method overload-method`— Specifies how SRC-ACP deals with situations where the components exceed the allocated bandwidth because the service was activated after the authorization was granted.

Value— Integer in the range -1–2147483647

- **-1**—SRC-ACP ignores overload
- Integer greater than or equal to 0—Bandwidth (in bps) by which the maximum may be exceeded

Default— 0

Editing Level—Basic

`reservation-timeout reservation-timeout`—(Optional) Time to wait until a bandwidth reservation expires. The reserved bandwidth is reclaimed by SRC-ACP when the reservation expires.

Value—Integer in the range 0–2147483647 ms

Default— 10000

Editing Level—Basic

`congestion-point-auto-completion`—(Optional) Specifies whether SRC-ACP uses the information acquired from the router to determine the congestion points.

Editing Level—Basic

`tuning-factor` *tuning-factor*—(Optional) Specifies factors that compensate for actual use of bandwidth, as opposed to allocated bandwidth.

Value— List of tuning factors, separated by commas; each tuning factor is a floating number in the range 0–1

Editing Level—Basic

`subscriber-bandwidth-exceed-message` *subscriber-bandwidth-exceed-message*— Error message that SRC-ACP sends when the subscriber exceeds the allocated bandwidth.

Value—Text

Default— Subscriber bandwidth exceeded

Editing Level—Basic

`network-bandwidth-exceed-message` *network-bandwidth-exceed-message*— Error message that SRC-ACP sends when traffic flow exceeds the allocated bandwidth on an interface between the subscriber and the router.

Value—Text

Default— Network bandwidth exceeded

Editing Level—Basic

`backup-database-maximum-size` *backup-database-maximum-size*— Value by which the sum of the sizes of the files that contain SRC-ACP data can increment before SRC-ACP reorganizes the files. Reorganizing the files reduces their size. Choose a value that is significantly lower than the capacity of the machine's hard disk.

Value— Text string in the format *numbem* or *numberg*

- *numbem*—Size of database in megabytes
- *numberg*—Size of database in gigabytes

Default— 100m

Editing Level—Basic

`remote-update-database-index-keys` *remote-update-database-index-keys*— Values to look for in the configuration data. Specifying index keys can improve performance by filtering the data. For information about the values you can specify, see the documentation that describes how to configure SRC-ACP operation.

Value— List of attributes, separated by commas

Default— interfaceName, routerName, portId

Editing Level—Basic

`interface-tracking-filter` *interface-tracking-filter*— A filter specifying the interfaces to be tracked by SRC-ACP. Filtering the interface tracking events can improve performance and can reduce the amount of memory required for keeping the congestion points updated. For information about the values you can specify, see the documentation that describes how to configure SRC-ACP operation.

Value— Filter strings in the format of a list of <attribute>=<value> pairs; that can be contained within query operations. For example: (&(interfaceName=*)(interfaceSpeed=1000000))

Editing Level—Basic

`state-sync-bulk-size` *state-sync-bulk-size*—(Optional) Number of events the SAE sends to SRC-ACP in a single method call during state synchronization.

Value—Integer in the range 1–1000

Default— 100

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared acp configuration corba

Syntax

```
shared acp configuration corba {
    acp-ior acp-ior;
    remote-update-ior remote-update-ior;
}
```

Hierarchy Level

```
[edit shared acp configuration corba]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure CORBA interfaces.

Options

acp-ior acp-ior— Object reference for SRC-ACP that is exported through either a local file or a Common Object Services (COS) naming service.

Value— One of the following references:

- *file://path*—Exports object reference through a local file where *path* is the absolute path to local file
- *corbaname::cosNameServer#KEY*—Exports object reference through COS naming services
 - *cosNameServer*—IP address or Domain Name System (DNS) name of COS naming server
 - *KEY*—Object reference of SRC-ACP
- *corbaname:rir#KEY*—Exports object reference through COS naming service; resolve-initial-references (rir) function finds DNS name of COS naming server

Default— *file:///var/acp/acp.ior*

Editing Level—Basic

remote-update-ior remote-update-ior—(Optional) Object reference for the SRC-ACP external interface.

Value— One of the following references:

- `file://path`—Exports object reference through a local file where *path* is the absolute path to local file
- `corbaname::cosNameServer#KEY`—Exports object reference through COS naming services
 - *cosNameServer*—IP address or Domain Name System (DNS) name of COS naming server
 - *KEY*—Object reference of SRC-ACP
- `corbaname:rir#KEY`—Exports object reference through COS naming service; resolve-initial-references (rir) function finds DNS name of COS naming server

Default— `file:///var/acp/sra.ior`

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared acp configuration ldap service-data

Syntax

```
shared acp configuration ldap service-data {
    edge-congestion-point-dn edge-congestion-point-dn;
    backbone-congestion-point-dn backbone-congestion-point-dn;
    reload-congestion-points;
    congestion-points-eventing;
    server-address server-address;
    server-port server-port;
    dn dn;
    principal principal;
    password password;
    event-dn event-dn;
    directory-eventing;
    polling-interval polling-interval;
    secured-ldap-protocol (ldaps);
}
```

Hierarchy Level

```
[edit shared acp configuration ldap service-data]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure SRC-ACP connection to the directory that stores information about services.

Options

edge-congestion-point-dn edge-congestion-point-dn— DN of the directory that contains information about network interfaces for edge congestion points.

Value— DN

Default— o=AdmissionControl, o=umc

Editing Level—Expert

backbone-congestion-point-dn backbone-congestion-point-dn— DN of the directory that contains information about network interfaces for backbone congestion point objects.

Value— DN

Default— o=CongestionPoints, o=umc

Editing Level—Expert

`reload-congestion-points`—(Optional) Specifies whether SRC-ACP detects changes in the backbone congestion point for a service while SRC-ACP is operative.

Enable only when you want to modify a congestion point. Disable when you have modified the congestion point.

Editing Level—Basic

`congestion-points-eventing`—(Optional) Enables directory eventing for congestion points.

Editing Level—Basic

`server-address server-address`— List of primary and redundant servers that manage data.

Value— List of IP addresses or hostnames separated by spaces

Default— 127.0.0.1

Editing Level—Normal

`server-port server-port`— TCP port for the directory.

Value—Integer in the range 0–65535

Default— 389

Editing Level—Normal

`dn dn`— DN of the root of the directory.

Value— List of attribute = value pairs separated by commas

Editing Level—Advanced

`principal principal`— DN used to authorize connections to the directory.

Value— List of attribute = value pairs separated by commas

Default— cn=umcadmin, o=umc

Editing Level—Advanced

`password password`— Password used to authorize connections to the directory.

Value—Secret text
Default— admin123
Editing Level—Advanced

`event-dn` *event-dn*— DN of the directory that contains event information.

Value— DN
Editing Level—Expert

`directory-eventing`—(Optional) Enable directory eventing.

Editing Level—Advanced

`polling-interval` *polling-interval*— Time interval at which the SRC component polls the directory.

Value— Number of seconds in the range 15–86400
Default— 30
Editing Level—Advanced

`secured-ldap-protocol` (*ldaps*)—(Optional) Secured LDAP protocol

Value

- *ldaps*—

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Normal

shared acp configuration ldap subscriber-data

Syntax

```
shared acp configuration ldap subscriber-data {
    congestion-points-eventing;
    server-address server-address;
    server-port server-port;
    dn dn;
    principal principal;
    password password;
    event-dn event-dn;
    directory-eventing;
    polling-interval polling-interval;
    secured-ldap-protocol (ldaps);
}
```

Hierarchy Level

```
[edit shared acp configuration ldap subscriber-data]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure SRC-ACP connection to the directory that stores subscriber information.

Options

congestion-points-eventing—(Optional) Enables directory eventing for congestion points.

Editing Level—Basic

server-address server-address— List of primary and redundant servers that manage data.

Value— List of IP addresses or hostnames separated by spaces

Default— 127.0.0.1

Editing Level—Normal

server-port server-port— TCP port for the directory.

Value—Integer in the range 0–65535

Default— 389

Editing Level—Normal

`dn dn`— DN of the root of the directory.

Value— List of attribute = value pairs separated by commas

Editing Level—Advanced

`principal principal`— DN used to authorize connections to the directory.

Value— List of attribute = value pairs separated by commas

Default— cn=umcadmin, o=umc

Editing Level—Advanced

`password password`— Password used to authorize connections to the directory.

Value—Secret text

Default— admin123

Editing Level—Advanced

`event-dn event-dn`— DN of the directory that contains event information.

Value— DN

Editing Level—Expert

`directory-eventing`—(Optional) Enable directory eventing.

Editing Level—Advanced

`polling-interval polling-interval`— Time interval at which the SRC component polls the directory.

Value— Number of seconds in the range 15–86400

Default— 30

Editing Level—Advanced

`secured-ldap-protocol (ldaps)`—(Optional) Secured LDAP protocol

Value

- `ldaps—`

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Normal

shared acp configuration logger

Syntax

```
shared acp configuration logger name ...
```

Hierarchy Level

```
[edit shared acp configuration logger]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the logging destination.

Options

name name— Name of logging destination.

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared acp configuration logger *name* file

Syntax

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

Hierarchy Level

```
[edit shared acp configuration logger name file]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure logging of messages to a file.

filter filter—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

Editing Level—Basic

filename filename— Absolute path of the filename that contains the current logs.

Note: 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.

Value— Filename

Default— No value

Editing Level—Basic

rollover-filename rollover-filename—(Optional) 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— Path of filename

Example—/opt/UMC/sae/var/log/sae.alt

Default— The default value is different for each type of component.

Editing Level—Normal

`maximum-file-size` *maximum-file-size*—(Optional) Maximum size of the log file and the rollover file.

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

Value—Integer in the range 0–2147483647 kbytes

Default— 1000000

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared acp configuration logger *name* syslog

Syntax

```
shared acp configuration logger name syslog {
    filter filter;
    host host;
    facility facility;
    format format;
}
```

Hierarchy Level

```
[edit shared acp configuration logger name syslog]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure logging of messages to system logging.

filter filter—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default—/error-

Editing Level—Basic

host host— IP address or name of a host that collects event messages by means of a standard system logging daemon.

Value— IP address or hostname

Default—loghost

Editing Level—Basic

facility facility—(Optional) Type of system log in accordance with the system logging protocol.

Value—Integer in the range 0–23

Default— 3

Editing Level—Advanced

format format—(Optional) MessageFormat string that specifies how the information in an event message is printed. (The strings {#} are replaced with the log information [...]).

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

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Basic

shared acp configuration nic-proxy-configuration

Syntax

```
shared acp configuration nic-proxy-configuration name {  
}
```

Hierarchy Level

```
[edit shared acp configuration nic-proxy-configuration]
```

Options

name name—

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared acp configuration nic-proxy-configuration *name* cache

Syntax

```
shared acp configuration nic-proxy-configuration name cache {
    cache-size cache-size;
    cache-cleanup-interval cache-cleanup-interval;
    cache-entry-age cache-entry-age;
}
```

Hierarchy Level

```
[edit shared acp configuration nic-proxy-configuration name cache]
```

Description

Configure the NIC proxy cache properties. You can modify cache properties for the NIC proxy to optimize the resolution performance for your network configuration and system resources. Typically, you can use the default settings for the cache properties.

cache-size cache-size—(Optional) Maximum size of the cache in which the NIC proxy retains data. If you decrease the cache size or disable the cache while the NIC proxy is running, the NIC proxy removes entries in order of descending age until the cache size meets the new limit.

Value— Integer in the range 0–2147483647

Default—10000

Editing Level—Advanced

cache-cleanup-interval cache-cleanup-interval— Time interval at which the NIC proxy removes expired entries from its cache.

Value— Number of seconds in the range 5–2147483

Default—15

Editing Level—Advanced

cache-entry-age cache-entry-age—(Optional) Maximum time that the NIC proxy can cache an entry. The NIC proxy compares this property with the life expectancy of each entry and uses the lower value to determine when to remove the entry.

Value— Number of seconds in the range 0–4294967295

- 0 or unspecified—Life expectancy of the data, which determines expiration of data
- Other values—Actual time that the NIC proxy caches entries

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Advanced

shared acp configuration nic-proxy-configuration *name* nic-host-selection

Syntax

```
shared acp configuration nic-proxy-configuration name nic-host-selection {
    groups [groups...];
    selection-criteria (roundRobin | randomPick | priorityList);
}
```

Hierarchy Level

```
[edit shared acp configuration nic-proxy-configuration name nic-host-selection]
```

Description

Configure the mechanism that a NIC proxy uses to select NIC system if multiple systems are available. You use NIC host selection when you use NIC replication.

groups [*groups...*]—(Optional) List of groups of NIC hosts that the NIC proxy can contact for resolution requests.

Value— Names of groups.

Default— No value

Editing Level—Advanced

selection-criteria (roundRobin | randomPick | priorityList)— Selection criteria that the NIC proxy uses to determine which NIC host to contact. Configure selection criteria if you configure more than one group.

Value— One of the following criteria:

- roundRobin—NIC proxy selects NIC hosts in a fixed, cyclic order. The NIC proxy always selects the next host in the list.
- randomPick—NIC proxy selects NIC hosts randomly from the list.
- priorityList—NIC proxy selects NIC hosts according to their assigned priorities in the list. If the host with the highest priority in the list is not available, the NIC proxy tries the host with the next-highest priority, and so on.

Use round-robin or random pick to distribute resolution requests among NIC hosts. Use priority list if you prefer to use a particular NIC host; for example, you may reduce operating cost by using a local NIC host.

Default— roundRobin

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Advanced

shared acp configuration nic-proxy-configuration *name* nic-host-selection blacklisting

Syntax

```
shared acp configuration nic-proxy-configuration name nic-host-
selection blacklisting {
    try-next-system-on-error;
    number-of-retries-before-blacklisting number-of-retries-before-blacklisting;
    blacklist-retry-interval blacklist-retry-interval;
}
```

Hierarchy Level

```
[edit shared acp configuration nic-proxy-configuration name nic-host-
selection blacklisting]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure how to handle nonresponsive NIC hosts. When a NIC host does not respond, it is blacklisted which means that other NIC hosts are contacted until the blacklisted host becomes available again.

Options

try-next-system-on-error—(Optional) Specifies whether or not the NIC proxy should contact the next specified NIC host if a NIC host is determined to be unavailable. Configure this property only if you configure more than one group.

Default—true

Editing Level—Advanced

number-of-retries-before-blacklisting *number-of-retries-before-blacklisting*— Number of times the NIC proxy tries to communicate with a NIC host before the NIC proxy stops communicating with the NIC host for a period of time.

Value—Integer in the range 0–2147483647

Default—3

Editing Level—Advanced

blacklist-retry-interval *blacklist-retry-interval*— Interval at which the

NIC proxy attempts to connect to an unavailable NIC host.

Value—Integer in the range 15–2147483647 s
Default—15
Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Basic

shared acp configuration nic-proxy-configuration *name* resolution

Syntax

```
shared acp configuration nic-proxy-configuration name resolution {
    resolver-name resolver-name;
    key-type key-type;
    value-type value-type;
    expect-multiple-values;
    constraints constraints;
}
```

Hierarchy Level

```
[edit shared acp configuration nic-proxy-configuration name resolution]
```

Description

Configure properties for a NIC proxy (NIC locator), the NIC component that requests information on behalf of an application.

resolver-name resolver-name— NIC resolver that the NIC proxy uses. This resolver must be the same as one that is configured on the NIC host.

Value— Path to the NIC resolver.

Example—/realms/ip/A1,/realms/dn/A1.

Default— No value

Editing Level—Basic

key-type key-type— Type of data used that the key provides for the NIC resolution. You can provide a qualifier to a data type to distinguish between different instances of a data type in a resolution scenario, or to provide information about a data type to clarify the use of that data type in a resolution.

Value— One of the following types:

- Ip —Subscriber's IP address
- Vr—Virtual router
- Interface—Name of router's interface
- InterfaceId—Identifier of an interface on the router
- Dn—LDAP distinguished name for subscriber
- LoginName—Subscriber login ID
- AnyString—Other information

To qualify data types, enter a qualifier within parentheses.

Example—LoginName(username).

Default— No value

Editing Level—Basic

value-type value-type— Type of value to be returned in the resolution. The value type varies according to the application that uses the NIC proxy.

Value— One of the following types:

- SaelId—SAE server ID
- LoginName—Subscriber login ID
- AnyString—Other information

To qualify data types, enter a qualifier within parentheses.

Example—LoginName(username).

Default— No value

Editing Level—Basic

expect-multiple-values—(Optional) Specifies whether or not the key can have multiple corresponding values.

Editing Level—Basic

constraints constraints—(Optional) Data type that a resolver uses during the resolution process. A constraint represents a condition that must or may be satisfied before the next stage of the resolution process can proceed.

Configure a constraint only if the constraint will be provided by the application in the resolution request. Typically, you do not need to configure constraints.

Value— Data types of constraints specified for the NIC resolution.

Separate data types with commas.

Default— No value

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Normal

shared acp configuration nic-proxy-configuration *name* test-nic-bindings

Syntax

```
shared acp configuration nic-proxy-configuration name test-nic-bindings {
    use-test-bindings;
}
```

Hierarchy Level

```
[edit shared acp configuration nic-proxy-configuration name test-nic-bindings]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure key-value mappings to be used to test a NIC resolution.

Options

`use-test-bindings`—(Optional) Test the NIC resolutions without having to configure or run a NIC host. The values returned are those configured in the key-values property.

Default—false

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared acp configuration nic-proxy-configuration *name* test-nic-bindings key-values

Syntax

```
shared acp configuration nic-proxy-configuration name test-nic-bindings key-
values name {
    value;
}
```

Hierarchy Level

```
[edit shared acp configuration nic-proxy-configuration name test-nic-bindings key-
values]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure keys and associated values to use for testing. Define all of values to be returned for specified keys.

Options

name *name*—

Value—Text

value—

Value—Text

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Advanced

shared acp configuration redundancy

Syntax

```
shared acp configuration redundancy {
    enable-redundancy;
    local-ior local-ior;
    remote-ior remote-ior;
    ignore-user-tracking-out-of-sync;
    community-heartbeat community-heartbeat;
    community-acquire-timeout community-acquire-timeout;
    community-blackout-timeout community-blackout-timeout;
    redundant-naming-service redundant-naming-service;
}
```

Hierarchy Level

```
[edit shared acp configuration redundancy]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure redundancy and state synchronization for SRC-ACP.

Options

`enable-redundancy`—(Optional) Enables SRC-ACP redundancy.

Editing Level—Basic

`local-ior local-ior`— In a redundant SRC-ACP configuration, exports the object reference for this SRC-ACP (local interface) through a Common Object Services (COS) naming service.

Value— One of the following references:

- `corbaname::cosNameServer#KEY`—Exports object reference through COS naming services
 - `cosNameServer`—IP address or Domain Name System (DNS) name of COS naming server
 - `KEY`—Object reference of SRC-ACP
- `corbaname:rir#KEY`—Exports object reference through COS naming service; resolve-initial-references (rir) function finds DNS

name of COS naming server

For example: corbaname::coshost#acp.redundancy.primary

Editing Level—Basic

`remote-ior remote-ior`— In a redundant SRC-ACP configuration, resolves the object reference for the other SRC-ACP (remote interface) through a Common Object Services (COS) naming service. For redundancy, the remote IOR value of one SRC-ACP must match the local IOR value of the other SRC-ACP.

Value— One of the following references:

- corbaname::cosNameServer#KEY—Exports object reference through COS naming services
 - cosNameServer—IP address or Domain Name System (DNS) name of COS naming server
 - KEY—Object reference of SRC-ACP
- corbaname:rir#KEY—Exports object reference through COS naming service; resolve-initial-references (rir) function finds DNS name of COS naming server

For example: corbaname::coshost#acp.redundancy.backup

Editing Level—Basic

`ignore-user-tracking-out-of-sync`—(Optional) Specifies whether user tracking events should be ignored when they raise an OutOfSync exception to the SAE when state synchronization is enabled. SRC-ACP raises an OutOfSync exception when SRC-ACP handles service tracking or authentication events without receiving a user start event first.

Default— false

Editing Level—Basic

`community-heartbeat community-heartbeat`—(Optional) Time interval for community members to check each other's availability when both redundancy and state synchronization are enabled.

Value—Integer in the range 0–2147483647 s

Default— 30

Editing Level—Basic

`community-acquire-timeout community-acquire-timeout`—(Optional) Time to wait before trying to reacquire the distributed lock when both redundancy and state synchronization are enabled.

Value—Integer in the range 0–2147483647 s

Default— 15

Editing Level—Basic

`community-blackout-timeout` *community-blackout-timeout*—(Optional) Time to wait before regaining control when both redundancy and state synchronization are enabled.

Value—Integer in the range 0–2147483647 s

Default— 30

Editing Level—Basic

`redundant-naming-service` *redundant-naming-service*—(Optional) In a redundant SRC-ACP configuration, exports the object reference for the backup naming service through a local file or COS naming service. The primary SRC-ACP registers the IOR and redundancy IOR to both naming services, while the secondary SRC-ACP registers the redundancy IOR to both naming services.

Value— One of the following references:

- `file://path`—Exports object reference through a local file where *path* is the absolute path to local file
- `corbaname::cosNameServer#KEY`—Exports object reference through COS naming services
 - *cosNameServer*—IP address or Domain Name System (DNS) name of COS naming server
 - *KEY*—Object reference of SRC-ACP
- `corbaname:rir#KEY`—Exports object reference through COS naming service; resolve-initial-references (rir) function finds DNS name of COS naming server

Default— None

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared acp configuration scripts-and-classification

Syntax

```
shared acp configuration scripts-and-classification {
    script-factory-class script-factory-class;
    classification-factory-class classification-factory-class;
    classification-script classification-script;
    congestion-point-profile-script congestion-point-profile-script;
    extension-path extension-path;
}
```

Hierarchy Level

```
[edit shared acp configuration scripts-and-classification]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure SRC-ACP scripts and classification.

Options

`script-factory-class script-factory-class`— Script factory class name.

Value—Text

Default— net.juniper.smgmt.acp.classify.ScriptFactory

Editing Level—Expert

`classification-factory-class classification-factory-class`— Congestion point classifier factory class name.

Value—Text

Default— net.juniper.smgmt.acp.classify.ClassifyCPFactory

Editing Level—Expert

`classification-script classification-script`— Class name for congestion point classification.

Value—Text

Default— cpClassify

Editing Level—Expert

`congestion-point-profile-script` *congestion-point-profile-script*—
Class name for generating the congestion point DN by using the congestion point profile.

Value—Text
Default— cpProfile
Editing Level—Expert

`extension-path` *extension-path*— Extension class path for classes not located in the /
opt/UMC/acp/lib directory.

Value—Text
Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Advanced

shared acp congestion-point-classifier rule

Syntax

```
shared acp congestion-point-classifier rule name {
    target target;
}
```

Hierarchy Level

```
[edit shared acp congestion-point-classifier rule]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure a congestion point classification script.

Options

name name— Name of a congestion point classification script.

Value—Text

target target—(Optional) Result of the classification script. The result is the DN of a congestion point in the directory or an LDAP query that uniquely identifies a congestion point entry in the directory.

Value—Text

Editing Level—Basic

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

shared acp congestion-point-classifier rule *name* condition

Syntax

```
shared acp congestion-point-classifier rule name condition criteria ...
```

Hierarchy Level

```
[edit shared acp congestion-point-classifier rule name condition]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure classification criteria that is used to find a target.

Options

criteria criteria— Classification criteria. For information about configuring classification criteria, see *Classifying Congestion Points* in the *SRC PE Network Guide*.

Value— Classification criteria are organized by putting one criterion per line. A criterion is joined with the previous criterion by:

- OR if the line does not contain a prefix or if it is prefixed with a | (pipe) character. A criterion joined by OR is examined only if the previous conditions have not produced a positive match. If any of the criteria joined by OR matches, the target is selected.
- AND if the line is prefixed with an & (ampersand) character. A criterion joined by AND is examined only if the previous condition matches.

You can use glob or regular expression matching to configure each target's criteria.

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

shared acp congestion-point-classifier rule *name* script

Syntax

```
shared acp congestion-point-classifier rule name script {
    script-value;
    include include;
}
```

Hierarchy Level

```
[edit shared acp congestion-point-classifier rule name script]
```

Release Information

Statement introduced in SRC Release 1.0.0

Options

script-value—(Optional) Script target. A script that can contain definitions of custom functions that can be called during the matching process. The complete content of the script is interpreted when the classifier is initially loaded. Because you can insert code into a script target, you can use the classification script to perform various tasks.

Value— Script enclosed in quotation marks.

Default— No value

Editing Level—Basic

include include—(Optional) Script reference

Value—Text

Editing Level—Basic

Required Privilege Level

No specific privilege required.

Required Editing Level

Basic

shared acp group

Syntax

```
shared acp group name ...
```

Hierarchy Level

```
[edit shared acp group]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure group of SRC-ACP configuration properties.

Options

name name— Name of an SRC-ACP configuration.

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared admission-control device

Syntax

```
shared admission-control device name {
    description description;
}
```

Hierarchy Level

```
[edit shared admission-control device]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the locations of congestion points in the directory.

Options

name name— Network device name.

Value—Text

description description—(Optional) Network device description.

Value—Text

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared admission-control device *name* interface

Syntax

```
shared admission-control device name interface name {
    description description;
    upstream-provisioned-rate upstream-provisioned-rate;
    downstream-provisioned-rate downstream-provisioned-rate;
    upstream-background-bandwidth [upstream-background-bandwidth...];
    downstream-background-bandwidth [downstream-background-bandwidth...];
    action-type (url | python | java-class | java-archive);
    action-class-name action-class-name;
    action-file-url action-file-url;
    action-parameters [action-parameters...];
    action-file-name action-file-name;
    detect-link-rate;
}
```

Hierarchy Level

```
[edit shared admission-control device name interface]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure the network interfaces that represent locations of congestion points in the directory.

Options

name *name*— Interface name.

Value—Text

description *description*—(Optional) Network interface description.

Value—Text

Editing Level—Basic

upstream-provisioned-rate *upstream-provisioned-rate*—(Optional) Upstream provisioned rate.

Value—Integer in the range 0–9223372036854775807 bps
Editing Level—Basic

`downstream-provisioned-rate` *downstream-provisioned-rate*—(Optional)
 Downstream provisioned rate.

Value—Integer in the range 0–9223372036854775807 bps
Editing Level—Basic

`upstream-background-bandwidth` [*upstream-background-bandwidth...*]—
 (Optional) Upstream background bandwidth.

Value—Integer in the range 0–9223372036854775807 bps
Editing Level—Basic

`downstream-background-bandwidth` [*downstream-background-bandwidth...*]
 —(Optional) Downstream background bandwidth.

Value—Integer in the range 0–9223372036854775807 bps
Editing Level—Basic

`action-type` (`url` | `python` | `java-class` | `java-archive`)—(Optional) Type
 of action congestion point. Determines how the contents of the "action-file-url" attribute will be
 interpreted.

Value

- `url`— The value of attribute "action-file-url" is a URL that specifies where to find a Java archive (.jar file) containing the script service implementation.
- `python`— The value of attribute "action-file-url" is Python code.
- `java-class`— The value of attribute "action-file-url" is the binary contents of a compiled Java class file (.class file).
- `java-archive`— The value of attribute "action-file-url" is the binary contents of a Java archive file (.jar file).

Editing Level—Basic

`action-class-name` *action-class-name*—(Optional) Name of Java or Python class
 implementing the action congestion point. The ACP instantiates the named class.

Value—Text
Editing Level—Basic

`action-file-url` *action-file-url*—(Optional) If the action type is "URL", this attribute contains the URL of a Java archive (.jar) file containing the action congestion point implementation. Otherwise, this attribute contains the action congestion point implementation itself (i.e. python code, the binary contents of a compiled .class file, or the binary contents of a .jar file).

Editing Level—Basic

`action-parameters` [*action-parameters...*]—(Optional) Parameters used by the action congestion point.

Value—Text string in the format of a list of <attribute> = <value> pairs

Editing Level—Basic

`action-file-name` *action-file-name*—(Optional) The file needs to exist locally. Its content will be read and loaded into the "action-file-url" attribute.

Value—Text

Editing Level—Basic

`detect-link-rate`—(Optional) To identify the possibility of getting the actual link rate information for a congestion point via L2C or other solutions developed later. By default , it is false for the sake of backward compatibility.

Default—false

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared congestion-points congestion-point-profile

Syntax

```
shared congestion-points congestion-point-profile name {
    expression [expression...];
}
```

Hierarchy Level

```
[edit shared congestion-points congestion-point-profile]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure congestion point profile.

Options

name *name*— Congestion point profile name.

Value—Text

expression [*expression...*]—(Optional) Congestion point expression.

Value—Text

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

shared congestion-points profile

Syntax

```
shared congestion-points profile name {
    interface [interface...];
}
```

Hierarchy Level

```
[edit shared congestion-points profile]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure congestion point.

Options

name name— Congestion point name.

Value—Text

interface [interface...]—(Optional) Congestion point reference.

Value—Text

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

slot *number* acp

Syntax

```
slot number acp {
    java-runtime-environment java-runtime-environment;
    java-heap-size java-heap-size;
    java-garbage-collection-options java-garbage-collection-options;
    base-dn base-dn;
    snmp-agent;
    shared shared;
}
```

Hierarchy Level

```
[edit slot number acp]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure local properties for SRC-ACP.

Options

`java-runtime-environment java-runtime-environment`— Path to the Java Runtime Environment (JRE). The SRC software requires a JRE that conforms to the Java 2 specification.

Value—Text
Default— `../jre/bin/java`
Editing Level—Expert

`java-heap-size java-heap-size`— Maximum amount of Java heap (memory) available to the JRE.

Value— Number of megabytes in the format *integern*
Default— 64m
Editing Level—Advanced

`java-garbage-collection-options java-garbage-collection-options`— Garbage collection functionality of the Java Virtual Machine.

Value—

Default— -Xbatch -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=80 -XX:NewRatio=5 -XX:+UseParNewGC -XX:SurvivorRatio=1 -XX:InitialTenuringThreshold=8 -XX:MaxTenuringThreshold=10 -XX:TargetSurvivorRatio=90 -XX:+UseCMSCompactAtFullCollection -XX:CMSFullGCsBeforeCompaction=0 -XX:+CMSClassUnloadingEnabled -XX:+CMSParallelRemarkEnabled

Editing Level—Advanced

`base-dn` *base-dn*— DN of the root of the SDX data in the directory.

If you are storing non-SDX data in the directory, and that data changes frequently whereas the SDX data does not, you may need to adjust the default value to improve performance. For optimal performance, set the value to the DN of an entry superior to both the SDX data and the changing non-SDX data.

Value— DN

Editing Level—Advanced

`snmp-agent`—(Optional) Enables SRC-ACP to communicate with the SNMP agent.

Editing Level—Basic

`shared` *shared*— Shared configuration object that holds most of the SRC-ACP specific configuration.

Value— Name of the object in the format "`/<path>`". If the `<path>` contains multiple levels, the levels are separated by a slash (`/`). The effective configuration is combined by all configuration objects in the path, with more specific configuration in the lower levels of the path.

Default— `/config`

Editing Level—Basic

Required Privilege Level

system

Required Editing Level

Basic

slot *number* acp initial

Syntax

```
slot number acp initial {
    static-dn static-dn;
    dynamic-dn dynamic-dn;
}
```

Hierarchy Level

```
[edit slot number acp initial]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Configure initial properties for SRC components.

Options

static-dn static-dn—(Optional) Location of administrator-defined configuration data in the directory.

Value—Text

Default—ou=staticConfiguration,ou=Configuration,o=Management,o=umc

Editing Level—Expert

dynamic-dn dynamic-dn—(Optional) Location of programmatically-defined configuration data in the directory.

Value—Text

Default—ou=dynamicConfiguration,ou=Configuration,o=Management,
o=umc

Editing Level—Expert

Required Privilege Level

system

Required Editing Level

Basic

slot *number* acp initial directory-connection

Syntax

```
slot number acp initial directory-connection {
    url url;
    backup-urls [backup-urls...];
    principal principal;
    credentials credentials;
    protocol (ldaps);
    timeout timeout;
    check-interval check-interval;
    blacklist;
    snmp-agent;
}
```

Hierarchy Level

```
[edit slot number acp initial directory-connection]
```

Description

Configure properties for the directory connection.

Options

url url—(Optional) URL that identifies the location of the primary directory server.

Value— URL

Default—ldap://127.0.0.1:389

Editing Level—Basic

backup-urls [backup-urls...]—(Optional) URLs that identify the locations of backup directory servers. Backup servers are used if the primary directory server is not accessible.

Value— List of URLs

Editing Level—Basic

principal principal— DN that the SRC component uses for authentication to access the directory.

Value— DN.

When you specify the DN, you can use <base> to indicate the base DN.

Editing Level—Basic

`credentials credentials`— Password with which the SRC component accesses the directory.

Value— Password

Editing Level—Basic

`protocol (ldaps)`—(Optional) Security protocol used to connect to the directory. If you do not configure a security protocol, plain socket is used.

Value

- `ldaps`— LDAPS which uses SSL.

Editing Level—Expert

`timeout timeout`—(Optional) Maximum amount of time during which the directory must respond to a connection request.

Value— Integer in the range 1–2147483647 s

Default—10

Editing Level—Expert

`check-interval check-interval`—(Optional) Time interval at which the directory monitoring system verifies its connection to the directory. If the directory connection fails after this interval, the directory monitoring system initiates a connection to another directory.

Value— Integer in the range 15–2147483647 s

Default—60

Editing Level—Expert

`blacklist`—(Optional) Specifies whether the directory monitoring system prevents connection to a directory if the directory fails to respond during 10 polling intervals.

Default—false

Editing Level—Basic

`snmp-agent`—(Optional) Specifies whether the SDX SNMP agent exports MIBs for this directory connection.

Default—false
Editing Level—Expert

Required Privilege Level

system

Required Editing Level

Basic

slot *number* acp initial directory-eventing

Syntax

```
slot number acp initial directory-eventing {
    eventing;
    signature-dn signature-dn;
    polling-interval polling-interval;
    event-base-dn event-base-dn;
    dispatcher-pool-size dispatcher-pool-size;
}
```

Hierarchy Level

```
[edit slot number acp initial directory-eventing]
```

Release Information

Statement introduced in SRC Release 1.0.0

Description

Change configuration for directory eventing properties. In most cases, you can use the default configuration for these properties.

Options

eventing—(Optional) Enable an SRC component to poll the directory for changes.

Default—true

Editing Level—Normal

signature-dn *signature-dn*—(Optional) DN of the directory entry that specifies the usedDirectory attribute for the SRC CLI. The usedDirectory attribute identifies the vendor of the directory server.

Value— DN

Default—o=umc

Editing Level—Expert

polling-interval *polling-interval*—(Optional) Interval at which an SRC component polls the directory to check for directory changes.

Value—Integer in the range 15–2147483647 s

Default—30
Editing Level—Normal

`event-base-dn` *event-base-dn*—(Optional)

DN of an entry superior to the data associated with an SRC component in the directory.

If you are storing non-SRC data in the directory, and that data changes frequently whereas the SRC data does not, you may need to adjust the default value to improve performance. For optimal performance, set the value to the DN of an entry superior to both the SRC data and the changing non-SRC data.

Value—DN
Default—o=UMC
Editing Level—Expert

`dispatcher-pool-size` *dispatcher-pool-size*—(Optional) Number of directory change notifications that can be sent simultaneously to the SRC component.

Value—Integer in the range 0–2147483647
Default—1
Editing Level—Expert

Required Privilege Level

system

Required Editing Level

Basic

request acp reorganize-backup-database

Syntax

```
request acp reorganize-backup-database <slot slot>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Reorganize the files that contain SRC-ACP data about subscribers, services, and congestion points. This action reduces the sizes of these files.

Options

`slot slot`—(Optional) Number of the slot for which you want to configure values.

Value— Currently, the chassis has only one slot. The valid value is 0.

Default—0

Required Privilege Level

maintenance

show acp backbone congestion-point congestion-point-expression

Syntax

```
show acp backbone congestion-point congestion-point-expression <slot slot>
<virtual-router-name virtual-router-name> <service-name service-name> <interface-
name interface-name> <interface-description interface-description> <interface-
alias interface-alias> <nas-port-id nas-port-id> < (brief) >
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display congestion point by service congestion point expression.

Options

slot slot—(Optional) Number of the slot for which you want to configure values.

Value— Currently, the chassis has only one slot. The valid value is 0.

Default—0

virtual-router-name virtual-router-name—(Optional) Name of virtual router from which to list congestion points.

Value— Virtual router name

Default— No value

service-name service-name—(Optional) Name of service used by backbone service to generate congestion points.

Value— Service name

Default— No value

interface-name interface-name—(Optional) Name of interface related to congestion points.

Value— Interface name

Default— No value

`interface-description` *interface-description*—(Optional) Description of interface used by backbone service to generate congestion points.

Value— Interface description
Default— No value

`interface-alias` *interface-alias*—(Optional) Interface alias used by backbone service to generate congestion points.

Value— Interface alias
Default— No value

`nas-port-id` *nas-port-id*—(Optional) Interface NAS port ID used by backbone service to generate congestion points.

Value— NAS port ID
Default— No value

(Optional) Output style.

Value

- `brief`— Display congestion point attributes.

Default—detail

Required Privilege Level

view

show acp backbone congestion-point dn

Syntax

```
show acp backbone congestion-point dn <slot slot> <congestion-point-dn congestion-point-dn> <virtual-router-name virtual-router-name> < (brief) >
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display congestion point by DN.

Options

`slot slot`—(Optional) Number of the slot for which you want to configure values.

Value— Currently, the chassis has only one slot. The valid value is 0.

Default—0

`congestion-point-dn congestion-point-dn`—(Optional) DN of congestion point for which you want to list all matching congestion points.

Value— All or part of the congestion point DN.

Default— No value

`virtual-router-name virtual-router-name`—(Optional) Name of virtual router from which to list congestion points.

Value— Virtual router name

Default— No value

(Optional) Output style.

Value

- `brief`— Display congestion point DN.

Default—detail

Required Privilege Level

view

show acp backbone service

Syntax

```
show acp backbone service <slot slot> <virtual-router-name virtual-router-name>
<service-name service-name> < (brief) >
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display information about services that SRC-ACP manages in the backbone network.

Options

`slot slot`—(Optional) Number of the slot for which you want to configure values.

Value— Currently, the chassis has only one slot. The valid value is 0.

Default—0

`virtual-router-name virtual-router-name`—(Optional) Name of virtual router from which to list backbone services.

Value— Virtual router name

Default— No value

`service-name service-name`—(Optional) Name of service used by backbone service to generate congestion points.

Value— Service name

Default— No value

(Optional) Output style.

Value

- `brief`— Display backbone service attributes.

Default—detail

Required Privilege Level

view

show acp edge congestion-point dn

Syntax

```
show acp edge congestion-point dn <slot slot> <congestion-point-dn congestion-  
point-dn> <instance-id instance-id> <virtual-router-name virtual-router-name> <  
(brief) > <maximum-results maximum-results>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display congestion point by DN.

Options

`slot slot`—(Optional) Number of the slot for which you want to configure values.

Value— Currently, the chassis has only one slot. The valid value is 0.

Default—0

`congestion-point-dn congestion-point-dn`—(Optional) DN of congestion point for which you want to list all matching congestion points.

Value— All or part of the congestion point DN.

Default— No value

`instance-id instance-id`—(Optional) Name of an instance generated for a congestion point that is automatically created.

Value— All or part of the congestion point instance ID.

Default— No value

`virtual-router-name virtual-router-name`—(Optional) Name of virtual router from which to list congestion points.

Value— Virtual router name

Default— No value

(Optional) Output style.

Value

- **brief**— Display congestion point DN.

Default—detail

maximum-results *maximum-results*—(Optional) Number of results to be displayed.

Value—Integer in the range 1–2147483647

Default— 25

Required Privilege Level

view

show acp edge congestion-point subscriber-session-id

Syntax

```
show acp edge congestion-point subscriber-session-id <slot slot> <session-id
session-id> <virtual-router-name virtual-router-name> < (brief) > <maximum-
results maximum-results>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display congestion point by subscriber session ID.

Options

`slot slot`—(Optional) Number of the slot for which you want to configure values.

Value— Currently, the chassis has only one slot. The valid value is 0.

Default—0

`session-id session-id`—(Optional) Subscriber session ID for which you want to list all matching congestion points.

Value— All or part of the subscriber session ID.

Default— No value

`virtual-router-name virtual-router-name`—(Optional) Name of virtual router from which to list congestion points.

Value— Virtual router name

Default— No value

(Optional) Output style.

Value

- `brief`— Display congestion point attributes.

Default—detail

`maximum-results` *maximum-results*—(Optional) Number of results to be displayed.

Value—Integer in the range 1–2147483647

Default— 25

Required Privilege Level

view

show acp edge subscriber

Syntax

```
show acp edge subscriber <slot slot> <virtual-router-name virtual-router-name>
<session-id session-id> < (brief) >
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display subscriber sessions in the edge network.

Options

`slot slot`—(Optional) Number of the slot for which you want to configure values.

Value— Currently, the chassis has only one slot. The valid value is 0.

Default—0

`virtual-router-name virtual-router-name`—(Optional) Name of virtual router from which to list subscriber sessions.

Value— Virtual router name

Default— No value

`session-id session-id`—(Optional) Subscriber session ID for which you want to list all matching subscriber sessions.

Value— All or part of the subscriber session ID.

Default— No value

(Optional) Output style.

Value

- `brief`— Display subscriber session attributes.

Default—detail

Required Privilege Level

view

show acp remote-update congestion-point dn

Syntax

```
show acp remote-update congestion-point dn <slot slot> <congestion-point-dn
congestion-point-dn> < (brief) >
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display congestion point by DN.

Options

slot slot—(Optional) Number of the slot for which you want to configure values.

Value— Currently, the chassis has only one slot. The valid value is 0.

Default—0

congestion-point-dn congestion-point-dn—(Optional) DN of congestion point for which you want to list all matching congestion points.

Value— All or part of the congestion point DN.

Default— No value

(Optional) Output style.

Value

- *brief*— Display congestion point DN.

Default—detail

Required Privilege Level

view

show acp remote-update congestion-point name

Syntax

```
show acp remote-update congestion-point name <slot slot> <device-name device-name> <interface-name interface-name> < (brief) >
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display congestion point by interface name.

Options

slot slot—(Optional) Number of the slot for which you want to configure values.

Value— Currently, the chassis has only one slot. The valid value is 0.

Default—0

device-name device-name—(Optional) Device name of the congestion point.

Value— Device name

Default— No value

interface-name interface-name—(Optional) Interface name of the congestion point.

Value— Interface name

Default— No value

(Optional) Output style.

Value

- *brief*— Display congestion point DN.

Default—detail

Required Privilege Level

view

show acp remote-update subscriber

Syntax

```
show acp remote-update subscriber <slot slot> <device-name device-name> <nas-port-id nas-port-id> <nas-ip nas-ip> <subscriber-ip subscriber-ip> <phone phone> <(brief) >
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display information about subscribers added through an external application.

Options

`slot slot`—(Optional) Number of the slot for which you want to configure values.

Value— Currently, the chassis has only one slot. The valid value is 0.

Default—0

`device-name device-name`—(Optional) Device name connected to subscriber.

Value— Device name

Default— No value

`nas-port-id nas-port-id`—(Optional) NAS port ID of interface connected to subscriber.

Value— NAS port ID

Default— No value

`nas-ip nas-ip`—(Optional) NAS IP address of device connected to subscriber.

Value— IP address

Default— No value

`subscriber-ip subscriber-ip`—(Optional) Subscriber IP address.

Value— IP address

Default— No value

phone *phone*—(Optional) Subscriber phone number.

Value— Phone number

Default— No value

(Optional) Output style.

Value

- *brief*— Display congestion point DN.

Default—detail

Required Privilege Level

view

show acp statistics device

Syntax

```
show acp statistics device <filter filter> < (brief) >
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display SNMP information for each device.

Options

filter filter—(Optional) Name of the device.

Value— All or part of the device name.

Default— No value

(Optional) Output style.

Value

- *brief*— Display only device names.

Default—detail

Required Privilege Level

view

show acp statistics directory

Syntax

```
show acp statistics directory
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display directory SNMP information.

Required Privilege Level

view

show acp statistics general

Syntax

```
show acp statistics general
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Display SRC-ACP SNMP information.

Required Privilege Level

view

License Management

The following table summarizes the SRC command-line interface (SRC CLI) for supporting license management. Configuration statements and operational commands are listed in alphabetical order.

License Management
Configuration Statements
shared license-server alarm
shared license-server corba
shared license-server email
shared license-server engine
shared license-server logging logger
shared license-server logging logger name file-logger
shared license-server logging logger name syslog-logger
shared license-server persistence-control
shared license-server repository
Operational Commands
request license import
request license remove
request license usage-report
show license allocated

shared license-server alarm

Syntax

```
shared license-server alarm {
    threshold threshold;
    report-server report-server;
}
```

Hierarchy Level

```
[edit shared license-server alarm]
```

Release Information

Statement introduced in SRC Release 3.1.0

Description

Configure the SRC license server to send alarms to administrators through SNMP and e-mail messages.

Options

`threshold threshold`— A threshold as a percentage of licensed capacity that, when exceeded, sends SNMP minor traps and initiates e-mail alerts to the system administrator.

Value—Integer in the range 0–100

Default— 80

Editing Level—Normal

`report-server report-server`—(Optional) SNMP server to receive warning traps.

Value— IP address or hostname

Default— No value

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared license-server corba

Syntax

```
shared license-server corba {
    orb-configuration-property-file orb-configuration-property-file;
}
```

Hierarchy Level

```
[edit shared license-server corba]
```

Release Information

Statement introduced in SRC Release 3.1.0

Description

Use the CORBA configuration to define the location of the property file for the object request broker (ORB). Typically, you do not need to change this property.

Options

`orb-configuration-property-file orb-configuration-property-file`— ORB configuration property file.

Value— *filename*

Default— *etc/jacorb.properties*

Editing Level—Expert

Required Privilege Level

system

Required Editing Level

Expert

shared license-server email

Syntax

```
shared license-server email {
    server server;
    alarm-report-address alarm-report-address;
    usage-report-address usage-report-address;
}
```

Hierarchy Level

```
[edit shared license-server email]
```

Release Information

Statement introduced in SRC Release 3.1.0

Description

Configure e-mail addresses to receive messages about license server warnings or license server usage reports.

Options

server server— SMTP e-mail server to receive alarms and usage reports.

Value— IP address or hostname

Default— No value

Editing Level—Normal

alarm-report-address alarm-report-address— E-mail address of the system administrator to receive warning e-mail messages.

Value— E-mail address

Default— No value

Editing Level—Normal

usage-report-address usage-report-address—(Optional) E-mail address of the system administrator to receive usage report e-mail messages.

Value— E-mail address

Default— No value

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared license-server engine

Syntax

```
shared license-server engine {
    service-session-unit-size service-session-unit-size;
    sae-service-unit-size sae-service-unit-size;
    lease-renew-interval lease-renew-interval;
    allocate-license-threshold allocate-license-threshold;
    release-license-threshold release-license-threshold;
}
```

Hierarchy Level

```
[edit shared license-server engine]
```

Release Information

Statement introduced in SRC Release 3.1.0

Description

Configure general properties for the SRC license server.

Options

service-session-unit-size service-session-unit-size— Size of each license unit for the service session property; this is the size of the license unit allocated to the SAE.

Value—Integer in the range -2147483648–2147483647

Default— 50

Editing Level—Expert

sae-service-unit-size sae-service-unit-size—(Optional) Size of each license unit for the SAE service property; this is the size of the license unit allocated to the SAE.

Value—Integer in the range -2147483648–2147483647

Default— 25

Editing Level—Expert

lease-renew-interval lease-renew-interval— Lease period for the licenses that the SAE client receives.

Value— Number of seconds in the range 0-129600 **Note:** 604800 is 1

week; 129600 is 2 weeks.

Default— 604800 (one week)

Editing Level—Expert

`allocate-license-threshold` *allocate-license-threshold*— Threshold, as a percentage of the chunk size, at which the SAE client obtains more licenses.

Value—Integer in the range 0–100

Default— 90

Editing Level—Expert

`release-license-threshold` *release-license-threshold*— Threshold, as a percentage of the chunk size, at which the SAE client releases one license unit.

Value—Integer in the range 0–100

Default— 10

Editing Level—Expert

Required Privilege Level

system

Required Editing Level

Expert

shared license-server logging logger

Syntax

```
shared license-server logging logger name ...
```

Hierarchy Level

```
[edit shared license-server logging logger]
```

Release Information

Statement introduced in SRC Release 3.1.0

Description

Configure logging properties for the SRC license server.

Options

name name—

Value—Text

Required Privilege Level

system

Required Editing Level

Basic

shared license-server logging logger *name* file-logger

Syntax

```
shared license-server logging logger name file-logger {
    filter filter;
    filename filename;
    rollover-filename rollover-filename;
    maximum-file-size maximum-file-size;
}
```

Hierarchy Level

```
[edit shared license-server logging logger name file-logger]
```

Release Information

Statement introduced in SRC Release 3.1.0

Description

Configure logging of messages to a file.

filter filter—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default— The default value is different for each type of component.

Editing Level—Basic

filename filename— Absolute path of the filename that contains the current logs.

Note: 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.

Value— Filename

Default— No value

Editing Level—Basic

rollover-filename rollover-filename—(Optional) 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— Path of filename

Example—/opt/UMC/sae/var/log/sae.alt

Default— The default value is different for each type of component.

Editing Level—Normal

`maximum-file-size` *maximum-file-size*—(Optional) Maximum size of the log file and the rollover file.

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

Value—Integer in the range 0–2147483647 kbytes

Default— 1000000

Editing Level—Normal

Required Privilege Level

system

Required Editing Level

Basic

shared license-server logging logger *name* syslog-logger

Syntax

```
shared license-server logging logger name syslog-logger {
    filter filter;
    host host;
    facility facility;
    format format;
}
```

Hierarchy Level

```
[edit shared license-server logging logger name syslog-logger]
```

Release Information

Statement introduced in SRC Release 3.1.0

Description

Configure logging of messages to system logging.

filter filter—(Optional) Filter to define which event messages the software logs or ignores. Filters can specify the logging level, such as debug, or can specify expressions. For information about expressions, see the documentation that describes how to configure logging.

Value— Log filter

Default—/error-

Editing Level—Basic

host host— IP address or name of a host that collects event messages by means of a standard system logging daemon.

Value— IP address or hostname

Default—loghost

Editing Level—Basic

facility facility—(Optional) Type of system log in accordance with the system logging protocol.

Value—Integer in the range 0–23

Default— 3

Editing Level—Advanced

format format—(Optional) MessageFormat string that specifies how the information in an event message is printed. (The strings {#} are replaced with the log information [...]).

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

Editing Level—Advanced

Required Privilege Level

system

Required Editing Level

Basic

shared license-server persistence-control

Syntax

```
shared license-server persistence-control {
    root-directory-of-the-license-server root-directory-of-the-license-server;
    work-directory-of-the-license-server work-directory-of-the-license-server;
    license-server-state-cache-file license-server-state-cache-file;
}
```

Hierarchy Level

```
[edit shared license-server persistence-control]
```

Release Information

Statement introduced in SRC Release 3.1.0

Description

Configure the root directory, the working directory, and the cache file location for the SRC license server.

Options

root-directory-of-the-license-server root-directory-of-the-license-server— Root directory of the license server.

Value— DN

Default— */opt/UMC/licsvr*

Editing Level—Expert

work-directory-of-the-license-server work-directory-of-the-license-server— Work directory of the license server, in which license server states are saved.

Value— Directory path

Default— *var/run*

Editing Level—Expert

license-server-state-cache-file license-server-state-cache-file— Cache file for license server state information.

Value— *filename*

Default— *state*

Editing Level—Expert

Required Privilege Level

system

Required Editing Level

Expert

shared license-server repository

Syntax

```
shared license-server repository {
    ldap-server-address ldap-server-address;
    server-port server-port;
    search-base search-base;
    authentication-dn authentication-dn;
    password password;
}
```

Hierarchy Level

```
[edit shared license-server repository]
```

Release Information

Statement introduced in SRC Release 3.1.0

Description

Configure access to the Juniper Networks database for the SRC license server.

Options

`ldap-server-address ldap-server-address`— IP address or hostname of the LDAP server that stores licensing data.

This is a required property. If no value is assigned, the license server does not start. If this value is removed while the license server is running, the server rejects licensing requests. After a new value is entered and the license server connects to the LDAP server, the license server accepts license requests again.

Value— IP address or hostname

Default— 127.0.0.1

Editing Level—Expert

`server-port server-port`— Port of the LDAP server that stores licensing data.

Value—Integer in the range 0–65535

Default— 389

Editing Level—Expert

`search-base` *search-base*— Base directory of the LDAP server that stores licensing data.

Value— DN

Default— *o=umc*

Editing Level—Expert

`authentication-dn` *authentication-dn*— DN used by the SAE to authenticate access to the LDAP server that stores licensing data.

Value— DN

Default— *cn=licsvr, ou=Components, o=Operators, o=umc*

Editing Level—Expert

`password` *password*— Password used to authenticate access to the LDAP server that stores licensing data.

Value— *password*

Default— *licsvr*

Editing Level—Expert

Required Privilege Level

system

Required Editing Level

Expert

request license import

Syntax

```
request license import file-name file-name <server-address server-address> <name-space name-space> <authentication-dn authentication-dn> <password password> <master-license>
```

Release Information

Command introduced in SRC Release 1.0.0

Description

Import an SRC license into the directory. The license can be either a pilot license or a server license. Use the `master-license` option to install a server, or master, license.

Options

`file-name file-name`— Name of the file that contains the SRC license information.

Value— Filename

Default— No value

`server-address server-address`—(Optional) IP address for the primary directory server. For C-series platforms, this is the platform that has the Juniper Networks database configured to have a primary role.

Value— IP address

Default— No value

`name-space name-space`—(Optional) Base distinguished name (DN) for the directory. In most cases you can use the default `<base>`.

Value— Base DN

Default— `<base>`

`authentication-dn authentication-dn`—(Optional) DN used for directory authentication.

Value— DN

Default— No value

`password password`—(Optional) Password used for directory authentication.

Value— Password

Default— No value

`master-license`—(Optional) License is a server, or master, license.

Required Privilege Level

maintenance

request license remove

Syntax

```
request license remove <license-id license-id> <server-address server-address>
<name-space name-space> <authentication-dn authentication-dn> <password password>
<master-license> <all>
```

Release Information

Command introduced in SRC Release 3.0.0

Description

Remove an SRC license from the directory. Use the `master-license` option to remove a server, or master, license.

Options

`license-id license-id`—(Optional) License ID identifying the license to be removed.

Value— license ID

Default— No value

`server-address server-address`—(Optional) IP address for the primary directory server. For C-series platforms, this is the platform that has the Juniper Networks database configured to have a primary role.

Value— IP address

Default— No value

`name-space name-space`—(Optional) Base distinguished name (DN) for the directory. In most cases you can use the default `<base>`.

Value— Base DN

Default— `<base>`

`authentication-dn authentication-dn`—(Optional) DN used for directory authentication.

Value— DN

Default— No value

`password password`—(Optional) Password used for directory authentication.

Value— Password

Default— No value

`master-license`—(Optional) Remove the master license.

`all`—(Optional) Remove all licenses.

Required Privilege Level

maintenance

request license usage-report

Syntax

```
request license usage-report <slot slot>
```

Release Information

Command introduced in SRC Release 3.1.0

Description

Create a license usage report. The report lists the date the report was created, and for each license the customer identification information, the license serial number, and the number of licenses installed. It also lists the number of concurrent active SAE service sessions (maximum number of license units) that can be allocated, and the maximum number of concurrent active SAE service sessions allocated since the license was installed or since the last license usage report was created.

Options

`slot slot`—(Optional) Number of the slot for which you want to request a license report.

Value— Currently the chassis has only one slot. The valid value is 0.

Default— 0

Required Privilege Level

maintenance

show license allocated

Syntax

```
show license allocated <virtual-router virtual-router> <slot slot>
```

Release Information

Command introduced in SRC Release 3.1.0

Description

Display information stored in the most recent usage report for the license server. The usage report provides information about the maximum number of concurrent service sessions in use per virtual router since the last time a usage report was generated, and compares this number with the maximum number of sessions allowed by the SRC server license.

Options

virtual-router virtual-router—(Optional) Name of virtual router for which to display license usage information.

Value— VR name

Default— No value

slot slot—(Optional) Number of the slot for which you want to display license usage information.

Value— Currently the chassis has only one slot. The valid value is 0.

Default— 0

Required Privilege Level

view

COS Naming Service

The following table summarizes the SRC command-line interface (SRC CLI) for supporting the COS naming service. Operational commands are listed in alphabetical order.

COS Naming Service Operational Commands
request_naming_add
request_naming_clear
request_naming_translate
show_naming_data
show_naming_statistics

request naming add

Syntax

```
request naming add name name object-reference object-reference
```

Release Information

Command introduced in SRC Release 3.2.0

Description

Add a name binding.

Options

name *name*— Object name.

Value—Text

object-reference *object-reference*— Interoperable object reference (IOR).

Value—Text

Required Privilege Level

maintenance

request naming clear

Syntax

```
request naming clear <name name>
```

Release Information

Command introduced in SRC Release 3.2.0

Description

Remove name bindings.

Options

name name—(Optional) Object name.

Value—Text

Required Privilege Level

clear

request naming translate

Syntax

```
request naming translate name
```

Release Information

Command introduced in SRC Release 3.2.0

Description

Display details about the specified name or IOR. If a name is specified, then the command looks up the name in the naming server and then displays the details. If a literal IOR is specified, then the command just displays the details for it.

Options

name— Name or object reference.

Value—Text

Required Privilege Level

maintenance

show naming data

Syntax

```
show naming data <name name> <detailed>
```

Release Information

Command introduced in SRC Release 3.2.0

Description

Display information for name bindings.

Options

name name—(Optional) Object name.

Value—Text

detailed—(Optional) Add detailed information.

Required Privilege Level

maintenance

show naming statistics

Syntax

```
show naming statistics
```

Release Information

Command introduced in SRC Release 3.2.0

Description

Display statistics.

Required Privilege Level

maintenance