



SRC-PE Software

Getting Started Guide

Release 3.0.x

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, California 94089
USA

408-745-2000

www.juniper.net

Part Number: 530-026628-01, Revision 1

This product includes the following software: Fontconfig, X FreeType library, X Render extension headers, and X Render extension library, copyright © 2001, 2003 Keith Packard.

Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Keith Packard not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Keith Packard makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

KEITH PACKARD DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL KEITH PACKARD BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark 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 Getting Started Guide

Release 3.0.x

Copyright © 2008, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Writing: Linda Creed, Justine Kangas, Betty Lew, Helen Shaw, Brian Wesley Simmons, Sarah Lesway-Ball, Diane Florio

Editing: Fran Mues

Illustration: Nathaniel Woodward

Cover Design: Edmonds Design

Revision History

15 August 2008—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 software 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 <http://www.juniper.net/techpubs>.

End User License Agreement

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

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

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

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

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

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

c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Abbreviated Table of Contents

	About This Guide	xxi
Part 1	SRC Overview	
Chapter 1	SRC Product Overview	3
Chapter 2	SRC Components	9
Part 2	Managing Your C-series Controller	
Chapter 3	Planning a Deployment of C-series Controllers	35
Chapter 4	Configuring a C-series Controller	39
Chapter 5	Accessing and Starting the SRC CLI	45
Chapter 6	Accessing and Using the C-Web Interface	51
Chapter 7	Configuring Remote Access to a C-series Controller (SRC CLI)	69
Part 3	Managing SRC Licenses	
Chapter 8	Overview of SRC Licenses	87
Chapter 9	Overview of the SRC License Server	89
Chapter 10	Installing Licenses for C-series Controllers	93
Part 4	Managing an Environment of C-series Controllers	
Chapter 11	Configuring System Time on C-Series Controllers (SRC CLI)	101
Chapter 12	Configuring NTP for C-Series Controllers	103
Chapter 13	Configuring NTP on C-Series Controllers (SRC CLI)	107
Chapter 14	Configuring System Logging for a C-series Controller (SRC CLI)	117
Chapter 15	Configuring Static Host Mapping (SRC CLI)	123
Chapter 16	Overview of the Juniper Networks Database	125
Chapter 17	Managing the Juniper Networks Database (SRC CLI)	129
Chapter 18	Setting Up an SAE (SRC CLI)	145
Chapter 19	Managing System Software on a C-series Controller	151
Chapter 20	Using the Web Application Server on a C-series Controller	157
Chapter 21	Integrating Steel-Belted Radius/SPE Server	165
Part 5	Managing SRC Access and Security with the CLI	
Chapter 22	Configuring User Access (SRC CLI)	169

Chapter 23	Authenticating Users on a C-series Controller (SRC CLI)	189
Chapter 24	Managing Security Digital Certificates	197
Chapter 25	Connecting to Remote Hosts from the SRC Software	203
Chapter 26	Configuring and Starting the SNMP Agent (SRC CLI)	205
Part 6	Configuring Operating Properties for Components	
Chapter 27	Distributing Directory Changes to SRC Components	227
Chapter 28	Configuring Local Properties (SRC CLI)	229
Part 7	Reference Material	
Chapter 29	SRC-Related Abbreviations	239
Chapter 30	SRC-Related References	247
Part 8	Index	
	Index	257

Table of Contents

	About This Guide	xxi
	SRC Guides and Release Notes	xxi
	Audience	xxi
	Documentation Conventions	xxi
	Related Juniper Networks Documentation	xxiii
	Obtaining Documentation	xxv
	Documentation Feedback	xxv
	Requesting Technical Support	xxv
Part 1	SRC Overview	
Chapter 1	SRC Product Overview	3
	SRC Product Description	3
	SRC Product Features and Benefits	5
Chapter 2	SRC Components	9
	SRC Component Overview	9
	SRC Server Components	13
	Service Activation Engine	13
	Policy and Service Management	14
	Accounting Support	14
	SAE Extensions	14
	Juniper Policy Server	14
	Network Information Collector	14
	Redirect Server	15
	SRC Repository for Data	15
	Juniper Networks Database as a Data Repository on C-series Controllers	16
	Directory as Repository for Subscriber Data	16
	SRC Configuration and Management Tools	16
	SRC CLI	16
	C-Web Interface	17
	Policy and Management	18
	SDX SNMP Agent	18

SRC Service Management Applications	18
SRC SOAP Gateway	18
Deep Packet Inspection Integration Application	19
Benefits of the DPI Integration	19
Threat Mitigation Portal	20
SRC Programming Interfaces	20
NETCONF API	20
CORBA Plug-In SPI	21
CORBA Remote API	21
NIC Access API	21
SAE Core API	21
Script Services	22
SRC Authentication and Accounting Applications	22
AAA RADIUS Servers	22
SRC Admission Control Plug-In	23
Flat-File Accounting	24
SRC Volume Tracking Application	24
Managing Subscriber Accounts with Web Portals	25
SRC Demonstration Applications	25
Enterprise Audit Plug-In	25
Enterprise Manager Portal	25
IDP Integration Applications	26
IVE Host Checker Integration Application	27
Monitoring Agent Application	27
Prepaid Account Administration Application	27
Prepaid Service Application	27
Sample Enterprise Service Portal	28
Residential Service Selection Portals	28
Traffic-Mirroring Administration Application	30
Traffic-Mirroring Application	30
SRC Auxiliary Applications	30
Application Server	30
Other Applications	31

Part 2

Managing Your C-series Controller

Chapter 3

Planning a Deployment of C-series Controllers 35

Components in an SRC Deployment	35
Considerations When Planning a Deployment of C-series Controllers	36
Deployment Scenario	37

Chapter 4

Configuring a C-series Controller 39

Before You Begin Configuring the SRC Software on a C-series Controller	39
Configuring the SRC Software	40
Configuring SRC Components	41

Chapter 5	Accessing and Starting the SRC CLI	45
	Overview of Configuration for the SRC CLI	45
	Configuration Statements for SRC CLI Directory Access	45
	Changing Access to the Directory that Stores SRC Configuration Data	46
	Verifying the Configuration for SRC Directory Access	48
	Starting the SRC CLI	48
	Policies, Services, and Subscribers CLI	49
	Overview of the Policies, Services, and Subscribers CLI	49
	Configuring Access to the Policies, Services, and Subscribers CLI	49
	Starting the Policies, Services, and Subscribers CLI	49
Chapter 6	Accessing and Using the C-Web Interface	51
	C-Web Interface Overview	51
	Navigating the C-Web Interface	52
	Layout of the C-Web Interface	52
	Elements of the C-Web Interface	53
	Top Pane Elements	53
	Main Pane Elements	53
	Side Pane Elements	54
	Accessing the C-Web Interface	55
	Enabling the C-Web Interface	57
	Starting the C-Web Interface	58
	Policies, Services, and Subscribers Subtasks in the C-Web Interface	58
	Overview of the Policies, Services, and Subscribers Management Subtasks in the C-Web Interface	58
	Configuring Access to Policies, Services, and Subscribers (C-Web Interface)	59
	Starting Policies, Services, and Subscribers	59
	Getting Help in the C-Web Interface	59
	Enabling Help	59
	Disabling Help	59
	Changing a Username or Password for the C-Web Interface	59
	Enabling Remote Users to Access the C-Web Interface	60
	Accessing the C-Web Interface Through Secure HTTP	60
	Accessing the C-Web Interface Through HTTP	60
	Modifying the Editing Level in the C-Web Interface	61
	Displaying Icons for Objects in the C-Web Interface	62
	Enabling Icons for Objects	62
	Disabling Icons for Objects	62
	Editing SRC Configurations (C-Web Interface)	62
	Loading Configuration Values in the C-Web Interface	63
	Committing a Configuration	64
	Reverting to a Previous Configuration	64
	Updating the Configuration Data	64
	Modifying Objects in the C-Web Interface	65
	Copying a Configuration for an Object (C-Web Interface)	65
	Renaming an Object	65

Moving an Object	65
Deleting an Object	66
Configuring Logging Properties in the C-Web Interface	66
Configuring File Properties	66
Configuring Syslog Properties	66
Configuration Statements for Logging for the C-Web Interface	67
Logging Out of the C-Web Interface	67

Chapter 7 Configuring Remote Access to a C-series Controller (SRC CLI) 69

Configuring External Interfaces on a C-series Controller	69
Configuring Gigabit Ethernet Interfaces for IPv4 (SRC CLI)	70
Configuring Gigabit Ethernet Interfaces for IPv6 (SRC CLI)	71
Configuring Tunnel Interfaces (SRC CLI)	72
Configuring Ethernet Redundancy (SRC CLI)	74
Configuring Group Interfaces (SRC CLI)	75
Configuring the MII Monitor (SRC CLI)	77
Configuring the ARP Monitor (SRC CLI)	77
Configuring the Virtual IP Address (SRC CLI)	78
Configuring a Static Route to Devices on Other Networks (SRC CLI)	78
Securing Connections Between a C-series Controller and Remote Hosts	79
Configuring a C-series Controller to Accept SSH Connections (SRC CLI)	80
Configuring a C-series Controller to Accept Telnet Connections (SRC CLI)	80
Configuring a C-series Controller to Accept NETCONF Connections (SRC CLI)	81
Port Settings for SRC Components	81

Part 3 Managing SRC Licenses

Chapter 8 Overview of SRC Licenses 87

Types of SRC Licenses	87
Obtaining an SRC License	88
Pilot License	88
Server License	88

Chapter 9 Overview of the SRC License Server 89

Overview of the SRC License Server	89
Server License	89
License Server Errors	89
License Requests	90
Example: License Allocation	90
Example: License Release Example	90

	Lease Renewal	91
	Directory Location and Access	91
	Unsuccessful Connections from the SAE to the SRC License Server	91
	SRC License Server Redundancy	92
Chapter 10	Installing Licenses for C-series Controllers	93
	Installing a Pilot License from the SRC CLI	93
	Installing Server Licenses for C-series Controllers	94
	Configuring License Manager for an SAE on a C-series Controller	95
Part 4	Managing an Environment of C-series Controllers	
Chapter 11	Configuring System Time on C-Series Controllers (SRC CLI)	101
	Setting the Time Zone (SRC CLI)	101
	Setting the System Date (SRC CLI)	102
Chapter 12	Configuring NTP for C-Series Controllers	103
	NTP Support on C-series Controllers	103
	Configuring NTP on a C-series Controller	104
Chapter 13	Configuring NTP on C-Series Controllers (SRC CLI)	107
	Configuration Statements for NTP on C-series Controllers	107
	Specifying Which NTP Server a C-series Controller Contacts on Startup	108
	Configuring NTP Client Mode for a C-series Controller (SRC CLI)	109
	Configuring an NTP Peer on a C-series Controller (SRC CLI)	109
	Configuring NTP Broadcast Mode on a C-series Controller (SRC CLI)	110
	Configuring NTP Authentication on a C-series Controller (SRC CLI)	111
	Configuring NTP as a Broadcast Client on a C-series Controller (SRC CLI)	113
	Configuring NTP as a Multicast Client on a C-series Controller (SRC CLI)	114
	Verifying NTP Configuration on a C-series Controller	115
Chapter 14	Configuring System Logging for a C-series Controller (SRC CLI)	117
	Overview of the C-series Controller Log Server	117
	Message Groups	117
	Severity Levels	118
	Before You Configure System Logging (SRC CLI)	118
	Configuration Statements for System Logging on a C-series Controller	118
	Saving System Log Messages to a File (SRC CLI)	119
	Sending System Log Messages to Other Servers (SRC CLI)	119
	Sending Notifications for System Log Messages to Users (SRC CLI)	120

Chapter 15	Configuring Static Host Mapping (SRC CLI)	123
	Overview of Static Host Mapping	123
	Configuring Static Host Mapping (SRC CLI)	123
Chapter 16	Overview of the Juniper Networks Database	125
	Overview of the Juniper Networks Database	125
	Redundancy for a Juniper Networks Database	126
	Security for a Juniper Networks Database	126
Chapter 17	Managing the Juniper Networks Database (SRC CLI)	129
	Configuration Statements for the Juniper Networks Database (SRC CLI)	129
	Enabling the Juniper Networks Database to Run in Standalone Mode (SRC CLI)	130
	Enabling the Juniper Networks Database to Run in Community Mode (SRC CLI)	131
	Securing the Juniper Networks Database (SRC CLI)	132
	Changing the Mode of a Juniper Networks Database (SRC CLI)	133
	Adding a Juniper Networks Database to an Established Community(SRC CLI)	133
	Promoting a Secondary Database to a Primary Role in a Configuration with One Primary Database (SRC CLI)	134
	Updating Data on a Juniper Networks Database (SRC CLI)	135
	Synchronizing Data on a Juniper Networks Database (SRC CLI)	135
	Loading Sample Data in to a Juniper Networks Database (SRC CLI)	135
	Securing Communications Between the Juniper Networks Database and SRC Components (SRC CLI)	137
	Verifying Configuration for a Juniper Networks Database with the SRC CLI	137
	Getting Information About Operations in a Juniper Networks Database (SRC CLI)	138
	Example: Configuration for a Database Community	139
	Troubleshooting Data Synchronization for Juniper Networks Databases (SRC CLI)	142
	Recovering Data in a Community with One Primary Database and One Secondary Database (SRC CLI)	142
Chapter 18	Setting Up an SAE (SRC CLI)	145
	Initially Configuring the SAE	145
	Grouped Configurations for the SAE	145
	Creating Grouped Configurations for the SAE (SRC CLI)	146
	Configuring an SAE Group	146
	Configuring Local Properties for the SAE (SRC CLI)	147
	Configuring the RADIUS Local IP Address and NAS ID (SRC CLI)	148
	Starting the SAE (SRC CLI)	149
	Stopping the SAE (SRC CLI)	149

Chapter 19	Managing System Software on a C-series Controller	151
	Overview of Software Management on a C-series Controller	151
	Before You Upgrade the Software on a C-series Controller	152
	Creating a Snapshot of Files on a C-series Controller	152
	Upgrading the System Software on a C-series Controller	153
	Upgrading SRC Software for a Component	154
	Installing SRC Software for a Component	155
	Removing an Installed Component	155
	Restoring the Files in a Snapshot	155
Chapter 20	Using the Web Application Server on a C-series Controller	157
	Overview of the Web Application Server on C-series Controllers	157
	Configuration Statements for the Web Application Server	158
	Configuring the Web Application Server (SRC CLI)	159
	Configuring Local Properties for Web Application Server (SRC CLI)	159
	Configuring Remote Access to the Application Server (SRC CLI)	160
	Configuring Access to the Application Server Through Secure HTTP	160
	Configuring Access to the Application Server Through HTTP	160
	Configuring Virtual Hosts for the Web Applications (SRC CLI)	161
	Configuring User Accounts for Web Applications (SRC CLI)	162
	Installing Web Applications in the Application Server	163
	Removing Web Applications From the Application Server	163
	Starting the Web Application Server on a C-series Controller	164
	Restarting the Web Application Server on a C-series Controller	164
	Stopping the Web Application Server on a C-series Controller	164
	Viewing Statistics for the Web Application Server (SRC CLI)	164
	Viewing Statistics for the Web Application Server (C-Web Interface)	164
Chapter 21	Integrating Steel-Belted Radius/SPE Server	165
	Integrating Steel-Belted Radius/SPE Server	165
Part 5	Managing SRC Access and Security with the CLI	
Chapter 22	Configuring User Access (SRC CLI)	169
	Overview of SRC User Accounts	169
	Login Classes for SRC User Accounts	169
	Login Class Permission Options for the SRC Software	170
	Predefined Login Classes for the SRC Software	174

Access to Individual Commands and Configuration Statements (SRC CLI)	174
Regular Expressions for Allow and Deny Statements	175
Guidelines for Using Regular Expressions	176
Timeout Value for Idle Login Sessions	176
Before You Configure Login Classes (SRC CLI)	177
Configuring an SRC Login Class	177
User Accounts for the SRC Software	180
Configuration Statements for SRC User Accounts	180
Configuring an SRC User Account	181
Types of Authentication for SRC User Accounts	183
Configuring Authentication for SRC User Accounts	184
Configuring a Plain Text Password	184
Configuring SSH Authentication	184
Example: SRC User Accounts	185
Changing the root Password for the SRC Software	186
Configuring a System Login Announcement (SRC CLI)	186

Chapter 23**Authenticating Users on a C-series Controller (SRC CLI) 189**

Configuring RADIUS and TACACS + Authentication on a C-series Controller	189
Configuring RADIUS Authentication (SRC CLI)	190
Configuring TACACS + Authentication (C-Web Interface)	191
A C-series Controller as a RADIUS Client and TACACS + Client	191
Configuring More Than One Authentication Method (SRC CLI)	192
Configuring Authentication Order	192
Configuring TACACS + or RADIUS Authentication	192
Configuring TACACS + and RADIUS Authentication	193
Removing an SRC Authentication Method from the Authentication Order	194
SRC Template Accounts for RADIUS and TACACS + Authentication	194
Named Template Accounts	194
Using Remote SRC Template Accounts	195
Configuring a Local SRC User Template	195
Example: Configuring SRC Authentication	196

Chapter 24**Managing Security Digital Certificates 197**

Overview of Digital Certificates	197
Before You Use Digital Certificates	197
Commands to Manage Digital Certificates	198
Manually Obtaining Digital Certificates	198
Obtaining Digital Certificates through SCEP	200
Removing a Certificate Request	201
Removing a Certificate	202

Chapter 25**Connecting to Remote Hosts from the SRC Software 203**

Connecting to a Remote Host Through SSH	203
Connecting to a Remote Host Through Telnet	203

Chapter 26	Configuring and Starting the SNMP Agent (SRC CLI)	205
	Configuration Statements for the SDX SNMP Agent	206
	Configuring the SDX SNMP Agent	207
	Configuring General Properties for the SDX SNMP Agent	207
	Configuring Initial Properties for the SDX SNMP Agent	208
	Configuring Directory Connection Properties for the SDX SNMP Agent	209
	Configuring Directory Monitoring Properties for the SDX SNMP Agent	210
	Configuring Logging Destinations for the SDX SNMP Agent	211
	Configuring JRE Properties	211
	Configuration Statements for the SNMP Agent	212
	Configuring the SNMP Agent	213
	Configuring System Information for the SNMP Agent	213
	Configuring Access Control for SNMPv3 Users	215
	Configuring Authentication	215
	Configuring Encryption	215
	Configuring Access Control for Communities	216
	Configuring Access Control for the VACM	217
	Associating Security Names with a Community	217
	Defining Named Views	218
	Defining Access Privileges for an SNMP Group	219
	Assigning Security Names to Groups	221
	Configuring Notification Targets	222
	Operating the SNMP Agent	223
	Starting the SDX SNMP Agent	223
	Stopping the SDX SNMP Agent	223
	Monitoring the SDX SNMP Agent	223
 Part 6	 Configuring Operating Properties for Components	
 Chapter 27	 Distributing Directory Changes to SRC Components	 227
	Overview of the Directory Eventing System	227
	Managing Directory Communication	228
 Chapter 28	 Configuring Local Properties (SRC CLI)	 229
	Local Properties for SRC Components	229
	Configuration Statements for Local Configuration	229
	Configuring Basic Local Properties	230
	Changing the Location of Data in the Directory	231
	Configuring Directory Connection Properties	232
	Configuring Initial Directory Eventing Properties for SRC Components	234
	Verifying the Local Configuration for a Component	234

Part 7	Reference Material	
Chapter 29	SRC-Related Abbreviations	239
Chapter 30	SRC-Related References	247
	RFCs	247
	Draft RFCs	248
	Other Software Standards	249
	URLs	249
Part 8	Index	
	Index	257

List of Figures

Figure 1: SRC Network with C-series Controllers	4
Figure 2: SRC-Managed PCMM Network	5
Figure 3: C-Web Page for SAE Configuration	17
Figure 4: Position of SRC-ACP in the Network	24
Figure 5: Sample Page in Enterprise Manager Portal	26
Figure 6: Sample Residential Web Portal	29
Figure 7: Sample Login Page for a Residential Portal on a PDA	29
Figure 8: C-series Controller and Related Components	36
Figure 9: Deployment Scenario for C-series Controllers	38
Figure 10: C-Web Layout	52
Figure 11: Top Pane Elements	53
Figure 12: Main Pane Elements	54
Figure 13: Side Pane Elements	55
Figure 14: Policy Icon	62
Figure 15: Configuration Options for the C-Web Interface	63
Figure 16: Sample Configuration	64
Figure 17: Sample Community of Juniper Network Databases	139
Figure 18: Authentication Order: RADIUS, TACACS + , Password	192

List of Tables

Table 1: Notice Icons	xxii
Table 2: Text Conventions	xxii
Table 3: Juniper Networks C-series and SRC Technical Publications	xxiii
Table 4: SRC Software Features and Benefits	5
Table 5: Descriptions of SRC Components	10
Table 6: Available NIC Resolutions	15
Table 7: Configuration Information for Other SRC Components	42
Table 8: Editing Levels	61
Table 9: Applications to Remotely Access the C-series ControllerTable 9: Applications to Remotely Access the C-series Controller	79
Table 10: Default Port Settings for SRC Components	82
Table 11: Package Names for Components on a C-series Controller	151
Table 12: Login Class Permission Options	170
Table 13: Default System Login Classes (Sheet of) (Sheet of)	174
Table 14: Common Regular Expression Operators to Allow or Deny Operational Mode and Configuration Mode Commands	175
Table 15: RFCs	247
Table 16: Draft RFCs	248
Table 17: Non-RFC Software Standards	249
Table 18: Juniper Networks URLs	249
Table 19: Third-Party URLs	250

About This Guide

- SRC Guides and Release Notes on page xxi
- Audience on page xxi
- Documentation Conventions on page xxi
- Related Juniper Networks Documentation on page xxiii
- Obtaining Documentation on page xxv
- Documentation Feedback on page xxv
- Requesting Technical Support on page xxv

SRC Guides and Release Notes

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

Audience

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

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 xxii defines the notice icons used in this guide. Table 2 on page xxii 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.	<code>user@host# set cache-entry-age cache-entry-age</code>
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"> ■ <code>system ldap server{ stand-alone;</code> ■ Use the <code>request sae modify device failover</code> command with the <code>force</code> option ■ <code>user@host# . . .</code> ■ <code>http://www.juniper.net/techpubs/software/ management/src/api-index.html</code>
<i>Italic sans serif typeface</i>	Represents variables in SRC CLI commands.	<code>user@host# set local-address local-address</code>
Angle brackets	In text descriptions, indicate optional keywords or variables.	Another runtime variable is <code>< gfwif ></code> .
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.srmt.sae.plugin\RadiusTrackingPluginEvent
Words separated by the symbol	Represent a choice to select one keyword or variable to the left or right of this symbol. (The keyword or variable may be either optional or required.)	diagnostic line

Related Juniper Networks Documentation

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

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

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

Document	Description
Core Documentation Set	
<i>C2000 and C4000 Hardware Guide</i>	Describes the hardware platforms and how to install, maintain, replace, and troubleshoot them. The guide also includes specifications.
<i>C2000 and C4000 Quick Start Guide</i>	Describes how to get the C-series Controller up and running quickly. Intended for experienced installers who want to expedite the installation process.
<i>SRC-PE Getting Started Guide</i>	Describes the SRC software, how to set up an initial software configuration, how to integrate RADIUS servers, and how to upgrade the SRC software. It also explains how to manage a C-series Controller. The guide describes how to set up and start the SRC CLI and the C-Web interface, as well as other SRC configuration tools. It includes reference material for the SRC documentation.
<i>SRC-PE CLI User Guide</i>	Describes how to use the SRC CLI, configure and monitor the platform with the CLI, and control the CLI environment. The guide also describes how to manage SRC components with the CLI.

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

Document	Description
<i>SRC-PE Network Guide: SAE, Juniper Networks Routers, NIC, and SRC-ACP</i>	Describes how to use and configure the SAE, the NIC, and the SRC-ACP (Admission Control Plug-In) application. This guide also provides detailed information about using JUNOSe routers, JUNOS routing platforms, and other network devices in the SRC network.
<i>SRC-PE Services and Policies Guide</i>	Describes how to work with services and policies. The guide provides an overview, configuration procedures, and management information. The guide also provides information about the SRC tools for configuring policies.
<i>SRC-PE Subscribers and Subscriptions Guide</i>	Describes how to work with residential and enterprise subscribers and subscriptions. The guide provides an overview, configuration procedures, and management information. This guide also provides information about the enterprise service portals, including the Enterprise Manager Portal.
<i>SRC-PE Monitoring and Troubleshooting Guide</i>	Describes how to use logging, the SNMP agent, the SRC CLI, and the C-Web interface to monitor and troubleshoot SRC components. This guide also describes the SNMP traps.
<i>SRC-PE Solutions Guide</i>	Provides high-level instructions for SRC implementations. The guide documents the following scenarios: managing QoS services on JUNOSe routers; managing subscribers in a wireless roaming environment; providing voice over IP (VoIP) services; integrating the SRC software in a PCMM environment, including the use of the Juniper Policy Server (JPS); and mirroring subscriber traffic on JUNOSe routers.
<i>SRC-PE CLI Command Reference, Volume 1</i> <i>SRC-PE CLI Command Reference, Volume 2</i>	Together constitute information about command and statement syntax; descriptions of commands, configuration statements, and options; editing level of statement options; and a history of when a command was added to the documentation.
<i>SRC-PE NETCONF API Guide</i>	Describes how to use the NETCONF application programming interface (API) to configure or request information from the NETCONF server on a C-series Controller that runs the SRC software.
<i>SRC-PE XML API Configuration Reference</i>	Describes the tag elements in the SRC Extensible Markup Language (XML) application programming interface (API) that are equivalent to configuration statements in the SRC command-line interface (SRC CLI).
<i>SRC-PE XML API Operational Reference</i>	Describes the tag elements in the SRC Extensible Markup Language (XML) application programming interface (API) that are equivalent to operational commands in the SRC command-line interface (SRC CLI).
Application Library	
<i>SRC Application Library Guide</i>	Describes how to install and work with applications that you can use to extend the capabilities of the SRC software. The guide documents the following applications: SRC-SG (SOAP Gateway) Web applications, an application to provide threat mitigation, an application to provide tracking and QoS control at the application level by integrating the SRC software with the Ellacoya deep packet inspection (DPI) platform, and an application to control volume usage .
Release Notes	

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

Document	Description
<i>SRC-PE Release Notes</i>	In the <i>Release Notes</i> , you will find the latest information about features, changes, known problems, resolved problems, supported platforms and network devices (such as Juniper Networks routers and CMTS devices), and third-party software. If the information in the <i>Release Notes</i> differs from the information found in the documentation set, follow the <i>Release Notes</i> .
<i>SRC Application Library Release Notes</i>	
Release notes are available on the Web.	

Obtaining Documentation

To obtain the most current version of all Juniper Networks technical documentation, see the products documentation page on the Juniper Networks Web site at <http://www.juniper.net/>.

To order a documentation CD, which contains this guide, contact your sales representative.

Copies of the Management Information Bases (MIBs) available in a software release are included on the documentation CDs and at <http://www.juniper.net/>.

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 <http://www.juniper.net/techpubs/docbug/docbugreport.html>. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version (not required for *Network Operations Guides [NOGs]*)

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/customers/support/downloads/710059.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 Manager: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool located at <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 Manager 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).

Part 1

SRC Overview

- SRC Product Overview on page 3
- SRC Components on page 9

Chapter 1

SRC Product Overview

- SRC Product Description on page 3
- SRC Product Features and Benefits on page 5

SRC Product Description

The Juniper Networks C2000 and C4000 systems, collectively referred to as C-series Controllers, are self-contained units with known capacity designed to optimize delivery of the features in the Juniper Networks Session and Resource Control (SRC) software. The model in use determines the number of service session licenses and concurrent subscribers allowed.

The SRC software is a robust, customizable product that allows a service provider's customers to dynamically activate SAE services in real time. Consequently, service providers can instantly realize gains in revenue without significant effort from sales, operations, and provisioning teams.

By using the SRC software, service providers can rapidly create and deploy many new SAE services to hundreds of thousands of business and residential subscribers. These Internet services, such as video on demand, IP television, or integrated voice and data, are offered over a variety of broadband access technologies, such as wireless Internet service provider roaming (WISPr), wireless fidelity (Wi-Fi) 802.11, digital subscriber line (DSL), cable, Ethernet, asynchronous transport mode (ATM), Frame Relay, SONET, and fixed wireless.

The SRC software offers a service-optimized architecture, which ensures quick time to revenue, flexible subscriber service management, and reliable service delivery. The management products use a modular design, which gives service providers the ability to select the components that meet their network requirements and business needs.

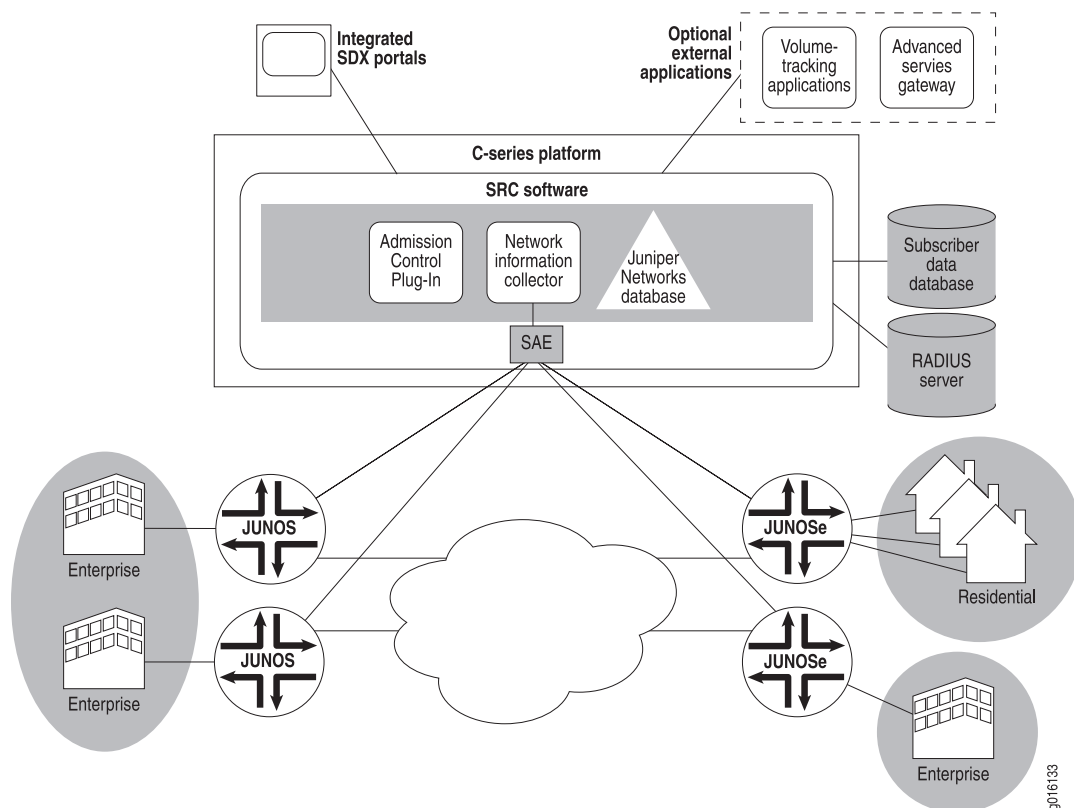
The SRC software can manage policies on Juniper Networks routers and cable modem termination system (CMTS) devices and can activate policies on other systems to provide end-to-end service quality.

The SRC software is designed to simplify the three major steps in the IP service life-cycle process:

1. Creating innovative, revenue-generating services
2. Delivering numerous on-demand services to subscribers
3. Tracking services with intelligent accounting applications

Figure 1 on page 4 illustrates how the SRC software manages JUNOSe routers and JUNOS routing platforms in an SRC network.

Figure 1: SRC Network with C-series Controllers

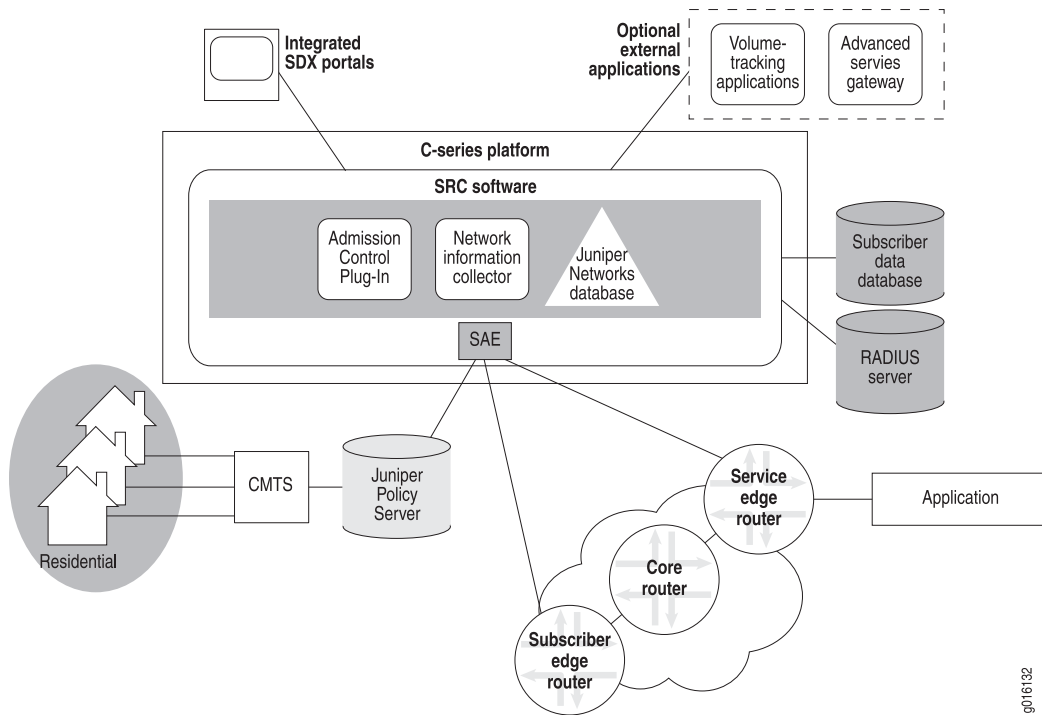


In addition, the SRC software can be used in a PacketCable MultiMedia (PCMM) environment to simplify other management tasks, such as:

1. Creating end-to-end service quality for subscribers in a PCMM environment
2. Marking traffic forwarded from specified systems, such as video servers

In general, service offerings supported by the SRC can be used in a cable environment.

Figure 2 on page 5 illustrates how the SRC software can be used in a PCMM environment to manage JUNOSe routers, JUNOS routing platforms, and CMTS devices. The SRC software can use the Juniper Policy Server as shown in Figure 2 on page 5, or a policy server embedded in the SAE.

Figure 2: SRC-Managed PCMM Network

SRC Product Features and Benefits

The SRC software provides a host of features for today's Internet service challenges. Table 4 on page 5 lists some of the many features and benefits that service providers need.

Table 4: SRC Software Features and Benefits

Feature	Benefit
Carrier-class architecture	<ul style="list-style-type: none"> ■ Provides a distributed architecture for flexibility. ■ Integrates with provider subscriber databases and supports customer profiles to define subscriber groups. ■ Instantiates each key server multiple times for either load distribution or failover. ■ Facilitates a variety of wholesale and retail models. ■ Uses CLI and GUI management and monitoring.
Seamless integration with operations support systems (OSS)	<ul style="list-style-type: none"> ■ Uses modular design and standards-based interfaces such as HTML/XML, RADIUS, LDAP, Common Object Request Broker Architecture (CORBA), and Simple Object Access Protocol (SOAP). ■ Supports open interfaces and mediation mechanisms to facilitate system integration with diverse OSS applications, including systems for subscriber management, customer care, order entry, provisioning, billing, security, and sales support. ■ Ensures smooth integration with back office solutions. (We partner with leading providers of telecommunications, RADIUS/authentication, authorization, and accounting (AAA), and billing systems to offer these services.)

Table 4: SRC Software Features and Benefits *(continued)*

Feature	Benefit
Financial advantages	<ul style="list-style-type: none"> ■ Avoids the misconception of a one-size-fits-all Internet access model by offering compelling content options with the appropriate level of bandwidth, quality of service (QoS), and network functions (for example, security, traffic prioritization, and filtering). ■ Allows providers to hold down on capital expenditures and operating expenses by offering a wide range of flexible services, tools, billing models, and revenue streams, and by using the same network infrastructure.
Optimal scalability	<ul style="list-style-type: none"> ■ Scales for rapidly growing networks and subscriber bases. ■ Works with JUNOSe routers, JUNOS routing platforms, and PCMM-compliant CMTS devices to automatically provision and support thousands to millions of subscribers in a distributed environment. ■ Uses zero-touch subscriber provisioning, which removes the roadblocks that can slow large-scale broadband subscriber acquisition.
Easy-to-build wholesale-retail model	<ul style="list-style-type: none"> ■ Provides a transparent infrastructure to Internet service provider (ISP), application service provider (ASP), and content partners, which lets partners retain ownership and management of their subscriber bases. ■ Frees partners from the responsibility of handling network operations so that they can focus solely on service delivery.
Intelligent accounting	<ul style="list-style-type: none"> ■ Tracks service usage to enable rich and creative tariff models. ■ Supports customer care, rating and billing, security, and sales support systems. ■ Simplifies the task of collecting and managing retailer and subscriber accounting data. ■ Uses a configuration interface to choose the policy rules to be used for accounting per interface direction (ingress and egress). ■ Activates multiple service sessions simultaneously for a given subscriber; each session can be tracked separately. ■ Supports plug-in software that gives service providers the ability to extend system capabilities. ■ Allows for flexible accounting rules.
Easy subscriber management	<ul style="list-style-type: none"> ■ Uses configuration interfaces for service definition and subscriber management. ■ Uses a directory that acts as a central repository of customer information and service portal configurations. The directory stores router information. ■ Works with JUNOSe routers, JUNOS routing platforms, and PCMM-compliant CMTS to collect subscribers' credentials and queries the RADIUS server for authentication and authorization. ■ Accommodates and manages a very large number of subscribers (for example, a typical subscriber base may be in the millions).
Dynamic policy management	<ul style="list-style-type: none"> ■ Gives subscribers consistent service experience across the network, regardless of the actual network deployment and the mode of connection to the network. ■ Enables real-time provisioning and collection of subscriber usage data. ■ Offers high availability based on seamless failover. ■ Uses configuration interfaces to define policies and store them in a central repository. ■ Provides robust support for access, QoS, and activation of new services on demand with configurable policies. ■ Performs dynamic policy decisions while services are activated, leveraging on the directory content to make policy decisions. ■ Provides end-to-end service levels across the network.

Table 4: SRC Software Features and Benefits *(continued)*

Feature	Benefit
Web-based portal	<ul style="list-style-type: none"> ■ Creates dynamic Web pages, giving subscribers personalized displays to select services on demand. ■ Offers branding opportunities for network provider/service provider partners. ■ Identifies subscribers, grants them access to defined services, and maps their selected service(s) to the network by means of dynamically provisioned policies. ■ Allows portals to be deployed in any application server with support for CORBA or SOAP. ■ Provides a starting point for rapid portal development through documented sample portals supplied for Java 2 Enterprise Edition (J2EE) application servers.
Easy service creation	<ul style="list-style-type: none"> ■ Uses the SRC CLI and the C-Web interface to enable the definition of various policy objects. ■ Uses configuration interfaces to define new services and to create service templates for future use. Service templates provide the service-provisioning information that configures the router for efficient, real-time delivery of that service. ■ Provides flexible service creation, a reusable service library, and automated service implementation. ■ Allows providers to define policies once and apply them network-wide.
Service activation engine (SAE)	<ul style="list-style-type: none"> ■ Translates services into lists of policies to be enforced on the router. ■ Initiates the service-usage data-collection process. ■ Customizes services with differentiated QoS and policies. ■ Collects usage data (time and volume) by subscriber and service to enable differentiated rating and billing.
Flexible open interface support	<ul style="list-style-type: none"> ■ Allows an external entity or system to control the SRC software's behavior. ■ Uses application programming interfaces (APIs) to authenticate managers; to navigate among retailers, enterprises, and sites; and to create, delete, activate, and deactivate service sessions. ■ Provides a Common Open Policy Service for policy provisioning (COPS-PR) interface. ■ Integrates into a PCMM environment with support for CableLabs PCMM specification. ■ Extends policies to systems that do not have a supported router driver. ■ Integrates with the Ellacoya Networks Deep Packet Inspection (DPI) platform to provide a traffic management solution that combines the advanced traffic identification and reporting features of the Ellacoya DPI with the SRC software's intelligent service policy enforcement. With this solution, providers can identify, monitor, and control traffic on a per-application or per-subscriber basis. ■ Integrates into an IP multimedia system (IMS) environment. The SRC software provides a Diameter protocol-based interface that allows the SRC software to integrate with services found on the application layer of IMS.

Chapter 2

SRC Components

- SRC Component Overview on page 9
- SRC Server Components on page 13
- SRC Repository for Data on page 15
- SRC Configuration and Management Tools on page 16
- SRC Service Management Applications on page 18
- SRC Programming Interfaces on page 20
- SRC Authentication and Accounting Applications on page 22
- SRC Demonstration Applications on page 25
- SRC Auxiliary Applications on page 30
- Other Applications on page 31

SRC Component Overview

The SRC software is a dynamic system. It contains many components that you use to build a subscriber management environment. You can use these tools to customize and extend the SRC software for your use and to integrate the SRC software with other systems. The SRC software also provides the operating system and management tools for C-series Controllers.

Table 5 on page 10 gives a brief description of the components that make up the SRC software.

Table 5: Descriptions of SRC Components

Component	Description
Server Components	
Service activation engine (SAE)	<ul style="list-style-type: none"> ■ Authorizes, activates, and deactivates subscriber and service sessions by interacting with systems such as Juniper Networks routers, cable modem termination system (CMTS) devices, RADIUS servers, and directories. ■ Collects accounting information about subscribers and services from routers, and stores the information in RADIUS accounting servers, flat files, and other accounting databases. ■ Provides plug-ins and application programming interfaces (APIs) for starting and stopping subscriber and service sessions and for integrating with systems that authorize subscriber actions and track resource usage.
Juniper Policy Server (JPS)	Acts as a policy decision point (PDP) and policy enforcement point (PEP) that manages the relationships between application managers and CMTS devices in a PCMM environment.
Network information collector (NIC)	Collects information about the state of the network and can provide a mapping from a given type of network data to another type of network data.
Redirect Server	Redirects HTTP requests received from IP Filter to a captive portal page.
Repository	
Directory	Provides a repository of subscriber information, services, policies, and service portal configurations. The SRC software uses the Lightweight Directory Access Protocol (LDAP) for interactions with the directory.
Juniper Networks Database	Repository for SRC data on a C-series Controller.
SRC Configuration and Management Tools	
SRC command line interface (CLI)	Provides a way to configure the SRC software on a C-series Controller from a JUNOS-like CLI. The SRC CLI includes the policies, services, and subscribers CLI, which has separate access privileges.
C-Web interface	Provides a way to configure, monitor, and manage the SRC software on a C-series Controller through a Web browser. The C-Web interface includes a policies, services, and subscribers component, which has separate access privileges.
Simple Network Management Protocol (SNMP) agent	Monitors system performance and availability. It runs on all the SRC hosts and makes management information available through SNMP tables and sends notifications by means of SNMP traps.
Service Management Applications (Run on external system)	

Table 5: Descriptions of SRC Components *(continued)*

Component	Description
Server Components	
SRC SOAP Gateway (SRC-SG)	Allows a gateway client—an application that is not part of the SRC network—to interact with SRC components through a Simple Object Access Protocol (SOAP) interface. (Available in the application library.)
Deep Packet Inspection Integration application	Integrates Ellacoya Networks Deep Packet Inspection (DPI) platform to provide a traffic management solution that combines the advanced traffic identification and reporting features of the Ellacoya DPI with the SRC software's intelligent service policy enforcement. (Available in the application library.)
Threat Mitigation Portal (SRC-TMP)	Manages threats on the SRC-managed network using information provided by Juniper Networks IDP Sensors and Juniper Networks NetScreen-Security Manager. Provides the SRC Threat Mitigation Portal (SRC-TMP) and application to manage the response to attacks. (Available in the application library.)
SRC Programming Interfaces	
NETCONF API	Allows you to configure or request information from the NETCONF server on a C-series Controller that runs the SRC software. Applications developed with the NETCONF API run on a system other than a C-series Controller.
CORBA plug-in service provider interface (SPI)	Tracks sessions and enables linking the rest of the service provider's operations support system (OSS) with the SRC software so that the OSS can be notified of events in the life cycle of SAE sessions. Hosted plug-ins only.
CORBA remote API	Provides remote access to the SAE core API. Applications that use these extensions to the SRC software run on a system other than a C-series Controller.
NIC access API	Performs NIC resolutions. Applications that use these extensions to the SRC software run on a system other than a C-series Controller.
SAE core API	Controls the behavior of the SRC software. Applications that use these extensions to the SRC software run on a system other than a C-series Controller.
Script services	Provides an interface to call scripts that supply custom services such as provisioning policies on a number of systems across a network.
Authorization and Accounting Applications	
AAA RADIUS servers	Authenticates subscribers and authorizes their access to the requested system or service. Accepts accounting data—time active and volume of data sent—about subscriber and service sessions. RADIUS servers run on a system other than a C-series Controller.

Table 5: Descriptions of SRC Components *(continued)*

Component	Description
Server Components	
SRC Admission Control Plug-In (SRC-ACP)	Authorizes and tracks subscribers' use of network resources associated with services that the SRC application manages.
Flat file accounting	Stores tracking data to accounting flat files that can be made available to external systems that send the data to a rating and billing system.
SRC Volume Tracking Application (SRC-VTA)	Monitors subscriber resource usage to allow service providers to offer flexible usage quotas, limit bandwidth to subscribers that overuse network resources, and to notify subscribers who may have been compromised by viruses or worms that overuse network resources. (Available in the application library.) The SRC-VTA runs on a Solaris platform.
Demonstration Applications (available on the Juniper Networks Web site)	
Enterprise Audit Plug-In	Defines a callback interface, which receives events when IT managers complete specified operations.
Enterprise Manager Portal	<p>Allows service providers to provision services for enterprise subscribers on JUNOSe routers and JUNOS routing platforms and that allows IT managers to manage services.</p> <p>Enterprise Manager Portal can be used with NAT Address Management Portal to allow service providers to manage public IP addresses for use with NAT services on JUNOS routing platforms and to all IT managers to make requests about public IP addresses through the Enterprise Manager Portal.</p>
Intrusion detection and protection (IDP) integration applications	Integrates IDP into an SRC-managed environment to manage malicious traffic sent to or received by subscribers. The IDP integration applications run on a Solaris platform.
Instant Virtual Extranet (IVE) Host Checker integration application	Integrates the IVE Host Checker into an SRC-managed environment to verify that the subscriber systems used to connect to a service provider comply with the service provider's policies. The IVE Host Checker integration application runs on a Solaris platform.
Monitoring Agent application	Integrates IP address managers, such as a DHCP server or a RADIUS server, into an SRC-managed network so that the SAE is notified about subscriber events. The Monitoring Agent application runs on a Solaris platform.
Prepaid Account Administration application	Manages prepaid accounts for the prepaid services demonstration application. The Prepaid Account Administration application runs on a Solaris platform.
Prepaid service application	Demonstrates how the SRC software might be used to manage prepaid accounts. The Prepaid service application runs on a Solaris platform.

Table 5: Descriptions of SRC Components *(continued)*

Component	Description
Server Components	
Residential service selection portals	Provides a framework for building Web applications that allow residential and enterprise subscribers to manage their own network services. It comes with several full-featured sample Web applications that are easy to customize and suitable for deployment. The Residential service selection portals run on a Solaris platform.
Sample enterprise service portal	Lets service providers supply an interface to their business customers for managing and provisioning services.
Traffic-Mirroring Administration application	Manages and monitors mirroring tasks. The Traffic-Mirroring Administration application runs on a Solaris platform.
Traffic-Mirroring Application	Mirrors subscriber traffic on any subscriber access platform supported by the SRC software. Provides the Traffic-Mirroring Administration portal to manage the mirroring of subscriber traffic. The Traffic-Mirroring application runs on a Solaris platform.
Auxiliary Applications	
Application server	Enables J2EE applications, including Web applications, to be used with the SRC software. These third-party applications run on a system other than a C-series Controller.
Other applications	Third-party applications created to run in an SRC environment.

SRC Server Components

The SRC server components are:

- Service Activation Engine on page 13
- Juniper Policy Server on page 14
- Network Information Collector on page 14
- Redirect Server on page 15

Service Activation Engine

The Service Activation Engine (SAE) is the core manager of an SRC network. It interacts with other systems, such as Juniper Networks routers, CMTS devices, directories, Web application servers, and RADIUS servers to retrieve and disseminate data in the SRC environment. The SAE authorizes, activates and deactivates, and tracks sessions during which a subscriber is logged in to the network and during which a service is active. The SAE can track more than one service session for a subscriber at a time.

Policy and Service Management

The SAE makes decisions about the deployment of policies on JUNOS routers and JUNOS routing platforms. When a subscriber's IP interface comes up on the router, the SAE determines whether it manages the interface. If the interface is managed—or controlled by—the SAE, the SAE sends the subscriber's default policy configuration to the router. These default policies define the subscriber's initial network access. When the subscriber activates an SAE service (a service that supplements a subscriber's standard services), the SAE translates the service into lists of policies and sends them to the router. This process lets subscribers manage their own subscriptions, typically through a Web page.

Accounting Support

The SAE also collects usage information about subscribers and services and passes the information to the appropriate rating and billing system. The SRC software allows a variety of accounting deployments, and provides a standard deployment that incorporates a RADIUS server. You can also create deployments that do not require a RADIUS server.

SAE Extensions

The SAE provides plug-ins and APIs that extend the capabilities of the SRC software. Plug-ins are software programs that augment existing programs and make them more flexible. SRC plug-ins provide authentication, authorization, and tracking capabilities. The SAE APIs let you create customized programs to integrate with the SAE.

Juniper Policy Server

The Juniper policy Server (JPS) is a PCMM-compliant policy server. In a PCMM environment, the policy server acts as a policy decision point (PDP) and policy enforcement point (PEP) that manages the relationships between application managers and cable management termination system (CMTS) devices.

Network Information Collector

The Network Information Collector (NIC) is the component that locates which SAE manages a subscriber or an interface. The NIC uses information that identifies the subscriber or the interface to identify the managing SAE. The NIC collects information about the state of the network and can provide a mappings from a given type of network data, known as a key, to another type of network data, known as a value.

For services to be activated for a subscriber session, applications such as the SRC-VTA, Dynamic Service Activator, Enterprise Manager Portal, or a residential portal need to locate the SAE that manages the subscriber. An application such as the SRC-TMP needs to locate the SAE that manages interfaces through which traffic destined for a specified IP address enters the network. The NIC component includes a Web administration application to monitor and inspect the state of NIC servers. Other SRC components such as an enterprise service portal and the sample residential portal use NIC.

Table 6 on page 15 shows the NIC resolutions that the standard SRC software can perform. For customized NIC implementations that provide other resolutions, contact Juniper Networks Professional Services.

Table 6: Available NIC Resolutions

Key	Value
Accounting ID of a subscriber	SAE reference
Enterprise's distinguished name (DN)	SAE reference
Subscriber's IP address	Subscriber's login name
Subscriber's IP address	Accounting ID
Subscriber's IP address for situations in which the SAE manages the subscriber	SAE reference
Subscriber's IP address for situations in which the SAE manages the interface that the subscriber uses, but not the subscriber	SAE reference
Subscriber's login name	SAE reference
Subscriber's primary username	SAE reference

The NIC comprises a set of software components that work together to collect, process, and provide data.

Redirect Server

The redirect server redirects filtered HTTP requests to a captive portal page. The redirect server examines requested paths and detects proxy HTTP requests. If the requested URL is served by the captive portal server, the redirect server opens a TCP connection to the captive portal and directs traffic to the captive portal rather than to the requested URL.

SRC Repository for Data

The Juniper Networks database, an LDAP directory, on a C-series Controller contains most SRC configuration data, including license information, service definitions, policies, and SAE configurations, as well as user profile data. You use user profiles to categorize groups of users, allowing you to keep your user data separate in your own directory.

We provide sample data to demonstrate how to provision the directory for different application scenarios. You can use the sample data as a starting place when developing or configuring specified applications of the SRC software. The SRC documentation provides references to the sample data to show sample implementations.

Many SRC components, such as the SAE and the policy engine are designed to run nonstop. These components get most of their configuration and provisioning data from the Juniper Networks database. If the data in the directory changes, it is not necessary to manually reload the data into affected components. The SRC directory client running in each of these components detects changes that affect the component, and the appropriate updates are made.

The directory client is configured with a list of directory servers to use: one primary and any number of backups. If connectivity to the primary directory is lost, the directory client switches to an available backup directory server. If connectivity to the primary directory is restored, the directory client detects the connection and switches back to the primary directory. This capability makes it possible to fine tune SRC deployments for added levels of availability and performance.

Juniper Networks Database as a Data Repository on C-series Controllers

The Juniper Networks database is a robust data repository that keeps your data highly available. It supports data distribution to other Juniper Networks databases and redundancy between Juniper Networks databases. Client applications control which database they connect to as their primary database and as their backup database. You can configure particular SRC components, such as SAE, NIC, and SAE to use a specified database to provide load sharing.

The Juniper Networks database also can also be run standalone to use in demonstrations or for testing purposes.

Directory as Repository for Subscriber Data

For environments that have large subscriber databases, the SRC software supports external third-party directories. The SRC software is compatible with any LDAP version 3-compliant directory. Integration work might be necessary, such as schema extension and access control. If you want the SRC software to automatically update existing subscriber sessions when you change your subscriber directory, and to cache subscriber data for performance, use a directory that supports the LDAP virtual list view control.

SRC Configuration and Management Tools

The SRC software provides the following configuration and management tools:

- SRC CLI on page 16
- C-Web Interface on page 17
- Policy and Management on page 18
- SDX SNMP Agent on page 18

SRC CLI

The SRC CLI is the software interface that you use to configure, monitor, and manage a C-series Controller and SRC software. The SRC CLI uses the same operational model as the JUNOS CLI, which you use to configure and monitor JUNOS routing platforms.

The CLI provides numerous commands and statements and organizes them in a hierarchical fashion. Commands that perform a similar function are grouped together under the same level of the hierarchy. You type commands on a single line, and the commands are executed when you press the Enter key. The CLI provides command help and command completion, and supports Emacs-style keyboard sequences that allow you to move around on a command line and scroll through recently executed commands.

C-Web Interface

The C-Web interface is an application that allows you to configure, monitor, and manage a C-series Controller and SRC software by means of a Web browser through Hypertext Transfer Protocol (HTTP) or HTTP over Secure Sockets Layer (HTTPS). The C-Web interface uses the same operational model as the J-Web interface, which you use to configure and monitor JUNOS routing platforms.

The C-Web interface supports the configuration, monitoring, and management tasks that you can perform with the SRC CLI. Figure 3 on page 17 shows a C-Web configuration page for the SAE.

Figure 3: C-Web Page for SAE Configuration

Monitor **Configure** Diagnose Manage Logged in as: admin Refresh Preferences About Logout

Shared
SAE / Configuration

Create new:

Compress Session Data	<input type="checkbox"/>	<p>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.</p> <p>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.</p> <p><i>Default:</i> Disabled</p>
Substs Cache Size	<input type="text"/>	<p>Substitution Engine Cache Size</p> <p><i>Default value:</i> 5000</p>
Substs Num Engines	<input type="text"/>	<p>Number of Substitution Engines</p> <p><i>Default value:</i> 5</p>

Copyright © 2007, Juniper Networks, Inc. All Rights Reserved. Trademark Notice. Privacy. Juniper Your Net.

Policy and Management

The SRC software works with Juniper Networks routers and PacketCable Multimedia Specification (PCMM) compliant CMTS platforms to provide differentiated QoS. The SRC software uses policies to define how the router or the CMTS device treats subscriber traffic. Policy management is responsible for defining policies and deploying the policies in an SRC network.

On JUNOS routing platforms, the SRC software supports class-of-service (CoS), firewall filters, policing, stateful firewall, stateless firewall, and Network Address Translation (NAT) services.

On JUNOSe routers, the SRC software supports policy routing, rate limiting, QoS classification and marking, packet forwarding, and packet filtering.

The Policies, Services, and Subscribers CLI and the Policies, Services, and Subscriptions subtasks in the C-Web interface allow easy specification and validation of policies. The policies are stored in the Juniper Networks database. It works closely with a policy engine, which performs dynamic policy decisions while activating services, leveraging on the directory content to decide which policies to use in a given context.

SDX SNMP Agent

The SDX SNMP agent monitors system performance and availability, system resources, and SRC processes that are running on the system. The agent obtains information from traps through SNMP. The SNMP agent is preconfigured to monitor SRC processes, such as those associated with infrastructure components (DirX for SRC software on Solaris platforms, and Interlink RADIUS). Additionally, it provides detailed monitoring and configuration of SRC server components such as the residential and enterprise portals, the SAE, NIC hosts, and the policy engine.

The master agent determines the SNMP version that supports integration with other network management systems. The SRC SNMP agent runs as a subagent to an installed master agent using the Agent Extensibility (AgentX) protocol. The SRC SNMP agent cannot act as a master agent.

SRC Service Management Applications

The SRC application library provides the following service management applications:

- SRC SOAP Gateway on page 18
- Deep Packet Inspection Integration Application on page 19
- Threat Mitigation Portal on page 20

SRC SOAP Gateway

The SRC SOAP Gateway (SRC-SG) allows a gateway client—an application that is not part of the SRC network—to interact with SRC components through a SOAP interface. This feature is useful for business-to-business situations, such as a wholesaler-retailer environment. Typically, the wholesaler owns and administers the SRC components,

and the retailer maintains a database of subscribers. Retailers purchase services from one or more wholesalers and sell the services to their subscribers. Using information provided by the wholesaler, the retailer creates a gateway client to communicate with the components in the SRC software.

The SRC-SG provides the Dynamic Service Activator which allows a gateway client to dynamically activate and deactivate SRC services for subscribers and to run scripts that manage the SAE.

Deep Packet Inspection Integration Application

The SRC software has been integrated with the Ellacoya Networks Deep Packet Inspection (DPI) platform to provide a traffic management solution that combines the advanced traffic identification and reporting features of the Ellacoya DPI with the SRC software's intelligent service policy enforcement. With this solution, providers can identify, monitor, and control traffic on a per-application or per-subscriber basis.

Application traffic such as peer-to-peer file sharing or instant messaging, which in many cases originates or terminates outside of a provider's network, can cause abusive or indiscriminate consumption of bandwidth and impact a provider's ability to deliver its own services. In particular, services that require higher, guaranteed levels of performance, such as Voice-over-IP (VoIP) or video-on-demand (VoD), can be impacted. Having visibility into applications that are transported over the network and their associated bandwidth consumption at various times is important as is the ability to control those applications.

The DPI solution allows providers to implement service control policies on specific traffic flows quickly and effectively. Such policies include throttling back, capping volume, or even enhancing bandwidth or service quality for sanctioned peer-to-peer applications.

Benefits of the DPI Integration

By identifying and effectively controlling traffic at the application level, service providers can:

- Put usage controls on applications on a subscriber basis. For example, you can put a quota limit on the amount of peer-to-peer traffic that a subscriber can consume in a month.

Once subscribers have used their quota, you can apply a policy that throttles back on or blocks a subscriber's peer-to-peer traffic, bill the subscriber for additional usage, or allow the subscriber to purchase additional quota.
- Limit the total percentage of network resources that a specific type of traffic is allowed to consume.
- Provide higher or guaranteed levels of performance for premium services by applying QoS control to application sessions. For example, two subscribers start an Xbox Live session. The Ellacoya DPI platform detects activity for this application, and sends application usage counters to the SRC software. The SRC software pushes policies that deliver a specific level of QoS for this application session to a router or other network device.
- Charge subscribers based on their usage of premium content-based services.

- Offer and charge for tiered Internet services based on both speed and application.
- Better support network planning functions by gaining an in depth understanding of traffic flows and patterns on a per subscriber and per application basis.

Threat Mitigation Portal

The Threat Mitigation Portal (SRC-TMP) and application allows service providers to respond to threats on the SRC-managed network. The application for the SRC-TMP can be customized based on customer-supplied data to control the description and recommended actions for each type of threat. The application includes the ability to log all user operations to provide an audit trail of actions.

The application uses these components to respond to threats:

- Juniper Networks Intrusion Detection and Prevention (IDP) Sensors to detect the threats.
- Juniper Networks NetScreen-Security Manager to manage the IDP Sensors and to signal the SRC-TMP when a threat is detected.
- The SRC-TMP, which is the user interface for the application, to manage threats and act upon them.

SRC Programming Interfaces

You can use the APIs provided with the SRC software to extend SRC capabilities.

Other components within the SRC software may provide programming interfaces. These interfaces are described in the documentation for the associated component.

The SRC software also includes plug-ins, such as plug-ins for accounting and authentication, admission control, customized accounting and authentication, and prepaid access.

The SRC software provides the following APIs to extend SRC capabilities:

- NETCONF API on page 20
- CORBA Plug-In SPI on page 21
- CORBA Remote API on page 21
- NIC Access API on page 21
- SAE Core API on page 21
- Script Services on page 22

NETCONF API

The NETCONF API allows you to configure or request information from the NETCONF server on a C-series Controller that runs the SRC software. The NETCONF API uses the tag elements in the SRC Extensible Markup Language (XML) application programming interface (API) that are equivalent to configuration statements and operational commands in the SRC CLI.

Client applications can use the operations in the NETCONF API to request and change the configuration data represented by the tag elements and to request information about the operational status of a C-series Controller.

CORBA Plug-In SPI

The CORBA-plug-in SPI is an interface that allows you to implement external plug-ins to integrate SAE with OSS software written in a wide variety of languages and distributed across a variety of hardware and operating system platforms. The SPI lets you link the rest of a service provider's OSS with the SRC software so that the OSS is notified of events in the life cycle of SAE sessions. For example, plug-ins can notify the OSS when a subscriber attempts to log in, and the OSS can evaluate general data and resource allocation to make authorization decisions.

The CORBA plug-in SPI is also used for internal plug-ins; the internal plug-ins must be written in Java and use the Java binding for CORBA.

CORBA Remote API

The CORBA remote API provides remote access to the SAE. It comprises an interface module manager and the following interface modules:

- SAE access interface module—Provides remote access to the SAE core API
- Java script interface module—Allows you to control the SAE with a Java script
- Python script interface module—Allows you to control the SAE with a Python script
- Event notification interface module—Allows you to integrate the SAE with external IP address managers

Most functions that are available through the SAE core API are also available through the CORBA remote API.

NIC Access API

The NIC access interface module (*nicAccess.idl*) is a simplified CORBA interface used to perform NIC resolutions. Use the NIC access module to develop applications not written in Java.

SAE Core API

The SAE core API is used to control the behavior of the SRC software, including subscribers, services, and subscriptions, as well as the SAE itself. For example, it can be used to provide subscriber credentials information (username and password) or to request subscription activation or deactivation for a subscriber.

The Java and Python script interface modules in the CORBA remote API run locally in the SAE, and have access to the SAE core API.

Script Services

Script services are SAE services that provide an interface to call scripts that supply custom services. You can use script services to create custom service implementations, such as:

- Provisioning of layer 2 devices, such as digital subscriber line access multiplexers (DSLAMs).
- Setting up of network connections such as MPLS tunnels.
- Provisioning of policies for network devices that do not have a supported SAE router driver.

You can use script services to provision policies on a number of systems across a network, including networks that do not contain a JUNOS router or JUNOS routing platform.

SRC Authentication and Accounting Applications

The following components help to provide accounting or authentication:

- AAA RADIUS Servers on page 22
- SRC Admission Control Plug-In on page 23
- Flat-File Accounting on page 24
- SRC Volume Tracking Application on page 24

AAA RADIUS Servers

RADIUS enables remote access servers to communicate with a central server to authenticate subscribers and authorize their access to the requested system or service. RADIUS allows a company to maintain subscriber profiles in a central database that all remote servers can share. With a central service, it is easier to track usage for billing and to keep network statistics. The router provides RADIUS accounting and authentication, while the SAE provides SAE accounting and authentication.

We recommend that service providers use a RADIUS server such the Juniper Networks Steel-Belted Radius/SPE server or integrate the SRC software with another RADIUS server that is already in use. We test and support system integration only with RAD-Series RADIUS Server and Steel-Belted Radius/SPE server software.

You can use any RADIUS server for authentication and accounting that is compliant with these standards:

- RFC 2882—Network Access Servers Requirements: Extended RADIUS Practices (July 2000)
- RFC 2869—RADIUS Extensions (June 2000)
- RFC 2865—Remote Authentication Dial In User Service (RADIUS) (June 2000)

When a provider uses the SDX schema to integrate the RADIUS server with the directory, the SRC software provides the highest level of subscriber control. For

example, when subscriber information is stored in the directory, the SRC software can provide a list of services for each individual subscriber.

The less integration the RADIUS server has with the directory, the less control the SRC software provides for individual subscribers. For example, subscribers may have to be grouped based on criteria such as domain name, router, or interface.

The SRC software can work without a RADIUS server. The SRC software can use either LDAP authentication and flat-file accounting, or it can rely on plug-ins to perform authentication and accounting.

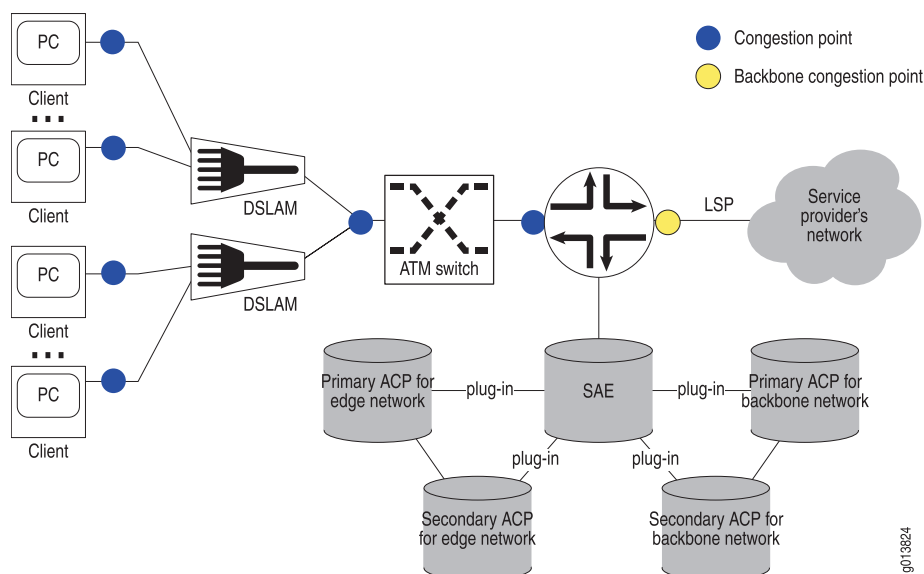
SRC Admission Control Plug-In

SRC-ACP authorizes and tracks subscribers' use of the network resources that are associated with services that the SRC software manages. SRC-ACP operates in two separate regions of the SRC network: the *edge* network and the *backbone* network. The edge network is the layer 2 access network through which subscribers connect to a router configured as a Broadband Remote Access Server (B-RAS). The backbone network is the region between the router and the service provider's network.

Congestion often occurs in the network at points where connections are aggregated. SRC-ACP monitors congestion points at interfaces between devices in the edge network. In the backbone network, SRC-ACP monitors one congestion point, a point-to-point label-switched path (LSP), between the router and the service provider's network.

Typically, network administrators use their own network management applications and external applications to provide data for SRC-ACP. SRC-ACP first obtains updates from external applications through its remote CORBA interface and then obtains updates from the directory through LDAP. SRC-ACP does not interact directly with the network to assess the capacity of a congestion point or actual use of network resources.

Figure 4 on page 24 shows a typical network topology.

Figure 4: Position of SRC-ACP in the Network

Flat-File Accounting

The SAE can write tracking data to accounting flat files. External systems can then collect the accounting log files and feed them to a rating and billing system. When the SAE writes data to a flat file, it writes into the first line the headers that identify the attributes in the file. Subsequent lines list the actual data in each field.

SRC Volume Tracking Application

The SRC Volume Tracking Application (SRC-VTA) allows service providers to track and control the network usage of subscribers and services. You can control volume and time usage on a per subscriber or per service basis. This level of control means that service providers can offer tiered services that use volume as a metric, while also controlling abusive subscribers and applications.

When a subscriber or service exceeds bandwidth limits (or quotas), the SRC-VTA can take actions including directing the subscriber to a portal to activate additional services or purchase additional bandwidth, imposing rate limits on traffic, sending an e-mail notification, or charging extra for additional bandwidth consumed.

If you use the SRC-VTA with the SRC deep packet inspection (DPI) feature, you can control the volume of traffic for specific applications, such as peer-to-peer file sharing.

You can use the VTA Configuration Manager to configure the SRC-VTA, including event handlers, events, actions, and processors. You can also use it to configure identifiers for subscribers and sessions and to set up logging for the SRC-VTA. VTA Configuration Manager lets you store your configurations in local files or in a directory.

Managing Subscriber Accounts with Web Portals

We provide two sample portals that manage subscriber accounts. One is an administrator portal that administrators can use to manage SRC-VTA subscriber accounts. The second is a subscriber portal that subscribers can use to manage their own accounts. Before you can use these portal, you need to configure the Web applications for the SRC-VTA.

The suggested billing model for services managed by VTAs is one in which subscribers pay for services when they select them through a Web portal.

SRC Demonstration Applications

The SRC software provides the following unsupported demonstration applications that you can use as a basis to create your own applications to extend the SRC software:

- Enterprise Audit Plug-In on page 25
- Enterprise Manager Portal on page 25
- IDP Integration Applications on page 26
- IVE Host Checker Integration Application on page 27
- Monitoring Agent Application on page 27
- Prepaid Account Administration Application on page 27
- Prepaid Service Application on page 27
- Sample Enterprise Service Portal on page 28
- Residential Service Selection Portals on page 28
- Traffic-Mirroring Administration Application on page 30
- Traffic-Mirroring Application on page 30

Enterprise Audit Plug-In

The Enterprise Service Portal audit plug-in, also referred to as the enterprise service portal IT Manager Audit Plug-In, defines a callback interface, which receives events when IT managers complete specified operations, such as subscribing to a service or changing the parameter substitutions of a subscription. The events report the type of operation, the identity of the IT manager, and other attributes.

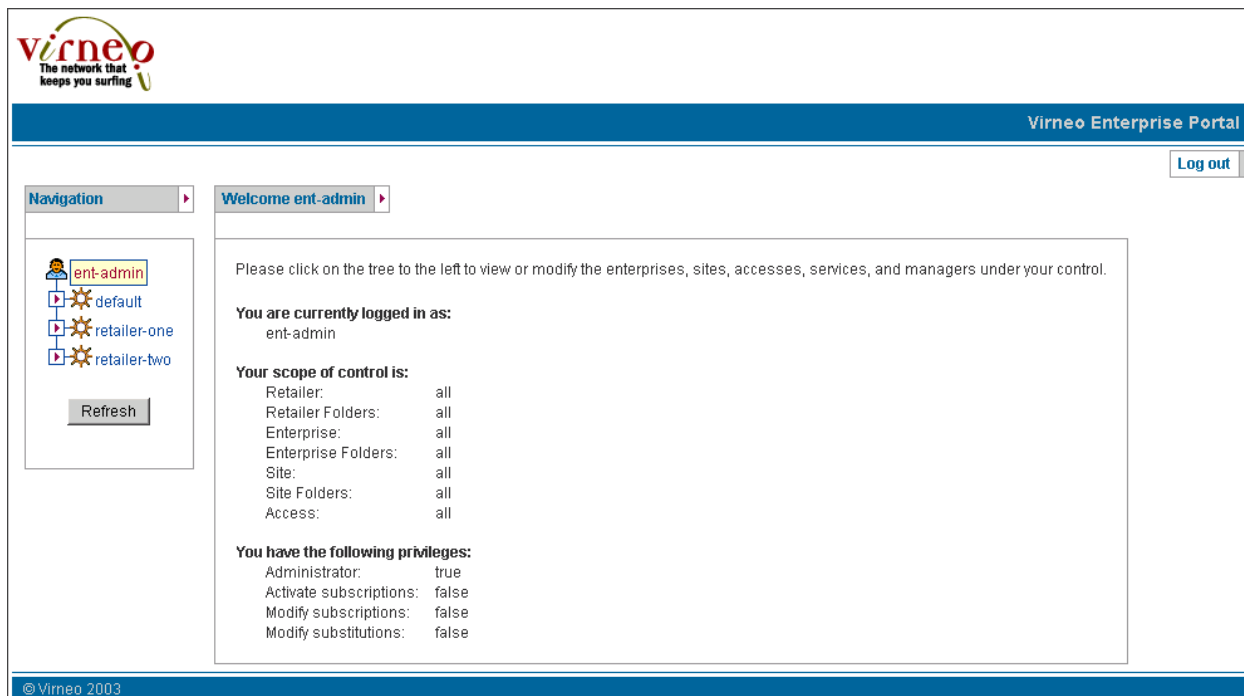
You can write audit plug-in event listeners by implementing the callback interface. A listener performs tasks such as processing received events and then publishing the events to one or more event handlers, such as a log file, system log, or database. Events are sent after the corresponding operations have been completed.

Enterprise Manager Portal

Enterprise Manager Portal is an application that allows service providers to provision services for enterprise subscribers on JUNOS routers and JUNOS routing platforms and that allows IT managers to manage services. This Enterprise manager Portal is a complete application that requires little customization.

Figure 5 on page 26 shows a sample page in the Enterprise Manager Portal.

Figure 5: Sample Page in Enterprise Manager Portal



You can use the Enterprise Manager Portal with the NAT Address Management Portal to allow service providers to manage public IP addresses for use with NAT services on JUNOS routing platforms and to allow IT managers to make requests about public IP addresses through the Enterprise Manager Portal. The NAT Address Management Portal is a complete application that requires little customization.

IDP Integration Applications

The IDP integration applications allow you to use IDP to monitor subscriber traffic for detecting malicious network traffic sent to or received by subscribers. In addition to the actions that IDP can take in response to detected incidents, you can configure the SRC software to respond to these incidents by taking one or more of the following actions for subscribers associated with malicious traffic:

- Applying policies, such as policies that limit subscriber bandwidth, to subscriber interfaces
- Sending e-mail messages that describe the nature of an incident
- Redirecting Web requests to an IDP captive portal where a page provides the source or destination of the problem traffic and a description of the incident

The SRC application library provides robust sample data for IDP integration, a sample e-mail gateway application, and a sample IDP captive portal. You can customize the implementation provided, or create a new one based on the samples.

IVE Host Checker Integration Application

The IVE Host Checker integration application allows you to verify that the subscriber systems used to connect to a service provider comply with the service provider's policies. You can deploy IVE Host Checker in a network so that it is activated according to the service provider's requirements. Based on the host-checking results, the subscriber may be allowed full, limited, or no access to the Internet.

The SRC application library provides sample data for IVE Host Checker integration, a sample Host Check Result portal, and a sample SRC-VTA application for scheduling host checking. You can customize the implementation provided, or create a new one based on the samples.

Monitoring Agent Application

The Monitoring Agent application integrates IP address managers into an SRC-managed PCMM environment and provides event notification for the SAE from subscribers who log into CMTS devices.

You can use the Monitoring Agent application to allow IP address managers, such as a DHCP server or a RADIUS server, to notify the SAE about subscriber events. You can use the SRC software to notify the SAE when:

- A subscriber logs in
- An address assignment is terminated

Prepaid Account Administration Application

You can use the Prepaid Account Administration application to manage prepaid accounts. From Prepaid Account Administration, you can:

- View or update information about current accounts
- Create new accounts
- Clear expired accounts

Prepaid Service Application

The prepaid service application is a demonstration application that illustrates how to integrate prepaid service applications with the SRC software.

The demonstration application consists of two components:

- Prepaid account server—Provides the central data repository for the prepaid services demonstration application. It maintains the different accounts and provides access for the other SRC components.
- Prepaid Account Administration application—Allows you to manage prepaid accounts.

The demonstration supports two types of prepaid service applications, time based and volume based.

Sample Enterprise Service Portal

An enterprise service portal is a Web application that lets service providers supply a management interface to its customers for managing and provisioning services. The sample enterprise service portal provides is an application that illustrates how service providers can make their services available to IT managers in an enterprise and that provides developers with a starting point from which they can create their own enterprise service portals.

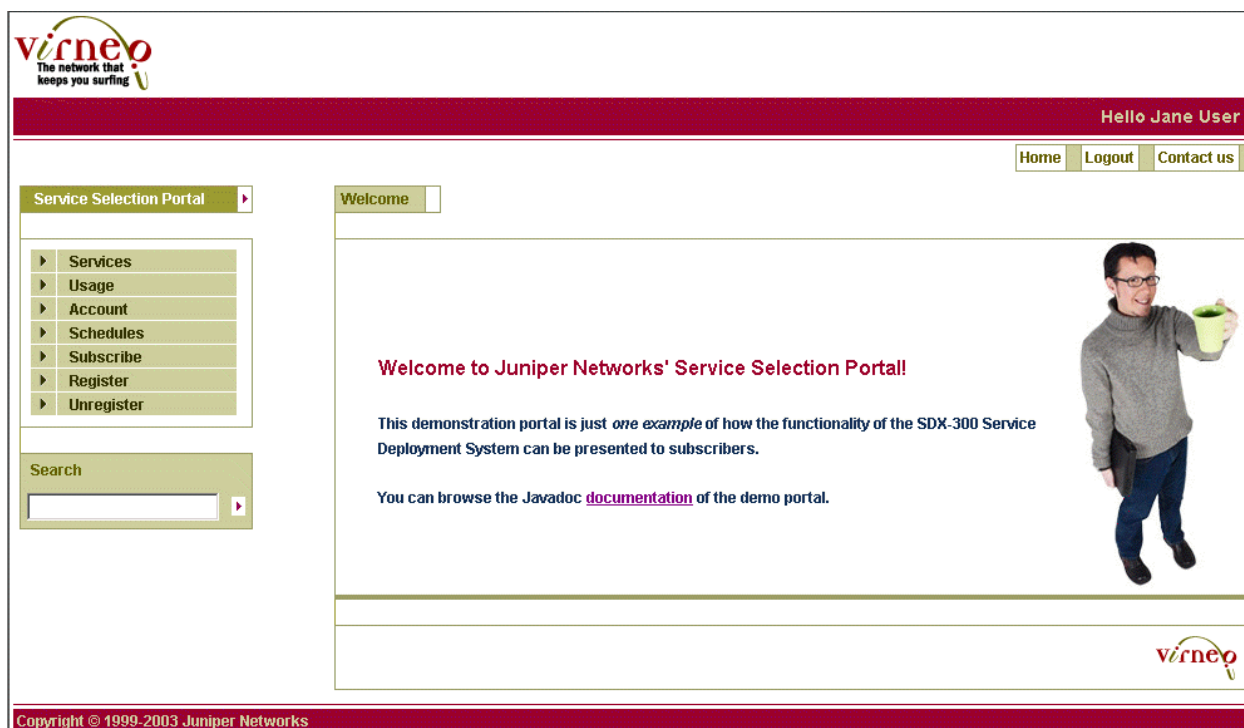
Residential Service Selection Portals

A residential portal is a Web portal application designed for use by individual subscribers to manage their subscriptions to Internet services and to log in to and out of a subscriber session. The portal pages, which are dynamically generated from information stored for subscribers, give subscribers instant access to personalized services, without the need to interact with customer representatives for a service provider. Proprietary client software is not required; subscribers can use a standard Web browser on a workstation or a personal digital assistant (PDA).

A residential portal can locate a specific SAE by using information that is dynamically obtained when subscribers connect. Because the data-processing function of the SRC software is separate from the access function, you can easily integrate the SRC software with existing portals, regardless of the technology used to deliver the portal. If your portal environment provides schemes for checking availability of Web servers and balancing loads between Web servers, you can also take advantage of these schemes for the portal.

The SRC software provides examples of residential portals.

Figure 6 on page 29 shows a residential Web portal that could be created with the SRC software.

Figure 6: Sample Residential Web Portal

Web-based residential portals that you develop for the SRC software are compatible with PDAs. Figure 7 on page 29 shows a login page for a sample residential portal that is being accessed from a PDA.

Figure 7: Sample Login Page for a Residential Portal on a PDA

Traffic-Mirroring Administration Application

You can use the Traffic-Mirroring administrative application to manage the mirroring of subscriber traffic. When traffic-mirroring services are activated in an SRC-managed environment, you can:

- Specify the subscriber whose traffic is to be mirrored and the IP addresses of the traffic to be mirrored
- Manage currently active mirroring tasks
- Manage pending actions

The Traffic-Mirroring administrative application is included with the Traffic-Mirroring application. The administrative application provides a GUI to simplify management tasks.

Traffic-Mirroring Application

The Traffic-Mirroring application allows service providers to mirror subscriber traffic on any subscriber access platform supported by the SRC software. By activating traffic-mirroring services in an SRC-managed environment, service providers can set up SRC policies to:

- Monitor subscriber traffic and intercept traffic from a particular source or to a particular destination.
- Take actions for subscribers with intercepted traffic by applying policies to the subscriber traffic.

The sample data provided with the application illustrates configurations for a network that contains JUNOS routers and JUNOS routing platforms and includes policies, services, and router definitions.

SRC Auxiliary Applications

The following applications can be integrated with SRC components or applications:

- Application Server on page 30

Application Server

To run a residential portal, the Enterprise Manager portal, or other enterprise portals you need an application server in your SRC environment you need an application server. Typically, you should use a J2EE application servers that includes a Web application server.

The Web application server should support JavaServer Pages (JSP) technology. JSP pages are Web pages that contain Java code and JSP tags (similar to HTML tags) embedded in normal HTML. The Java code and JSP tags produce dynamic HTML content and invoke the SAE functionality.

For use on a Solaris platform, the SRC software provides the JBoss application server as a convenience to let you quickly set up an SRC environment. This application server is J2EE compliant and supports the J2EE applications that the SRC software offers.

We have tested the SRC software with other application servers. For a list of the application servers that we have tested with the SRC software, see the release notes.

Other Applications

Other companies have created applications for use with the SRC software. For information about applications created by Juniper Networks partners, see http://www.juniper.net/partners/content_partners.html.

Part 2

Managing Your C-series Controller

- Planning a Deployment of C-series Controllers on page 35
- Configuring a C-series Controller on page 39
- Accessing and Starting the SRC CLI on page 45
- Accessing and Using the C-Web Interface on page 51
- Configuring Remote Access to a C-series Controller (SRC CLI) on page 69

Chapter 3

Planning a Deployment of C-series Controllers

- Components in an SRC Deployment on page 35
- Considerations When Planning a Deployment of C-series Controllers on page 36
- Deployment Scenario on page 37

Components in an SRC Deployment

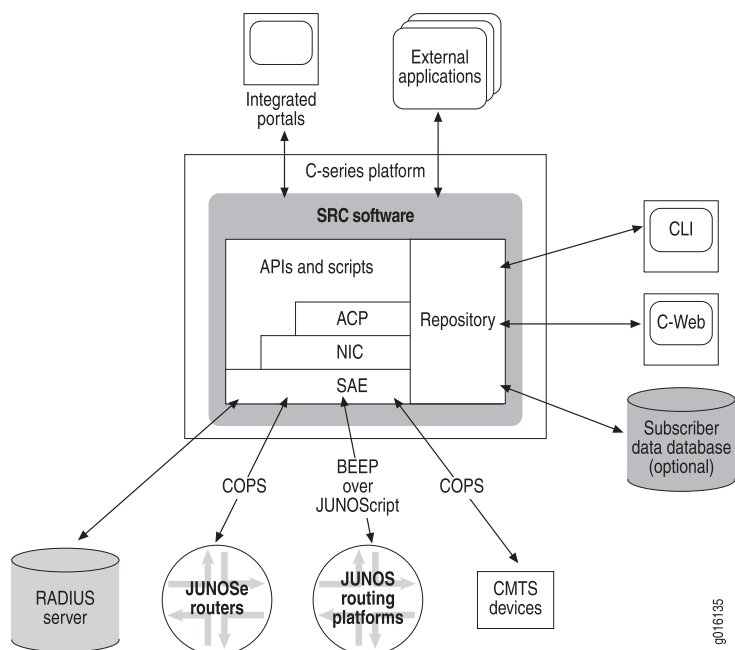
Using C-series Controllers that run the SRC software simplifies planning, deployment, configuration, and management of an SRC environment. The software on a C-series Controller provides an embedded data repository and the following SRC core components:

- Admission Control Plug-in
- Juniper Policy Server
- Network information collector
- Redirect server
- SAE
- SNMP agent
- Policies, services, subscribers, and subscriptions management

Applications that you develop and Web-based applications such as the Enterprise Manager Portal, SRC SOAP Gateway (SRC-SG) applications, and residential portals run on other systems. You configure these applications to communicate with the SRC software. The software on C-series Controllers provides a Web application server which hosts the SRC-ASG SOAP gateway in production environment. (This Web server can also be used to run applications that you create for testing and demonstration purposes only.)

You can integrate Juniper Networks routing platforms, cable modem termination system, Remote Authentication Dial-In User Service (RADIUS) servers, and databases that contains subscriber information into your SRC environment.

Figure 8 on page 36 illustrates the interaction of the various components in an SRC environment that includes a C-series Controller.

Figure 8: C-series Controller and Related Components

Considerations When Planning a Deployment of C-series Controllers

When you plan an SRC deployment, take into consideration requirements for security and high availability to comply with your organization's standard practices:

- **Hardware redundancy**—Because each C-series Controller contains all SRC core components, the platforms can provide redundancy for each other. If a C-series Controller is inaccessible, other platforms can manage the routers, services, and subscribers.

In the event of a hardware failure, one C-series Controller can be replaced with another one. The Juniper Networks database and the SAE synchronize with the software on other platforms. During routine system maintenance and software upgrades, a C-series Controller can be taken out of service then returned to service and the data synchronized.

- **High availability for the Juniper Networks database**—The database provides a robust redundancy scheme that you can customize for your deployment. The configuration lets you specify which databases are primary and which are secondary, and how data is propagated among a number of databases.
- **High availability for SRC components** —Components such as SAE and NIC let you configure high availability separately for each software component, which means that software redundancy can be configured as a mesh over a number of C-series Controllers.
- **Secure remote access**—Remote access to the SRC CLI can be set up through Telnet or SSH and to the C-Web interface through http or https.

- Directory connections—You can secure connections between the directory and other applications through secure LDAP.
- Web applications—Applications can leverage the security configured for your Web application server.
- RADIUS server—Because RADIUS is stateless, you can configure a sufficient number of RADIUS servers for the load, and you can configure both the routers and the SAE to load balance across them.
- Common Open Policy Service (COPS) connections— The JUNOSe routers can be configured with primary, secondary, and tertiary COPS servers, so it is possible to configure many failover schemes. This flexibility lets you locate backup SAEs remotely to provide geographical redundancy or close to the routers they manage to improve network performance.

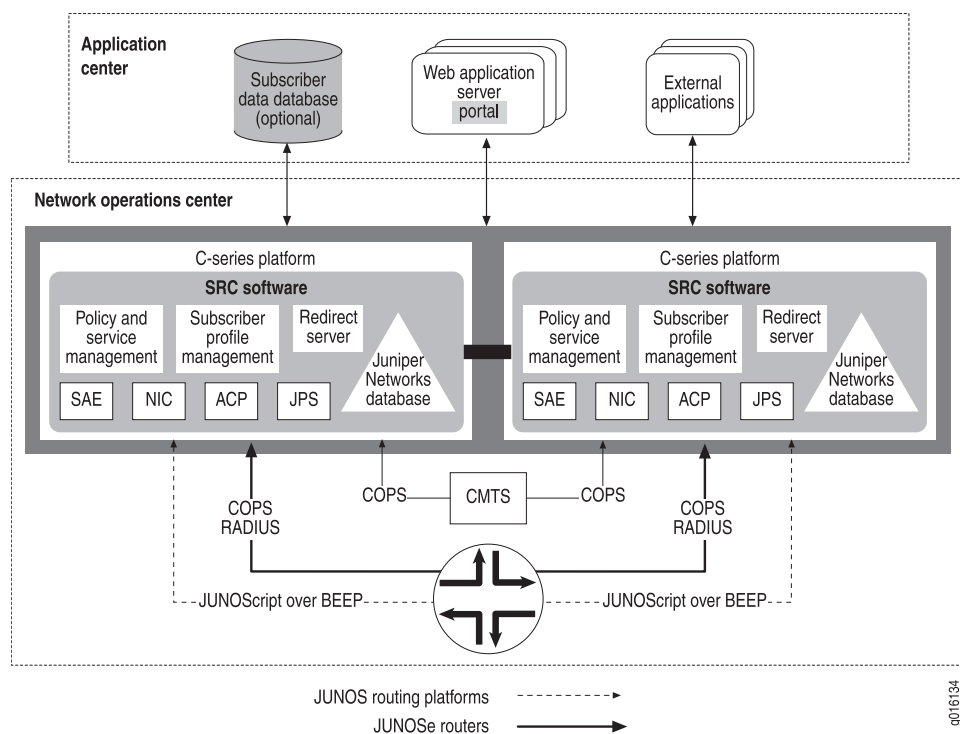
It is also possible for SAE servers to redirect existing and new COPS connections to other, more lightly loaded SAE servers. This COPS connection redirection can be triggered manually during a scheduled maintenance window or automatically based on SAE load monitoring.

- Load balancing for the network information collector (NIC)—You can provide load balancing for the NIC in the following ways:
 - Deploy two or more NIC hosts that each have the same configuration, and then configure NIC proxies to load balance across the NIC hosts.
 - Run the NIC hosts locally in the Dynamic Service Activator (DSA).
 - For NIC scenarios that require an SAE plug-in to track data about individual subscribers for a deployment in a large network, deploy NIC hosts to handle parts of the network with a different set of NIC hosts to aggregate requests.

Deployment Scenario

Typically, C-series Controllers reside in network operations centers, in a scenario that affords the systems the same physical security as other network devices. Routing platforms, RADIUS servers, and CMTS devices may also reside at the same site or at another location. Subscriber databases and external applications probably reside on servers located with other servers external to a network operations center.

Figure 9 on page 38 shows how C-series Controllers can be deployed. The example shows two platforms in a network operations center. Any number of C-series Controllers can be deployed at one or more sites.

Figure 9: Deployment Scenario for C-series Controllers

Juniper Networks Professional Services can assist you in determining the best deployment scenario for your environment.

Chapter 4

Configuring a C-series Controller

- Before You Begin Configuring the SRC Software on a C-series Controller on page 39
- Configuring the SRC Software on page 40
- Configuring SRC Components on page 41

Before You Begin Configuring the SRC Software on a C-series Controller

Before you begin configuring the SRC software on a C-series Controller, be sure that:

- You are familiar with how to use the SRC CLI.
 - Initial system setup and configuration have been completed, including configuration for:
 - C-series Controller hostname
 - Initial configuration for the Juniper Networks database and the database enabled on the system



NOTE: The Juniper Networks database must be running before you start configuring the SRC software.

- Domain name system
 - Eth0 interface
 - An administrative account that has superuser privileges
-



CAUTION: Although root access is used for initial configuration of a C-series Controller, user accounts are used to enter commands and statements at the CLI.

- Telnet and or SSH access

Related Topics

- *C-series Hardware Guide*
- Before You Start the SRC CLI

Configuring the SRC Software

To configure the SRC software on a C-series Controller:

1. Review the configuration by running the **show configuration** command in operation mode.

```
user@host> show configuration
system {
  host-name my-host;
  domain-search [ mylab.jnpr.net jnpr.net juniper.net ];
  name-server [ 192.0.20.10 192.0.20.30 ];
  time-zone America/New_York;
  services {
    telnet;
    ssh {
      root-login allow;
    }
  }
}
```

...

Make any updates needed to the initial configuration.

2. If the password for the root user was not changed from the default value, change it now.

```
root@host> set cli password
```

Do not use the root account for normal operation.

3. If the time zone is not set to the time zone where the system resides, set the time zone.

See Setting the Time Zone (SRC CLI).

4. Configure NTP.

See Configuring NTP on a C-series Controller.

5. Complete the configuration of the Juniper Networks database, and load sample data.

See Overview of the Juniper Networks Database.

If the Juniper Networks database is configured to run in community mode, the admin account already exists.

6. Configure remote access to other interfaces.

See Configuring External Interfaces on a C-series Controller, Configuring Gigabit Ethernet Interfaces for IPv4 (SRC CLI), Configuring Gigabit Ethernet Interfaces for IPv6 (SRC CLI).

7. Configure static routes to networks that contain devices to be managed by the SRC software.

See Configuring a Static Route to Devices on Other Networks (SRC CLI).

8. (Optional) Configure other external access to the C-series Controller and secure communications to remote hosts.

See Securing Connections Between a C-series Controller and Remote Hosts, Configuring a C-series Controller to Accept SSH Connections (SRC CLI), Configuring a C-series Controller to Accept Telnet Connections (SRC CLI).

9. (Optional) Configure the system log server.

See Overview of the C-series Controller Log Server.

10. (Optional) Configure user accounts.

See Overview of SRC User Accounts.

11. Configure SRC components.

See Configuring SRC Components .

Configuring SRC Components

After you create the basic SRC configuration, you can configure other SRC components and establish configurations for service providers and enterprises.

To configure SRC components in a deployment on C-series Controllers:

1. If your configuration includes a RADIUS server, start it.

See *SRC-PE Integration Guide* for information about starting RADIUS servers.

2. Configure SAE local properties.

See Initially Configuring the SAE.

3. Obtain your SRC software license.

See Types of SRC Licenses and Obtaining an SRC License.

4. Install the license, and start the license server if you have a server license.

See Installing Server Licenses for C-series Controllers or Installing a Pilot License from the SRC CLI.

5. (Optional) Configure and start the SNMP agent.

See Configuring the SDX SNMP Agent.

6. Start the SAE.

See Starting the SAE (SRC CLI).

7. If you use firewall software on your internal network, review firewall access for SRC components.

See Port Settings for SRC Components.

8. Configure other SRC components.

Table 7 on page 42 lists the principle SRC components that you can configure and names the document that provides information about configuring the components, typically from the CLI.

Table 7: Configuration Information for Other SRC Components

Component	Document
SRC-ACP	Configuring SRC-ACP
JPS	Configuring the JPS
C-Web interface	Enabling the C-Web Interface Accessing the C-Web Interface
Network information collector (NIC)	Configuring the NIC (SRC CLI)
Policies	Configuring Policy Groups Configuring Policy Lists
Redirect server	Configuring the Redirect Server (SRC CLI)
SAE	Initially Configuring the SAE Configuring the SAE to Manage JUNOS Routing Platforms Configuring the SAE to Manage JUNOS Routers with the CLI
SAE access to external database that stores subscriber data	Configuring LDAP Access to Directory Data
Services	Adding a Normal Service (SRC CLI) Adding an Infrastructure Service (SRC CLI) Overview of SRC Aggregate Services
Subscribers and subscriptions	Adding Subscribers (SRC CLI) Configuring Subscriptions (SRC CLI)
Enterprise Service Portals	Overview of NAT Address Management Portal Overview of the Sample Enterprise Service Portal Overview of Enterprise Manager Portal

Related Topics For information about using the C-Web interface to configure components, see the *SRC-PE C-Web Interface Configuration Guide*

Chapter 5

Accessing and Starting the SRC CLI

- Overview of Configuration for the SRC CLI on page 45
- Configuration Statements for SRC CLI Directory Access on page 45
- Changing Access to the Directory that Stores SRC Configuration Data on page 46
- Verifying the Configuration for SRC Directory Access on page 48
- Starting the SRC CLI on page 48
- Policies, Services, and Subscribers CLI on page 49

Overview of Configuration for the SRC CLI

You can use the SRC CLI on a C-series Controller. Most SRC configuration data is stored in the Juniper Networks database on the C-series Controller. When you use the Juniper Networks database, you can use the default configuration for the directory connection. You can add backup directories and change the password to the directory.

The CLI for policies, services, and subscribers requires that you configure access and that you explicitly start that part of the CLI.

You configure access to the SRC CLI by setting up user access accounts.

Related Topics

- Overview of the Policies, Services, and Subscribers CLI
- Overview of SRC User Accounts
- *SRC-PE CLI Command Reference*

Configuration Statements for SRC CLI Directory Access

Use the following configuration statements to change the connection to the directory that stores SRC configuration information. You enter the system ldap client statement at the [edit] hierarchy level:

```
system ldap client {  
  base-dn base-dn ;  
  url url ;  
  backup-urls backup-urls ;  
  authentication-dn authentication-dn ;  
  credentials credentials ;  
  connect-timeout connect-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;
}

```



NOTE: Do not change the value for the `enable-eventing`, `polling-interval`, `connection-manager-id`, `dispatcher-pool-size`, or `event-base-dn` statements unless instructed to do so by Juniper Networks.

The `eventing` statement is enabled by default.

Changing Access to the Directory that Stores SRC Configuration Data

Use the following configuration statements to change connection properties for the directory that stores SRC configuration data:

```

system ldap client {
  base-dn base-dn ;
  url url ;
  backup-urls [ backup-urls ...];
  principal principal ;
  credentials credentials ;
  timeout timeout ;
  time-limit time-limit ;
}

```



NOTE: Before you change directory connection properties, make sure that all configuration changes have been committed.

To change connection information to the directory that stores SRC configuration information:

1. From configuration mode, access the configuration statement that configures the directory connection.

```

[edit]
user@host# edit system ldap client

```

2. (Optional) Change the DN of the root directory to store SRC configuration information. You can use the default root `o = umc`.

```

[edit system ldap client]
user@host# set base-dn base-dn

```

3. (Optional) Change the URL that identifies the location of the primary directory server.

```
[edit system ldap client]
user@host# set url url
```

4. (Optional) Specify URLs that identify the locations of backup directory servers.

```
[edit system ldap client]
user@host# set backup-urls backup-url-n backup-url-n2
```

Backup servers are used if the primary directory server is not accessible.

5. (Optional) Change the DN that defines the username with which an SRC component accesses the directory.

```
[edit system ldap client]
user@host# set principal principal
```

For example:

```
[edit system ldap client]
user@host# set principal-dn cn=area1,o=Operators,o=umc
```

6. (Optional) Change the password used for authentication with the directory server.

```
[edit system ldap client]
user@host# set credentials credentials
```

7. (Optional) Specify the maximum amount of time during which the directory must respond to a connection request.

```
[edit system ldap client]
user@host# set timeout timeout
```

8. (Optional) Specify the length of time to wait for a connection to the directory to be established. If you set the value to 0, there is no time limit.

```
[edit system ldap client]
user@host# set time-limit time-limit
```

9. (Optional) Change directory eventing properties for the CLI.



NOTE: Do not change the value for the `enable-eventing`, `polling-interval`, `connection-manager-id`, `dispatcher-pool-size`, or `event-base-dn` statements unless instructed to do so by Juniper Networks.

The `eventing` statement is enabled by default.

In most cases, you use the default configuration for directory eventing properties. .

Verifying the Configuration for SRC Directory Access

Purpose Verify the configuration for directory connections.

Action 1. From configuration mode, access the configuration statement that configures the directory connection for the CLI.

```
[edit]
user@host# edit system ldap client
```

2. Run the `show` command. For example:

```
[edit system ldap client]
user@host# show
base-dn o=UMC;
url ldap://127.0.0.1;
principal cn=cli,ou=components,o=operators,<base>;
credentials *****;
timeout 10;
time-limit 5000;
eventing;
polling-interval 30;
connection-manager-id CLI_DATA_MANAGER;
dispatcher-pool-size 1;
event-base-dn o=UMC;
signature-dn o=UMC;
blacklist;
```

Starting the SRC CLI

When you log in to the CLI, the privileges for your user account determine which commands and configuration statements you can access. A login account with superuser privileges gives a user access to all commands and statements.

To log in to a C-series Controller and start the CLI:

1. Log in to a C-series Controller through an account that has super-user privileges.

For example, to log in to a C-series Controller through an SSH session:

```
# ssh my_admin@my_cseries_platform
```

2. Start the CLI:

```
root# cli
--- SRC CLI 7.0 build CLI.B.7.0.0.006
(c) 2005–2006 Juniper Networks Inc.
user@host>
```

The `>` command prompt shows you are in operational mode. Later, when you enter configuration mode, the prompt will change to `#`.

Policies, Services, and Subscribers CLI

- Overview of the Policies, Services, and Subscribers CLI on page 49
- Configuring Access to the Policies, Services, and Subscribers CLI on page 49
- Starting the Policies, Services, and Subscribers CLI on page 49

Overview of the Policies, Services, and Subscribers CLI

The Policies, Services, and Subscribers CLI is a part of the CLI that requires separate configuration. Before you can configure policies, services, and subscribers from the CLI, configure access to Policies, Services, and Subscribers CLI, and then enable it.

When you use the Policies, Services, and Subscribers CLI, ensure that only one user makes changes to the data at one time. If more than one user makes changes to the same configuration information for policies, services, or subscriptions, the software stores the first change to the data; subsequent changes are discarded.

Configuring Access to the Policies, Services, and Subscribers CLI

To make the Policies, Services, and Subscribers CLI accessible to users:

1. From configuration mode, access the [edit system services editor] hierarchy level.

```
[edit]
user@host# edit system services editor
```

2. Specify the type of password encryption to be used.

```
[edit system services editor]
user@host# password-encryption (crypt | md5 | sha | plain)
```

where:

- crypt—UNIX crypt, 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

Starting the Policies, Services, and Subscribers CLI

Before you start the Policies, Services, and Subscribers CLI, configure access to it.

See Configuring Access to the Policies, Services, and Subscribers CLI.

The Policies, Services, and Subscribers CLI lets you modify data shared by the instances of the SRC software that are running on a C-series Controller across the network.

To start the Policies, Services, and Subscribers CLI:

- Enter the `enable component` command.

```
user@host> enable component editor
```

Chapter 6

Accessing and Using the C-Web Interface

- C-Web Interface Overview on page 51
- Navigating the C-Web Interface on page 52
- Accessing the C-Web Interface on page 55
- Enabling the C-Web Interface on page 57
- Starting the C-Web Interface on page 58
- Policies, Services, and Subscribers Subtasks in the C-Web Interface on page 58
- Getting Help in the C-Web Interface on page 59
- Changing a Username or Password for the C-Web Interface on page 59
- Enabling Remote Users to Access the C-Web Interface on page 60
- Modifying the Editing Level in the C-Web Interface on page 61
- Displaying Icons for Objects in the C-Web Interface on page 62
- Editing SRC Configurations (C-Web Interface) on page 62
- Modifying Objects in the C-Web Interface on page 65
- Configuring Logging Properties in the C-Web Interface on page 66
- Logging Out of the C-Web Interface on page 67

C-Web Interface Overview

The C-Web interface lets you monitor, configure, troubleshoot, and manage the SRC components and C-series Controllers.

You can perform the following tasks with the C-Web interface:

- Monitoring—Display the current configuration and information about the system and SRC components.
- Configuring—View the current configurations at a glance and configure SRC components.
- Diagnosing—Diagnose problems with the NIC component.
- Managing—Manage files and licenses, enable and disable components, clear certificates and lists, upgrade the software, and reboot the system.

- Related Topics** ■ For information about using the C-Web interface to monitor SRC components, see the *SRC-PE SRC-PE Monitoring and Troubleshooting Guide*.

Navigating the C-Web Interface

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

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

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

Layout of the C-Web Interface

Each page of the C-Web interface is divided into the following panes, as shown in Figure 10 on page 52.

Figure 10: C-Web Layout



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

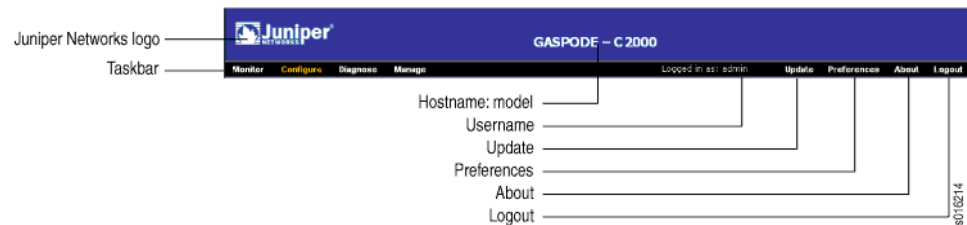
Elements of the C-Web Interface

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

Top Pane Elements

The top pane comprises the elements shown in Figure 11 on page 53.

Figure 11: Top Pane Elements

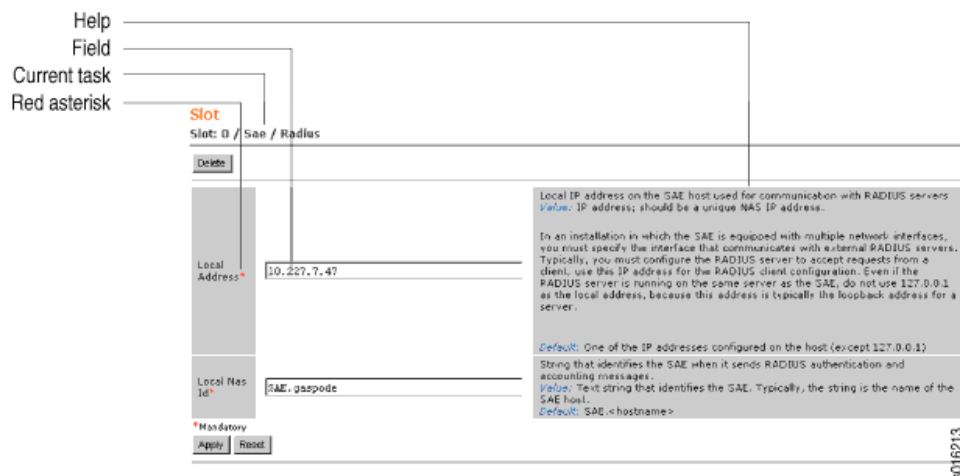


- Juniper Networks logo—Link to <http://www.juniper.net> in a new browser window.
- Taskbar—Menu of C-Web tasks:
 - Monitor—View monitoring information for core SRC components.
 - Configure—Configure SRC software on C-series Controllers.
 - Diagnose—Troubleshoot NIC component problems.
 - Manage—Manage files and licenses, upgrade the software, and reboot the system.
- *hostname - model*—Hostname and model of the C-series Controller.
- Logged in as: *username*—Username you used to log in to the C-series Controller or the SRC software.
- Update—Update the display of tasks and objects after modifying SRC software.
- Preferences—Link to C-Web display and configuration preferences, such as the display of Help text.
- About—Link to information about the C-Web interface, such as the version number.
- Logout—Ends your current login session with the C-Web interface and returns you to the login page.

Main Pane Elements

The main pane comprises the elements shown in Figure 12 on page 54.

Figure 12: Main Pane Elements

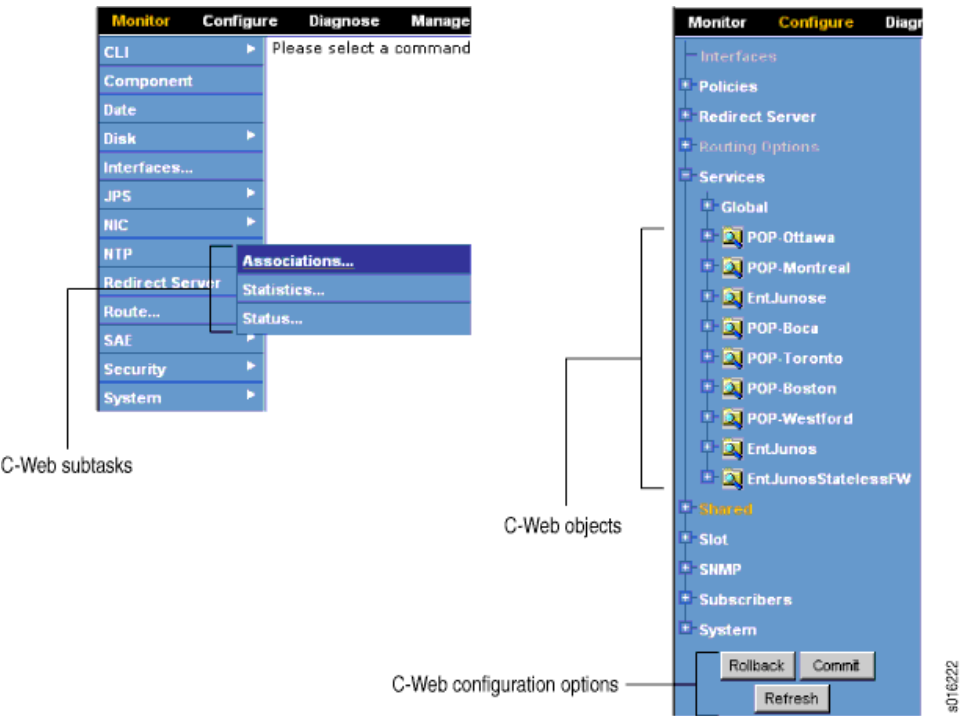


- **Help**—Displays field-specific information, such as the definition, format, and valid range of data in the field.
- **Current task**—Shows the successive C-Web tasks and subtasks you selected to display in the current main and side panes.
- **Red asterisk (*)**—Indicates a required field.

Side Pane Elements

The side pane comprises the elements shown in Figure 13 on page 55.

Figure 13: Side Pane Elements



In the Monitor, Diagnose, and Manage side panes, each subtask displays options related to the selected task in the C-Web taskbar. In these side panes, click the arrow signs (>) to expand individual items. Figure 13 on page 55 shows an example of the Monitor side pane.

In the Configure side pane, each subtask displays options related to the selected task in the C-Web taskbar. Objects represent configuration that you have created. For example, Figure 13 on page 55 displays objects that represent services. Click the plus signs (+) to expand both individual subtasks and objects. Click the minus signs (-) to hide individual subtasks and objects.

To edit a configuration, click the configuration options buttons at the bottom of the Configure side pane. For more information, see Editing SRC Configurations (C-Web Interface) .

Accessing the C-Web Interface

Configuring Access to the C-Web Interface Through Secure HTTPS

Before you can start using the C-Web interface, you need to configure and enable access to the C-Web interface with the SRC CLI. You can make the C-Web interface accessible to remote users through secure HTTP (HTTPS) or HTTP.

Before you configure access to the C-Web interface through HTTPS, obtain a digital security certificate on the system.

See Overview of Digital Certificates.

To make the C-Web interface accessible to remote users through HTTPS:

1. From configuration mode, access the hierarchy level for Web-management HTTPS.

```
[edit]
user@host# edit system services web-management https
```

2. Specify which TCP port is to receive incoming connection requests for the C-Web interface.

```
[edit system services web-management https]
user@host# set port port
```

The default port for HTTPS is 443.

3. Specify the interface to be used for Web browser connections to the C-Web interface.

```
[edit system services web-management https]
user@host# set interface interface
```

On a C-series Controller, use eth0; you can use eth2 or eth3 if installed.

On C-series Controllers, specifying an interface is important if your C-series Controller has eth2 and eth3 interfaces and you want to restrict C-Web interface access to one or both of these interfaces.

4. Specify the name of the certificate on the local system.

```
[edit system services web-management https]
user@host# set local-certificate local-certificate
```

5. Configure logging for the C-Web interface.

See Overview of Logging for SRC Components.

6. (Optional) Configure user accounts to allow specified users to log in to the C-Web interface.

Users who have privileges to log in to the SRC CLI also have privileges to log in to the C-Web interface.



NOTE: Like access to the SRC CLI, we recommend that you not use root access. If you do use root access, it must be through a secure terminal on a C-series Controller.

See Overview of SRC User Accounts.

Configuring Access to the C-Web Interface Through HTTP

Although you can configure access to the C-Web interface through HTTP rather than HTTPS, be aware of the following restrictions:

- An HTTP connection is not secure. At login, the password is sent in clear text across the network and could be intercepted.

- If you use the redirect server, you must change the port that the C-Web interface uses from the default port, 80. If the redirect server is enabled, and the C-Web interface is configured to use HTTP on port 80, the redirect server will intercept traffic destined for the C-Web interface.

To make the C-Web interface accessible to remote users through HTTP:

1. From configuration mode, access the hierarchy level for Web-management HTTP.

```
[edit]
user@host# edit system services web-management http
```

2. (Required if you use redirect server) Specify which TCP port is to receive incoming connection requests for the C-Web interface.

```
[edit system services web-management https]
user@host# set port port
```

The default port for HTTP is 80. Use another port if you use the redirect server.

3. (Optional) Specify the interface to be used for Web browser connections to the C-Web interface.

```
[edit system services web-management https]
user@host# set interface interface
```

On the C-series Controller, use eth0; you can use eth2 or eth3 if installed.

On C-series Controllers, specifying an interface is important if your C-series Controller has eth2 and eth3 interfaces and you want to restrict C-Web interface access to one or both of these interfaces.

4. Configure logging for the C-Web interface.

See *Configuring a Component to Store Log Messages in a File with SRC CLI* or *Configuring System Logging with SRC CLI*.

5. (Optional) Configure user accounts to allow specified users to log in to the C-Web interface.

Users who have privileges to log in to the SRC CLI also have privileges to log in to the C-Web interface.



NOTE: Like access to the SRC CLI, we recommend that you not use root access. If you do use root access, it must be through a secure terminal on a C-series Controller.

Enabling the C-Web Interface

To enable the C-Web interface with the SRC CLI:

- Enter the `enable component` command.

```
user@host> enable component webadm
```

Starting the C-Web Interface

Before you start the C-Web interface, verify whether access is configured for HTTP or HTTPS.

To start the C-Web interface:

1. From a Web browser, enter the name or IP address of the SAE and the port number for the C-Web interface.

https:// host :port/

or

http:// host :port/

The C-Web interface login page appears.

2. On the login page, type your username and password, and click Log In.

The Monitor page appears.

Policies, Services, and Subscribers Subtasks in the C-Web Interface

- Overview of the Policies, Services, and Subscribers Management Subtasks in the C-Web Interface on page 58
- Configuring Access to Policies, Services, and Subscribers (C-Web Interface) on page 59
- Starting Policies, Services, and Subscribers on page 59

Overview of the Policies, Services, and Subscribers Management Subtasks in the C-Web Interface

The Policies, Services, and Subscribers subtasks in the C-Web interface require separate configuration. Before you can configure policies, services, and subscribers from the C-Web interface, you need to configure and enable access to the Policies, Services, and Subscribers subtasks.

When you configure policies, services, and subscribers in the C-Web interface, ensure that only one user makes changes to the data at one time. If more than one user makes changes to the same configuration information for policies, services, or subscriptions, the software stores the first change to the data; subsequent changes are discarded.

Configuring Access to Policies, Services, and Subscribers (C-Web Interface)

To make the Policies, Services, and Subscribers subtasks accessible to users:

1. Click **Configure > System > Services > Editor**.
2. In the Password Encryption box, select the type of password encryption to be used.
3. Click **Apply**.

Starting Policies, Services, and Subscribers

The Policies, Services, and Subscribers subtasks in the C-Web interface enable you to modify data shared by the instances of the SRC software that are running on a C-series Controller across the network.

To start the Policies, Services, and Subscribers subtasks:

1. Click **Manage > Enable**.
2. From the Component list, select **editor**.
3. Click **OK**.

Getting Help in the C-Web Interface

The C-Web interface provides Help for each option. Each field description contains information about the definition, format, and valid range of the data in the field.

By default, the Help is enabled to display information for any task. To minimize the text on a pane, you can disable the Help display.

The Help settings are stored on a per-user basis. If you disable Help from displaying, your Web browser stores a cookie; the next time you log in, the Help is disabled.

Enabling Help

To enable Help to display information:

- Click **Preferences > Help: On**.

Disabling Help

To disable Help from displaying information:

- Click **Preferences > Help: Off**.

Changing a Username or Password for the C-Web Interface

To correct or change the username or password you use to log in to the C-Web interface:

1. In the C-Web login window, click **Reset**.
2. Type the new entry or entries.
3. Click **Log In**.

Enabling Remote Users to Access the C-Web Interface

You can make the C-Web interface accessible to remote users through secure HTTP (HTTPS) or HTTP. You can configure access through the C-Web interface or by using the SRC CLI.

Accessing the C-Web Interface Through Secure HTTP

Before you configure access to the C-Web interface through HTTPS, obtain a digital security certificate on the system.

See Overview of Digital Certificates.

To make the C-Web interface accessible to remote users through HTTPS:

1. Click **Configure**, expand **System > Services > Web Management**, and then click **HTTPS**.

The HTTP pane appears.

2. Click **Create**.
3. To configure HTTPS for an Ethernet port:
 - a. Select the Ethernet port from the list.
 - b. To configure a TCP port, type the value in the Port box, and click **Apply**.
4. To configure HTTPS for an interface:
 - a. Type a list of incoming network interfaces in the Interface box.
 - b. To configure a TCP port, type the value in the Port box, and click **Apply**.

Accessing the C-Web Interface Through HTTP

Although you can configure access to the C-Web interface through HTTP rather than HTTPS, be aware of the following restrictions:

- An HTTP connection is not secure. At login, the password is sent in clear text across the network and could be intercepted.
- If you use the redirect server, you must change the port that the C-Web interface uses from the default port, 80. If the redirect server is enabled, and the C-Web interface is configured to use HTTP on port 80, the redirect server will intercept traffic destined for the C-Web interface.

To make the C-Web interface accessible to remote users through HTTP:

1. Click **Configure**, expand **System > Services > Web Management**, and then click **HTTP**.

The HTTP pane appears.

2. Click **Create**.
3. To configure HTTP for an Ethernet port:
 - a. Select the Ethernet port from the list.
 - b. To configure a TCP port, type the value in the Port box, and click **Apply**.
4. To configure HTTP for an interface:
 - a. Type a list of incoming network interfaces in the Interface box.
 - b. To configure a TCP port, type the value in the Port box, and click **Apply**.

Modifying the Editing Level in the C-Web Interface

You can modify the editing level for users when they access the C-Web interface.

The editing level determines which configuration statements and commands are visible to a user from the C-Web interface. Table 8 on page 61 describes the editing levels.

Table 8: Editing Levels

Level	Description
Basic	Only values that must be configured are visible.
Normal	Common values and basic values are visible; this is the default setting.
Advanced	All configurable values, including the common and basic values, are visible.
Expert	All configurable values and internal values used for debugging are visible.

If you log in to the C-Web interface as root, the default editing level, normal, is available to you because root does not require a user profile to access the C-Web interface. Although root access is used for initial configuration of a C-series Controller, user accounts are used to configure, manage, diagnose, and monitor components in the C-Web interface.

The editing level can be set for:

- Specified users in the user profiles.
- A current user session.

To modify the editing level:

- Click **Configure**, click **Preferences** in the task bar, and then click the user level that you want to modify.

Displaying Icons for Objects in the C-Web Interface

By default, certain C-Web objects display icons that indicate the type of configuration. You can disable and enable the icons.

You can view icons for interfaces, policies, services, and subscribers. Figure 14 on page 62 displays an example of the policy icon.

Figure 14: Policy Icon



Enabling Icons for Objects

To enable icons:

- Click **Configure**, and then click **Preferences > Icons On**.

Icons are displayed in the side pane.

Disabling Icons for Objects

To disable icons:

- Click **Configure**, and then click **Preferences > Icons Off**.

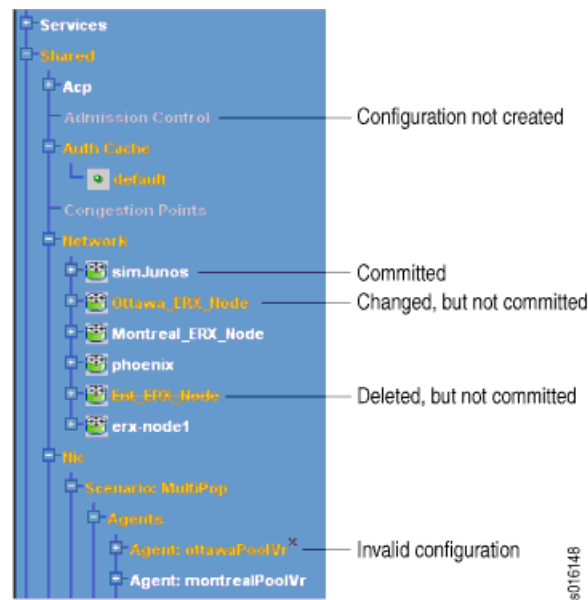
The icons are removed from the side pane.

Editing SRC Configurations (C-Web Interface)

The C-Web interface enables you to edit a graphical version of the SRC CLI configuration statements and hierarchy.

When you edit a configuration, you work in a copy of the current configuration to create a candidate configuration.

The changes you make to the candidate configuration are visible through the user interface immediately, but they do not take effect on the SRC software or the C-series Controller until you *commit* the changes.

Figure 15: Configuration Options for the C-Web Interface

The style of objects in the side pane indicates the status of the configuration. For example:

- White text—Indicates a committed configuration.
- Gray text—Indicates that an object is a configuration that has not been created.
- Orange—Indicates that an item has been changed, but not yet committed.
- Crossed-out orange text—Indicates that an item has been deleted, but not yet committed.
- Red x mark—Indicates an invalid configuration.

Loading Configuration Values in the C-Web Interface

When you access an object that does not have a configuration created (indicated by gray text in the side pane), the main pane contains only information about the configuration values that can be created.

Figure 16 on page 64 shows the main pane of a configuration that has not been created.

Figure 16: Sample Configuration

Shared
SAE / Configuration / Aggregate Services

Activation Deactivation Time*	Time to wait before retrying failed activation or deactivation of the fragment service session. <i>Value:</i> Number of seconds in the range 1-2147483647 <i>Default:</i> 900
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. <i>Value:</i> Number of seconds in the range 1-2147483647 <i>Default:</i> 86400
Keepalive Retry Time*	Time to wait before resending unacknowledged keepalive messages. <i>Value:</i> Number of seconds in the range 1-2147483647 <i>Default:</i> 900
Keepalive Time*	Interval at which keepalive messages are sent from an aggregate service session and an associated fragment service session. <i>Value:</i> Number of seconds in the range 1-2147483647 <i>Default:</i> 86400

*Mandatory

To access and edit the configuration, you must load the configuration values in the main pane.

To load the configuration values:

1. In the side pane, click an object that does not have a configuration created.
2. In the main pane, click the **Create** button.

Committing a Configuration

To save software configuration changes to the directory and activate the configuration:

- In the **Configure** side pane, click the **Commit** button.

When you commit the configuration, the software reviews the configuration for errors (commit check). Then, if the configuration is correct, the configuration is activated and becomes the active configuration.

If the configuration contains errors, a message indicates the location of the error, and the configuration is not activated.

Reverting to a Previous Configuration

You can revert to the active configuration and discard configuration changes not yet committed.

To revert to the full committed configuration:

- In the **Configure** side pane, click the **Rollback** button.

Updating the Configuration Data

You can update the configuration data based on changes made by other users.

To update the configuration:

- In the **Configure** side pane, click the **Refresh** button.

Modifying Objects in the C-Web Interface

Tasks to rename, move, or delete any type of object in the C-Web interface are:

- Copying a Configuration for an Object (C-Web Interface) on page 65
- Renaming an Object on page 65
- Moving an Object on page 65
- Deleting an Object on page 66

Copying a Configuration for an Object (C-Web Interface)

You can copy configuration information from one place in the configuration to another. This process simplifies configuration so that you do not need to configure the same information in more than one place.

To copy a configuration to another configuration object:

1. In the side pane, select the object that contains the configuration to be copied.
2. In the main pane, click the **Copy** button.
3. In the side pane, select an object that represents the location of the new object.
4. In the main pane, click the **Paste** button.
5. At the prompt, enter the name for the new object.

The application creates a new object with the name you specified and copies the configuration to this object.

Renaming an Object

After creating an object, you can rename it if needed.

To rename an object:

1. In the main pane, click the **Rename** button.
2. Type a new name for the object in the dialog box. and click **OK**.

The object's new name appears in the side and main panes.

Moving an Object

After creating an object, you can move it from the side pane if needed (above or below another object).

To move an object:

1. In the side pane, click the object.
2. In the Move to list in the main pane, select where you want to move the object, and click **OK**.

The object appears in the desired location in the side pane.

Deleting an Object

After creating an object, you can delete it if needed.

To delete an object:

1. In the side pane, click the object.
2. In the main pane, click **Delete**.

The object no longer appears in the side pane.

Configuring Logging Properties in the C-Web Interface

You can configure file and syslog properties for logging in the C-Web interface.

Tasks to configure properties in the C-Web interface are:

- Configuring File Properties on page 66
- Configuring Syslog Properties on page 66

Configuring File Properties

To configure file properties for logging:

1. Click **Configure**, expand **System > Web Management**, and then click **Logger**.

The Logger pane appears.

2. From the Create new list, select **Logger**.
3. Type a name for the logging file in the dialog box, and click **OK**.
4. In the side pane, expand the logger that you created, and click **File**.

The File pane appears.

5. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Syslog Properties

To configure system logging properties:

1. Click **Configure**, expand **System > Web Management**, and then click **Logger**.

The Logger pane appears.

2. From the Create new list, select **Logger**.
3. Type a name for the logging file in the dialog box, and click **OK**.
4. In the side pane, expand the logger that you created, and click **Syslog**.

The Syslog pane appears.

5. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuration Statements for Logging for the C-Web Interface

Use the following configuration statements to configure the logging for the C-Web interface at the [edit] hierarchy level.

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

Logging Out of the C-Web Interface

To end a C-Web session at any time:

- In the top pane, click **Logout**.

Chapter 7

Configuring Remote Access to a C-series Controller (SRC CLI)

- Configuring External Interfaces on a C-series Controller on page 69
- Configuring Gigabit Ethernet Interfaces for IPv4 (SRC CLI) on page 70
- Configuring Gigabit Ethernet Interfaces for IPv6 (SRC CLI) on page 71
- Configuring Tunnel Interfaces (SRC CLI) on page 72
- Configuring Ethernet Redundancy (SRC CLI) on page 74
- Configuring the Virtual IP Address (SRC CLI) on page 78
- Configuring a Static Route to Devices on Other Networks (SRC CLI) on page 78
- Securing Connections Between a C-series Controller and Remote Hosts on page 79
- Configuring a C-series Controller to Accept SSH Connections (SRC CLI) on page 80
- Configuring a C-series Controller to Accept Telnet Connections (SRC CLI) on page 80
- Configuring a C-series Controller to Accept NETCONF Connections (SRC CLI) on page 81
- Port Settings for SRC Components on page 81

Configuring External Interfaces on a C-series Controller

The C-series Controller provides the following interfaces:

- Serial port—9600 baud

The serial port is enabled by default. You can use the serial port to connect to a console terminal and perform initial configuration as well as configuration updates.

- Two external Gigabit Ethernet interfaces—eth0 and eth1

The eth0 interface is designed to provide access from a network that is behind a firewall. This interface accepts connections from protocols supported by the SRC software. When you configure an SRC component, the specified port is opened on this interface.

The eth1 interface is designed to provide access for applications on an external network, such as the Internet. You can configure a limited number of ports on this interface. By default, no inbound ports are open.

- Optional two additional Gigabit Ethernet interfaces—eth2 and eth3

These interfaces require an additional input/output module. You can obtain a module to support either RJ-45 or optical connections.

- Two USB interfaces

Configuring Gigabit Ethernet Interfaces for IPv4 (SRC CLI)

You can configure the Gigabit Ethernet interfaces to use IPv4 or IPv6 to allow remote access to the C-series Controller. You can specify an IP address with mask or a broadcast address with mask for an interface.

Use the following configuration statements to configure Gigabit Ethernet interfaces to use IP v4 and the [edit] hierarchy level:

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

To configure a Gigabit Ethernet interface to use IPv4:

1. From configuration mode, access the configuration statement that configures the interface.

```
[edit]
user@host# edit interfaces name unit unit-number
```

where *unit-number* is a number that you can assign for a logical interface identifier.

For example:

```
[edit]
user@host# edit interfaces eth0
```

2. Specify the unit, family, and IP address for the interface.

```
[edit interfaces eth0]
user@host# set unit number family inet address address
```

For example, to configure an interface with only an IP address:

```
[edit interfaces eth0]
user@host# set unit 0 family inet6 address 192.2.0.10/24
```

3. Verify the interface configuration.

```
[edit interfaces eth0]
user@host# show
unit 0 {
  family {
    inet6 {
      address 192.2.0.10/24;
    }
  }
}
```

Configuring Gigabit Ethernet Interfaces for IPv6 (SRC CLI)

You can configure the Gigabit Ethernet interfaces to use IPv4 or IPv6 to allow remote access to the C-series Controller. You can specify an IP address with mask or a broadcast address with mask for an interface.

Use the following configuration statement to configure Gigabit Ethernet interfaces to use IPv6 at the [edit] hierarchy level:

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

To configure a Gigabit Ethernet interface to use IPv6:

1. From configuration mode, access the configuration statement that configures the interface.

```
[edit]
user@host# edit interfaces name unit unit-number
```

where *unit-number* is a number that you can assign for a logical interface identifier.

For example:

```
[edit]
user@host# edit interfaces eth0
```

2. Specify the unit, family, and IP address for the interface.

```
[edit interfaces eth0]
user@host# set unit number family inet6 address address
```

For example:

```
[edit interfaces eth0]
user@host# set unit 0 family inet6 address 2001:DB8:10AB:CD30::1/64
```

3. Verify the interface configuration.

```
[edit interfaces eth0]
user@host# show
unit 0 {
```

```

family {
  inet6 {
    address 10AB:0:0:CD30::/20;
  }
}

```

Configuring Tunnel Interfaces (SRC CLI)

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 a JUNOSe router does not have a direct connection to the C-series Controller.

The C-series Controller supports the following types of tunnel interfaces:

- GRE—Generic routing encapsulation. Encapsulates traffic that can use various network protocols within IP. For C-series Controllers, the tunnel interface encapsulates IP packets.
- IP-over-IP—Encapsulates IP packets within IP packets.
- SIT—Encapsulates IPv6 traffic in an IPv4 tunnel. This type of tunnel allows compatibility of IPv6 traffic within an IPv4 network.

The other endpoint for the tunnel on a device must be configured for the tunnel to be operational.

The local address of a tunnel connection is an IP address that is configured for a unit (logical interface). Before you configure a tunnel interface, configure the interface on the C-series Controller.

See [Configuring Gigabit Ethernet Interfaces for IPv4 \(SRC CLI\)](#) .

Use the following configuration statements to configure tunnel interfaces at the **[edit]** hierarchy level:

```

interfaces name tunnel {
  mode (ipip | gre | sit);
  destination destination ;
  source source;
  key key ;
  interface interface ;
  ttl ttl ;
}
interfaces name unit unit-number family inet {
  address address ;
}

```

To configure a tunnel interface on a C-series Controller:

1. From configuration mode, access the configuration statement that configures tunnel interfaces.

```
[edit]
user@host# edit interfaces name tunnel
```

For example:

```
[edit]
user@host# edit interfaces ip-tunnel tunnel
```

2. Configure the type of tunnel.

```
[edit interfaces ip-tunnel tunnel]
user@host# set mode ipip
```

or

```
[edit interfaces ip-tunnel tunnel]
user@host# set mode gre
```

or

```
[edit interfaces ip-tunnel tunnel]
user@host# set mode sit
```

3. Specify the IP address of the remote end of the tunnel.

```
[edit interfaces ip-tunnel tunnel]
user@host# set destination destination
```

For example:

```
[edit interfaces ip-tunnel tunnel]
user@host# set destination 192.0.2.20
```

4. (Optional) Specify an IP address that will not change for the local tunnel endpoint. It must be an address on another interface of this host.

```
[edit interfaces ip-tunnel tunnel]
user@host# set source source
```

For example:

```
[edit interfaces ip-tunnel tunnel]
user@host# set source 192.20.10.5
```

5. (Optional) For a GRE tunnel, specify a key.

```
[edit interfaces ip-tunnel tunnel]
user@host# set key key
```

For example:

```
[edit interfaces ip-tunnel tunnel]
user@host# set key 250
```

6. (Optional) Specify an existing physical interface on the C-series Controller.

```
[edit interfaces ip-tunnel tunnel]
user@host# set interface interface
```

For example:

```
[edit interfaces ip-tunnel tunnel]
user@host# set interface eth0
```

7. (Optional) Specify the lifetime of tunneled packets.

```
[edit interfaces ip-tunnel tunnel]
user@host# set ttl ttl
```

For example:

```
[edit interfaces ip-tunnel tunnel]
user@host# set ttl 110
```

8. Verify the configuration by running the **show** command. For example:

```
[edit interfaces]
user@host# show

unit 0 {
  family {
    inet6 {
      address 192.2.0.10/24;
    }
  }
}
ip-tunnel {
  tunnel {
    mode ipip;
    destination 192.0.2.20;
    source 192.20.10.5;
    interface eth0;
    ttl 110;
  }
}
```

Configuring Ethernet Redundancy (SRC CLI)

Group interfaces let you aggregate network interfaces into a single logical interface to support Ethernet redundancy. The group interfaces provide either hot standby or load-balancing services.

When you configure group interfaces, be aware of the following restrictions:

- 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 at the [edit interfaces name unit] hierarchy level.
- Group interface and tunnel interface configurations are mutually exclusive. You cannot configure both types at the same time.

You can group interfaces in the following modes:

- Round-robin policy (balance-rr)—Transmit packets in sequential order from the first available device through the last.
- Active-backup policy (active-backup)—Create only one device that is active. A different device becomes active if, and only if, the active device fails.
- XOR policy (balance-xor)—Transmit based on the selected transmit hash policy.
- Broadcast policy (broadcast)—Transmit everything on all device interfaces.
- IEEE 802.3ad Dynamic link aggregation (802.3ad)—Create aggregation groups that share the same speed and duplex settings.
- Adaptive transmit load balancing (balance-tlb)—Create channel bonding that does not require any special switch support.
- Adaptive load balancing (balance-alb)—Includes adaptive transmit load balancing (balance-tlb) plus receive load balancing (rlb) for IPv4 traffic, and does not require any special switch support.

You can monitor link integrity with the ARP monitor or the MII monitor. You cannot use both the ARP monitor and the MII monitor at the same time.

The MII monitor monitors only the carrier state of the local network interface. The MII monitor does not provide a high level of detection for end-to-end connectivity failures.

The ARP monitor sends ARP queries to one or more designated peer systems on the network, and uses the response as an indication that the link is operating. The ARP monitor provides more reliable monitoring of end-to-end connectivity because you can set up several targets for high availability. However, some of the advanced load balancing modes do not support use of the ARP monitor.

Configuring Group Interfaces (SRC CLI)

Use the following statements to configure the group interface:

```
interfaces name group {
  mode (balance-rr | active-backup | balance-xor | broadcast | 802.3ad | balance-tlb |
    balance-alb);
  lacp-rate (slow | fast);
  interfaces [interfaces...];
  primary primary;
  transmit-hash-policy (layer2 | layer3+4);
```

```
}
```

To configure an Ethernet group interface:

1. From configuration mode, access the configuration statement that configures the bonded interface.

```
[edit]
user@host# edit interfaces name group
```

2. Specify the mode in which you want to group the interfaces.

```
[edit interfaces name group]
user@host# set mode mode
```

3. (Optional) Specify the rate at which the link partner is requested to transmit Link Aggregation Control Protocol Data Unit (LACPDU) packets in 802.3ad mode. This option is valid only for the 802.3ad mode.

```
[edit interfaces name group]
user@host# set lacp-rate (slow | fast)
```

where:

- **slow**—Request partner to transmit LACPDU every 30 seconds.
- **fast**—Request partner to transmit LACPDU every 1 second.

4. Specify the Ethernet interfaces in this group.

```
[edit interfaces name group]
user@host# set interfaces [interfaces...]
```

5. (Optional) Specify the device that will always be the active device while it is available. This option is valid only for the active-backup mode.

```
[edit interfaces name group]
user@host# set primary primary
```

6. (Optional) Specify the transmit hash policy to use for device selection in balance-xor and 802.3ad modes. This option is valid only for the balance-xor or 802.3ad mode.

```
[edit interfaces name group]
user@host# set transmit-hash-policy (layer2 | layer3+4)
```

where:

- **layer2**—Uses XOR of hardware MAC addresses to generate the hash.
- **layer3 + 4**—Uses upper-layer protocol information, when available, to generate the hash.

7. Configure the unit for the group interface.

Configuring the MII Monitor (SRC CLI)

Use the following statements to configure MII link monitoring:

```
interfaces name group {
  downdelay downdelay;
  updelay mii-monitoring-interval;
  mii-monitoring-interval mii-monitoring-interval;
}
```

To configure the MII monitor:

1. From configuration mode, access the configuration statement that configures the bonded interface.

```
[edit]
user@host# edit interfaces name group
```

2. (Optional) Specify the time to wait before disabling a device after a link failure has been detected. This option is valid only for the MII monitor.

```
[edit interfaces name group]
user@host# set downdelay downdelay
```

3. (Optional) Specify the time to wait before enabling a device after a link recovery has been detected. This option is valid only for the MII monitor.

```
[edit interfaces name group]
user@host# set updelay updelay
```

4. (Optional) Specify the MII link monitoring frequency.

```
[edit interfaces name group]
user@host# set mii-monitoring-interval mii-monitoring-interval
```

Configuring the ARP Monitor (SRC CLI)

Use the following statements to configure ARP link monitoring:

```
interfaces name group arp-monitoring {
  interval interval;
  ip-target [ip-target...];
}
```

To configure the ARP monitor:

1. From configuration mode, access the configuration statement that configures the ARP link monitoring for the bonded interface.

```
[edit]
user@host# edit interfaces name group arp-monitoring
```

2. Specify the ARP link monitoring frequency.

```
[edit interfaces name group arp-monitoring]
```

```
user@host# set interval interval
```

3. Specify the IP addresses to use as ARP monitoring peers. You must specify at least one address.

```
[edit interfaces name group arp-monitoring]
user@host# set ip-target [ip-target...]
```

Configuring the Virtual IP Address (SRC CLI)

You can configure the virtual IP address on the loopback interface.

To configure the virtual IP address:

1. From configuration mode, access the configuration statement that configures logical interface 1 for the loopback interface.

```
[edit]
user@host# edit interfaces lo unit 1
```

2. Specify the protocol family and virtual IP address.

```
[edit interfaces lo unit 1]
user@host# set family (inet | inet6) address address
```

For example, to configure a virtual IPv4 address:

```
[edit interfaces lo unit 1]
user@host# set family inet address 198.168.254.1/24
```

3. Verify the interface configuration.

```
[edit interfaces lo unit 1]
user@host# show
family {
  inet {
    address 198.168.254.1/24;
  }
}
```

Configuring a Static Route to Devices on Other Networks (SRC CLI)

In some instances, the SRC software might need to connect to devices that reside on networks other than the one that the SRC software accesses directly. You can configure a static route for the software to be able to connect devices on other networks.

When you specify IP addresses for a static route, include a network mask.

To configure a static route to another network:

- From configuration mode, enter the following command at the top level of the hierarchy.

```
[edit]
user@host# set routing-options static route destination next-hop next-hop
```

The **next-hop** option is required.

You can also specify that packets to the specified destination be dropped and that an ICMP unreachable message be returned.

To specify that packets to a specified network be dropped:

- From configuration mode, enter the following command at the top level of the hierarchy.

```
[edit]
user@host# set routing-options static route destination next-hop next-hop
reject
```

Securing Connections Between a C-series Controller and Remote Hosts

For security reasons, take care to limit the number of open ports you configure for applications and SRC components on the external interfaces.

By default, SSH for nonroot users is enabled on C-series Controllers. Otherwise, you configure the C-series Controller to explicitly allow users on remote systems to access it. Table 9 on page 79 lists the applications through which remote users can access a C-series Controller.

Table 9: Applications to Remotely Access the C-series Controller

Application	Information About Access Configuration
SSH	Configuring a C-series Controller to Accept SSH Connections (SRC CLI)
Telnet	Configuring a C-series Controller to Accept Telnet Connections (SRC CLI)
NETCONF	Configuring a C-series Controller to Accept NETCONF Connections (SRC CLI)
C-Web interface	Accessing the C-Web Interface
Policies, Services, and Subscribers CLI	Configuring Access to the Policies, Services, and Subscribers CLI

You can also configure security certificates for use by HTTPS connections.

You can connect from a C-series Controller to remote hosts through:

- SSH
- Telnet
- FTP by means of a file URL

Configuring a C-series Controller to Accept SSH Connections (SRC CLI)

You can enable SSH to let users who have the appropriate privileges connect to a C-series Controller. For security reasons, we recommend that you do not allow remote users to access the CLI as root.

Use the following configuration statements to enable SSH access from the [edit] hierarchy level:

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

To configure the C-series Controller to accept SSH connections:

1. From configuration mode, access the [edit system services ssh] hierarchy level.
2. (Optional) Specify that SSH version 1 be used.

```
[edit system services ssh]
user@host> set protocol-version v1
```

SSH version 2 is enabled by default.

3. (Optional) Specify whether or not to allow root login through SSH:

```
[edit system services ssh]
user@host> set root-login (allow | deny | deny-password)
```

where:

- **allow**—Allow users to log in to the C-series Controller as root through SSH.
- **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. (Default)

Configuring a C-series Controller to Accept Telnet Connections (SRC CLI)

You can enable Telnet to let users who have the appropriate privileges connect to a C-series Controller. The system does not allow root access over a Telnet connection.

Use the following configuration statements to enable Telnet access from the [edit] hierarchy level:

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

To configure the C-series Controller to accept Telnet connections:

```
[edit]
user@host# set system services telnet
```

Configuring a C-series Controller to Accept NETCONF Connections (SRC CLI)

Use the following configuration statements to enable NETCONF access from the [edit] hierarchy level:

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

To configure the C-series Controller to accept NETCONF connections:

1. From configuration mode, access the [edit system services netconf] hierarchy level.

```
[edit]
user@host# edit system services netconf
```

2. (Optional) Enable NETCONF to run over SSH.

```
[edit system services netconf]
user@host# set ssh
```

Port Settings for SRC Components

If you use firewall software within your internal network, ensure that firewall settings allow traffic to and from components in your SRC environment. Table 10 on page 82 lists the default port settings for SRC components.

For information about default port settings for applications in the SRC application library, see Reviewing SRC Port Settings for SRC Applications.

Table 10: Default Port Settings for SRC Components

Component	Type of Communication	Default Port Setting
Applications, such as portals, that use the SAE Common Object Request Broker Architecture (CORBA) remote application programming interface (API)	CORBA remote API connections to the SAE.	TCP 8801
Cable modem termination system (CMTS) devices	Connection requests.	TCP 3918
Sample residential portal with Tomcata	Starting Tomcat server.	TCP 8005
	Apache JServ Protocol (AJP) requests for Tomcat.	TCP 8009
	Responses to incoming HTTP requests from Tomcat.	TCP 8080)
	This port is an alternative to port 80.	
JBossb	Remote method invocation (RMI) requests.	TCP 1099
	Communications for the Java Naming and Directory Interface (JNDI).	TCP 1100
License server	Messages from SAEs to the license server.	TCP 9000
	All SAEs in a configuration must be able to reach the license server.	
LDAP	Communications between LDAP and other components in an SRC environment, such as the SAE, NIC, and SNMP.	TCP 389
Network information collector (NIC)	Communications between the NIC host and components, such as portals, that use the NIC.	TCP 8810
	All components that use NIC resolution must be able to reach the NIC host.	
RADIUS	Communications between RADIUS and the SAE.	UDP 1812
	Communications between RADIUS and the SAE for RADIUS accounting.	UDP 1813
Redirect engine	Redirection requests.	TCP 8800

Table 10: Default Port Settings for SRC Components *(continued)*

Component	Type of Communication	Default Port Setting
SAE	Common Open Policy Service (COPS) connection from JUNOSe routers.	TCP 3288
	Blocks Extensible Exchange Protocol (BEEP) connection from JUNOS routers.	TCP 3333
	BEEP with Transport Layer Security (TLS)	TCP 3434
	Session store data replication.	TCP 8820
SAE Web Admin	Secure HTTP.	TCP 8443
SNMP agent	SNMP communications between SNMP subagents and the master SNMP agent.	UDP 8030
	SNMP get and set messages.	UDP 161
	SNMP traps.	UDP 162

In addition, we recommend that TCP port 123 be open for the Network Time Protocol (NTP). We recommend that you configure NTP to synchronize time on the network. See the documentation for the NTP server for your system.

Part 3

Managing SRC Licenses

- Overview of SRC Licenses on page 87
- Overview of the SRC License Server on page 89
- Installing Licenses for C-series Controllers on page 93

Chapter 8

Overview of SRC Licenses

- Types of SRC Licenses on page 87
- Obtaining an SRC License on page 88

Types of SRC Licenses

You must obtain a license for the SRC software from Juniper Networks Customer Services and Support. Juniper Networks provides two mutually exclusive types of licenses for the SRC software:

- Pilot license—Limits the number of concurrent active subscriber sessions on an SAE. The number of sessions used at any one time cannot exceed the number permitted by the pilot license. The SAE license manager manages pilot licenses. Use the pilot license for field trials of the SRC software.
- Server license—Limits the number of concurrent active SAE service sessions. The server license is managed by the SRC license server, which reads the license, leases a portion of the license on demand to each SAE client, monitors the consumption of the license, and raises alarms when necessary. For server licenses, the SAE client does not involve the directory for license management. Use the server license for a production implementation of the SRC software.

The server license replaces the production license used in earlier releases of the SRC software. A production license limited the capacity of the entire network under SAE management and optionally specified the maximum number of SAE services that were concurrently available to be activated by subscribers, an expiration date, or both.



NOTE: The license server must be the same version as the SAE. For example, if you are using the license server and upgrade the SAE version, you must upgrade the license server to the same version.

If you have both a server license and a pilot license, the SRC software enforces the server license.

Related Topics

- Obtaining an SRC License
- Installing a Pilot License from the SRC CLI
- Installing Server Licenses for C-series Controllers

Obtaining an SRC License

Before you install the SRC software, collect information about the system that will run the SAE as described in the following sections; then contact Juniper Networks Customer Services and Support and provide this system information to obtain a license.

Pilot License

To obtain a pilot license, you must provide the following information:

- Username to be listed in the license key
- Host ID of the SAE host (or the host IDs of all hosts if you have more than one)
- Number of concurrent users that you want to be able to connect to the SAE

You can determine the host ID by issuing the following command on a C-series Controller:

```
user@host> show system information
```

Look for the value for **Hostid** in the output; for example:

```
Hostid      e30a2e07
```

Server License

To obtain a server license, you must provide the following information:

- Username to be listed in the license key
- Maximum number of concurrently active SAE services that you require
- Time interval for which you need the server license
- IP address or hostname of the license server. The SAE requires access to this IP address or hostname.

Related Topics

- Types of SRC Licenses
- Installing a Pilot License from the SRC CLI
- Installing Server Licenses for C-series Controllers

Chapter 9

Overview of the SRC License Server

- Overview of the SRC License Server on page 89
- Unsuccessful Connections from the SAE to the SRC License Server on page 91
- SRC License Server Redundancy on page 92

Overview of the SRC License Server

The SRC license server manages server licenses for the SAE by using Common Object Request Broker Architecture (CORBA) to communicate with its client SAEs.

The SAE retrieves its licensing configuration properties from the SRC directory at startup. The license manager for an SAE maintains the licenses for that SAE and communicates with the license server to obtain more licenses or return unused licenses. You can configure properties specific to each SAE license manager.

Server License

The server license includes a license key signature, customer name, expiration date, number of concurrent active service sessions, a CORBA reference for the license server, and other attributes.

The CORBA reference enables the license server's SAE clients to locate the server to obtain a license unit. (A license unit is also referred to as a lease.) The SAE disregards who activates service sessions and simply monitors the number of active service sessions.

License Server Errors

If the license checking process does not discover a valid license, it logs an error message and terminates itself. This check can take a while to finish; on a slow server at the first start after an installation, it can take up to several minutes.

You may wish to look at the information log during the startup for a message declaring a missing license or indicating that the SAE startup has been completed.

License Requests

When the license server receives a request for a lease from the SAE, the license server calculates the number of leases in use if the request is granted and compares that value to a limit specified in the license:

- When the new total is below the limit, the license server grants the requested lease to the client.
- If the new total exceeds the limit, the license server grants leases up to the amount available.
- If the current total exceeds the license limit, the license server denies all requests.

On startup, client SAEs search for a valid license in the LDAP object `cn = @License, ou = licSvr, ou = Licenses, o = Management, < base >`. If the SAE finds a valid license that includes a reference to the license server (`license.server.corbaloc` property), then before it activates new service sessions the SAE contacts the license server to lease a license unit. The SAE request includes the name of a virtual router that it associates with service sessions.

When a lease is granted, it specifies the:

- Chunk size—Number of active service sessions
- Lease duration—Length of time allotted to a grant
- Allocation threshold—A percentage of the license chunk size that defines how many licenses are available for allocation
- Release threshold—A percentage of the license chunk size that defines when a lease is released

The license server stores the number of granted license units associated with each virtual router name in an internal table.

Because license leases are allocated in advance of actual need, a license is available when a subscriber tries to activate a service. The SAE requests an additional license lease when the number of active service sessions on a particular virtual router reaches the allocation threshold.

Example: License Allocation

This example shows how the SAE requests another lease when its current lease reaches a specified threshold. For a chunk size of 50 and an allocation threshold of 90 %, the SAE requests a second lease when the number of active service sessions reaches 45 ($50 \times 90\%$). Once the lease is granted, if the active service sessions continue to increase, the SAE requests another lease when the number of active service sessions reaches 95, and again at 145.

Example: License Release Example

License units are released as active service sessions decrease, with the SAE retaining more licenses than it currently needs to avoid fluctuation around the threshold. For

example, a lease has a chunk size of 50, a release threshold of 10 %, and four license chunks (200 licenses) allocated to the SAE. In this case:

- If the number of active service sessions drops to 105, the fourth license unit is released, leaving three units and 150 licenses.
- If the number of active service sessions drops to 55, the third license unit is released, leaving two units and 100 licenses.
- If the number of active service sessions drops to 5, the second license unit is released, leaving one unit and 50 licenses.

Lease Renewal

The SAE renews a lease every one-third of the lease duration even if the number of active service sessions stays in the same range. If the SAE cannot renew the lease for any reason (such as a network failure) before the lease expires, the SAE releases the lease and does not accept new service sessions until it receives a new grant from the license server. While in this state, the SAE logs an error message for each request and returns the same message through the API. The message includes the service name, subscriber, and reason for rejection.

Directory Location and Access

Server licenses are stored in the directory entry *cn = @License, ou = licSvr, ou = Licenses, ou = Configuration, o = Management, < base >*. The authentication distinguished name (DN) and password needed to access the license object are stored in the */opt/UMC/licsvr/etc/bootstrap.properties* file. The license server reads its configuration properties from the object (default) *l = config, l = LICSVR, ou = staticConfiguration, ou = Configuration, o = Management, < base >*.

The license server reads the license from the SRC directory at startup. The license server continues to poll the directory to check for updated licenses. The master license is *cn = @License*. The license server does not accept client requests without the master license. You can add more licenses to increase the limit on the number of service sessions. Adding these licenses does not require restarting the license server.

Unsuccessful Connections from the SAE to the SRC License Server

If the SAE fails to connect to the license server at startup or the license does not include the CORBA reference, then the SAE goes into a fallback mode and looks for a server license of the type issued for earlier releases of the SRC software. These early licenses limited the capacity of the network managed by the SAE and/or the number of SAE services that were concurrently available to be activated by subscribers; Juniper Networks no longer issues these licenses.

If the SAE cannot find any server licenses, then it looks for a pilot license associated in the directory with its host ID. If the SAE cannot obtain a license, it closes itself.

The SAE polls the directory at specified intervals to detect license upgrades or additions. Server licenses are preferred over pilot licenses. If the SAE detects a license with a higher preference than the one in current use, it switches to that license. For

example, if the SAE is using a pilot license and detects a server license, it switches to the server license.

If the current license is removed from the directory or if the directory becomes unavailable, the SAE goes into an idle mode and does not accept any further requests to activate a new service session.

SRC License Server Redundancy

When a primary SAE becomes unavailable, the secondary SAE issues a request to take over the service sessions from the primary SAE. Because the license server keeps track of granted license units by associating them with virtual routers, the secondary SAE is always granted license units for the same virtual routers that the primary SAE has been managing.

If an SAE loses connectivity to the license server, the SAE continues to grant licenses up to the maximum number of licenses configured for the license server for up to 14 days. Subscribers connecting to the SAE should see no service disruption.

When the SAE has access to the license server again, the total number of licenses in use is evaluated. License grants are made on a first-come first-served basis, with SAEs being granted licenses within the license limit:

- If the total number of licenses in use is lower than the licenses limit, all SAEs continue operating in the same manner as before the outage.
- If the total number of licenses in use is higher than the license limit, an SAE does not receive new license grants if it asks to renew its licenses. Each SAE continues to grant service sessions within the licenses currently owned. The SAE does not terminate any active sessions.

Chapter 10

Installing Licenses for C-series Controllers

- Installing a Pilot License from the SRC CLI on page 93
- Installing Server Licenses for C-series Controllers on page 94
- Configuring License Manager for an SAE on a C-series Controller on page 95

Installing a Pilot License from the SRC CLI

You install pilot licenses on C-series Controllers from the SRC CLI. Before you install a pilot license, make sure that the Juniper Networks database is running on a C-series Controller.

When you enable the SAE on a C-series Controller, the software verifies that a license is installed.

To install a pilot license:

1. On a C-series Controller on which the Juniper Networks database is configured to have a primary role, use the `request sae import-pilot-license` command:

```
user@host> request sae import-pilot-license file-name file-name <server-address  
server-address > <name-space name-space > <authentication-dn  
authentication-dn > <password password >
```

where:

- *file-name* —Name of the file that contains the SRC license
 - *server-address* —IP address for the primary directory server. For C-series Controllers, this is the platform that has the Juniper Networks database configured to have a primary role.
 - *namespace* —Base DN for the directory. In most cases you can use the default <base>.
 - *authentication-dn* —DN used for directory authentication.
 - *password* —Password used for directory authentication.
2. Verify that a valid license is available:

```

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

Type of license: Pilot. Status: OK.

The following valid licenses are found:

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

```

- Related Topics**
- Types of SRC Licenses
 - Obtaining an SRC License

Installing Server Licenses for C-series Controllers

To use a server license on a C-series Controller, a Juniper Networks database must run on the same C-series Controller as the license server.

To install server licenses for C-series Controllers:

1. From operational mode, enable the license server.

```
user@host> enable component licSrv
```

2. Install the server license.

```
user@host> request license import master-license file-name file-name
```

3. Verify that a valid license is available.

```
user@host> show sae licenses
```

4. Configure license manager for the SAE.

See Configuring License Manager for an SAE on a C-series Controller .

- Related Topics**
- Types of SRC Licenses
 - Obtaining an SRC License

Configuring License Manager for an SAE on a C-series Controller

Use the following configuration statements to configure the SAE license manager at the [edit] hierarchy level.

```
shared sae configuration license-manager client {
    type type ;
    cache cache ;
}
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;
}
```

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

To configure the SAE license manager:

1. From configuration mode, access the configuration statement that configures the SAE client for the license manager at the [edit] hierarchy level.

```
[edit]
user@host# edit shared sae configuration license-manager client
```

2. Specify the client type.

```
[edit shared sae configuration license-manager client]
user@host# edit type SDX
```

SDX is the only supported license type.

3. Specify the path to the cache file.

```
[edit shared sae configuration license-manager client]
user@host# edit cache cache
```

The default is *var/run/lic_cache*.

4. Access the configuration statement that configures directory access for the SAE client for the license manager at the [edit] hierarchy level.

```
[edit shared sae configuration license-manager client]
user@host# up
```

```
[edit shared sae configuration license-manager]
user@host# edit directory-access
```

```
[edit shared sae configuration license-manager directory-access]
user@host#
```

5. (Optional) Specify the IP address or hostname of the server that stores licensing data.

```
[edit shared sae configuration license-manager directory-access]
user@host# set server-address server-address
```

6. Specify the port number of the LDAP connection to the directory server that stores licensing data.

```
[edit shared sae configuration license-manager directory-access]
user@host# set server-port server-port
```

The default port is 389.

7. Specify the DN of the subtree in the directory where licensing information is stored. The SAE searches for the license key below this path.

```
[edit shared sae configuration license-manager directory-access]
user@host# set license-dn license-dn
```

The default is ou = Licenses,o = Management, < base > .

8. Specify the DN used by the SAE to authenticate access to the directory server.

```
[edit shared sae configuration license-manager directory-access]
user@host# set authentication-dn authentication-dn
```

The default is cn = license-operator,o = Operators, < base > .

9. Specify the password used to authenticate access to the directory.

```
[edit shared sae configuration license-manager directory-access]
user@host# set password password
```

10. (Optional) Enable LDAPS as the secure protocol for connections to the directory server that stores license data.

```
[edit shared sae configuration license-manager directory-access]
user@host# set ldaps
```

11. Specify the connection manager for the directory eventing system within the Java Naming and Directory Interface (JNDI) framework

```
[edit shared sae configuration license-manager directory-access]
user@host# set connection-manager-id connection-manager-id
```

The default is LICENSE_MANAGER.

12. (Optional) Specify the base DN for the license manager data.

```
[edit shared sae configuration license-manager directory-access]
user@host# set event-base-dn event-base-dn
```

The default is `< base >` which refers to the globally configured base DN.

13. (Optional. Not needed if you use the Juniper Networks database.) Specify the DN of the entry identified by the LDAP schema attribute `usedDirectory`. This attribute identifies the type of directory, such as DirX on which the license data is stored.

```
[edit shared sae configuration license-manager directory-access]
user@host# set signature-dn signature-dn
```

14. (Optional) Enable the SRC SNMP agent to export MIBs for this directory connection.

```
[edit shared sae configuration license-manager directory-access]
user@host# set snmp-agent
```


Part 4

Managing an Environment of C-series Controllers

- Configuring System Time on C-Series Controllers (SRC CLI) on page 101
- Configuring NTP for C-Series Controllers on page 103
- Configuring NTP on C-Series Controllers (SRC CLI) on page 107
- Configuring System Logging for a C-series Controller (SRC CLI) on page 117
- Configuring Static Host Mapping (SRC CLI) on page 123
- Overview of the Juniper Networks Database on page 125
- Managing the Juniper Networks Database (SRC CLI) on page 129
- Setting Up an SAE (SRC CLI) on page 145
- Managing System Software on a C-series Controller on page 151
- Using the Web Application Server on a C-series Controller on page 157
- Integrating Steel-Belted Radius/SPE Server on page 165

Chapter 11

Configuring System Time on C-Series Controllers (SRC CLI)

- Setting the Time Zone (SRC CLI) on page 101
- Setting the System Date (SRC CLI) on page 102

Setting the Time Zone (SRC CLI)

Use one of the following formats for the **set time-zone** command to set the time zone on a C-series Controller:

- (Recommended) Continent or nation with major city or province.

To see a list of entries in this format, use the ? help at the CLI:

```
[edit system]
user@host# set time-zone ?
Possible completions:
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
Africa/Algiers
Africa/Asmera
Africa/Bamako
Africa/Bangui
Africa/Banjul
. . .
```

- GMT offset to set the time zone relative to UTC (GMT) time in the format */Etc/GMToffset* . Time zone files are stored in the */Etc* directory.
- A common zone such as UTC, MDT, or EST.

To modify the local time zone:

1. In configuration mode at the [edit system] hierarchy level, set the time zone.

```
[edit system]
user@host# set time-zone time-zone
```

For example, to set the time zone for New York:

```
[edit system]
```

```
user@host# set system time-zone America/New_York
```

2. Verify the configuration. For example:

```
[edit system]
user@host# show
time-zone America/New_York;
```

3. For the time zone change to take effect for all processes running on the system, reboot the system.

- Related Topics**
- Setting the System Date (SRC CLI)
 - NTP Support on C-series Controllers

Setting the System Date (SRC CLI)

If you need to set the date and time on the system and NTP is not configured, you can use the **set date** command. This command is available only if NTP is not running on the system.

To set the system date and time:

- In operational mode, set the date and time in the format YYYYMMDDhhmm.ss.

```
user@host> set date date
```

For example, to set the date and time to 1:05 PM on February 21, 2007:

```
user@host> set date 200702211305:00
```

- Related Topics**
- Setting the Time Zone (SRC CLI)
 - NTP Support on C-series Controllers

Chapter 12

Configuring NTP for C-Series Controllers

- NTP Support on C-series Controllers on page 103
- Configuring NTP on a C-series Controller on page 104

NTP Support on C-series Controllers

NTP synchronizes and coordinates time among NTP clients and servers. It uses a returnable-time design in which a distributed subnet of time servers operate in a self-organizing, hierarchical, master-slave configuration. NTP synchronizes time for local clocks within a subnet and to another server or other time source such as a high-precision clock or satellite receiver. NTP clients are also servers that distribute a time synchronized to another NTP server.

NTP is defined in RFC 1305—Network Time Protocol (Version 3) Specification Implementation and Analysis (March 1992)..



NOTE: We highly recommend that you use NTP to set the system time to ensure that the SRC software operates correctly.

For NTP servers on C-series Controllers, if the time difference between the local NTP server and the servers with which it synchronizes time is more than 1000 seconds, the local NTP server stops running. Configure a boot server for NTP so that the software obtains the initial time from the boot server before the NTP server starts.

When you configure NTP, you can specify which system on the network is the authoritative time source, or time server, and how time is synchronized between systems on the network. You can configure NTP to operate in one or more of the following modes:

- Client mode—The local system can be synchronized with the remote system, but the remote system cannot be synchronized with the local system.
- Symmetric active (peer) mode—The local system and the remote system can synchronize with each other. You use this mode in a network in which either the local system or the remote system might be a better source of time.



NOTE: Symmetric active mode can be initiated by either the local or the remote system. Only one system needs to be configured to do so. This means that the local system can synchronize with any system that offers symmetric active mode without any configuration whatsoever. However, we highly recommend that you configure authentication to ensure that the local system synchronizes only with known time servers.

- Broadcast 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.
- Server mode—The local system operates as an NTP server.

You can also configure NTP to operate as a broadcast client or a multicast client.

Related Topics

- Configuring NTP on a C-series Controller
- Configuration Statements for NTP on C-series Controllers

Configuring NTP on a C-series Controller

To configure NTP on a C-series Controller:

1. (Recommended) Configure NTP to automatically set the time when it starts.
 - See [Specifying Which NTP Server a C-series Controller Contacts on Startup](#).
 - See [Specifying a Basic NTP Configuration on a C-series Controller \(C-Web Interface\)](#).
2. Specify the time source and the manner in which time is synchronized between systems on the network. Configure NTP to operate in one or more of the following modes:
 - Client mode:
 - See [Configuring NTP Client Mode for a C-series Controller \(SRC CLI\)](#).
 - See [Configuring NTP Client Mode for a C-series Controller \(C-Web Interface\)](#).
 - Symmetric active (peer) mode:
 - See [Configuring an NTP Peer on a C-series Controller \(SRC CLI\)](#).
 - See [Configuring an NTP Peer for a C-series Controller \(C-Web Interface\)](#).
 - Broadcast mode:
 - See [Configuring NTP Broadcast Mode on a C-series Controller \(SRC CLI\)](#).
 - See [Configuring NTP Broadcast Mode on a C-series Controller \(C-Web Interface\)](#).

3. (Recommended) Configure NTP authentication.
 - See Specifying an Authentication Key for NTP on C-series Controllers (C-Web Interface).
 - See Configuring NTP Authentication (C-Web Interface).
4. (Optional) Configure NTP to listen for broadcast messages.
 - See Configuring NTP as a Broadcast Client on a C-series Controller (SRC CLI).
 - See Specifying a Basic NTP Configuration on a C-series Controller (C-Web Interface).
5. (Optional) Configure NTP to listen for multicast messages.
 - See Configuring NTP as a Multicast Client on a C-series Controller (SRC CLI).
 - See Configuring NTP as a Multicast Client on a C-series Controller (C-Web Interface).

- Related Topics**
- NTP Support on C-series Controllers
 - Verifying NTP Configuration on a C-series Controller

Chapter 13

Configuring NTP on C-Series Controllers (SRC CLI)

- Configuration Statements for NTP on C-series Controllers on page 107
- Specifying Which NTP Server a C-series Controller Contacts on Startup on page 108
- Configuring NTP Client Mode for a C-series Controller (SRC CLI) on page 109
- Configuring an NTP Peer on a C-series Controller (SRC CLI) on page 109
- Configuring NTP Broadcast Mode on a C-series Controller (SRC CLI) on page 110
- Configuring NTP Authentication on a C-series Controller (SRC CLI) on page 111
- Configuring NTP as a Broadcast Client on a C-series Controller (SRC CLI) on page 113
- Configuring NTP as a Multicast Client on a C-series Controller (SRC CLI) on page 114
- Verifying NTP Configuration on a C-series Controller on page 115

Configuration Statements for NTP on C-series Controllers

Use the following configuration statements to configure NTP on a C-series Controller at the [edit] hierarchy level.

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

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

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

```
system ntp multicast-client {
```

```

        address;
    }

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

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

```

- Related Topics**
- *SRC-PE CLI Command Reference*
 - NTP Support on C-series Controllers
 - Specifying Which NTP Server a C-series Controller Contacts on Startup

Specifying Which NTP Server a C-series Controller Contacts on Startup

When you boot a C-series Controller, it issues an `ntpdate` request, which polls a network server to determine the local date and time. Configure a server that the system uses to determine the time when the system boots. Otherwise, NTP cannot synchronize with a time server if the server's time is very far off the local system's time.

To configure the NTP boot server:

1. From configuration mode, access the configuration statement that configures NTP.

```

[edit]
user@host# edit system ntp

```

2. Specify the address or hostname of the network NTP server.

```

[edit system ntp]
user@host# set boot-server address

```

For example:

```

[edit system ntp]
user@host# set boot-server 192.0.2.20

```

- Related Topics**
- NTP Support on C-series Controllers
 - Configuration Statements for NTP on C-series Controllers
 - Verifying NTP Configuration on a C-series Controller

Configuring NTP Client Mode for a C-series Controller (SRC CLI)

Use the following configuration statements to configure NTP on a C-series Controller to operate in client mode:

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

To configure NTP to operate in client mode:

1. From configuration mode, access the configuration statement that configures an NTP server, and specify the IP address or hostname of an NTP server.

```
[edit system ntp]
user@host# edit server address
```

For example, to specify an NTP server that has an IP address of 192.0.2.30:

```
[edit system ntp]
user@host# edit server 192.0.2.30
```

```
[edit system ntp server 192.0.2.30]
user@host#
```

2. (Optional) Specify the version of NTP to be used for outgoing packets.

```
[edit system ntp server address ]
user@host# set version version
```

3. (Optional) If you configure more than one time server, specify whether this server is to be contacted first for synchronization.

```
[edit system ntp server address ]
user@host# set prefer
```

- Related Topics**
- NTP Support on C-series Controllers
 - Specifying Which NTP Server a C-series Controller Contacts on Startup
 - Configuration Statements for NTP on C-series Controllers
 - Verifying NTP Configuration on a C-series Controller

Configuring an NTP Peer on a C-series Controller (SRC CLI)

Use the following configuration statements to configure NTP on a C-series Controller to operate in symmetric active mode:

```
edit system ntp peer address {
  version version;
```

```
    prefer;
}
```

To configure NTP to operate in symmetric active mode:

1. From configuration mode, access the configuration statement that configures an NTP peer, and specify the IP address or hostname of an NTP peer.

```
[edit system ntp]
user@host# edit peer address
```

For example, to specify an NTP peer that has an IP address of 192.0.2.40:

```
[edit system ntp]
user@host# edit peer 192.0.2.40
```

```
[edit system ntp peer 192.0.2.40]
user@host#
```

2. (Optional) Specify the version of NTP to be used for outgoing packets.

```
[edit system ntp server address ]
user@host# set version version
```

3. (Optional) If you configure more than one peer, specify whether this server is to be contacted first for synchronization.

```
[edit system ntp server address ]
user@host# set prefer
```

- Related Topics**
- NTP Support on C-series Controllers
 - Specifying Which NTP Server a C-series Controller Contacts on Startup
 - Configuration Statements for NTP on C-series Controllers
 - Verifying NTP Configuration on a C-series Controller

Configuring NTP Broadcast Mode on a C-series Controller (SRC CLI)

Use the following configuration statements to configure NTP on a C-series Controller to operate in broadcast mode:

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

To configure NTP to operate in broadcast mode:

1. From configuration mode, access the configuration statement that configures NTP broadcast, and specify the broadcast address on one of the local networks

or a multicast address assigned to NTP. You can specify an IP address or a hostname.

We recommend that you use the multicast address 224.0.1.1 because the Internet Assigned Numbers Authority (IANA) assigns this address for NTP; however, you can use a different address for local deployments.

```
[edit system ntp]
user@host# edit broadcast address
```

For example, to specify the broadcast address of 244.0.1.1:

```
[edit system ntp]
user@host# edit broadcast 224.0.1.1
```

```
[edit system ntp broadcast 224.0.1.1]
user@host#
```

2. (Optional) Specify the version of NTP to be used for outgoing packets.

```
[edit system ntp broadcast address ]
user@host# set version version
```

3. (Optional) Specify the time-to-live value to transmit.

```
[edit system ntp server address ]
user@host# set ttl ttl
```

- Related Topics**
- NTP Support on C-series Controllers
 - Specifying Which NTP Server a C-series Controller Contacts on Startup
 - Configuration Statements for NTP on C-series Controllers
 - Verifying NTP Configuration on a C-series Controller

Configuring NTP Authentication on a C-series Controller (SRC CLI)

You can authenticate time synchronization to ensure that a C-series Controller obtains its time services only from known sources. By default, network time synchronization is unauthenticated; the system synchronizes to whatever system appears to have the most accurate time. We highly recommend that you configure authentication of network time services.

Use the following configuration mode statements to configure authentication for NTP on a C-series Controller:

```
system ntp {
  trusted-key [trusted-key...];
}
```

```
system ntp authentication-key key-number {
```

```

    value value;
}

system ntp broadcast address {
    key key;
}

system ntp peer address {
    key key;
}

system ntp server address {
    key key;
}

```

To configure NTP authentication:

1. Specify authentication for other time servers.

Only time servers transmitting network time packets that contain one of the specified key numbers and whose key matches the value configured for that key number are eligible for synchronization. Other systems can synchronize with the local system without being authenticated.

```

[edit system ntp]
user@host# set trusted-key [trusted-key...]

```

where *trusted-key* is a value in the range 1–2147483647.

For example:

```

[edit system ntp]
user@host# set trusted-key 1

```

2. Depending on the mode configured for NTP, specify a key value at the [edit system ntp server], [edit system ntp peer], or [edit system ntp broadcast] hierarchy level. For example:

```

[edit system ntp server address ]
user@host# set key key

```

For example:

```

[edit system ntp server 192.0.2.30]
user@host# set key key1

```

The system transmits the specified authentication key when transmitting packets. The key is necessary if the remote system has authentication enabled so that it can synchronize with the local system.

3. Define the authentication keys by assigning a number to the key and configuring its value.

```

[edit system ntp]

```

```
user@host# edit authentication-key key-number
```

```
[edit system ntp authentication-key key-number ]
user@host# set value value
```

The *key-number* is the key number for the key. The key number must match on all systems using that particular key for authentication.

For example:

```
[edit system ntp]
user@host# edit authentication-key 1

[edit system ntp authentication-key 1]
user@host# set value X7VY4ZE
```

4. Verify the configuration.

```
[edit system ntp]
user@host# show
trusted-key 1;
server 192.0.2.30 key 1;
authentication-key 1 {
    value *****;
}
```

- Related Topics**
- NTP Support on C-series Controllers
 - Specifying Which NTP Server a C-series Controller Contacts on Startup
 - Configuration Statements for NTP on C-series Controllers

Configuring NTP as a Broadcast Client on a C-series Controller (SRC CLI)

You can configure NTP on a C-series Controller to listen for broadcast messages on the local network to discover other servers on the same subnet. When NTP receives a broadcast message for the first time, it measures the nominal network delay using a brief client-server exchange with the remote server. It then enters *broadcast client* mode, in which it listens for, and synchronizes with, succeeding broadcast messages.

To avoid accidental or malicious disruption in this mode, both the local and remote systems must use authentication and the same trusted key and key identifier.

To configure NTP to listen for broadcast messages:

1. From the [edit system ntp] hierarchy level, specify that NTP listen for broadcast messages.

```
[edit system ntp]
user@host# set broadcast-client
```

2. Authenticate time synchronization to ensure that the local system obtains its time only from known sources.

See Configuring NTP Authentication on a C-series Controller (SRC CLI) .

3. Verify the configuration. For example:

```
[edit system ntp]
user@host# show
broadcast-client;
trusted-key 1;
server 192.0.2.30 key 1;
authentication-key 1 {
  value *****;
}
```

- Related Topics**
- NTP Support on C-series Controllers
 - Specifying Which NTP Server a C-series Controller Contacts on Startup
 - Configuration Statements for NTP on C-series Controllers

Configuring NTP as a Multicast Client on a C-series Controller (SRC CLI)

You can configure NTP on a C-series Controller to listen for multicast messages on the local network to discover other servers on the same subnet. When NTP receives a multicast message for the first time, it measures the nominal network delay using a brief client-server exchange with the remote server. It then enters *multicast client* mode, in which it listens for, and synchronizes with, succeeding multicast messages.

You can specify one or more IP addresses or hostnames. The hosts then join those multicast groups.

To avoid accidental or malicious disruption in this mode, both the local and remote systems must use authentication and the same trusted key and key identifier.

To configure NTP to listen for multicast messages:

1. From the [edit system ntp] hierarchy level, specify that NTP listen for multicast messages.

```
edit system ntp]
user@host# set multicast-client address
```

For example:

```
[edit system ntp]
user@host# set multicast-client 224.0.1.1
```

2. Authenticate time synchronization to ensure that the local system obtains its time only from known sources.

See Configuring NTP Authentication on a C-series Controller (SRC CLI) .

3. Verify the configuration. For example:

```
[edit system ntp]
user@host# show
multicast-client 224.0.1.1;
trusted-key 1;
server 192.0.2.30 key 1;
authentication-key 1 {
    value *****;
}
```

- Related Topics**
- NTP Support on C-series Controllers
 - Specifying Which NTP Server a C-series Controller Contacts on Startup
 - Configuration Statements for NTP on C-series Controllers

Verifying NTP Configuration on a C-series Controller

Purpose To verify the configuration for NTP.

Action At the [edit system ntp] hierarchy level, enter the **show** command. For example:

```
[edit system ntp]
user@host# show
boot-server 192.0.2.20;
multicast-client 192.0.2.15;
trusted-key 1;
server 192.0.2.30 key 1;
server 192.0.2.25;
authentication-key 1 {
    value *****;
}
```

- Related Topics**
- NTP Support on C-series Controllers
 - Specifying Which NTP Server a C-series Controller Contacts on Startup
 - Configuration Statements for NTP on C-series Controllers

Chapter 14

Configuring System Logging for a C-series Controller (SRC CLI)

- Overview of the C-series Controller Log Server on page 117
- Before You Configure System Logging (SRC CLI) on page 118
- Configuration Statements for System Logging on a C-series Controller on page 118
- Saving System Log Messages to a File (SRC CLI) on page 119
- Sending System Log Messages to Other Servers (SRC CLI) on page 119
- Sending Notifications for System Log Messages to Users (SRC CLI) on page 120

Overview of the C-series Controller Log Server

The C-series Controller includes a system log server that you can configure to manage messages generated on the system. These messages record events that occur to system processes and components.

You can configure the system log server on a C-series Controller to send messages about events to:

- A local file
- Other hosts that are running a system log server
- Users who need to be notified about particular error conditions

You configure which groups of messages are to be forwarded by message type and severity level.

Message Groups

Message groups (also called facilities) define sets of messages generated by the same software process or concerned with a similar condition or activity (such as authentication attempts).

You can configure the following message groups for the system log server:

- 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 Levels

You can specify the following severity levels for groups of messages to be forwarded:

- 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.

Before You Configure System Logging (SRC CLI)

Before you configure the syslog server on a C-series Controller, you should be familiar with:

- The syslog protocol
- Logging for SRC components

See *Configuring System Logging with SRC CLI* or *Configuring a Component to Store Log Messages in a File with SRC CLI*.

Configuration Statements for System Logging on a C-series Controller

Use the following configuration statements to configure the system log server at the [edit] hierarchy level.

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

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

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

Saving System Log Messages to a File (SRC CLI)

Use the following statements to configure the system log server to store messages in a file:

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

By default, message files are stored in the */var/log* directory. All log files are rotated daily. When a new log file is created, the previous day's file is compressed and saved. After rotation, the software retains only the last five compressed log files.

To configure the system log server to send messages to a file on the local C-series Controller:

1. From configuration mode, access the configuration statement that configures the system log server.

```
[edit]
user@host# edit system syslog
```

2. Specify the name of the file to store messages, and group and severity level for the messages.

```
[edit system syslog]
user@host# set file file-name message-group severity
```

For example, to configure the system log server to save critical messages generated by authentication and authorization attempts to the file named *access*:

```
[edit system syslog]
user@host# set file access authorization critical
```

Sending System Log Messages to Other Servers (SRC CLI)

Use the following statements to configure the system log server to send messages to another system log server:

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

```
}
```

Before you configure the system log server to send messages to other system log servers, ensure that the remote system log server is configured to receive messages on the standard UDP port, 514.

To configure the system log server to send messages to another system log server:

1. From configuration mode, access the configuration statement that configures the system log server.

```
[edit]
user@host# edit system syslog
```

2. Specify the remote system log server to receive messages as well as the groups and severity level for those messages.

```
[edit system syslog]
user@host# set host log-host-name message-group severity
```

For example, to configure the system log server to send error messages generated by processes on the C-series Controller to my-syslog-server:

```
[edit system syslog]
user@host# set my-syslog-server.mydomain.com local7 error
```

Sending Notifications for System Log Messages to Users (SRC CLI)

Use the following statements to configure the system log server to send notifications to users:

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

To configure the system log server to send notifications to users:

1. From configuration mode, access the configuration statement that configures the system log server.

```
[edit]
user@host# edit system syslog
```

2. Specify the user to receive notifications and the types of notifications to be sent.

```
[edit system syslog]
user@host# set user user-name message-group severity
```

For example, to configure the system log server to send notifications to admin for conditions that require immediate attention:

```
[edit system syslog]
```

```
user@host# set user admin any critical
```


Chapter 15

Configuring Static Host Mapping (SRC CLI)

Topics in this chapter include:

- Overview of Static Host Mapping on page 123
- Configuring Static Host Mapping (SRC CLI) on page 123

Overview of Static Host Mapping

You can configure static host mapping to resolve host names. To configure static host mapping, you map the name to one or more IP addresses and aliases. Static host mapping supports both forward and reverse name lookups.

Configuring Static Host Mapping (SRC CLI)

Use the following statements to configure static host mapping:

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

To configure static host mapping:

1. From configuration mode, access the configuration statement that configures static host mapping and specify the fully-qualified name of the system.

```
[edit]  
user@host# edit system static-host-mapping host-name
```

2. Specify the IPv4 or IPv6 addresses to which you want to map the hostname.

```
[edit system static-host-mapping host-name]  
user@host# set inet inet
```

3. (Optional) Specify the aliases for this host.

```
[edit system static-host-mapping host-name]  
user@host# set alias alias
```


Chapter 16

Overview of the Juniper Networks Database

- Overview of the Juniper Networks Database on page 125

Overview of the Juniper Networks Database

Each C-series Controller contains a Juniper Networks database. The database can store SRC data, SRC sample data, SRC configuration information, and a number of user profiles. You store subscriber data in another database.

When the C-series Controller starts for the first time, you must enable the Juniper Networks database. After the database is operational, you can load sample data and perform other configuration activities that use this database.

You can operate this database as a standalone database or as a member of a community of Juniper Networks databases. Typically, you run the database in standalone mode only in testing environments. In standalone mode, the database does not communicate with other Juniper Networks databases; there is no data distribution and no redundancy. In community mode, databases distribute data changes among specified databases. When you have two or more C-series Controllers, enable the Juniper Networks database to run in community mode, and assign a role to each database:

- **Primary role**—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.

We recommend that you configure at least two databases to have a primary role.

- **Secondary role**—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.

Neighbors are Juniper Networks databases that receive data from another Juniper Networks database. When you configure a database to be a neighbor, you configure it as one of the following types:

- **Primary neighbor**—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.

We recommend that you configure at least two databases as primary neighbors.

- Secondary neighbor—A database that only receives database changes. A secondary neighbor must be assigned a secondary role.

When you configure neighbors for the databases, keep in mind the following guidelines:

- A database assigned a primary role can have primary and secondary neighbors.
- A database assigned a secondary role must have at least one primary neighbor, but no secondary neighbors. Because a secondary database cannot distribute changes to its neighbors, if you do configure a secondary neighbor for a secondary database, the software does not use the configuration for the secondary neighbor.

To share processing load, you can configure SRC components, such as SRC-ACP, NIC, or SAE, to use a specified database. In the local configuration for SRC components, you configure the URL of the directory.

Redundancy for a Juniper Networks Database

Protect SRC data by setting up a redundancy scheme for your Juniper Networks databases. Client applications control which database they connect to as their primary database and as their backup database.

Use the following guidelines to plan which databases are assigned primary or secondary roles, and which databases are primary or secondary neighbors:

- Each Juniper Networks database that is assigned a primary role should have at least one primary neighbor. If a database assigned a primary role become inoperable, a client application fails over to a primary neighbor.
- Each database that is assigned a secondary role should have at least two primary neighbors.
- Applications that frequently perform write operations to the database should connect to databases that have a primary role. Applications that perform frequent write operations are the C-Web interface, the SRC CLI, back-office applications that provision data, and in some cases the SRC-ACP.
- Applications that rarely perform updates, such as the NIC and SAE, can communicate with databases assigned a secondary role. For example, you could configure the NIC and SAE to communicate with the local directory on a C-series Controller, and configure the database on this system to have a secondary role.

Security for a Juniper Networks Database

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 to 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.

The type of secure connection you configure determines which ports are open to a Juniper Networks database:

- Remote component access through LDAP—Port 389
- Remote component access through LDAPS—Port 636
- Secure database access for replication—Port 636
- Database access without security for replication—Port 389
- Local component access through LDAP—Port 389

You can also increase the security of your Juniper Networks database by changing the passwords that SRC components use to communicate with the database.

Related Topics

- For information about configuring the SAE to access subscriber data, see [Configuring LDAP Access to Directory Data](#).
- [Configuration Statements for the Juniper Networks Database \(SRC CLI\)](#)
- [Example: Configuration for a Database Community](#)

Chapter 17

Managing the Juniper Networks Database (SRC CLI)

- Configuration Statements for the Juniper Networks Database (SRC CLI) on page 129
- Enabling the Juniper Networks Database to Run in Standalone Mode (SRC CLI) on page 130
- Enabling the Juniper Networks Database to Run in Community Mode (SRC CLI) on page 131
- Securing the Juniper Networks Database (SRC CLI) on page 132
- Changing the Mode of a Juniper Networks Database (SRC CLI) on page 133
- Adding a Juniper Networks Database to an Established Community (SRC CLI) on page 133
- Promoting a Secondary Database to a Primary Role in a Configuration with One Primary Database (SRC CLI) on page 134
- Updating Data on a Juniper Networks Database (SRC CLI) on page 135
- Synchronizing Data on a Juniper Networks Database (SRC CLI) on page 135
- Loading Sample Data in to a Juniper Networks Database (SRC CLI) on page 135
- Securing Communications Between the Juniper Networks Database and SRC Components (SRC CLI) on page 137
- Verifying Configuration for a Juniper Networks Database with the SRC CLI on page 137
- Getting Information About Operations in a Juniper Networks Database (SRC CLI) on page 138
- Example: Configuration for a Database Community on page 139
- Troubleshooting Data Synchronization for Juniper Networks Databases (SRC CLI) on page 142
- Recovering Data in a Community with One Primary Database and One Secondary Database (SRC CLI) on page 142

Configuration Statements for the Juniper Networks Database (SRC CLI)

Use the following configuration statements to configure the Juniper Networks database at the [edit] hierarchy level:

```
system ldap server {
```

```

    stand-alone;
}
system ldap server community {
    role (primary | secondary);
    primary-neighbors [primary-neighbor...];
    secondary-neighbors [secondary-neighbor...];
}
system ldap server security {
    (enable | strict);
}

```

The strict statement is supported only on C-series Controllers.

- Related Topics**
- Overview of the Juniper Networks Database
 - Enabling the Juniper Networks Database to Run in Standalone Mode (SRC CLI)
 - Enabling the Juniper Networks Database to Run in Community Mode (SRC CLI)
 - Securing the Juniper Networks Database (SRC CLI)

Enabling the Juniper Networks Database to Run in Standalone Mode (SRC CLI)

When you run a Juniper Networks database in standalone mode, the database does not communicate with other Juniper Networks databases.

Use the following configuration statements to enable the Juniper Networks database on a C-series Controller in standalone mode:

```

system ldap server {
    stand-alone;
}

```

To enable a Juniper Networks database to run in standalone mode:

1. From configuration mode, access the configuration statement that configures the Juniper Networks database.

```

user@host# edit system ldap server

```

2. Enable standalone mode.

```

[edit system ldap server]
user@host# set stand-alone

```

- Related Topics**
- Overview of the Juniper Networks Database
 - Configuration Statements for the Juniper Networks Database (SRC CLI)
 - Enabling the Juniper Networks Database to Run in Community Mode (SRC CLI)
 - Securing the Juniper Networks Database (SRC CLI)

Enabling the Juniper Networks Database to Run in Community Mode (SRC CLI)

If you are adding a Juniper Networks database to an existing community, see Adding a Juniper Networks Database to an Established Community (SRC CLI) .

Use the following configuration statements to enable the Juniper Networks database on a C-series Controller in community mode:

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

To enable the Juniper Networks database to run in community mode:

1. From configuration mode, access the configuration statement that configures the Juniper Networks database in community mode:

```
user@host# edit system ldap server community
```

2. Specify the role of the database as primary or secondary:

```
[edit system ldap server community]
user@host# set role primary
```

or

```
[edit system ldap server community]
user@host# set role secondary
```

3. Configure primary neighbors. Specify each neighbor by IP address, fully qualified hostname, or a hostname that can be resolved through the domain name system:

```
[edit system ldap server community]
user@host# set primary-neighbors neighbor ...
```

For example, set C1 and C2 as primary neighbors:

```
[edit system ldap server community]

user@host# set primary-neighbors C1 C2
```

4. Configure secondary neighbors. Specify each neighbor by IP address, fully qualified hostname, or a hostname that can be resolved through the domain name system:

```
[edit system ldap server community]
user@host# set secondary-neighbors neighbor ...
```

For example, set C3 and C4 as secondary neighbors:

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

```
user@host# set secondary-neighbors C3 C4
```

- Related Topics**
- Overview of the Juniper Networks Database
 - Configuration Statements for the Juniper Networks Database (SRC CLI)
 - Enabling the Juniper Networks Database to Run in Standalone Mode (SRC CLI)
 - Securing the Juniper Networks Database (SRC CLI)
 - Example: Configuration for a Database Community

Securing the Juniper Networks Database (SRC CLI)

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 to 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.

Use the following configuration statements to secure connections to the Juniper Networks database on a C-series Controller:

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

The **strict** statement is supported only on C-series Controllers.

To secure the Juniper Networks database, perform one of the following tasks:

- (Optional) From configuration mode, access the configuration statement that configures the Juniper Networks database to secure connections to other Juniper Networks databases for data replication:

```
user@host# edit system ldap server security enable
```

- (Optional) From configuration mode, access the configuration statement that configures the Juniper Networks database to accept connections only through LDAPS:

```
user@host# edit system ldap server security strict
```

- Related Topics**
- Overview of the Juniper Networks Database
 - Securing Communications Between the Juniper Networks Database and SRC Components (SRC CLI)

Changing the Mode of a Juniper Networks Database (SRC CLI)

Because the Juniper Networks database can run in either standalone or community mode, to change modes you must disable the current mode and enable the other mode. Typically, you change from standalone mode, which was used for testing, to community mode for a full deployment.

To change the mode of the Juniper Networks database from standalone to community:

1. Disable standalone mode:

```
[edit system ldap server]
user@host# delete stand-alone
```

2. Enable the database in community mode, and configure the role and neighbors.

See Enabling the Juniper Networks Database to Run in Community Mode (SRC CLI) .

Related Topics ■ Configuration Statements for the Juniper Networks Database (SRC CLI)

Adding a Juniper Networks Database to an Established Community (SRC CLI)

When you add a Juniper Networks database to an existing community, make sure that you configure the primary neighbor relationships from the existing primary databases before you enable the new database.



WARNING: If you assign a primary role to a database new to an existing community before you configure the neighbor relationships from existing community databases that have a primary role, you can lose data on neighbor databases that already have a primary role.

To add a Juniper Networks database to an existing community:

1. On existing databases that have a primary role, configure neighbor relationships for the new database.

For example, to configure primary neighbors for the existing servers C1 and C2 for the new server C-new:

On C1:

```
[edit system ldap server community]
user@C1# set primary-neighbor C-new
```

On C2:

```
[edit system ldap server community]
user@C2# set primary-neighbor C-new
```

2. On the new database, enable the primary role and configure primary neighbors.

For example, to enable the database in primary role and configure C1 and C2 as primary neighbors:

```
[edit]
user@C-new# edit system ldap server community
[edit system ldap server community]
user@C-new# set role primary
```

```
user@C-new# set primary-neighbors C1 C2
```

- Related Topics**
- Overview of the Juniper Networks Database
 - Enabling the Juniper Networks Database to Run in Community Mode (SRC CLI)

Promoting a Secondary Database to a Primary Role in a Configuration with One Primary Database (SRC CLI)

Although all communities should have two databases with a primary role, if a community includes one database assigned a primary role and another database assigned a secondary role, promote the database assigned a secondary role to a primary role.

To promote a Juniper Networks database from a secondary role to a primary role:

1. On the database that has a secondary role, set the role to primary.

For example, if the database on C2 has a secondary role:

```
user@C2# edit system ldap server community
[edit system ldap server community]
user@C2# set role primary
user@C2# commit
```

C2 already has C1 configured as primary neighbor.

2. On the existing database that has a primary role, remove the neighbor as secondary and add it as primary.

For example, to remove C2 as a secondary neighbor and add it as a primary neighbor for the database on C1:

```
user@C1# edit system ldap server community
[edit system ldap server community]
user@C1# set primary-neighbors C2
user@C1# commit
```

3. (Optional if you have two databases with a primary role in a community) Switch the role of the database that originally had a secondary role back to secondary:

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

```
user@C2# set role secondary
user@C2# commit
```

- Related Topics**
- Overview of the Juniper Networks Database
 - Enabling the Juniper Networks Database to Run in Community Mode (SRC CLI)

Updating Data on a Juniper Networks Database (SRC CLI)

After you bring a Juniper Networks database online after some period of inaccessibility, update the database with any database changes that occurred while the database was offline.

To update data in a neighbor (for example, neighbor1) in a community of Juniper Networks databases:

```
user@host> request system ldap community force-update neighbor neighbor1
```

- Related Topics**
- Getting Information About Operations in a Juniper Networks Database (SRC CLI)

Synchronizing Data on a Juniper Networks Database (SRC CLI)

You can initialize a Juniper Networks database with data from a neighbor. This process takes the following actions on the database to be initialized:

- Removes any existing data
- Copies data from the system on which the **request system ldap initialize neighbor** command is run

To replace data with data from a neighbor (for example, neighbor1):

- On the system that contains the source database to be replicated:

```
user@host> request system ldap community initialize neighbor neighbor1
```

- Related Topics**
- Updating Data on a Juniper Networks Database (SRC CLI)
 - Getting Information About Operations in a Juniper Networks Database (SRC CLI)

Loading Sample Data in to a Juniper Networks Database (SRC CLI)

The SRC software provides sample data that you can load into the Juniper Networks database. Typically, this data is used for testing or for demonstration purposes. You can load sample data for:

- Enterprise service portals
- SNMP traps for the SNMP agent
- Sample applications:

- Dynamic Service Activator application (in the SRC Application Library)
- Intrusion Detection and Prevention (IDP) integration application (unsupported sample application)
- Instant Virtual Extranet (IVE) Host Checker integration application (unsupported sample application)
- Traffic-Mirroring Application (unsupported sample application)
- Sample residential portal (unsupported sample application)
 - Equipment registration mode
 - Internet service provider (ISP) mode

Loading sample data is not required to run the SRC software.

To load sample data for new entries, including deleted entries, from the specified file:

- Enter the **request system ldap load merge** command.

If you do not specify an option, **merge** is the default option.

To load sample data for all entries from the specified file:

- Enter the **request system ldap load replace** command.

This option will overwrite all existing entries.

To load sample data for the Enterprise Manager Portal and the sample enterprise service portal:

```
user@host> request system ldap load enterprise-portal
```

To load sample data for the SNMP agent:

```
user@host> request system ldap load snmp-agent
```

To load sample data for the Dynamic Service Activator application:

```
user@host> request system ldap load dsa-configuration
```

To load sample data for the Intrusion Detection and Prevention (IDP) integration application:

```
user@host> request system ldap load idp-configuration
```

To load sample data for the Instant Virtual Extranet (IVE) Host Checker integration application:

```
user@host> request system ldap load hostchecker-configuration
```

To load sample data for the Traffic-Mirroring Application:

```
user@host> request system ldap load tm-configuration
```

To load 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:

```
user@host> request system ldap load isp-service-portal
```

To load 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:

```
user@host> request system ldap load equipment-registration
```

Related Topics ■ Overview of the Juniper Networks Database

Securing Communications Between the Juniper Networks Database and SRC Components (SRC CLI)

Communications between SRC components and the Juniper Networks database use password authentication. You can change the default passwords for the following software components to ensure that communications are secure.

- SRC CLI
- NIC
- Configuration for SRC components other than the CLI and the NIC

To change a user password:

```
user@host> request system ldap change-component-password component-name
new-password new-password
```

where *component-name* is:

- cli—Specifies communication between the SRC CLI and the database
- conf—Specifies communication about configuration
- nic—Specifies communication between NIC components and the database

Related Topics ■ Securing the Juniper Networks Database (SRC CLI)

Verifying Configuration for a Juniper Networks Database with the SRC CLI

Purpose Review the configuration for the Juniper Networks database on a C-series Controller.

- Action** ■ Run the `show system ldap server` command at the `[edit]` hierarchy level. For example:

```
[edit]
user@host# show system ldap server
community {
  role primary;
  primary-neighbors C2;
}
```

The output indicates the mode, standalone or community. If the database is running in community mode, the output also includes information about the community configuration on this system.

If the command does not display any output, the Juniper Networks database on the system is disabled.

- Related Topics** ■ Configuration Statements for the Juniper Networks Database (SRC CLI)
- Enabling the Juniper Networks Database to Run in Standalone Mode (SRC CLI)
 - Enabling the Juniper Networks Database to Run in Community Mode (SRC CLI)
 - Securing the Juniper Networks Database (SRC CLI)

Getting Information About Operations in a Juniper Networks Database (SRC CLI)

Purpose Get information about operations performed on a Juniper Networks database.

Action user@host> `show system ldap statistics`

```
Local JDB statistics
Number of Add operations since startup          0
Number of Delete operations since startup       0
Number of Modify operations since startup       0
Number of Rename operations since startup       0
Number of Read operations since startup        265
Number of List operations since startup         129
Number of Subtree Search operations since startup 114
Number of Bind operations                     110
Number of Anonymous Bind operations since startup 94
Number of Compare operations since startup      0
Number of current connections                  3
Number of all connections since startup        110
Number of bind errors since startup            0
Number of all errors since startup             59
```

- Related Topics** ■ Updating Data on a Juniper Networks Database (SRC CLI)
- Recovering Data in a Community with One Primary Database and One Secondary Database (SRC CLI)
 - Troubleshooting Data Synchronization for Juniper Networks Databases (SRC CLI)

Example: Configuration for a Database Community

A community of Juniper Networks databases lets you set up redundancy for client applications that connect to these databases.

This sample configuration describes the tasks for configuring Juniper Networks databases on C-series Controllers:

- Requirements on page 139
- Overview and Sample Topology on page 139
- Configuration on page 140

Requirements

Software

Minimum SRC Release 1.0.0

Hardware

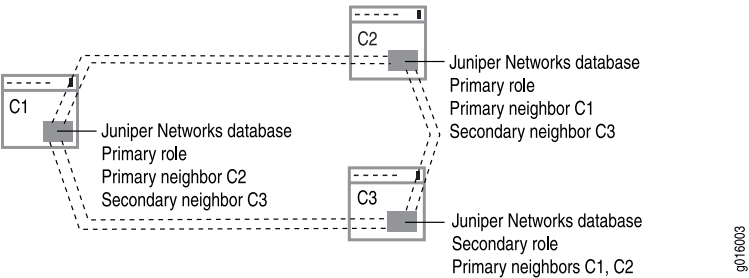
C2000 or C4000

Overview and Sample Topology

You configure a number of Juniper Networks databases as members of a community to protect data by replicating data from one database to another, and by specifying relationships between databases to support failover if a database that has the primary role for a set of applications becomes inoperable. This example uses C1 and C2 as databases that have a primary role, and C3 as a database that has a secondary role.

Figure 17 on page 139 shows the sample configuration.

Figure 17: Sample Community of Juniper Network Databases



The following configuration shows the configuration statements for databases shown in Figure 17 on page 139.

Configuration

Configuring C1

CLI Quick Configuration To quickly configure a Juniper Networks database, copy the following commands into a text editor, and modify them; then load the configuration from the file.

```
[edit]
set system ldap server community role primary
set system ldap server community primary-neighbors C2
set system ldap server community secondary-neighbors C3
```

Step-by-Step Procedure To configure the C1 system:

1. From configuration mode, access the configuration statement that configures the Juniper Networks database in community mode.

```
[edit]
user@C1# edit system ldap server community
```

2. Specify the database role as primary.

```
[edit system ldap server community]
user@C1# set role primary
```

3. Specify primary neighbors.

```
[edit system ldap server community]
user@C1# set primary-neighbors C2
```

4. Specify secondary neighbors.

```
[edit system ldap server community]
user@C1# set secondary-neighbors C3
```

Configuring C2

CLI Quick Configuration To customize the configuration example for your needs, copy the following commands into a text editor, and modify them; then load the configuration from the file.

```
[edit]
set system ldap server community role primary
set system ldap server community primary-neighbors C1
set system ldap server community secondary-neighbors C3
```

Step-by-Step Procedure To configure the C2 system:

1. From configuration mode, access the configuration statement that configures the Juniper Networks database in community mode.

```
[edit]
```

```
user@C2# edit system ldap server community
```

2. Specify the database role as primary.

```
[edit system ldap server community]
user@C2# set role primary
```

3. Specify primary neighbors.

```
[edit system ldap server community]
user@C2# set primary-neighbors C1
```

4. Specify secondary neighbors.

```
[edit system ldap server community]
user@C2# set secondary-neighbors C3
```

Configuring C3

CLI Quick Configuration To customize the configuration example for your needs, copy the following commands into a text editor, and modify them; then load the configuration from the file.

```
[edit]
set system ldap server community role secondary
set system ldap server community primary-neighbors C1 C2
```

Step-by-Step Procedure To configure the C3 system:

1. From configuration mode, access the configuration statement that configures the Juniper Networks database in community mode.

```
[edit]
user@C3# edit system ldap server community
```

2. Specify the database role as primary.

```
[edit system ldap server community]
user@C3# set role secondary
```

3. Specify primary neighbors.

```
[edit system ldap server community]
user@C3# set primary-neighbors C1 C2
```

- Related Topics**
- Overview of the Juniper Networks Database
 - Configuration Statements for the Juniper Networks Database (SRC CLI)
 - Enabling the Juniper Networks Database to Run in Community Mode (SRC CLI)

Troubleshooting Data Synchronization for Juniper Networks Databases (SRC CLI)

Problem Data in a community of Juniper Networks databases may not be synchronized.

Solution 1. Obtain information about the replication status of Juniper Networks databases in a community by running the **show system ldap community** on system that runs the primary Juniper Networks database:

```
user@host> show system ldap community
```

The command output indicates that the databases are not synchronized by:

- Quantity of changes since last startup
- Start and end time of last update
- Status of last update

2. If the databases are not synchronized, initialize neighbors in the community from the primary Juniper Networks database:

```
user@host> request system ldap community initialize neighbor neighbor 1
```

where neighbor1 is the name of the neighbor to be synchronized.

- Related Topics**
- Recovering Data in a Community with One Primary Database and One Secondary Database (SRC CLI)
 - Promoting a Secondary Database to a Primary Role in a Configuration with One Primary Database (SRC CLI)
 - Updating Data on a Juniper Networks Database (SRC CLI)

Recovering Data in a Community with One Primary Database and One Secondary Database (SRC CLI)

In an environment in which a community includes one database assigned a primary role and another database assigned a secondary role, and the primary database is not operative, you must promote the secondary database to primary and reconfigure the inoperative primary database.

1. On the database that has a secondary role, set the role to primary.

For example, if the database on C2 has a secondary role:

```
user@C2# edit system ldap server community
[edit system ldap server community]
user@C2# set role primary
user@C2# commit
```

C2 already has C1 configured as primary neighbor.

2. On the existing database that has a primary role, remove the neighbor as secondary and add it as primary.

For example, to configure C1 as a primary database with C2 as a primary neighbor:

```
user@C1# edit system ldap server community
[edit system ldap server community]
user@C1# set role primary
user@C1# delete secondary-neighbors C2
user@C1# set primary-neighbors C2
user@C1# commit
```

Related Topics ■ Troubleshooting Data Synchronization for Juniper Networks Databases (SRC CLI)

Chapter 18

Setting Up an SAE (SRC CLI)

- Initially Configuring the SAE on page 145
- Grouped Configurations for the SAE on page 145
- Configuring Local Properties for the SAE (SRC CLI) on page 147
- Configuring the RADIUS Local IP Address and NAS ID (SRC CLI) on page 148
- Starting the SAE (SRC CLI) on page 149
- Stopping the SAE (SRC CLI) on page 149

Initially Configuring the SAE

To initially configure the SAE:

- (Optional) Create a configuration group for the SAE.

See Creating Grouped Configurations for the SAE (SRC CLI)
- Configure local properties for the SAE.

See Configuring Local Properties for the SAE (SRC CLI)
- Configure a local IP address and NAS ID that the SAE uses to communicate with RADIUS servers.

See Configuring the RADIUS Local IP Address and NAS ID (SRC CLI)
- Configure directory connection properties for the SAE.
- Configure directory eventing properties for the SAE.

See Configuring Initial Directory Eventing Properties for SRC Components

Grouped Configurations for the SAE

- Creating Grouped Configurations for the SAE (SRC CLI) on page 146
- Configuring an SAE Group on page 146

Creating Grouped Configurations for the SAE (SRC CLI)

We recommend that you configure the SAE within a group. When you create a configuration group, the software creates a configuration with default values filled in.

Configuration groups allow you to build hierarchies that define different levels of sharing. There is a shared SAE configuration that you configure at the **shared sae configuration** hierarchy level. The configuration is shared with all SAE instances in the SRC network.

You can then create a grouped SAE configuration that is shared with some SAE instances. For example, if you create an SAE group called **region** within the shared SAE configuration, you could share the SAE configuration with all SAE instances in a particular region.

You can then create a lower-level group called **location** in the SAE group **region**, which could be shared with SAE instances in a particular location.

Configuration options that are defined in a lower-level group override options in a higher-level group. This functionality allows you to define general configuration values (such as plug-in definitions) on a higher level and augment or specialize them on a lower level.

Configuring an SAE Group

Use the **shared** option of the **set slot number sae shared** command to add a new group. Use the **shared sae group name** command to configure the group.

To configure a group:

1. From configuration mode, add a group. For example, to add a group called **REGION-1** in the path **/SAE/**:

```
[edit]
user@host# set slot 0 sae shared /SAE/REGION-1
```

2. Commit the configuration.

```
[edit]
user@host# commit
commit complete.
```

3. Configure the group as you would a shared SAE configuration.

```
[edit]
user@host# edit shared sae group REGION-1 ?
Possible completions:
<[Enter]>          Execute this command
> configuration
> dhcp-classifier  Configure a DHCP classification script
> group            Group of SAE configuration properties
> user-classifier  Configure a subscriber classification script
|                Pipe through a command
```

Configuring Local Properties for the SAE (SRC CLI)

Use the following configuration statements to configure local properties for the SAE:

```
slot number sae {
  base-dn base-dn ;
  real-portal-address real-portal-address ;
  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 ;
  port-offset port-offset ;
  snmp-agent;
  shared shared ;
}
```

To configure local properties on the SAE:

1. From configuration mode, access the SAE RADIUS configuration. This configuration is under the slot 0 hierarchy.

```
[edit]
user@host# edit slot 0 sae
```

2. (Optional) If you store data in the directory in a location other than the default, *o = umc*, change this value.

```
[edit slot 0 sae]
user@host# set base-dn base-dn
```

3. Configure the interface on the SAE that the SAE uses to communicate with the router.

```
[edit slot 0 sae]
user@host# set real-portal-address real-portal-address
```

4. (Optional) If you encounter problems caused by lack of memory, change the maximum memory size available to the JRE.

```
[edit slot 0 sae]
user@host# set java-heap-size java-heap-size
```

5. Configure the amount of space available to the JRE when the SAE starts.

```
[edit slot 0 sae]
user@host# set java-new-size java-new-size
```

6. Configure the garbage collection functionality of the Java Virtual Machine.

```
[edit slot 0 sae]
user@host# set java-garbage-collection-options java-garbage-collection-options
```

7. If you install multiple instances of the SAE on the same host, set a port offset for SAE instances.

```
[edit slot 0 sae]
user@host# set port-offset port-offset
```

8. (Optional) Enable the SNMP agent to communicate with the SAE.

```
[edit slot 0 sae]
user@host# set snmp-agent
```

9. (Optional) Configure an SAE group configuration.

```
[edit slot 0 sae]
user@host# set shared shared
```

10. (Optional) Verify your configuration.

```
[edit slot 0 sae]
user@host# show
base-dn o=UMC;
real-portal-address 10.10.4.24;
java-runtime-environment ../jre/bin/java;
java-heap-size 896m;
java-new-size 22m;
java-garbage-collection-options "-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:+CMSPermGenSweepingEnabled
-XX:+CMSClassUnloadingEnabled -XX:+CMSParallelRemarkEnabled";
port-offset 0;
snmp-agent;
shared /SAE/REGION-1;
```

Configuring the RADIUS Local IP Address and NAS ID (SRC CLI)

Use the following configuration statements to set the local RADIUS address and network access server (NAS ID):

```
slot number sae radius {
    local-address local-address ;
    local-nas-id local-nas-id ;
}
```

To set the local RADIUS address and NAS ID:

1. From configuration mode, access the SAE RADIUS configuration. This configuration is under the slot 0 hierarchy.

```
[edit]
user@host# edit slot 0 sae radius
```

2. Configure the local IP address that the SAE uses to communicate with RADIUS servers.

```
[edit slot 0 sae radius]
user@host# set local-address local-address
```

3. Configure the NAS ID that identifies the SAE when it sends RADIUS authentication and accounting records. Typically, the NAS ID is the name of the SAE host.

```
[edit slot 0 sae radius]
user@host# set local-nas-id local-nas-id
```

4. (Optional) Verify your configuration.

```
[edit slot 0 sae radius]
user@host# show
local-address 10.10.4.20;
local-nas-id SAE.host1;
```

Starting the SAE (SRC CLI)

You must configure licenses before you start the SAE. When you start the SAE, the software verifies that a valid license is available. If no license is found, the SAE does not start.

To start the SAE:

- From operational mode, enable the SAE.

```
user@host> enable component sae
Check license: OK
Starting sae: may take a few minutes...
```

Stopping the SAE (SRC CLI)

To stop the SAE:

- From operational mode, disable the SAE.

```
user@host> disable component sae
Shutting down the SAE server: done
```

To verify that the SAE is running:

- From operational mode, enter the `show component` command.

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

Chapter 19

Managing System Software on a C-series Controller

- Overview of Software Management on a C-series Controller on page 151
- Before You Upgrade the Software on a C-series Controller on page 152
- Creating a Snapshot of Files on a C-series Controller on page 152
- Upgrading the System Software on a C-series Controller on page 153
- Upgrading SRC Software for a Component on page 154
- Installing SRC Software for a Component on page 155
- Removing an Installed Component on page 155
- Restoring the Files in a Snapshot on page 155

Overview of Software Management on a C-series Controller

On a C-series Controller you can upgrade all the system software or the software package for a component. You can also install and uninstall a software package for an SRC component. Table 11 on page 151 lists the names of the packages for the components that run on the C-series Controller.

Table 11: Package Names for Components on a C-series Controller

Component	Package Name
Command-line interface (CLI)	UMCcli
C-Web interface	UMCwebadm
IP multimedia subsystem	UMCims
Java Web server	UMCtomcat
Juniper Networks database	UMCjdb
Juniper Policy Server (JPS)	UMCjps
License Server	UMClicsvr
Network information Collector (NIC)	UMCnic

Table 11: Package Names for Components on a C-series Controller *(continued)*

Component	Package Name
Policies, Services, and Subscribers CLI	UMCeditor
Redirect Server	UMCredir
Service activation engine (SAE)	UMCsae
SNMP agent	UMCagent
SRC-ACP	UMCacp

Before You Upgrade the Software on a C-series Controller

Before you upgrade system software on a C-series Controller:

- Create a snapshot of the software files currently on the C-series Controller.
See [Creating a Snapshot of Files on a C-series Controller](#).
- Make sure that other C-series Controllers can carry system load during the upgrade. The system will not be operational during the upgrade.

Creating a Snapshot of Files on a C-series Controller

You can create a snapshot of the system software to serve as a backup. When you create a snapshot, the software backs up the operating system and the SRC software to a partition on the C-series Controller. You can restore the files in a snapshot to the system software if needed.

To create a snapshot of the system software:

1. Verify which version of the software is running on the system.

```
user@host > show system information
```

2. Enter the **request system snapshot** command. Use the verbose option to view information about the snapshot process.

```
user@host> request system snapshot verbose
Create system snapshot [yes,no] ? (no) yes

Filesystem label=
mke2fs 1.35 (28-Feb-2004)
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
262144 inodes, 524288 blocks
26214 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=536870912
16 block groups
```

```

32768 blocks per group, 32768 fragments per group
16384 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912

Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 32 mounts or
180 days, whichever comes first. Use tune2fs -c or -i to override.
DUMP: Date of this level 0 dump: Thu Oct 19 09:43:44 2006
DUMP: Dumping /dev/mapper/vg0-root (/) to standard output
restore: cannot open /dev/tty: No such device or address
DUMP: Label: none
DUMP: Writing 64 Kilobyte records
DUMP: mapping (Pass I) [regular files]
DUMP: mapping (Pass II) [directories]
DUMP: estimated 1036678 blocks.
DUMP: Volume 1 started with block 1 at: Thu Oct 19 09:43:45 2006
DUMP: dumping (Pass III) [directories]
DUMP: dumping (Pass IV) [regular files]

DUMP: Volume 1 completed at: Thu Oct 19 09:48:13 2006
DUMP: Volume 1 1035200 blocks (1010.94MB)
DUMP: Volume 1 took 0:01:10
DUMP: Volume 1 transfer rate: 14788 kB/s
DUMP: 1035200 blocks (1010.94MB)
DUMP: finished in 70 seconds, throughput 14788 kBytes/sec
DUMP: Date of this level 0 dump: Thu Oct 19 09:47:02 2006
DUMP: Date this dump completed: Thu Oct 19 09:48:13 2006
DUMP: Average transfer rate: 14788 kB/s

```

Upgrading the System Software on a C-series Controller

You can upgrade all the system software or the software changes for an SRC component. If an image file (from which you upgrade) contains updates for all components or a number of components, you specify which component to upgrade if you do not want to upgrade all components.

For ease of use, you can manage upgrades for a number of C-series Controllers by copying a complete CD image file to be used for an upgrade to an FTP site in your network. You then upgrade each system by using the files on the FTP site. Alternatively, you can copy the complete CD image to a USB drive and install from there.

To upgrade C-series Controller software:

- Enter the **request system upgrade** command.

```
user@host> request system upgrade url url
```

For example:

```

user@host> request system upgrade url ftp://myserver/pub/UMC/7.0.0/B
Setting up Upgrade Process
Setting up repositories
Reading repository metadata in from local files
Resolving Dependencies
--> Populating transaction set with selected packages. Please wait.
---> Downloading header for python-ldap to pack into transaction set.
---> Package python-ldap.i386 0:2.0.6-1 set to be updated
--> Running transaction check

```

Dependencies Resolved

Package Arch Version Repository Size

```

=====
Updating:
python-ldap          i386      2.0.6-1      umc-upgrade
150 k

```

Transaction Summary

```

=====
Install      0 Package(s)
Update       1 Package(s)
Remove       0 Package(s)
Total download size: 150 k
Downloading Packages:
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction

```

```

Updating : python-ldap ##### [1/1]

```

```

Updated: python-ldap.i386 0:2.0.6-1
Complete!

```

The C-series Controller automatically reboots at the end of the upgrade.

Upgrading SRC Software for a Component

To upgrade a specified SRC component:

- Specify the package name for a component when you enter the `request system upgrade` command.

```

user@host> request system upgrade url url package package

```

For example:

```
user@host> request system upgrade url ftp://myserver/pub/UMC/7.0.0/B
package UMCnic
```

The C-series Controller automatically reboots at the end of the upgrade.

Installing SRC Software for a Component

To install the software for a component:

- Specify the package name for a component when you enter the `request system install` command.

```
user@host> request system install url url package package
```

For example:

```
user@host> request system install url ftp://myserver/pub/UMC/7.0.0/B
package UMCnic
```

Removing an Installed Component

To remove a component that is installed on a C-series Controller:

- Specify the package name for a component when you enter the `request system uninstall` command.

```
user @ host> request system uninstall package package
```

For example:

```
user @ host > request system uninstall package UMCnic
```

Restoring the Files in a Snapshot

To revert to the system software stored in snapshot files:

- Enter the `request system restore` command.

```
user@host> request system restore
WARNING: restoring a snapshot will cause the system to
reboot and replace the software with the data from the
system snapshot.
Rebooting to start restore
```

The C-series Controller reboots twice during a restoration.

Chapter 20

Using the Web Application Server on a C-series Controller

This chapter describes how to use the Web application server on a C-series Controller.

Topics include:

- Overview of the Web Application Server on C-series Controllers on page 157
- Configuration Statements for the Web Application Server on page 158
- Configuring the Web Application Server (SRC CLI) on page 159
- Configuring Local Properties for Web Application Server (SRC CLI) on page 159
- Configuring Remote Access to the Application Server (SRC CLI) on page 160
- Configuring Virtual Hosts for the Web Applications (SRC CLI) on page 161
- Configuring User Accounts for Web Applications (SRC CLI) on page 162
- Installing Web Applications in the Application Server on page 163
- Removing Web Applications From the Application Server on page 163
- Starting the Web Application Server on a C-series Controller on page 164
- Restarting the Web Application Server on a C-series Controller on page 164
- Stopping the Web Application Server on a C-series Controller on page 164
- Viewing Statistics for the Web Application Server (SRC CLI) on page 164
- Viewing Statistics for the Web Application Server (C-Web Interface) on page 164

Overview of the Web Application Server on C-series Controllers

The SRC software on a C-series Controller includes a Web application server that hosts the SRC SOAP Gateway (SRC-SG). In production environments, this application server is designed to host only the SRC-SG. However, you can load your own applications into this server for testing or demonstration purposes.

The Web application server listens on port 8080 for HTTP connections on the `eth0` interface (interface to the trusted network) and on the configured ports for HTTP and HTTPS connections on the `eth1` interface (interface to the untrusted network).

You can control access to applications deployed in the Web application server by configuring virtual hosts. A virtual host contains aliases and lists of the clients that are allowed to access the virtual host.

The aliases are DNS names or IP addresses that appear in the host part of the URLs used by clients to access a Web application. When the Web application server receives a request for an application, it searches for the virtual host with the alias that matches the host in the URL. If a virtual host is found, the Web application server verifies that the application is deployed on this virtual host and the client making the request is allowed to access the virtual host. If no virtual host is found, or if access to the application or client is not allowed by the virtual host, the request is rejected and the client receives an error code.

For convenience, a built-in virtual host named `eth0` is automatically configured with two aliases:

- The IP address assigned to `eth0`.
- The name for the SRC host configured at the `[edit system host-name]` and `[edit system domain-name]` hierarchy levels.

For this reason, if you want to access the `eth0` virtual host with URLs containing the DNS name of your SRC host, you must configure your SRC hostname in your DNS server.

You configure the built-in applications, such as Dynamic Service Activator, to deploy the application to a specific virtual host. Other applications that you can load for demonstration purposes are automatically deployed on the built-in virtual host `eth0`.

Configuration Statements for the Web Application Server

Use the following configuration statements to configure the operating properties for the Web application server at the `[edit]` hierarchy level.

```
slot number application-server {
    java-garbage-collection-options java-garbage-collection-options;
    java-heap-size java-heap-size;
}

slot number application-server web http {
    port port;
    interface interface;
}

slot number application-server web https {
    local-certificate local-certificate;
    port port;
    interface interface;
}

slot number application-server web virtual-host host-name {
    alias alias;
    allow-address allow-address;
    allow-host allow-host;
    deny-address deny-address;
    deny-host deny-host;
}
```

```

shared application-server user name

shared application-server user name authentication {
    encrypted-password encrypted-password;
    plain-text-password;
}

```

Configuring the Web Application Server (SRC CLI)

Tasks to configure the Web application server are:

1. Configure the operating properties.

See Configuring Local Properties for Web Application Server (SRC CLI).

2. Configure remote access to the application server.

See Configuring Remote Access to the Application Server (SRC CLI).

3. Configure the virtual host for the Web application, including whether to allow or deny access by specific remote clients.

See Configuring Virtual Hosts for the Web Applications (SRC CLI).

4. Configure the user accounts for the Web application.

See Configuring User Accounts for Web Applications (SRC CLI).

Configuring Local Properties for Web Application Server (SRC CLI)

To configure basic local properties:

1. From configuration mode, access the configuration statement that configures the local properties.

```
user@host# edit slot 0 application-server
```

2. Configure the garbage collection functionality of the Java Virtual Machine.

```

[edit slot 0 application-server]
user@host# set java-garbage-collection-options java-garbage-collection-options

```

3. (Optional) If you encounter problems caused by lack of memory, change the maximum memory size available to the JRE.

```

[edit slot 0 application-server]
user@host# set java-heap-size java-heap-size

```

4. (Optional) Verify your configuration.

```

[edit slot 0 application-server]
user@host# show

```

Configuring Remote Access to the Application Server (SRC CLI)

Before you can start using the application server, you need to configure and enable access to the application server. You can make the application server accessible through secure HTTP (HTTPS) or HTTP.

- Configuring Access to the Application Server Through Secure HTTP on page 160
- Configuring Access to the Application Server Through HTTP on page 160

Configuring Access to the Application Server Through Secure HTTP

Before you configure access to the application server through HTTPS, obtain a digital security certificate on the system.

To make the application server accessible through HTTPS:

1. From configuration mode, access the statement that configures access through HTTPS.

```
user@host# edit slot 0 application-server web https
```

2. Specify which TCP port is to receive incoming connection requests for the application server.

```
[edit slot 0 application-server web https]
user@host# set port port
```

3. Specify the interface to be used for connections to the application server.

```
[edit slot 0 application-server web https]
user@host# set interface interface
```

On a C-series Controller, use **eth1** for built-in Web applications; you can use **eth0** for demonstration applications.

4. Specify the name of the certificate on the local system.

```
[edit slot 0 application-server web https]
user@host# set local-certificate local-certificate
```

5. (Optional) Configure user accounts to allow specified clients to authenticate with the application server.

Configuring Access to the Application Server Through HTTP

To make the application server accessible through HTTP:

1. From configuration mode, access the statement that configures access through HTTP.

```
user@host# edit slot 0 application-server web http
```

2. Specify which TCP port is to receive incoming connection requests for the application server.

```
[edit slot 0 application-server web http]
user@host# set port port
```

3. Specify the interface to be used for connections to the application server.

```
[edit slot 0 application-server web http]
user@host# set interface interface
```

On a C-series Controller, use **eth1** for built-in Web applications; you can use **eth0** for demonstration applications.

4. (Optional) Configure user accounts to allow specified clients to authenticate with the application server.

- Related Topics**
- Overview of Digital Certificates
 - Configuring User Accounts for Web Applications (SRC CLI)

Configuring Virtual Hosts for the Web Applications (SRC CLI)

Use the following configuration statements to configure virtual hosts at the [edit] hierarchy level:

```
slot number application-server web virtual-host host-name {
  alias [alias...];
  allow-address [allow-address...];
  allow-host [allow-host...];
  deny-address [deny-address...];
  deny-host [deny-host...];
}
```

To configure virtual hosts for the Web applications:

1. From configuration mode, access the statement that configures the virtual host.

```
user@host# edit slot 0 application-server virtual-host host-name
```

The hostname must be unique. You cannot specify **eth0**, the IP address of the **eth0** interface, or the hostname of the C-series Controller as the hostname of the virtual host.

2. Specify the alternate DNS names or IP addresses for the virtual host.

```
[edit slot 0 application-server virtual-host host-name]
user@host# set alias [alias ...]
```

The alias must be unique. You cannot specify **eth0**, the IP address of the **eth0** interface, or the hostname of the C-series Controller as the alias of the virtual host.

3. Configure access to the virtual host. Specify the IP addresses for remote clients that are allowed access to the virtual host.

```
[edit slot 0 application-server virtual-host host-name]
user@host# set allow-address [allow-address...]
```

4. Configure access to the virtual host. Specify the hostnames for remote clients that are allowed access to the virtual host.

```
[edit slot 0 application-server virtual-host host-name]
user@host# set allow-host [allow-host...]
```

5. Deny access to the virtual host. Specify the IP addresses for remote clients that are denied access to the virtual host.

```
[edit slot 0 application-server virtual-host host-name]
user@host# set deny-address [deny-address...]
```

6. Deny access to the virtual host. Specify the hostnames for remote clients that are denied access to the virtual host.

```
[edit slot 0 application-server virtual-host host-name]
user@host# set deny-host [deny-host...]
```

Configuring User Accounts for Web Applications (SRC CLI)

User accounts provide one way for clients to authenticate with the application server. For each account, you define the login name for the user and authentication information. You can configure plain text password or encrypted password as the type of authentication for user accounts. When you delete user accounts, the software verifies that the user account is not referenced by another configuration.



NOTE: Client profiles can be cached by applications for 30 minutes. If you change the password or role of a client that has been used within the last 30 minutes, it can take up to 30 minutes before these changes take effect.

If you do not want to wait 30 minutes for the changes to take effect, restart the Web application server.

Use the following configuration statements to configure user accounts at the [edit] hierarchy level:

```
shared application-server user name
```

```
shared application-server user name authentication {
  encrypted-password encrypted-password;
  plain-text-password;
}
```

To configure a user account:

1. From configuration mode, access the configuration statement that configures a user account, and specify a username that identifies the client.

```
user@host# edit shared application-server user name
```

The username must be unique within the system. Do not include spaces, colons, or commas in the username.

2. Configure authentication for the user account.

```
[edit shared application-server user name]
user@host# set authentication (plain-text-password | encrypted-password)
```

where:

- **plain-text-password**—Prompt for a plain text (unencrypted) password.
- **encrypted-password**—Password encoded with crypt. The format of encrypted passwords is "{crypt} < 13-characters in a-zA-Z0-9./> ".

We recommend that you do not enter the password in encrypted format.

For example:

```
user@host# set authentication plain-text-password
New password: type password here
Retype new password: retype password here
```

Installing Web Applications in the Application Server

To deploy a Web application in the Web application server:

1. Start the Web application server.
2. Prepare the Web application archive (WAR) file on a machine other than the C-series Controller.
3. Deploy the WAR file on the C-series Controller. The application server automatically starts the Web application when a new WAR file is deployed.

```
user@host> request appsvr deploy file name
```

For example:

```
user@host> request appsvr deploy file ftp://host/path/ssportal.war
```

- Related Topics**
- Removing Web Applications From the Application Server
 - Starting the Web Application Server on a C-series Controller
 - Restarting the Web Application Server on a C-series Controller

Removing Web Applications From the Application Server

To undeploy a Web application from the Web application server:

```
user@host> request appsvr undeploy file name
```

For example:

```
user@host> request appsvr undeploy file dsa.war
```

- Related Topics**
- Installing Web Applications in the Application Server
 - Stopping External Subscriber Monitor with the C-Web Interface

Starting the Web Application Server on a C-series Controller

To start the Web application server on a C-series Controller:

```
user@host> enable component appsvr
```

Restarting the Web Application Server on a C-series Controller

To restart the Web application server on a C-series Controller:

```
user@host> restart component appsvr
```

Stopping the Web Application Server on a C-series Controller

To stop the Web application server on a C-series Controller:

```
user@host> disable component appsvr
```

Viewing Statistics for the Web Application Server (SRC CLI)

Purpose View statistics for the Web application server.

Action user@host> show application-server statistics

```
Appsvr Process Statistics
JBoss Server Process
JBoss server up time(seconds) 4673
JBoss server up since         Thu Mar 13 11:07:30 EDT 2008
JBoss server thread(s)        63
Heap used(byte)               47316168 (9%)
Heap limit(byte)              520749056
```

Viewing Statistics for the Web Application Server (C-Web Interface)

Purpose View statistics for the Web application server.

Action Click **Monitor** > **Application Server** > **Statistics**.

The Statistics pane displays the application server process statistics.

Chapter 21

Integrating Steel-Belted Radius/SPE Server

- Integrating Steel-Belted Radius/SPE Server on page 165

Integrating Steel-Belted Radius/SPE Server

The Juniper Networks Steel-Belted Radius/Service Provider Edition (SPE) server is a carrier-grade RADIUS/AAA solution. It provides the reliability, performance, and specialized technology demanded by carriers, wholesalers, and service providers. Refer to the *SRC-PE Release Notes* for information about compatibility of this SRC release with Steel-Belted Radius/SPE server releases. The SRC software does not support the use of RADIUS with JUNOS routing platforms.

The SRC software can take advantage of a RADIUS server to authenticate against an LDAP server, which is used to store subscriber and service information, among other information.

You can find information about the system requirements for the Steel-Belted Radius server in the release notes at the following Web site:

http://www.juniper.net/techpubs/software/aaa_802/sbr.html

You need the Steel-Belted Radius/SPE software CD and a valid license string. Use the procedure that is appropriate for your installation.

You must have JNPRsbrsp.pkg and UMCsbrspa.pkg to install and integrate the Steel-Belted Radius/SPE software.

Related Topics

- For information about the installation and configuration procedures is located at the following Web site: http://www.juniper.net/techpubs/software/aaa_802/sbr.html

Part 5

Managing SRC Access and Security with the CLI

- Configuring User Access (SRC CLI) on page 169
- Authenticating Users on a C-series Controller (SRC CLI) on page 189
- Managing Security Digital Certificates on page 197
- Connecting to Remote Hosts from the SRC Software on page 203
- Configuring and Starting the SNMP Agent (SRC CLI) on page 205

Chapter 22

Configuring User Access (SRC CLI)

- Overview of SRC User Accounts on page 169
- Login Classes for SRC User Accounts on page 169
- Login Class Permission Options for the SRC Software on page 170
- Predefined Login Classes for the SRC Software on page 174
- Access to Individual Commands and Configuration Statements (SRC CLI) on page 174
- Before You Configure Login Classes (SRC CLI) on page 177
- Configuring an SRC Login Class on page 177
- User Accounts for the SRC Software on page 180
- Types of Authentication for SRC User Accounts on page 183
- Configuring Authentication for SRC User Accounts on page 184
- Example: SRC User Accounts on page 185
- Changing the root Password for the SRC Software on page 186
- Configuring a System Login Announcement (SRC CLI) on page 186

Overview of SRC User Accounts

All users who can log in to the SRC software must be a member of a login class. With login classes, you define the following:

- Access privileges users have when they are logged in to the SRC software
- Commands and statements that users can and cannot specify
- How long a login session can be idle before it times out and the user is logged out.

You can define any number of login classes. You then apply one login class to an individual user account.

Login Classes for SRC User Accounts

The SRC software provides four predefined login classes to use for configuring user accounts. A login class defines the access privilege levels to the SRC software. You

can also configure login classes to precisely define access privileges for the user accounts in your SRC environment.

In the SRC CLI, each top-level command-line interface (CLI) command and each configuration statement have an access privilege level associated with them. Similarly, each task and subtask in the C-Web interface have an access privilege level associated with them. Users can configure and view only those tasks for which they have access privileges. The access privileges for each login class are defined by one or more *permission options*.

Permission options specify which actions are allowed for users assigned to use a login class. More than one permission option can be configured for a login class. You can use the SRC CLI or the C-Web interface to configure permission options for all commands, statements, tasks, and subtasks. For example, if you configure a user to have the **system** permission class using the C-Web interface, that user will have the same permission when accessing the SRC CLI. The privilege level for each command and statement is listed in *SRC-PE CLI Command Reference*.

When you configure more than one permission, the resulting set of permissions is a combination of all of the permissions set, except for **all** and **control**.

When you configure permissions, include **view** to display information and **configure** to enter configuration mode. Two forms for the permissions control the individual parts of the configuration:

- “Plain” form—Provides read-only capability for that permission type. An example is **interface**.
- Form that ends in **-control**—Provides read and write capability for that permission type. An example is **interface-control**.

Login Class Permission Options for the SRC Software

Table 12 on page 170 lists the permission options available when you configure permissions with the SRC CLI and the C-Web interface. The SRC software also provides a default set of system login classes that have permissions preset.

Table 12: Login Class Permission Options

Permission	Description
admin	<p>SRC CLI—Can view user account information in configuration mode and with the show configuration command.</p> <p>C-Web interface—Can view user account information by accessing the Monitor > CLI > Authorization.</p>
admin-control	<p>SRC CLI—Can view user accounts and configure them at the [edit system login] hierarchy level.</p> <p>C-Web interface—Can view user accounts and configure them by accessing Configure > System > Login.</p>
all	SRC CLI and C-Web interface—Has all permissions.

Table 12: Login Class Permission Options *(continued)*

Permission	Description
clear	<p>SRC CLI—Can clear (delete) information learned from the network that is stored in various network databases using the clear commands.</p> <p>C-Web interface—Can clear (delete) information learned from the network that is stored in various network databases by accessing Manage > Clear.</p>
configure	<p>SRC CLI—Can enter configuration mode using the configure command.</p> <p>C-Web interface—Can access the Configure task and subtasks.</p>
control	SRC CLI and C-Web interface—Can perform all control-level operations (all operations configured with the -control permission).
field	SRC CLI and C-Web interface—Reserved for field (debugging) support.
firewall	<p>SRC CLI—Can view the firewall filter configuration in configuration mode.</p> <p>C-Web interface—Can view the firewall filter configuration by accessing Monitor > SAE > Services.</p>
firewall-control	<p>SRC CLI—Can view and configure firewall filter information at the [edit firewall] hierarchy level.</p> <p>C-Web interface—Can view and configure firewall filter information by accessing Configure > Services.</p>
interface	<p>SRC CLI—Can view the interface configuration in configuration mode and with the show configuration operational mode command.</p> <p>C-Web interface—Can view the interface configuration by accessing Monitor > Interfaces.</p>
interface-control	<p>SRC CLI—Can view chassis, class of service, groups, forwarding options, and interfaces configuration information. Can configure chassis, class of service, groups, forwarding options, and interfaces at the [edit] hierarchy level.</p> <p>C-Web interface—Can view chassis, class of service, groups, forwarding options, and interfaces configuration information. Can configure chassis, class of service, groups, forwarding options, and interfaces by accessing the Configure task and subtasks.</p>
maintenance	<p>SRC CLI—Can perform system maintenance, including starting a local shell on the system and becoming the superuser in the shell (by issuing the su root command), and can halt and reboot the system (using the request system commands).</p> <p>C-Web interface—Can perform system maintenance, including halting and reboot the system, by accessing Manage > Request > System.</p>

Table 12: Login Class Permission Options *(continued)*

Permission	Description
network	SRC CLI and C-Web interface—Can access the network by entering the SSH and telnet commands.
reset	<p>SRC CLI—Can restart software processes using the restart command, enable components using the enable command, and disable components using the disable command.</p> <p>C-Web interface—Can restart software processes by accessing Manage > Restart, enable components by accessing Manage > Enable, and disable components by accessing Manage > Disable.</p>
routing	<p>SRC CLI—Can view general routing information in configuration and operational modes.</p> <p>C-Web interface—Can view general routing information by accessing Monitor > SAE > Route.</p>
routing-control	<p>SRC CLI—Can view and configure general routing at the [edit routing-options] hierarchy level.</p> <p>C-Web interface—Can view general routing and configure general routing by accessing Configure > Routing Options.</p>
secret	SRC CLI and C-Web interface—Can view passwords and other authentication keys in the configuration.
secret-control	<p>SRC CLI—Can view passwords and other authentication keys in the configuration and can modify them in configuration mode.</p> <p>C-Web interface—Can view passwords and other authentication keys in the configuration and can modify them by accessing Configure > System > Login.</p>
security	<p>SRC CLI—Can view security configuration in configuration mode and with the show configuration operational mode command.</p> <p>C-Web interface—Can view security configuration by accessing Monitor > Security > Certificate.</p>
security-control	<p>SRC CLI—Can view and configure security information at the [edit security] hierarchy level.</p> <p>C-Web interface—Can view security information and configure security information by accessing Manage > Request > Security.</p>
service	<p>SRC CLI and C-Web interface—Can view service and policy definitions.</p> <p>C-Web interface—Can view service definitions by accessing Monitor > SAE > Services and policy definitions by accessing Monitor > SAE > Policies.</p>

Table 12: Login Class Permission Options *(continued)*

Permission	Description
service-control	<p>SRC CLI—Can view and modify service and policy definitions.</p> <p>C-Web interface—Can view and modify service and policy definitions by accessing Configure > Services and Configure > Policies.</p>
shell	SRC CLI and C-Web interface—Can start a local shell by entering the start shell command.
snmp	<p>SRC CLI—Can view Simple Network Management Protocol (SNMP) configuration information in configuration and operational modes.</p> <p>C-Web interface—Can view Simple Network Management Protocol (SNMP) configuration information by accessing Monitor > SAE > Statistics.</p>
snmp-control	<p>SRC CLI—Can view SNMP configuration information and configure SNMP (at the [edit snmp] hierarchy level).</p> <p>C-Web interface—Can view SNMP configuration information and configure SNMP by accessing Configure > SNMP.</p>
subscriber	<p>SRC CLI—Can view information about subscriber definitions.</p> <p>C-Web interface—Can view information about subscriber definitions by accessing Monitor > SAE > Subscribers.</p>
subscriber-control	<p>SRC CLI —Can view and control information about subscriber definitions.</p> <p>C-Web interface—Can view information about subscriber definitions and control information about subscriber definitions by accessing Configure > Subscribers.</p>
system	<p>SRC CLI—Can view system-level information in configuration and operational modes.</p> <p>C-Web interface—Can view system-level configuration information by accessing Monitor > System.</p>
system-control	<p>SRC CLI—Can view system-level configuration information and configure it at the [edit system] hierarchy level.</p> <p>C-Web interface—Can view system-level configuration and configure it by accessing Configure > System.</p>
view	<p>SRC CLI—Can use various commands to display current systemwide, routing table, and protocol-specific values and statistics.</p> <p>C-Web interface—Can access various Monitor subtasks to display current systemwide, routing table, and protocol-specific values and statistics.</p>

Table 12: Login Class Permission Options *(continued)*

Permission	Description
view-configuration	SRC CLI and C-Web interface—Can view all system configurations, excluding any secret configuration.

- Related Topics** ■ To review the default system login classes, see Predefined Login Classes for the SRC Software.

Predefined Login Classes for the SRC Software

Table 13 on page 174 lists the system login classes predefined in the SRC software.

Table 13: Default System Login Classes (Sheet of) (Sheet of)

Login Class	Permission Options Set
operator	clear, network, reset, view
read-only	view
super-user	all
unauthorized	None



NOTE: You cannot modify a predefined login class name. If you issue the **set** command on a predefined class name with the SRC CLI, the software will append **-local** to the login class name. The following message also appears:

```
warning: '< class-name >' is a predefined class name; changing to '< class-name >-local'
```

You cannot issue the **rename** or **copy** command on a predefined login class with the SRC CLI. Doing so results in the following error message:

```
error: target '< classname >' is a predefined class
```

Access to Individual Commands and Configuration Statements (SRC CLI)

By default, all top-level CLI commands have associated access privilege levels. Users can execute only those commands and view only those statements for which they have access privileges. For each login class, you can deny or allow the use of specified operational and configuration mode commands that would otherwise be permitted or not allowed by a specified privilege level.

Regular Expressions for Allow and Deny Statements

You can use extended regular expressions to specify which commands to allow or deny. By using extended regular expressions, you can list a number of commands in each statement.

You specify these regular expressions in the following statements at the [edit system login class] hierarchy level:

- allow-commands
- deny-commands
- allow-configuration
- deny-configuration

Command regular expressions implement the extended (modern) regular expressions as defined in POSIX 1003.2. Table 14 on page 175 lists common regular expression operators.

Table 14: Common Regular Expression Operators to Allow or Deny Operational Mode and Configuration Mode Commands

Operator	Match
Operation Mode and Configuration Mode	
	One of the two terms on either side of the pipe.
^	Character at the beginning of an expression. Used to denote where the command begins, where there might be some ambiguity.
\$	Character at the end of a command. Used to denote a command that must be matched exactly up to that point. For example, <code>allow-commands "show interfaces\$"</code> means that the user can issue the <code>show interfaces</code> command but cannot issue <code>show interfaces detail</code> or <code>show interfaces extensive</code> .
[]	Range of letters or digits. To separate the start and end of a range, use a hyphen (-).
()	A group of commands, indicating an expression to be evaluated; the result is then evaluated as part of the overall expression.
Configuration Mode Only	
*	0 or more terms.
+	One or more terms.
. (dot)	Any character except for a space.

Guidelines for Using Regular Expressions

Keep in mind the following considerations when using regular expressions to specify which statements or commands to allow or deny:

- Regular expressions are not case-sensitive.
- If a regular expression contains a syntax error, authentication fails and the user cannot log in.
- If a regular expression does not contain any operators, all varieties of the command are allowed.

Follow these guidelines when using regular expressions:

- Enclose the following in quotation marks:
 - A command name or regular expression that contains:
 - Spaces
 - Operators
 - Wildcard characters
 - An extended regular expression that connects two or more terms with the pipe (|) symbol. For example:

```
[edit system login class class-name ]
user@host# set deny-configuration "(system login class) | (system
services)"
```

- Do not use spaces between regular expressions separated with parentheses and connected with the pipe (|) symbol.
- Specify the full paths in the extended regular expressions with the `allow-configuration` and `deny-configuration` options.



NOTE: You cannot define access to keywords such as `set` or `edit`.

Timeout Value for Idle Login Sessions

An idle login session is one in which the CLI operational mode prompt is displayed but there is no input from the keyboard. By default, a login session remains established until a user logs out of the system, even if that session is idle. To close idle sessions automatically, you configure a time limit for each login class. If a session established by a user in that class remains idle for the configured time limit, the session automatically closes.

For users who belong to a login class for which an idle timeout is configured, the CLI displays messages similar to the following when an idle user session times out.

```
user@host# Session will be closed in 5 minutes if there is no activity.
```

Warning: session will be closed in 1 minute if there is no activity
 Warning: session will be closed in 10 seconds if there is no activity
 Idle timeout exceeded: closing session

If you configure a timeout value, the session closes after the specified time has elapsed, except if the user is running commands such as `ssh`, `start shell`, or `telnet`.

The C-Web interface session closes after the specified time has elapsed with no message, and returns to the login window.

Before You Configure Login Classes (SRC CLI)

Before you configure a login class:

- Review the predefined login classes to determine whether you can use one of these classes rather than creating a new one.

See Predefined Login Classes for the SRC Software .

- Make sure you are familiar with how to use regular expressions to specify which commands and configuration statements to allow or deny.

Consider that you can issue one **allow** statement and one **deny** statement for operation mode commands, and one **allow** statement and one **deny** statement for configuration mode commands. Use regular expressions in a statement to specify more than one command in a statement.

See Access to Individual Commands and Configuration Statements (SRC CLI).

Configuring an SRC Login Class

Use the following configuration statements to configure login classes at the [edit] hierarchy level:

```
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
}
```

To configure a login class:

1. From configuration mode, access the configuration statement that configures login classes, and assign a name to the login class.

```
[edit]
user@host# edit system login class name
```

2. Specify the permissions for the login class.

```
[edit system login class name ]
user@host# set permissions permissions
```

For example, the following statement specifies that the user-account class can configure and view only user accounts:

```
[edit system login class user-accounts]
user@host# set permissions [configure admin admin-control]
```

The following statement specifies that the network-mgmt class can configure and view only SNMP parameters:

```
[edit system login class network-mgmt]
user@host# set permissions [configure snmp snmp-control]
```

3. (Optional) Configure access to specified operational mode commands that would otherwise be denied.

```
[edit system login class name ]
user@host# set allow-commands allow-commands
```

For example, the following statement specifies that the network-mgmt class can install system software:

```
[edit system login class network-mgmt]
user@host# set allow-commands "request system install"
```

4. (Optional) Deny access to specified operational mode commands that would otherwise be allowed.

```
[edit system login class class-name ]
user@host# set deny-commands deny-commands
```

For example, the following statement specifies that the remote class cannot connect to the SRC software through Telnet:

```
[edit system login class remote]
user@host# set deny-commands telnet
```

5. (Optional) Configure access to specified configuration mode commands that would otherwise be denied.

```
[edit system login class name ]
user@host# set allow-configuration allow-configuration
```

For example, the following statement specifies that the network-mgmt class can issue configuration mode commands at the [routing-options] hierarchy level:

```
[edit system login class network-mgmt]
user@host# set allow-configuration " routing options"
```

- (Optional) Deny access to specified configuration mode commands that would otherwise be allowed.

```
[edit system login class name ]
user@host# set deny-configuration deny-configuration
```

For example, the following statement specifies that the network-mgmt class does not have access to the [snmp address] hierarchy level:

```
[edit system login class network-mgmt]
user@host# set deny-configuration "snmp address"
```

- Specify the number of minutes that a session can be idle before it is automatically closed.

```
[edit system login class class-name]
user@host# set idle-timeout minutes
```

- Display the results of the configuration.

```
[edit system login]
user@host# show

class network-mgmt {
  allow-commands "request system install";
  allow-configuration routing-options;
  deny-configuration "snmp address";
}
class remote {
  deny-configuration "system services telnet";
  permissions all;
}
```

Examples: Configuring Access Privileges for SRC Operational Mode Commands

The following example allows access to the `request system reboot` command for the login class `operator-and-boot` that has operator privileges defined by the `clear`, `network`, `reset`, and `view` permissions.

```
[edit system login class operator-and-boot]
user@host# set permissions [ clear network reset view ]
user@host# set allow-commands "request system reboot"
```

The following example denies access to `set` commands for the login class `operator-no-set` that has operator privileges defined by the `clear`, `network`, `reset`, and `view` permissions.

```
[edit system login class operator-no-set]
user@host# set permissions [ clear network reset view ]
user@host# set deny-commands "set"
```

The following example allows software installation but denies access to the `show nic` command for the login class `operator-no-set` that has operator privileges defined by the `clear`, `network`, `reset`, and `view` permissions.

```
[edit system login class operator-and-install-no-nic]
```

```

user@host# set permissions [ clear network reset view ]
user@host# set allow-commands "request system install"
user@host# set deny-commands "show nic"

```

**Examples: Defining
Access Privileges for
SRC Configuration Mode
Commands**

The following example does not allow access the C-series Controller through a Telnet session for the login class remote that has permission set to all :

```

[edit system login class remote]
user@host# set permissions all
user@host# set deny-configuration "system services telnet"

```

The following example does not allow access to any login class whose name begins with “ m” for the login class local that has permission set to all:

```

[edit system login class local]
user@host# set permissions all
user@host# set deny-configuration "system login class m.*"

```

The following example does not allow access to configuration mode commands at the [system login class] or [system services hierarchy] levels for the login class config-admin that has permission set to all:

```

[edit system login class config-admin]
user@host# set permissions all
user@host# set deny-configuration "(system login class) | (system services)"

```

User Accounts for the SRC Software

User accounts provide one way for users to access the system. For each account, you define the login name for the user, properties for the user account, and authentication information. After you create an account, the software creates a home directory for the user when the user logs in to the system for the first time.

Each user has a home directory on the C-series Controller, which is created the first time that the user logs in. Home directories that have the same name as the user ID are created in the */var/home* directory; for example, the home directory for a user with the user ID Chris_Bee is */var/home/Chris_Bee*.

Configuration Statements for SRC User Accounts

Use the following configuration statements to configure user accounts at the [edit] hierarchy level.

```

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

```

```

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

```

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

Configuring an SRC User Account

To configure a user account:

1. From configuration mode, access the configuration statement that configures a user account, and specify a username that identifies the user.

```

[edit]
user@host# edit system login user user-name

```

The username must be unique within the system. Do not include spaces, colons, or commas in the username. For example:

```

[edit]
user@host# edit system login user JASmith

```

```

[edit system login user JASmith]

```

```

user@host#

```

2. Specify the name of the login class that defines the user's access privilege. [edit system login user *user-name*]

```

[edit system login user user-name ]
user@host# set class class

```

The login class is one of the login classes that you defined in the **class** statement at the [edit system login] hierarchy level, or one of the default classes listed in Table 7 on page 64.

3. Specify the user's full name.

```

[edit system login user user-name ]
user@host# set full-name full-name

```

If the full name contains spaces, enclose it in quotation marks. Do not include colons or commas. For example:

```

[edit system login user JASmith]
user@host# set full-name " John A. Smith"

```

4. (Optional) Specify a user identifier (UID) for the user.

```

[edit system login user user-name ]
user@host# set uid uid

```

The identifier must be a number in the range 0 through 64,000 and must be unique within the system. If you do not assign a UID to a username, the software assigns one when you commit the configuration, preferring the lowest available number.

You must ensure that the UID is unique. However, it is possible to assign the same UID to different users.

5. (Optional) Specify a prompt that the user sees at the SRC CLI.

```
[edit system login user user-name ]
user@host# set prompt prompt
```

6. (Optional) Specify the editing level available to the user. The level determines which configuration commands are visible to the user.

```
[edit system login user user-name ]
user@host# set level (basic | normal | advanced | expert)
```

where:

- **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.
7. (Optional) Specify whether entering a space completes a command.

```
[edit system login user user-name ]
user@host# set complete-on-space (on | off)
```

If you do not enter a value, **complete-on-space** is enabled by default.

8. Define the authentication methods that a user can use to log in to a C-series Controller.

See [Types of Authentication for SRC User Accounts](#) .

9. Display the results of the configuration.

```
[edit system login]
user@host# show
. . .
user JASmith {
  class network-mgmt;
  full-name "John A. Smith";
  uid 507;
  gid 100;
  authentication {
    encrypted-password "{crypt}caZEWdaE1au0c";
```

```

    }
    level normal;
    complete-on-space on;
}

```

- Display the results of the configuration.

```

[edit system login]
user@host# show
. . .
user JASmith {
  class network-mgmt;
  full-name "John A. Smith";
  uid 507;
  gid 100;
  authentication {
    encrypted-password "{crypt}caZEWDaE1au0c";
  }
  level normal;
  complete-on-space on;
}

```

Types of Authentication for SRC User Accounts

You can configure the following types of authentication for user accounts:

- Plain text password—Prompt for a plain text (unencrypted) password. The requirements for plain text passwords are:
 - Can contain between 6 and 128 characters
 - Can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters).



NOTE: We do not recommend that the password include control characters. We do recommend that the password include at least one change of case or character class.

If you configure a plain text password, you are prompted to enter and confirm the password.

- Encrypted password—Password encoded with crypt. The format of encrypted passwords is "{crypt}" < 13-characters in a-zA-Z0-9./>".



NOTE: We recommend that you *do not* enter the password in encrypted format.

- SSH—SSH authentication. For SSH authentication, you can copy the contents of an SSH keys file into a CLI session.

Do not configure a plain text password and an encrypted password at the same time because one value will overwrite the other.

Configuring Authentication for SRC User Accounts

You can configure user accounts by using the following methods:

- Configuring a Plain Text Password on page 184
- Configuring SSH Authentication on page 184

Configuring a Plain Text Password

To configure a plain text password for a user account:

- At the [edit system user *user-name*] hierarchy, enter the **set authentication plain-text-password** command. For example:

```
[edit system user JASmith]
user@host# set authentication plain-text-password
New password: type password here
Retype new password: retype password here
```

Configuring SSH Authentication

Before you configure SSH authentication, obtain the contents of SSH key files. You can copy the contents of an SSH keys file into a CLI session:

1. On a management machine such as a PC or personal workstation, create an ssh-rsa key:


```
> ssh-keygen
(provide input)
> cat ~/.ssh/id_rsa.pub
```
2. On the C-series Controller enter the **set system login user testuser authentication ssh-authorized-key** command, and paste in the SSH key:

```
user@host# set system login user testuser authentication ssh-authorized-key
“ pasted content of id_rsa.pub ”
```

For example:

```
user@host# set system login user testuser authentication ssh-authorized-key
"ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvSqAWNdmTQJS9eqG1eq
RANI3ML4hH+u7WX/HP0W82gDSPjghnt1e5de3D8U
kullEUBf1obgy/7AKc98FqAlvVp5onCiMg8ELD6
RYkgOgo7U6zERB25qy3sK1Rn9NzrB20qLzbvAcZW1
NlePmf1R99d/Rge7kB/5k6fq3NOG0fc= id@server" "ssh-rsa AAAA
B3NzaC1yc2EAAAABIwAAAIEAxIwe9HfZ78vdbfq1+AYOuCF79yGPxgGuw
GZd9QVdT+dnwGh/4HwLITvKd8SYrhMJsyz5dWuZm
94JSwQosm9BVhJwREt39NYIkLWQjGIMkk8Ccw4
TkPfelz1cSbeFxtFBFVaBbo4YkEv5ItbuxwvTWURkvsQa
```

```

2VJXAqls7z8= id2@server2
erian" "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAwW0o
UD4m+SazgzF2kRlq5Y2+lx2zQbCxqBS
D1rmW92eLPOQIBv/sEy2d8UNeHpoKot9Px8q9ABriOyO
Nc7vqNsSVnAMyicQB786uHoabSErVIYscapT
YvIGg+olbdhKySbSxOoXMehhgoQS0JZxHCbxsQJip7/7vJ
PCjRGU8Xq0= id@server3" ];

```

Example: SRC User Accounts

The following example shows the configuration for user accounts for three system users and the template user “remote.” All users use one of the default system login classes.

```

system login user philip {
  class super-user;
  full-name " Philip of Macedonia" ;
  uid 1001;
  authentication {
  }
  ssh-authorized-keys [ "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAA
    IEAvSqAWNMTQJS9eqG1eq
    RANI3ML4hH+u7WX/HP0W82gDSPjghnt1e5de3D8UkuIIeUB
    f1obgy/7AKc98FqAlvVp5onCiMg8ELD6
    RYkgOgo7U6zERB25qy3sK1Rn9NzrB20qLzbvAcZW1NlePmf
    1R99d/Rge7kB/5k6fq3NOG0fc= id@server" "ssh-rsa AAAAB3NzaC1yc2EA
    AAABlwAAAIEAxIwe9HfZ78vdbfq1+AY0uCF79yGPxgGuw
    GZd9QVdT+dniwGh/4HwLITvKd8SYrhMJsyz5dWuZm94JSwQ
    osm9BVhJwREt39NYIkLW0jGIMkk8Cw4
    TkpFfelz1cSbeFxtFBFVaBbo4YkEv5ltbuxwvbTWURkvsQa2VJXA
    qls7z8= id2@server2
    erian" "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAwW0oUD4
    m+SazgzF2kRlq5Y2+lx2zQbCxqBS
    D1rmW92eLPOQIBv/sEy2d8UNeHpoKot9Px8q9ABriOyONc7v
    qNsSVnAMyicQB786uHoabSErVIYscapT
    YvIGg+olbdhKySbSxOoXMehhgoQS0JZxHCbxsQJip7/7vJPCjRG
    U8Xq0= id@server3" ];
  user alexander {
    full-name " Alexander the Great" ;
    uid 1002;
  class view;
    authentication {
    }
  ssh-authorized-keys [ "ssh-rsa
    AAAAB3NzaC1yc2EAAAABIwAAAIEAvSqAWNMTQJS9eqG1eq
    RANI3ML4hH+u7WX/HP0W82gDSPjghnt1e5de3D8UkuIIeUBf1obgy
    /7AKc98FqAlvVp5onCiMg8ELD6
    RYkgOgo7U6zERB25qy3sK1Rn9NzrB20qLzbvAcZW1NlePmf1R99d
    /Rge7kB/5k6fq3NOG0fc= id@server" "ssh-rsa
    AAAAB3NzaC1yc2EAAAABIwAAAIEAxIwe9HfZ78vdbfq1+AY0uCF79y
    GPxgGuw
    GZd9QVdT+dniwGh/4HwLITvKd8SYrhMJsyz5dWuZm94JSwQosm9
    BVhJwREt39NYIkLW0jGIMkk8Cw4
    TkpFfelz1cSbeFxtFBFVaBbo4YkEv5ltbuxwvbTWURkvsQa2VJXA

```

```

qls7z8= id2@server2
eriand" "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAwwOoUD4m+Sazgz
F2kRIq5Y2+lx2zQbCqxBS
D1rmW92eLPOQIBv/sEy2d8UNeHpoKot9Px8q9ABriOyONc7vqNsS
VnAMyicQB786uHoabSErVIYscapT
YvIGg+olbdhKySbSxOoXMehhgoQS0JZxHCbxsQJip7/7vJPCjRGU
8Xq0= id@server3" ];
user darius {
    full-name " Darius King of Persia" ;
    uid 1003;
    class operator;
    authentication {
        ssh " 1024 37 12341234@ecbatana.per" ;
    }
}
user remote {
    full-name " All remote users" ;
    uid 9999;
    class read-only;
}

```

Changing the root Password for the SRC Software

An account for the user root is always present in the configuration. Only the root user can change the root password. You can change the root password with the SRC CLI, but not with the C-Web Interface.

To change the root password:

1. Log into the SRC software as root.
2. From operational mode, change the root password.

```

root@host> set cli password
Changing password for user root.
New UNIX password:

```

You can also create a regular account for root and set the SSH key there. The class for root is always super-user—if you create an account for root, the class is ignored.

Configuring a System Login Announcement (SRC CLI)

A system login announcement appears after the user logs in. By default, no login announcement is displayed.

To configure a system login announcement:

- At the [edit system login] hierarchy level, add the announcement statement.

```

[edit system login]
user@host# set announcement text

```

If the announcement text contains any spaces, enclose it in quotation marks.

Chapter 23

Authenticating Users on a C-series Controller (SRC CLI)

- Configuring RADIUS and TACACS + Authentication on a C-series Controller on page 189
- Configuring RADIUS Authentication (SRC CLI) on page 190
- Configuring TACACS + Authentication (C-Web Interface) on page 191
- A C-series Controller as a RADIUS Client and TACACS + Client on page 191
- Configuring More Than One Authentication Method (SRC CLI) on page 192
- Removing an SRC Authentication Method from the Authentication Order on page 194
- SRC Template Accounts for RADIUS and TACACS + Authentication on page 194
- Configuring a Local SRC User Template on page 195
- Example: Configuring SRC Authentication on page 196

Configuring RADIUS and TACACS+ Authentication on a C-series Controller

The SRC software always performs password authentication on a C-series Controller. You can configure RADIUS and/ or TACACS + authentication to complement password authentication. In this case, the software performs RADIUS and or TACACS + authentication before password authentication.

To configure RADIUS and TACACS + authentication for users who access a C-series Controller:

1. Configure the connection to the RADIUS or TACACS + server.

See Configuring RADIUS Authentication (SRC CLI).

2. Configure the authentication order.

See A C-series Controller as a RADIUS Client and TACACS + Client .

3. Configure template accounts.
4. (Optional) Configure individual user profiles.

See Overview of SRC User Accounts.

Configuring RADIUS Authentication (SRC CLI)

Use the following configuration statements to configure information about one or more RADIUS servers on the network at the [edit] hierarchy level:

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

To configure information about RADIUS servers for authentication:

1. From configuration mode, access the configuration statement that adds a RADIUS server.

```
[edit]
user@host# edit system radius-server address
```

2. Specify a port number on which to contact the RADIUS server.

```
[edit system radius-server address]
user@host# set port port
```

By default, port number 1812 is used.

3. Specify a password. Passwords can contain spaces. The secret used by the C-series Controller must match that used by the server.

```
[edit system radius-server address]
user@host# set secret secret
```

4. (Optional) Specify the amount of time that the C-series Controller waits to receive a response from a RADIUS server.

```
[edit system radius-server address]
user@host# set timeout timeout
```

By default, the C-series Controller waits 3 seconds. You can change the timeout to a value from 1 through 90 seconds.

5. Specify the number of times that the C-series Controller attempts to contact a RADIUS authentication server.

```
[edit system radius-server address]
user@host# set retry retry
```

By default, the C-series Controller retry property is set to 3 times. You can change the retry value to a number from 1 through 10 times.

To configure a set of users that share a single account for authorization purposes, you create a template user.

Configuring TACACS+ Authentication (C-Web Interface)

To configure information about TACACS + servers for authentication:

1. Click **Configure**, expand **System**, and then click **Tacplus Server**.

The Tacplus Server pane appears.

2. Click **Create**, enter information as described in the Help text in the main pane, and then click **Apply**.

To configure a set of users that share a single account for authorization purposes, you create a template user.

A C-series Controller as a RADIUS Client and TACACS+ Client

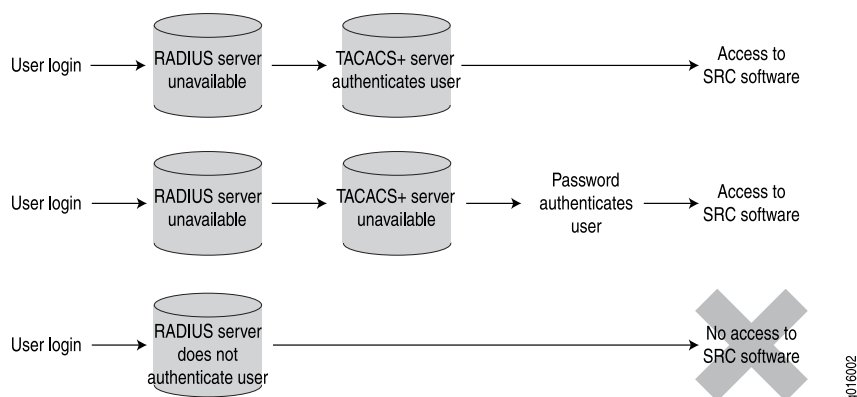
On a C-series Controller, you can use more than one authentication method. You can configure the C-series Controller to be a RADIUS and TACACS + client by:

- Configuring RADIUS and TACACS + authentication.
- Configuring the authentication order to prioritize the order in which the C-series Controller uses configured authentication methods.

For each login attempt, the SRC software tries the authentication methods in the order configured, until the password matches. If one of the authentication methods in the authentication order fails to authenticate a user, the user is denied access to the C-series Controller.

If password authentication does not appear in the prioritized list of authentication methods, the SRC software uses password authentication last. The SRC software always uses password authentication, whether or not it appears in the list of authentication methods to be used. As a result, users can log in to the C-series Controller through password authentication if configured authentication servers are unavailable.

Figure 18 on page 192 shows three authentication scenarios. In the first two, a user is authenticated while authentication servers are unavailable. In the third scenario, a users is not authenticated by an active server.

Figure 18: Authentication Order: RADIUS, TACACS+, Password

Configuring More Than One Authentication Method (SRC CLI)

Tasks to configure more than one authentication method at the SRC CLI are:

1. Configuring Authentication Order on page 192
2. Configuring TACACS + or RADIUS Authentication on page 192
3. Configuring TACACS + and RADIUS Authentication on page 193

Configuring Authentication Order

To configure the order in which to use authentication servers:

1. From configuration mode, access the [system] hierarchy level.
2. Specify the authentication order.

```
[edit system]
user@host# set authentication-order [(radius | tacplus | password)]
```

Specify one or more of the following in the preferred order, from first authentication method tried to last tried:

- **radius**—Verify the user using RADIUS authentication services.
- **tacplus**—Verify the user using TACACS + authentication services.
- **password**—Verify the user using the password configured for the user with the authentication statement at the [edit system login user] hierarchy level.

If you do not include the **authentication-order** statement, users are verified based on their configured passwords.

Configuring TACACS+ or RADIUS Authentication

To configure the SRC software to try to authenticate users through TACACS + and, if the TACACS + server is unavailable, to use password authentication:

- Specify the following authentication order:

```
[edit]
user@host# set system authentication-order [tacplus password]
```

or

```
[edit]
user@host# set system authentication-order tacplus
```

To configure the SRC software to try to authenticate users through RADIUS and, if the RADIUS server is unavailable, to use password authentication:

- Specify the following authentication order:

```
[edit]
user@host# set system authentication-order [radius password]
```

or

```
[edit]
user@host# set system authentication-order radius
```

Configuring TACACS+ and RADIUS Authentication

To configure the SRC software to try to authenticate users through TACACS + and, if the TACACS + server is unavailable, to use RADIUS authentication; and then, if the RADIUS server is unavailable, to use password authentication:

- Specify the following authentication order:

```
[edit]
user@host# set system authentication-order [tacplus radius password]
```

or

```
[edit]
user@host# set system authentication-order [tacplus radius]
```

To configure the SRC software to try to authenticate users through RADIUS and, if the RADIUS server is unavailable, to use TACACS + authentication; and then, if the TACACS + server is unavailable, to use password authentication:

- Specify the following authentication order:

```
[edit]
user@host# set system authentication-order [radius tacplus password]
```

or

```
[edit]
```

```
user@host# set system authentication-order [radius tacplus]
```

Removing an SRC Authentication Method from the Authentication Order

To delete the `radius` statement from the authentication order:

- Enter the following command:

```
[edit system]
user@host# delete authentication-order [(radius | tacplus)]
```

For example:

```
[edit system]
user@host# delete authentication-order radius
```

SRC Template Accounts for RADIUS and TACACS+ Authentication

When a user logs in to the CLI, the following authentication is performed:

- RADIUS and /or TACSACS + server authentication
- Authentication through a user account configured under `[system login user]`

For authorization purposes, you can use a template account to create a single account that can be shared by a set of users at the same time.

Typically when you use RADIUS and/or TACACS + authentication, the user account is shared among a group of users who have the same privileges. You create template accounts for sets of users. Template accounts can be named:

- **remote**—(Default) A single account that defines user permissions for all users that authenticate through RADIUS or TACACS +
- *name-of-your-choice* —Account for a group of users

Use a named template account when you need different types of templates. Each template can define a different set of permissions appropriate to a group of users who use that template. For example, you can configure a set of remote users to concurrently share a single UID.

When a user is part of a group that uses a template account, the command-line interface (CLI) username is the login name; however, the privileges, file ownership, and effective username are inherited from the template account.

Named Template Accounts

Template accounts for which you define a name are defined on a C-series Controller and are referenced by the TACACS + and RADIUS authentication servers through

usernames. All users who share a local user template account have the same access privileges.

When a user who accesses the C-series Controller through a name template account logs in:

1. The SRC software issues a request to the authentication server to authenticate the user's login name.
2. If a user is authenticated, the server returns the username to the SRC software.
3. The SRC software determines whether a username is specified for that login name.
4. If there is a username, the SRC software selects the appropriate template.
5. If a user template does not exist for the authenticated user, the C-series Controller uses the remote template.

Using Remote SRC Template Accounts

To configure the remote template account and specify the privileges that you want to grant to remote users:

- Include the system login user remote statement at the [edit] hierarchy level, and specify the “All remote users” for the full-name option:

```
[edit]
system login user remote {
  full-name "All remote users";
  uid uid-value ;
  class class-name ;
}
```

All users who share the remote template account have the same access privileges.

Configuring a Local SRC User Template

To configure a local user template and specify the privileges that you want to grant to the local users to whom the template applies:

- Include the system login user *local-username* statement at the [edit] hierarchy level, and specify the name of the group for the full-name option.

```
[edit]
system login user username {
  full-name " name of group ";
  uid uid-value ;
  class class-name ;
}
```

Example: Configuring SRC Authentication

The following example allows login only by:

- Individual user Philip
- Users who have been authenticated by a remote RADIUS server

If a user logs in and is not authenticated by the RADIUS server, the user is denied access to the C-series Controller. However, if the RADIUS server is not available, the user can be authenticated through an SRC password.

In this example, user configuration includes:

- An individual user account for Philip that provides privileges for the **super-user** class after RADIUS authentication.
- A remote user template account for all other users to share the same class and user ID (UID) after RADIUS authentication.

Individual SRC accounts are not configured for other users. When they log in to the system and the RADIUS server authenticates them, they are given access using the same UID 9999 and the same privileges for the **operator** class.

```
[edit]
system {
  authentication-order radius;
  login {
    user philip {
      full-name "Philip";
      uid 1001;
      class super-user;
    }
    user remote {
      full-name "All remote users";
      uid 9999;
      class operator;
    }
  }
}
```

Chapter 24

Managing Security Digital Certificates

- Overview of Digital Certificates on page 197
- Before You Use Digital Certificates on page 197
- Commands to Manage Digital Certificates on page 198
- Manually Obtaining Digital Certificates on page 198
- Obtaining Digital Certificates through SCEP on page 200
- Removing a Certificate Request on page 201
- Removing a Certificate on page 202

Overview of Digital Certificates

The SRC software provides support for digital certificates for use by other protocols to protect communications between the SRC software and other applications or network devices. You can manage certificates to:

- Support HTTPS connections between the SRC software and Web browsers.
- Allow BEEP TLS connections between the SRC software and JUNOS routing platforms.

You can use SRC CLI commands to manage certificates manually, or through the Simple Certificate Enrollment Protocol (SCEP).

Certificates are in the format defined in the X.509 standard for public key infrastructure. The certificate requests are in the Public Key Cryptology Standard (PKCS) #10 format.

Related Topics

- Before You Use Digital Certificates
- Commands to Manage Digital Certificates
- Manually Obtaining Digital Certificates
- Obtaining Digital Certificates through SCEP

Before You Use Digital Certificates

Before you use digital certificates, you should:

- Have a working relationship with a certificate authority (CA).
- Have a good working knowledge of how to work with certificates.
- Decide whether or not to use SCEP to assist with certificate management.
- Identify which connections should be secured by a protocol that requires digital certificates.
- Know how to use the file management commands in the CLI.

Related Topics

- Overview of Digital Certificates
- Manually Obtaining Digital Certificates
- Obtaining Digital Certificates through SCEP

Commands to Manage Digital Certificates

You can use the following operational mode commands to manage digital certificates. Which commands you use depends on whether or not you use SCEP.

- `clear security certificate`
- `clear certificate request`
- `request security generate-certificate-request`
- `request security enroll (SCEP)`
- `request security get-ca-certificate (SCEP)`
- `request security import-certificate`
- `show security certificate`

Related Topics

- Manually Obtaining Digital Certificates
- Obtaining Digital Certificates through SCEP
- For detailed information about each command, see the *SRC-PE CLI Command Reference*.

Manually Obtaining Digital Certificates

You can manually add digital certificates, or you can use SCEP to help manage how you obtain certificates.

For information about using SCEP to obtain certificates, see *Obtaining Digital Certificates through SCEP*.

To manually add a signed certificate:

1. Create a certificate signing request.

```
user@host> request security generate-certificate-request subject subject
password password
```

where:

- **subject** is the distinguished name of the SRC host; for example `cn=cseries1,ou=pop,o=Juniper,l=kanata,st=Ontario,c=Canada`.
- **password** is the password received from the certificate authority for the specified subject.

By default, this request creates the file `/tmp/certreq.csr` and encodes the file by using Privacy-Enhanced Mail (pem) encoding.

2. Copy the file generated to another system, and submit the certificate signing request file generated to the certificate authority.

You can transfer the file through FTP by using the `file copy` command.

```
user@host> file copy source_file ftp:// username @ server [: port ]/
destination_file
```

The remote system prompts you for your password.

3. When you receive the signed certificate, copy the file back to the system to the `/tmp` directory.

You can transfer the file through FTP, as shown in Step 2.

4. Add the certificate to the SRC configuration.

```
user@host> request security import-certificate file-name file-name identifier
identifier
```

where

- **file-name** is the name of the certificate file in the `/tmp` folder. The file has one of the following extensions:
 - CER—Windows extension
 - PEM—Privacy-Enhanced Mail encoding
 - DER—Binary encoding
 - BER—Binary encoding
- **identifier** is the name of the certificate.

For example, to import the file `sdx.cer` that is identified as `web`:

```
user@host> request security import-certificate file-name sdx.cer identifier web
```

5. Verify that the certificate is part of the SRC configuration.

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

If there are no certificates on the system, the CLI displays the following message:

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

- Related Topics**
- Before You Use Digital Certificates
 - Obtaining Digital Certificates through SCEP
 - Removing a Certificate Request
 - Overview of Digital Certificates
 - Commands to Manage Digital Certificates

Obtaining Digital Certificates through SCEP

You can use SCEP to help manage how you obtain digital certificates, or you can manually add certificates.

For information about manually obtaining certificates, see [Manually Obtaining Digital Certificates](#).

To add a signed certificate that you obtain through SCEP:

1. Request a CA certificate through SCEP.

```
user@host> request security get-ca-certificate url url ca-identifier ca-identifier
```

where:

- url is the URL of the certificate authority (which is the SCEP server).
- ca-identifier is the identifier that designates the authority.

For example, to request a certificate from the CA authority SdxCA at a specified URL on the server security_server:

```
user@host> request security get-ca-certificate url
http://security_server:8080/ejbca/publicweb/apply/scep/pkiclient.exe
ca-identifier SdxCA

Version: 3
Serial Number: 5721058705923989279
Signature Algorithm: SHA1withRSA
Issuer: CN=SdxCA
Valid From: Wed Sep 06 17:00:55 EDT 2006
Valid Until: Sat Sep 03 17:10:55 EDT 2016
Subject: CN=SdxCA
Public key: RSA
Thumbprint Algorithm: SHA1
Thumbprint: 3c 57 a9 77 af 83 3 e9 c7 1e ee e2 4a e8 ff f3 89 f4 11 a9
Do you want to add the above certificate as a trusted CA [yes,no] ? (no)
y
```

2. Request that the certificate authority automatically sign the certificate request.

```
user@host> request security enroll subject subject password password
```

where:

- **subject** is the distinguished name of the SRC host; for example **cn=myhost**.
- **password** is the password received from the certificate authority for the specified subject.

For example, to request a certificate from the CA authority SdxCA at a specified URL on the server `security_server`:

```
user@host> request security enroll url
http://security_server:8080/ejbca/publicweb/apply/scep/pkiclient.exe
identifier web ca-identifier SdxCA subject cn=myhost password mypassword
```

```
Received certificate:
Version: 3
Serial Number: 6822890691617224432
Signature Algorithm: SHA1withRSA
Issuer: CN=SdxCA
Valid From: Tue Sep 19 16:33:11 EDT 2006
Valid Until: Thu Sep 18 16:43:11 EDT 2008
Subject: CN=myhost
Public key: RSA
Do you want to install the above certificate [yes,no] ? (no) y
```

3. Verify that the certificate is part of the SRC configuration.

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

If there are no certificates on the system, the CLI displays the following message:

```
No entity certificates in key store
```

- Related Topics**
- Before You Use Digital Certificates
 - Manually Obtaining Digital Certificates
 - Removing a Certificate Request
 - Overview of Digital Certificates
 - Commands to Manage Digital Certificates

Removing a Certificate Request

To remove a certificate request:

1. Review the certificate request files on the system. These files are in the `/tmp` directory and have the file extension `.csr`.

2. Issue the `clear security certificate-request` command to remove a file. For example:

```
user@host> clear security certificate-request certreq.csr
```

- Related Topics**
- Manually Obtaining Digital Certificates
 - Obtaining Digital Certificates through SCEP

Removing a Certificate

To remove a certificate:

1. Issue the `show security certificate` command to view information about the local certificates. For example:

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

2. Issue the `clear security certificate` command to remove a certificate. Use the `trusted` option if the certificate is a CA certificate.

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

For example:

- To remove the certificate `web` (that is not a trusted certificate) from `myhost`:

```
user@host>clear security certificate web
```

- To remove a trusted (CA) certificate from `myhost`:

```
user@host>clear security certificate trusted CAcert 1
```

- Related Topics**
- Removing a Certificate Request
 - Manually Obtaining Digital Certificates
 - Obtaining Digital Certificates through SCEP

Chapter 25

Connecting to Remote Hosts from the SRC Software

- Connecting to a Remote Host Through SSH on page 203
- Connecting to a Remote Host Through Telnet on page 203

Connecting to a Remote Host Through SSH

To connect to a remote host through SSH:

- In operational mode, enter the following command.

```
user@host> ssh host host <v1 | v2>
```

where:

- *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.
- <v1 | v2>—Version of SSH, 1 or 2.

Connecting to a Remote Host Through Telnet

To connect to a remote host through Telnet:

- In operational mode, enter the following command.

```
user@host> telnet host <port port>
```

where:

- *host* —Hostname or IP address of the remote host.
- *port port* —(Optional) Port number or service name on the remote host.

Chapter 26

Configuring and Starting the SNMP Agent (SRC CLI)

- Configuration Statements for the SDX SNMP Agent on page 206
- Configuring the SDX SNMP Agent on page 207
- Configuring General Properties for the SDX SNMP Agent on page 207
- Configuring Initial Properties for the SDX SNMP Agent on page 208
- Configuring Directory Connection Properties for the SDX SNMP Agent on page 209
- Configuring Directory Monitoring Properties for the SDX SNMP Agent on page 210
- Configuring Logging Destinations for the SDX SNMP Agent on page 211
- Configuring JRE Properties on page 211
- Configuration Statements for the SNMP Agent on page 212
- Configuring the SNMP Agent on page 213
- Configuring System Information for the SNMP Agent on page 213
- Configuring Access Control for SNMPv3 Users on page 215
- Configuring Authentication on page 215
- Configuring Encryption on page 215
- Configuring Access Control for Communities on page 216
- Configuring Access Control for the VACM on page 217
- Associating Security Names with a Community on page 217
- Defining Named Views on page 218
- Defining Access Privileges for an SNMP Group on page 219
- Assigning Security Names to Groups on page 221
- Configuring Notification Targets on page 222
- Operating the SNMP Agent on page 223
- Starting the SDX SNMP Agent on page 223
- Stopping the SDX SNMP Agent on page 223
- Monitoring the SDX SNMP Agent on page 223

Configuration Statements for the SDX SNMP Agent

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

```
snmp agent {
  trap-history-limit trap-history-limit;
  component-polling-interval component-polling-interval;
  protocol-log-level protocol-log-level;
}
snmp agent initial {
  base-dn base-dn;
  host-id host-id;
}
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;
}
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;
}
snmp agent java {
  heap-size heap-size;
}
snmp agent logger name ...
snmp agent logger name file {
  filter filter;
  filename filename;
  rollover-filename rollover-filename;
  maximum-file-size maximum-file-size;
}
snmp agent logger name syslog {
  filter filter;
  host host;
  facility facility;
  format format;
}
```

- Related Topics**
- Configuring the SDX SNMP Agent
 - For detailed information about each configuration statement, see the *SRC-PE CLI Command Reference*.

Configuring the SDX SNMP Agent

The SNMP agent obtains most of its information from the directory, but you configure the local properties that cannot be stored in the directory.

To configure the local properties for the SDX SNMP agent:

1. Configure general properties for the SDX SNMP agent, including trap history limit, component polling interval, and protocol log level.

See [Configuring General Properties for the SDX SNMP Agent](#) .

2. Configure initial properties for the SDX SNMP agent, including the connection from the SDX SNMP agent to the directory and directory monitoring properties.

See [Configuring Initial Properties for the SDX SNMP Agent](#) .

See [Configuring Directory Connection Properties for the SDX SNMP Agent](#) .

See [Configuring Directory Monitoring Properties for the SDX SNMP Agent](#) .

3. Configure logging destinations for the SDX SNMP agent.

See [Configuring Logging Destinations for the SDX SNMP Agent](#) .

4. (Optional) Configure the Java heap memory for the SDX SNMP agent.

See “Configuring JRE Properties” on page 211 .

After you configure the local properties for the SDX SNMP agent, you can configure the SNMP agent. See [Configuring the SNMP Agent](#) .

Configuring General Properties for the SDX SNMP Agent

Use the following configuration statements to configure general properties for the SDX SNMP agent:

```
snmp agent {
  trap-history-limit trap-history-limit;
  component-polling-interval component-polling-interval;
  protocol-log-level protocol-log-level;
}
```

To configure properties for the SDX SNMP agent:

1. From configuration mode, access the configuration statement that configures the SDX SNMP agent.

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

2. (Optional) Specify the maximum number of elements stored in the SNMP trap history table.

```
[edit snmp agent]
```

```
user@host# set trap-history-limit trap-history-limit
```

3. (Optional) Specify the interval at which an SRC component is polled.

```
[edit snmp agent]
user@host# set component-polling-interval component-polling-interval
```

4. (Optional) Specify the log level for SNMP requests and responses received from the master agent.

```
[edit snmp agent]
user@host# set protocol-log-level protocol-log-level
```

To enable packet-level logging, set the **protocol-log-level** option to 9 or less.

5. (Optional) Verify your configuration.

```
[edit snmp agent]
user@host# show
```

The output indicates the trap history limit, the component polling interval, the protocol log level, the initial properties, the logging destinations, and the Java heap size.

- Related Topics**
- Configuring the SDX SNMP Agent
 - Configuration Statements for the SDX SNMP Agent on page 206

Configuring Initial Properties for the SDX SNMP Agent

Use the following configuration statements to configure initial properties for the SDX SNMP agent:

```
snmp agent initial {
  base-dn base-dn;
  host-id host-id;
}
```

To configure properties for the SDX SNMP agent:

1. From configuration mode, access the configuration statement that configures the SDX SNMP agent.

```
[edit]
user@host# edit snmp agent initial
```

2. Specify the DN of the directory used for the SNMP agent configuration data.

```
[edit snmp agent initial]
user@host# set base-dn base-dn
```

3. Identifies the system management configuration in the directory server that provides the remaining configuration for the SNMP agent.

```
[edit snmp agent initial]
user@host# set host-id host-id
```

If the entry does not exist, the entry and the subentries for the components and traps is automatically created in the system management configuration.

4. (Optional) Verify your configuration.

```
[edit snmp agent initial]
user@host# show
base-dn o=UMC;
host-id POP-ID;
directory-connection {
  url ldap://127.0.0.1:389/;
  principal cn=sysman,ou=components,o=operators,<base>;
  credentials *****;
}
directory-eventing {
  eventing;
}
```

- Related Topics**
- Configuring the SDX SNMP Agent
 - Configuration Statements for the SDX SNMP Agent on page 206

Configuring Directory Connection Properties for the SDX SNMP Agent

Use the following configuration statements to configure directory connection properties for the SDX SNMP agent:

```
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;
}
```

To configure directory connection properties:

1. From configuration mode, access the configuration statement that configures the SDX SNMP agent.

```
[edit]
user@host# edit snmp agent initial directory-connection
```

2. Specify the directory connection properties.

```
[edit snmp agent initial directory-connection]
user@host# set ?
```

For more information about the directory connection properties, see “Configuring Local Properties (SRC CLI)” on page 229.

3. (Optional) Verify your configuration.

```
[edit snmp agent initial directory-connection]
user@host# show
url ldap://127.0.0.1:389/;
principal cn=sysman,ou=components,o=operators,<base>;
credentials *****;
```

- Related Topics**
- Configuring the SDX SNMP Agent
 - Configuration Statements for the SDX SNMP Agent on page 206

Configuring Directory Monitoring Properties for the SDX SNMP Agent

Use the following configuration statements to configure directory monitoring properties for the SDX SNMP agent:

```
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;
}
```

To configure properties for the SDX SNMP agent:

1. From configuration mode, access the configuration statement that configures the SDX SNMP agent.

```
[edit]
user@host# edit snmp agent initial directory-eventing
```

2. Specify the properties for the SDX SNMP agent.

```
[edit snmp agent initial eventing]
user@host# set ?
```

3. (Optional) Verify your configuration.

```
[edit snmp agent initial directory-eventing]
user@host# show
eventing;
```

Related Topics ■ Configuring the SDX SNMP Agent

Configuring Logging Destinations for the SDX SNMP Agent

Use the following configuration statement to configure logging destinations for the SDX SNMP agent:

```
snmp agent logger name ...
```

To configure logging destinations:

1. From configuration mode, access the configuration statement that configures the SDX SNMP agent.

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

2. Specify the name and type of logging destination.

For file-based logging:

```
[edit snmp agent]
user@host# set logger name file
```

For syslog-based logging:

```
[edit snmp agent]
user@host# set logger name syslog
```

Related Topics ■ Configuring the SDX SNMP Agent
 ■ Configuring System Logging with SRC CLI
 ■ Configuring a Component to Store Log Messages in a File with SRC CLI
 ■ Configuring the SAE to Store Log Messages in a File (C-Web Interface)

Configuring JRE Properties

Use the following configuration statements to configure Java Runtime Environment (JRE) properties for the SDX SNMP agent:

```
snmp agent java {
    heap-size heap-size;
}
```

To configure properties for the SDX SNMP agent:

1. From configuration mode, access the configuration statement that configures the SDX SNMP agent.

```
[edit]
```

```
user@host# edit snmp agent java
```

2. (Optional) Specify the maximum amount of memory available to the JRE.

```
[edit snmp agent java]
user@host# set heap-size heap-size
```

Do not change this value unless instructed to do so by Juniper Networks.

3. (Optional) Verify your configuration.

```
[edit snmp agent java]
user@host# show
heap-size 160m;
```

Configuration Statements for the SNMP Agent

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

```
snmp {
  contact contact;
  name name;
  location location;
  description description;
  address [address...];
}
snmp community community {
  authorization (read-only|read-write);
  clients clients;
  oid oid;
}
snmp notify target target-name {
  address address;
  port port;
  community community;
  type (trapv1|trapv2|inform);
}
snmp v3 snmp-community community-index {
  community-name community-name;
  security-name security-name;
  address address;
}
snmp v3 usm local-engine user username ...
snmp v3 usm local-engine user username authentication-md5 {
  authentication-password authentication-password;
}
snmp v3 usm local-engine user username authentication-sha {
  authentication-password authentication-password;
}
snmp v3 usm local-engine user username privacy-aes {
  privacy-password privacy-password;
}
snmp v3 usm local-engine user username privacy-des {
```

```

    privacy-password privacy-password;
}
snmp v3 vacm access group group-name ...
snmp v3 vacm access group group-name default-context-prefix security-model
    (any|v1|v2c|usm) ...
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;
}
snmp v3 vacm security-to-group security-model (v1|v2c|usm) ...
snmp v3 vacm security-to-group security-model (v1|v2c|usm) security-name
    security-name {
    group-name group-name;
}
snmp view view-name ...
snmp view view-name oid oid {
    (include|exclude);
}

```

- Related Topics**
- Configuring the SNMP Agent
 - For detailed information about each configuration statement, see the *SRC-PE CLI Command Reference*.

Configuring the SNMP Agent

To configure the SNMP agent to control its operation:

1. Configure information supplied by the SNMP agent, including the listening address and system information.

See [Configuring System Information for the SNMP Agent](#) .

2. Configure access control for the SNMP agent, including access for SNMPv3 users, SNMPv1 and SNMPv2 communities (traditional access control), and the view-based access control model (VACM).

See [Configuring Access Control for SNMPv3 Users](#) .

See [Configuring Access Control for Communities](#) .

See [Configuring Access Control for the VACM](#) .

3. Configure active monitoring.

See [Configuring Notification Targets](#) .

Configuring System Information for the SNMP Agent

Use the following configuration statements to configure information supplied by the SNMP agent:

```
snmp {
```

```

contact contact;
name name;
location location;
description description;
address [address...];
}

```

To configure properties for the SNMP agent:

1. From configuration mode, access the configuration statement that configures the SNMP agent.

```

[edit]
user@host# edit snmp

```

2. (Optional) Specify the administrative contact for the system being managed by SNMP.

```

[edit snmp]
user@host# set contact contact

```

3. (Optional) Specify the name of the system being managed by SNMP.

```

[edit snmp]
user@host# set name name

```

4. (Optional) Specify the location of the system being managed by SNMP.

```

[edit snmp]
user@host# set location location

```

5. (Optional) Specify the description of the system being managed by SNMP.

```

[edit snmp]
user@host# set description description

```

6. (Optional) Specify the listening address on which to receive incoming SNMP requests.

```

[edit snmp]
user@host# set address [address...]

```

To list more than one IP address, enter the addresses separated by spaces within brackets. By default, the SNMP agent listens on all IPv4 interfaces.

7. (Optional) Verify your configuration.

```

[edit snmp]
user@host# show

```

If you did not configure the SNMP agent, the command displays only the SDX SNMP agent configuration.

- Related Topics**
- Configuring the SNMP Agent
 - Configuration Statements for the SNMP Agent

Configuring Access Control for SNMPv3 Users

To configure access control for SNMPv3 users:

1. Click **Configure**, and expand **SNMP > V3 > USM > Local Engine**.
2. From the Create new list, select User.
3. Enter a name for the new User in the dialog box, and click **OK**.
4. From the side pane, expand the name of the user, and (optional) specify the authentication type and (optional) the encryption.



NOTE: Before you configure encryption, you must configure the authentication type.

Configuring Authentication

To configure the authentication type for SNMPv3 users:

1. From configuration mode, access the configuration statement that configures the authentication type.

To configure MD5 authentication:

```
user@host# edit snmp v3 usm local-engine user username authentication-md5
```

To configure SHA authentication:

```
user@host# edit snmp v3 usm local-engine user username authentication-sha
```

2. Specify the authentication password.

```
user@host# set authentication-password authentication-password
```

The password must be at least eight characters.

- Related Topics**
- Configuring the SNMP Agent
 - Configuration Statements for the SNMP Agent

Configuring Encryption

Before you configure encryption, you must configure the authentication type. See [Configuring Authentication](#) .

To configure encryption for SNMPv3 users:

1. From configuration mode, access the configuration statement that configures the encryption.

To configure AES encryption:

```
user@host# edit snmp v3 usm local-engine user username privacy-aes
```

To configure DES encryption:

```
user@host# edit snmp v3 usm local-engine user username privacy-des
```

2. Specify the privacy password.

```
user@host# set privacy-password privacy-password
```

The password must be at least eight characters.

- Related Topics**
- Configuring the SNMP Agent
 - Configuration Statements for the SNMP Agent

Configuring Access Control for Communities

Use the following configuration statements to configure community strings for traditional access control:

```
snmp community community {
  authorization (read-only|read-write);
  clients clients;
  oid oid;
}
```

To configure community strings:

1. From configuration mode, access the configuration statement that configures the community string. Community names must be unique.

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

2. (Optional) Specify the authorization level.

To specify read-only access:

```
[edit snmp community community]
user@host# set authorization read-only
```

To specify read and write access:

```
[edit snmp community community]
user@host# set authorization read-write
```

3. Specify the IP address or subnet of the SNMP client hosts that are authorized to use this community.

```
[edit snmp community community]
user@host# set clients clients
```

By default, all clients are allowed.

4. (Optional) Specify the object identifier used to represent a subtree of MIB object to which access is allowed.

```
[edit snmp community community]
user@host# set oid oid
```

5. (Optional) Verify your configuration.

```
[edit snmp community community]
user@host# show
```

- Related Topics**
- Configuring the SNMP Agent
 - Configuration Statements for the SNMP Agent

Configuring Access Control for the VACM

To configure the access control for the view-based access control model (VACM):

1. Map an SNMPv1 or SNMPv2c community name to a security name.

See Associating Security Names with a Community .

2. Define a named view.

See “Defining Named Views” on page 218 .

3. Map from a group of users or communities to a view.

See Defining Access Privileges for an SNMP Group .

4. Map a security name into a named group.

See “Assigning Security Names to Groups” on page 221 .

- Related Topics**
- Configuring the SNMP Agent
 - Configuration Statements for the SNMP Agent

Associating Security Names with a Community

For SNMPv1 or SNMPv2c packets, you must assign security names to groups at the [edit snmp v3 vacm security-to-group] hierarchy level and you must associate a security name with an SNMP community.

Use the following configuration statements to configure SNMPv1 or SNMPv2c communities for the VACM:

```
snmp v3 snmp-community community-index {
    community-name community-name;
    security-name security-name;
    address address;
}
```

To configure the community:

1. From configuration mode, access the configuration statement that configures the community.

```
[edit]
user@host# edit snmp v3 snmp-community community-index
```

Unique index that identifies an SNMP community.

2. (Optional) Specify the community string for the SNMPv1 or SNMPv2c community.

```
[edit snmp v3 snmp-community community-index]
user@host# set community-name community-name
```

If a community name is not specified, the community index is used.

3. Specify the VACM security name to associate with the community string.

```
[edit snmp v3 snmp-community community-index]
user@host# set security-name security-name
```

4. (Optional) Specify the IP address or subnet of the SNMP clients that are authorized to use this community.

```
[edit snmp v3 snmp-community community-index]
user@host# set address address
```

If an address is not specified, all clients are authorized to use the community.

5. (Optional) Verify your configuration.

```
[edit snmp v3 snmp-community community-index]
user@host# show
```

Defining Named Views

Use the following configuration statements to define named views:

```
snmp view view-name ...
snmp view view-name oid oid {
    (include|exclude);
}
```

To configure named views:

1. From configuration mode, access the configuration statement that configures the named views.

```
[edit]
user@host# edit snmp view view-name
```

The view name identifies a group of MIB objects for which to define access.

2. Specify the object identifier (OID) that represents a subtree of MIB objects for the view and whether the OID is included in or excluded from the view.

To include the OID in the view:

```
[edit snmp view view-name]
user@host# set oid oid include
```

To exclude the OID from the view:

```
[edit snmp view view-name]
user@host# set oid oid exclude
```

3. (Optional) Verify your configuration.

```
[edit snmp view view-name]
user@host# show
```

Defining Access Privileges for an SNMP Group

Use the following configuration statements to define access privileges for SNMP groups:

```
snmp v3 vacm access group group-name ...
snmp v3 vacm access group group-name default-context-prefix security-model
  (any|v1|v2c|usm) ...
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;
  }
```

To configure MIB views with a group for the VACM:

1. From configuration mode, access the configuration statement that configures the VACM group.

```
[edit]
user@host# edit snmp v3 vacm access group group-name
```

The group name is the name for a collection of SNMP security names that belong to the same SNMP access policy.

2. Specify the security model for access privileges.

```
[edit snmp v3 vacm access group group-name]
user@host# set default-context-prefix security-model (any|v1|v2c|usm)
```

To specify any security model:

```
user@host# set default-context-prefix security-model any
```

To specify the SNMPv1 security model:

```
user@host# set default-context-prefix security-model v1
```

To specify the SNMPv2c security model:

```
user@host# set default-context-prefix security-model v2c
```

To specify the SNMPv3 user-based security model (USM):

```
user@host# set default-context-prefix security-model usm
```

3. Specify the security level for access privileges.

```
[edit snmp v3 vacm access group group-name]
user@host# set default-context-prefix security-model (any|v1|v2c|usm)
security-level (authentication|none|privacy)
```

To specify a security level that provides authentication but no encryption:

```
user@host# set default-context-prefix security-model (any|v1|v2c|usm)
security-level authentication
```

To specify a security level that provides no authentication and no encryption:

```
user@host# set default-context-prefix security-model (any|v1|v2c|usm)
security-level none
```

For SNMPv1 or SNMPv2c access, specify *none* as the security level.

To specify a security level that provides authentication and encryption:

```
user@host# set default-context-prefix security-model (any|v1|v2c|usm)
security-level privacy
```

4. (Optional) Specify the view used for SNMP read access. You must specify the *read-view* option or the *write-view* option.

```
[edit snmp v3 vacm access group group-name default-context-prefix security-model
(any|v1|v2c|usm) security-level (authentication|none|privacy)]
user@host# set read-view read-view
```

5. (Optional) Specify the view used for SNMP write access. You must specify the *read-view* option or the *write-view* option.

```
[edit snmp v3 vacm access group group-name default-context-prefix security-model
(any|v1|v2c|usm) security-level (authentication|none|privacy)]
user@host# set write-view write-view
```

Assigning Security Names to Groups

For SNMPv1 or SNMPv2c packets, you must assign security names to groups and you must associate a security name with an SNMP community at the [edit snmp v3 snmp-community *community-index*] hierarchy level.

Use the following configuration statements to assign security names to groups:

```
snmp v3 vacm security-to-group security-model (v1|v2c|usm) ...
snmp v3 vacm security-to-group security-model (v1|v2c|usm) security-name
  security-name {
    group-name group-name;
  }
```

To map security names to groups for the VACM:

1. From configuration mode, access the configuration statement that configures the security model for a group.

```
user@host# edit snmp v3 vacm security-to-group security-model (v1|v2c|usm)
```

To specify the SNMPv1 security model:

```
user@host# edit snmp v3 vacm security-to-group security-model v1
```

To specify the SNMPv2c security model:

```
user@host# edit snmp v3 vacm security-to-group security-model v2c
```

To specify the SNMPv3 user-based security model (USM):

```
user@host# edit snmp v3 vacm security-to-group security-model usm
```

2. Specify the security name.

```
user@host# edit snmp v3 vacm security-to-group security-model (v1|v2c|usm)
security-name security-name
```

If the security model is USM, the security name is the username configured at the [edit snmp v3 usm local-engine user] hierarchy level.

3. Specify the group to which the security name is assigned.

```
[edit snmp v3 vacm security-to-group security-model (v1|v2c|usm) security-name
security-name]
user@host# set group-name group-name
```

Configuring Notification Targets

Use the following configuration statements to configure notification targets:

```
snmp notify target target-name {
    address address;
    port port;
    community community;
    type (trapv1|trapv2|inform);
}
```

To configure notification targets:

1. From configuration mode, access the configuration statement that configures the notification target.

```
[edit]
user@host# edit snmp notify target target-name
```

Specify the notification target name.

2. Specify the IPv4 or IPv6 address of the system to receive notifications.

```
[edit snmp notify target target-name]
user@host# set address address
```

3. (Optional) Specify the SNMP trap port number.

```
[edit snmp notify target target-name]
user@host# set port port
```

4. Specify the community string used when sending traps.

```
[edit snmp notify target target-name]
user@host# set community community
```

5. Specify the notification types as traps or informs. Traps are unconfirmed notifications. Informs are confirmed notifications.

To specify the notification type as an SNMPv1 trap:

```
[edit snmp notify target target-name]
user@host# set type trapv1
```

To specify the notification type as an SNMPv2 trap:

```
[edit snmp notify target target-name]
user@host# set type trapv2
```

To specify the notification type as an SNMPv2 inform:

```
[edit snmp notify target target-name]
user@host# set type inform
```

6. (Optional) Verify your configuration.

```
[edit snmp notify target target-name]  
user@host# show
```

Operating the SNMP Agent

You must configure the SNMP agent and then manually start the agent. If you attempt to manually start the SNMP agent before it is configured, the software displays a message that the agent has not been configured and cannot start.

The SNMP agent automatically restarts in the event of a host reboot or process failure that stops the agent.

Starting the SDX SNMP Agent

Before you start the SDX SNMP agent:

1. Perform the initial configuration tasks.

See “Configuring a C-series Controller” on page 39.

2. Configure the SDX SNMP agent.

See Configuring the SDX SNMP Agent.

Manually start the SDX SNMP agent the first time it runs. Thereafter, the agent automatically restarts.

To start the SNMP agent:

```
user@host> enable component agent
```

The system responds with a start message. If the SNMP agent is already running, the system responds with a warning message indicating that fact.

Stopping the SDX SNMP Agent

To stop the SNMP agent:

```
user@host> disable component agent
```

The system responds with a stop message. If the SNMP agent is not running when you issue the command, the software responds with a warning message indicating that fact.

Monitoring the SDX SNMP Agent

Purpose Display the SDX SNMP agent status.

Action `user@host> show component`

The system responds with a status message.

Part 6

Configuring Operating Properties for Components

- Distributing Directory Changes to SRC Components on page 227
- Configuring Local Properties (SRC CLI) on page 229

Chapter 27

Distributing Directory Changes to SRC Components

- Overview of the Directory Eventing System on page 227
- Managing Directory Communication on page 228

Overview of the Directory Eventing System

The directory eventing system (DES) provides two functions:

- Automatic notification of changes in the directory

DES polls the directory periodically to determine changes that affect the configuration or operation of a particular component. If DES finds relevant changes, it automatically provides the changes to the component. However, if DES does not find relevant changes, it does not provide any information.

- Redundancy

You must define a primary directory for SRC components that require access to a directory. You can also define a list of secondary (backup) directories.

DES detects when a connection to the primary directory fails, and:

1. Connects to the first available secondary directory in the specified list.
2. Reverts to the primary directory when it becomes available.

If a connection to a secondary directory fails, DES:

1. Connects to the primary directory if it is available.
2. If the primary directory is unavailable, connects to the first available directory in the specified list.

DES is not a central service for all SRC components; rather, you configure a DES for an individual SRC component. On a C-series Controller, you configure initial eventing for each component for each slot. Other components such as the SAE and the license manager have additional configuration for directory eventing.

Some components have connections to multiple directories; consequently you must configure DES properties for each connection. For example, the SAE may use different directories for service, configuration, and subscriber information.

DES is a Java Naming and Directory Interface (JNDI)–compliant service and accepts standard JNDI properties. For more information about JNDI, see <http://java.sun.com/products/jndi/>.

Managing Directory Communication

When an SRC component communicates with the directory, that component may pass a time (known as a server timeout) to the directory to specify a time limit for the directory to respond. If the directory is not working correctly, however, it may not respond during this time, and will cause the SRC component to stop operating.

DES recovers if the directory is not working correctly. In addition, you can configure DES to prohibit communications with a directory if that directory repeatedly fails to respond. If you do so, DES starts the following procedure for all communication with the directory:

1. Assigns a client timeout to the communication.

The client timeout exceeds the server timeout.
2. If the directory does not respond during this time, DES closes the connection to the directory.
3. DES tries to reconnect to the directory and proceeds as follows:
 - If DES cannot connect to the directory, it connects to the next available directory specified by the DES redundancy properties.
 - If DES can connect to the directory, it contacts the directory again and repeats Steps [xref target has no title] to [xref target has no title].
4. If a directory fails to respond 10 times, DES prevents further communication with the directory.

Chapter 28

Configuring Local Properties (SRC CLI)

- Local Properties for SRC Components on page 229
- Configuration Statements for Local Configuration on page 229
- Configuring Basic Local Properties on page 230
- Changing the Location of Data in the Directory on page 231
- Configuring Directory Connection Properties on page 232
- Configuring Initial Directory Eventing Properties for SRC Components on page 234
- Verifying the Local Configuration for a Component on page 234

Local Properties for SRC Components

Before you configure an SRC component, configure the component's local properties. In many cases you can use the default configuration. From the CLI, local properties are configured for a slot. On a C-series Controller, the slot configuration is applied to the appropriate slot.

Configuration Statements for Local Configuration

Use the following configuration statements to configure local properties for a component. You enter these statements at various hierarchy levels for different SRC components. This list shows the configuration common to a number of components. For information about configuration specific to a component, such as SAE, NIC, SRC-ACP, or SNMP, see the documentation for that component.

```
slot number component-name {  
    base-dn base-dn ;  
    java-runtime-environment java-runtime-environment ;  
    java-heap-size java-heap-size ;  
    snmp-agent;  
}  
slot number component-name initial {  
    static-dn static-dn ;  
    dynamic-dn dynamic-dn ;  
}  
slot number component-name initial directory-connection {  
    url url ;  
    backup-urls [ backup-urls ...];  
    principal principal ;  
    credentials credentials ;
```

```

protocol (ldaps);
timeout timeout ;
check-interval check-interval ;
blacklist;
snmp-agent;
}
slot number component-name initial directory-eventing {
    eventing;
    signature-dn signature-dn ;
    polling-interval polling-interval ;
    event-base-dn event-base-dn ;
    dispatcher-pool-size dispatcher-pool-size ;
}

```

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

Configuring Basic Local Properties

In most cases you can use the default operating properties. Change the default properties if needed for your environment.

Use the following configuration statements to configure basic local properties for a component:

```

slot number component-name {
    base-dn base-dn ;
    java-runtime-environment java-runtime-environment ;
    java-heap-size java-heap-size ;
    snmp-agent;
}

```

To review the default local configuration and then change values:

1. From configuration mode, access the configuration statement that specifies the slot configuration for a component.

```

[edit]
user@host# edit slot number nic

```

For example:

```

[edit]
user@host# edit slot 0 nic

```

2. To view the default configuration, run the **show** command. For example:

```

[edit slot 0 nic]
user@host# show
base-dn o=umc;
java-runtime-environment ../jre/bin/java;
java-heap-size 128m;

```

```
hostname DemoHost;
initial {
```



NOTE: The `hostname` statement is specific to the NIC.

3. (Optional) If you store data in the directory in a location other than the default, `o = umc`, change this value.

```
[edit slot 0 nic]
user@host> set base-dn base-dn
```

4. (Optional) If you encounter problems caused by lack of memory, change the maximum memory size available to the JRE.

```
[edit slot 0 nic]
user@host> set java-heap-size java-heap-size
```

5. (Optional) Enable viewing of SNMP counters through an SNMP browser.

```
[edit slot 0 nic]
user@host> set snmp-agent
```

Changing the Location of Data in the Directory

In most cases, you use the default configuration for the location of SRC data in the directory:

- Administrator-defined configuration
data—ou = *staticConfiguration*, ou = *Configuration*, o = *Management*, o = *umc*
- Programmatically defined configuration
data—ou = *dynamicConfiguration*, ou = *Configuration*, o = *Management*, o = *umc*

You can specify the full distinguished name (DN), or a DN relative to a base DN, identified as `<base>`.

You can change the location of data in the directory at the Expert CLI editing level.

Use the following configuration statements to change the location of data for a component in the directory:

```
slot number component-name initial {
  static-dn static-dn ;
  dynamic-dn dynamic-dn ;
}
```

To change the location of data in the directory:

1. From configuration mode, access the configuration statement that specifies the configuration for a component on a slot.

```
[edit]
user@host# edit slot number nic initial
```

For example:

```
[edit]
user@host# edit slot 0 nic initial
```

2. (Optional) Change the location of administrator-defined configuration data in the directory

```
[edit slot 0 nic initial]
user@host# set static-dn static-dn
```

3. (Optional) Change the location of programmatically defined configuration data in the directory.

```
[edit slot 0 nic initial]
user@host# set dynamic-dn dynamic-dn
```

Configuring Directory Connection Properties

Use the following configuration statements to configure directory properties for a component:

```
slot number component-name initial directory-connection {
  url url ;
  backup-urls [ backup-urls ...];
  principal principal ;
  credentials credentials ;
  protocol (ldaps);
  timeout timeout ;
  check-interval check-interval ;
  blacklist;
  snmp-agent;
}
```

To configure directory connection properties for a component:

1. From configuration mode, access the configuration statement that specifies the directory configuration for a component on a slot.

```
user@host# edit slot number component initial directory-connection
```

For example:

```
user@host# edit slot 0 nic initial directory-connection
```

2. Specify the URL that identifies the location of the primary directory server.

```
[edit slot 0 nic initial directory-connection]
user@host# set url url
```

On a C-series Controller, this value is `ldap://127.0.0.1:389`.

3. (Optional) Specify URLs that identify the locations of backup directory servers. Backup servers are used if the primary directory server is not accessible.

```
[edit slot 0 nic initial directory-connection]
user@host# set backup-urls directory-backup-url1 directory-backup-url2
```

4. Specify the DN that the SRC component uses for authentication to access the directory.

```
[edit slot 0 nic initial directory-connection]
user@host# set principal principal
```

5. Specify the password with which the SRC component accesses the directory.

```
[edit slot 0 nic initial directory-connection]
user@host# set credentials credentials
```

6. (Optional) Specify whether the connection to the directory uses secure LDAP. If you do not configure a security protocol, plain socket is used.

```
[edit slot 0 nic initial directory-connection]
user@host# set protocol ldaps
```

7. (Optional) Specify the maximum amount of time during which the directory must respond to a connection request.

```
[edit slot 0 nic initial directory-connection]
user@host# set timeout timeout
```

8. (Optional) Specify the time interval at which the software attempts to connect to the directory.

```
[edit slot 0 nic initial directory-connection]
user@host# set check-interval check-interval
```

9. (Optional) Enable the directory eventing system to prevent a connection to a directory after the directory fails to respond during an interval in which the directory was polled 10 times.

```
[edit slot 0 nic initial directory-connection]
user@host# set blacklist
```

10. Specify that the SDX SNMP agent exports MIBs for this directory connection.

```
[edit slot 0 nic initial directory-connection]
user@host# set snmp-agent
```

Configuring Initial Directory Eventing Properties for SRC Components

You can use the default configuration for directory eventing properties, or you can change the configuration to comply with your environment.

The following configuration statements configure initial directory eventing properties for a component:

```
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 ;
}
```

To change directory eventing configuration:

1. From configuration mode, access the configuration statement that specifies the initial eventing configuration for a component on a slot.

```
[edit]
user@host# edit slot number component initial directory-eventing
```

For example:

```
[edit]
user@host# edit slot 0 nic initial directory-eventing
```

2. (Optional) Specify an interval at which an SRC component polls the directory to check for directory changes.

```
[edit slot 0 nic initial directory-eventing]
user@host# set polling-interval polling-interval
```

3. (Optional) Specify the DN of an entry superior to the data associated with an SRC component in the directory.

```
[edit slot 0 nic initial directory-eventing]
user@host# set event-base-dn event-base-dn
```

4. (Optional) Specify the number of events that an SRC component can receive simultaneously from the directory.

```
[edit slot 0 nic initial directory-eventing]
user@host# set dispatcher-pool-size dispatcher-pool-size
```

Related Topics ■ For information about the default setting for the directory eventing properties, see the *SRC-PE CLI Command Reference*.

Verifying the Local Configuration for a Component

Purpose Verify the local configuration for a component.

- Action** 1. From configuration mode, access the configuration statement that configures the slot connection. For example, to verify the slot configuration for the NIC:

```
user@host# edit slot 0 nic
```

2. Run the `show` command. For example:

```
[edit slot 0 nic ]
user@host# show
base-dn o=umc;
java-runtime-environment ../jre/bin/java;
java-heap-size 128m;
snmp-agent;
hostname DemoHost;
initial {
    dynamic-dn "ou=dynamicConfiguration, ou=Configuration,
o=Management,<base>";
    directory-connection {
        url ldap://127.0.0.1:389/;
        backup-urls ;
        principal cn=nic,ou=Components,o=Operators,<base>;
        credentials *****;
        timeout 10;
        check-interval 60;
    }
    directory-eventing {
        eventing;
        signature-dn <base>;
        polling-interval 15;
        event-base-dn <base>;
        dispatcher-pool-size 1;
    }
    static-dn "l=OnePop,l=NIC, ou=staticConfiguration, ou=Configuration,
o=Management,<base>";
}
```


Part 7

Reference Material

- SRC-Related Abbreviations on page 239
- SRC-Related References on page 247

Chapter 29

SRC-Related Abbreviations

The following table includes the abbreviations used throughout the SRC documentation.

Abbreviation	Description
3GPP	3rd Generation Partnership Project
AAA	authentication, authorization, and accounting
AATV	authentication/authorization transfer vector
ACI	access control information
ADSL	asymmetric digital subscriber line
AES	Advanced Encryption Standard
AH	authentication header
API	application programming interface
A-RACF	access-resource and admission control function
ASCII	American Standard Code for Information Interchange
ASP	<ul style="list-style-type: none">■ application service provider■ Adaptive Services PIC
ATM	Asynchronous Transfer Mode
AVP	attribute value pair
BCID	billing correlation identifier
BEEP	Blocks Extensible Exchange Protocol
BGF	border gateway function
BNF	Backus-Naur Format
BoD	bandwidth on demand
BOOTP	A bootstrap protocol

Abbreviation	Description
B-RAS	Broadband Remote Access Server
CA	certificate authority
CHAP	Challenge Handshake Authentication Protocol
CIDR	classless interdomain routing
CIM	Common Information Model
CLEC	competitive local exchange carrier
CLI	command-line interface
CMTS	cable modem termination system
COPS	Common Open Policy Service
COPS-PR	COPS usage for policy provisioning
CORBA	Common Object Request Broker Architecture
COS	Common Object Services
CoS	class of service
CSR	certificate signing request
DA	destination address
DCE	Distributed Computing Equipment
DCU	destination class usage
DES	directory eventing system
DHCP	Dynamic Host Configuration Protocol
DISP	Directory Information Shadowing Protocol
DIT	directory information tree
DMTF	Distributed Management Task Force
DN	distinguished name
DNS	Domain Name System
DOCSIS	Data over Cable Service Interface Specifications
DSCP	Differentiated Services (DiffServ) code point
DSL	digital subscriber line
DSLAM	digital subscriber line access multiplexer

Abbreviation	Description
DSML	Directory Services Markup Language
DSP	Directory Service Protocol
DTD	document type definition
EAR	enterprise archive (file format)
EGP	exterior gateway protocol
EJB	Enterprise JavaBean
ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standards Institute
FEID	financial entity identifier
FMC	fixed mobile convergence
FSM	finite state machine
FTP	File Transfer Protocol
GAL	Gateway Application Logic
GIF	graphic interchange format
GMT	Greenwich Mean Time
GRE	generic routing encapsulation
GUI	graphical user interface
HFC	hybrid fiber coaxial
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	Secure HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
ID	identification (identifying; identifier)
IDE	integrated development environment
IDL	interface definition language
IDP	Intrusion Detection and Prevention
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol

Abbreviation	Description
IIOP	Internet Inter-ORB Protocol
ILEC	incumbent local exchange carrier
IMAP	Internet Message Access Protocol
IMS	IP multimedia subsystem
IOR	interoperable object reference
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPSCS	IP Service Control System (product name from Ellacoya Networks)
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet service provider
IT	information technology
J2EE	Java 2 Platform, Enterprise Edition
J2SE	Java 2 Platform, Standard Edition
JAR	Java archive (file format)
JKS	Java Keystores
JMS	Java Message Service
JMX	Java Management Extension
JNDI	Java Naming and Directory Interface
JRE	Java Runtime Environment
JSP	JavaServer Pages
JVM	Java Virtual Machine
KB	kilobyte(s)
L2TP	Layer 2 Tunneling Protocol
LAN	local area network
LAS	local authorization service
LDAP	Lightweight Directory Access Protocol
LDAPS	LDAP over SSL

Abbreviation	Description
LDIF	LDAP Data Interchange Format
LNS	L2TP network server
LSA	link-state advertisement
MAC	Media Access Control
Mb	megabit(s)
MB	megabyte(s)
MBeans	manageable JavaBeans
MD5	Message Digest 5
MI	management information
MIB	Management Information Base
MPLS	Multiprotocol Label Switching
MSO	multiple service operator
MTU	maximum transmission unit
mutex	mutually exclusive
NAT	Network Address Translation
NBNS	NetBIOS Name Server
NGN	next-generation network
NIC	network information collector
NRTPS	non-real-time polling service
OID	object identification
ORB	object request broker
OS	operating system
OSM	object state manager
OSMW	object state manager for the Web
OSPF	Open shortest Path First
OSS	operations support system
PCIM	Policy Core Information Model
PCMM	PacketCable Multimedia Specification

Abbreviation	Description
PDF	portable document file
PDP	policy decision point
PEP	policy enforcement point
PFS	Perfect Forward Secrecy
PIB	Policy Information Base
PIM	Protocol Independent Multicast
PKCS	Public Key Cryptology Standard
PLP	packet loss priority
POP	point of presence
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PTA	PPP Terminated Aggregation
QoS	quality of service
QTP	QoS-tracking plug-in
RACS	resource and admission control subsystem
RADIUS	Remote Authentication Dial-In User Service
RAS	Remote Access Server
RCEF	resource control enforcement function
RDBMS	relational database management system
RDN	relative distinguished name
RED	random early detection
RF	radio frequency
RKS	record-keeping server
RPC	remote procedure call
RSpec	service request specification
RSVP	Resource Reservation Protocol
RTPS	real-time polling service
RTSP	Real Time Streaming Protocol

Abbreviation	Description
SA	source address
SAC	service activation context
SAE	service activation engine
SCEP	Simple Certificate Enrollment Protocol
SCU	source class usage
SDK	Software Development Kit
SDX	Service Deployment System (used only to refer to releases earlier than the new SRC 1.0)
SHA	Secure Hash Algorithm
SID	Oracle System Identifier
SIP	Session Initiation Protocol
SLE	service logic engine
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SPDF	service policy decision function
SPI	<ul style="list-style-type: none"> ■ security parameter index ■ service provider interface
SRC	Session and Resource Control (formerly SDX—Service Deployment System)
SRC-ACP	SRC Admission Control Plug-In
SRC CLI	SRC command-line interface
SRC-PE	SRC Policy Engine
SRC-SG	SRC SOAP Gateway
SRC-TMP	SRC Threat Mitigation Portal
SRC-VTA	SRC Volume Tracking Application
SSL	Secure Sockets Layer
SSM	service and subscriber management
SSP	Service Selection Portal
TCP	Transmission Control Protocol

Abbreviation	Description
TFTP	Trivial File Transfer Protocol
TISPAN	Telecommunications and Internet Converged Services and Protocols for Advanced Networks
TLS	Transport Layer Security
ToS	type of service
TSpec	traffic specification
TTL	<ul style="list-style-type: none"> ■ time to live ■ time-to-live
UDP	User Datagram Protocol
UGS	unsolicited grant service
UGS-AD	unsolicited grant service with activity detection
UML	Unified Modeling Language
URI	Uniform Resource Indicator
URL	Uniform Resource Locator
UTF-8	Unicode Transformation Format-8
UUID	universal unique identifier
VACM	view-based access control model
VLAN	virtual local area network
VoIP	voice over Internet Protocol
VPN	virtual private network
VR	virtual router
VSA	vendor-specific attribute (RADIUS)
WAR	Web archive (file format)
WDSL	Web Services Description Language
Wi-Fi	wireless fidelity
WINS	Windows Internet Name Service (Microsoft)
XDR	External Data Representation Standard
XML	Extensible Markup Language
XSLT	Extensible Stylesheet Language Transformation

Chapter 30

SRC-Related References

This chapter lists RFCs, draft RFCs, other software standards, hardware standards, and other references that provide information about the protocols and features supported by the SDX software. Topics include:

- RFCs on page 247
- Draft RFCs on page 248
- Other Software Standards on page 249
- URLs on page 249

RFCs

Table 15: RFCs

Reference	Protocol or Feature
RFC 3494—Lightweight Directory Access Protocol version 2 (LDAPv2) to Historic Status (March 2003)	LDAP
RFC 3084—COPS Usage for Policy Provisioning (COPS-PR)	COPS-PR
RFC 2882—Network Access Servers Requirements: Extended RADIUS Practices (July 2000)	RADIUS
RFC 1305—Network Time Protocol (Version 3) Specification Implementation and Analysis (March 1992)	NTP
RFC 2869—RADIUS Extensions (June 2000)	RADIUS
RFC 2866—RADIUS Accounting (June 2000)	RADIUS
RFC 2865—Remote Authentication Dial In User Service (RADIUS) (June 2000)	RADIUS
RFC 2748—The COPS (Common Open Policy Service) Protocol	COPS
RFC 2388—Returning Values from Forms: multipart/form-data	multipart/form data
RFC 2255—The LDAP URL Format (December 1997)	LDAP
RFC 2254—The String Representation of LDAP Search Filters (December 1997)	LDAP

Table 15: RFCs (continued)

Reference	Protocol or Feature
RFC 2253—Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names (December 1997)	LDAP
RFC 2252—Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions (December 1997)	LDAP
RFC 2251—Lightweight Directory Access Protocol (v3) (December 1997)	LDAP
RFC 2236—Internet Group Management Protocol, Version 2 (November 1997)	IGMP
RFC 2132—DHCP Options and BOOTP Vendor Extensions (March 1997)	DHCP
RFC 2131—Dynamic Host Configuration Protocol (March 1997)	DHCP
RFC 1558—White Pages Meeting Report (February 1994)	white pages directory
RFC 1213—Management Information Base for Network Management of TCP/IP-based internets: MIB-II (March 1991)	SNMP
RFC 793—Transmission Control Protocol (September 1981)	TCP
RFC 791—Internet Protocol (September 1981)	IP

Draft RFCs



NOTE: IETF drafts are valid for only 6 months from the date of issuance. They must be considered as works in progress. Please refer to the IETF Web site at <http://www.ietf.org> for the latest drafts.

Table 16: Draft RFCs

Reference	Protocol or Feature
LDAP Extensions for Scrolling View Browsing of Search Results—draft-ietf-ldapext-ldapv3-vlv-09.txt (June 2003 expiration)	LDAP
The syslog Protocol—draft-ietf-syslog-protocol-16.txt (July 2006 expiration)	System logging

Other Software Standards

Table 17: Non-RFC Software Standards

Reference	Protocol or Feature
CCITT ITU-T Recommendation X.500—Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services (February 2001)	LDAP
CCITT ITU-T Recommendation X.501—Information technology - Open Systems Interconnection - The Directory: Models (February 2001)	LDAP
PacketCable Multimedia Architecture Framework Technical Report (PKT-TR-MM-ARCH)	PCMM
PacketCable Multimedia Specification PKT-SP-MM-I02-040930	PCMM
PacketCable Multimedia Specification PKT-SP-MM-I03-051221	PCMM
PacketCable Security Specifications (PKT-SP-SEC)	PCMM

URLs

Table 18: Juniper Networks URLs

Reference
http://www.juniper.net
http://www.juniper.net/partners/content_partners.html
http://www.juniper.net/support
http://www.juniper.net/techpubs
http://www.juniper.net/techpubs/docbug/docbugreport.html
http://www.juniper.net/techpubs/software/junos/junos71/index.html
http://www.juniper.net/techpubs/software/junos/junos84/swconfig84-system-basics/swconfig84-system-basics.p

Table 18: Juniper Networks URLs *(continued)*

Reference
http://www.juniper.net/techpubs/software/erx/junose82/bookpdfs/swconfig-broadband.pdf
http://www.juniper.net/techpubs/software/management/idp/
http://www.juniper.net/techpubs/software/management/sdx
http://www.juniper.net/techpubs/software/management/security-manager/src/api-index.html

Table 19: Third-Party URLs

Reference	Protocol Feature
ftp://ftp.gtk.org/pub/gtk/python	GTK libr use with Python program
http://cui.unige.ch/db-research/Enseignement/analyseinfo/AboutBNF.html	BNF not
http://developer.java.sun.com/developer	JRE
http://jakarta.apache.org/tomcat	Servlet contain
http://jakarta.apache.org/regexp/apidocs/org/apache/regexp/RE.html	Java reg expressi docume
http://java.sun.com/j2se/1.4.2/docs/api/java/text/MessageFormat.html	Java me formats

Table 19: Third-Party URLs *(continued)*

Reference	Protocol Feature
http://java.sun.com/j2se/1.4.2/docs/api/java/text/SimpleDateFormat.html	Java date time for
http://java.sun.com/j2se/1.4.1/docs/api/java/util/logging/FileHandler.html	Java logg
http://java.sun.com/j2se/1.4.2/docs/api/java/util/regex/Pattern.html	Java reg expressi docume
http://java.sun.com/j2se/1.4/docs/guide/intl/encoding.doc.html	Characte encodin compile when lo Java sou files
http://java.sun.com/j2se/1.4/docs/guide/jar/	Web applicat
http://java.sun.com/j2ee/1.4/docs/tutorial/doc/index.html	Web applicat
http://java.sun.com/j2se/1.4.2/docs/tooldocs/solaris/java.html	Java docume
http://java.sun.com/j2se/1.4.1/docs/tooldocs/solaris/keytool.html	Java key docume
http://java.sun.com/products/jndi/	Java Nar and Dire Interfac
http://jsautret.free.fr/luci/index.html	LUCI
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndotnet/html/frameworkwinsupp.asp	.NET Framew
http://net-snmp.sourceforge.net/	Net-SNM agent
http://pauillac.inria.fr/~diaz/gnu-prolog/	GNUPRO
http://pysnmp.sourceforge.net	pysnmp
http://python-ldap.sourceforge.net	LDAP cli for Pyth
http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access	Solaris a J2SE pat clusters
http://www.apache.org	Apache server a extensio

Table 19: Third-Party URLs *(continued)*

Reference	Protocol Feature
http://docs.sun.com/app/docs/prod/solaris#hic	Sun Solaris documents
http://wp.netscape.com/eng/mozilla/3.0/handbook/javascript/index.html	JavaScript scripting language
http://www.eclipse.org	Portal development
http://www.entrust.net	Certification authority
http://www.gtk.org	GTK +
http://www.interlinknetworks.com	RAD-Server RADIUS
http://www.jacorb.org/documentation.html	JacORB documents
http://www.jboss.org/products/jbossas	JBoss application server
http://www.jython.org	Jython
http://www.mozilla.org/rhino	Rhino environment
http://www.mysql.com/	MySQL
http://www.omg.org	Object Management Group's 2.6 standard
http://www.opengroup.org/onlinepubs/9629399/apdxa.htm	Universal Unique Identifier (UUIDs) DCE RPC protocol
http://www.openssl.org	Certification authority
http://www.oracle.com/appserver/index.html	Oracle Application Server 1
http://www.packetcable.com/specifications/multimedia.html	PacketCable MultiMedia Specifications

Table 19: Third-Party URLs *(continued)*

Reference	Protocol Feature
http://www.python.org	Python program language
http://www.python.org/doc/2.0/lib/re-syntax.html	Python expressi syntax
http://docs.python.org/ref/keywords.html	Python keywor
http://www.sun.com	Sun and docume
http://www.sun.com/download	Sun ON Director Server
http://www.sun.com/share/text/termsofuse.html	JRE term use
http://www.sunfreeware.com	Freewar Solaris
http://www.sysdeo.com/eclipse/tomcatPlugin.html	Portal develop
http://www.verisign.com	Certifica authorit
http://www.w3.org/TR/SOAP/	Simple Access P (SOAP)
http://www.wi-fi-lliance.org/opensection/wispr.asp	Wi-Fi W docume

Part 8

Index

- Index on page 257

Index

Symbols

! regular expression operator.....	175
\$ regular expression operator.....	175
() regular expression operator.....	175
* regular expression operator.....	175
+ regular expression operator.....	175
. regular expression operator.....	175
\ regular expression operator.....	175
^ regular expression operator.....	175

A

access privilege levels	
permission options.....	170
user accounts.....	181
accounting	
applications.....	3
description.....	6
admin permission.....	170
admin-control permission.....	170
all permission.....	170
announcements at system login.....	186
APIs (application programming interfaces)	
CORBA plug-in SPI.....	21
CORBA remote API.....	21
description.....	7
SAE core API.....	21
application programming interfaces. <i>See</i> APIs	
architecture	
SRC software.....	3
ARP monitor	
configuring	
SRC CLI.....	77
authentication.....	183
configuration example.....	196
multiple methods.....	191
RADIUS	
configuring.....	189
configuring with SRC CLI.....	190
example.....	196
shared user accounts.....	195, 196
TACACS+, configuring.....	189

TACACS+, configuring with C-Web	
interface.....	191
template accounts	
configuring local user with SRC CLI.....	195
configuring remote users with SRC CLI.....	195
named.....	195
overview.....	194
<i>See also</i> user accounts	
authentication order	
configuring with C-Web interface.....	191
configuring with SRC CLI.....	192
overview.....	191, 192
removing authentication method.....	191
removing authentication method with SRC	
CLI.....	194

B

backup directory.....	227
base-dn, configuring.....	230
BEEP TLS connections.....	197
boot server, NTP.....	108
broadcast	
synchronizing NTP.....	113

C

C-series Controllers	
configuration prerequisites.....	39
deployment considerations.....	36
description.....	3
initial configuration.....	41
installing component software.....	155
interfaces.....	69
removing component software.....	155
restoring software snapshot	155
software packages.....	151
software snapshot.....	152
SRC components.....	35
static routes.....	78
upgrading software.....	152, 153, 154
C-Web interface	
committing a configuration.....	64
configuration options.....	62

configuring	
HTTP access.....	56, 60
HTTPS access.....	55, 60
logging properties.....	66
copying an object.....	65
deleting an object.....	66
editing level.....	61
elements.....	53
getting Help.....	59
icons.....	62
layout.....	52
loading configuration values.....	63
logging out.....	67
moving an object.....	65
navigating.....	52
overview.....	16, 51
password, changing.....	59
Policies, Services, and Subscribers	
password.....	59
starting.....	59
renaming an object.....	65
reverting a configuration.....	64
starting.....	58
updating configuration data.....	64
username, changing.....	59
C2000 Controller.....	3
C4000 Controller.....	3
clear permission.....	171
cli.....	45
client mode, NTP.....	109
commands	
access to.....	174
component software	
installing.....	154, 155
upgrading.....	154
configuration statements	
access to.....	174
configure permission.....	171
control permission.....	171
conventions	
notice icons.....	xxi
text.....	xxi
customer support.....	xxv
contacting JTAC.....	xxv
cweb-password.....	59

D

date on system.....	102
deployment scenarios	
C-series Controllers.....	35, 37
DES (directory eventing system)	
overview.....	227
properties.....	234
differentiated QoS.....	7
digital certificates. <i>See</i> security	

directory	
client.....	16
configuring	
redundancy.....	227
description.....	10
failover.....	227
LDAP version 3 compatibility.....	16
managing problems.....	228
primary.....	227
RADIUS.....	22
retrieving changed data.....	227
secondary (backup).....	227
directory connection properties.....	232
directory eventing system.....	227
directory server.....	10
documentation set	
comments on.....	xxv
draft RFCs.....	248
dynamic Web pages.....	7

E

enterprise service portals description.....	28
Ethernet redundancy	
configuring.....	74
SRC CLI.....	75, 77

F

failover directories.....	227
field permission.....	171
firewall permission.....	171
firewall ports for SRC-related components.....	81
firewall-control permission.....	171

G

Gigabit Ethernet interfaces, configuring IPv4.....	70
Gigabit Ethernet interfaces, configuring IPv6.....	71
GRE tunnel interfaces.....	72
group interfaces, configuring.....	74
SRC CLI.....	75

H

hostid command.....	88
HTTPS connections.....	197

I

idle timeout values, login classes.....	176
IDP (Intrusion Detection and Prevention)	
integration applications.....	26
installing software	
SPE.....	165
interface-control permission.....	171

- interfaces
 - C-series Controllers.....69
 - Gigabit Ethernet, configuring IPv4.....70
 - Gigabit Ethernet, configuring IPv6.....71
 - group, configuring.....74
 - tunnel, configuring.....72
- IP addresses
 - virtual, configuring.....78
- IP service, life-cycle process.....3
- IP-over-IP tunnel interfaces.....72
- IVE (Instant Virtual Extranet) Host Checker integration
 - application.....27
- J**
 - J2EE application server.....31
 - Java Naming and Directory Interface. *See* JNDI
 - java-heap-size, configuring.....230
 - JNDI (Java Naming and Directory Interface).....228
 - JSP (Java Server Pages) technology
 - Web application server.....30
 - Juniper Networks database
 - adding Juniper Networks database to community
 - SRC CLI.....133
 - changing modes
 - SRC CLI.....133
 - community mode configuration
 - SRC CLI.....131
 - configuration example.....139
 - configuration statements.....129
 - data recovery.....142
 - high availability.....36
 - loading sample data.....135
 - neighbors.....125, 126
 - overview.....15, 125
 - redundancy.....126
 - roles
 - changing secondary to primary, SRC
 - CLI.....134
 - overview.....125, 126
 - standalone mode
 - SRC CLI.....130
 - verifying configuration
 - SRC CLI.....137
 - JUNOS routing platforms
 - scalability.....6
 - JUNOSe routers
 - scalability with SRC software.....6
- L**
 - LDAP (Lightweight Directory Access Protocol). *See*
 - directory; directory server
 - LDAP directory. *See* directory
 - leases for licenses. *See* license server
 - license
 - obtaining.....88
 - pilot license
 - description.....87
 - installing, C-series Controller.....93
 - installing, Solaris platform.....93
 - server license
 - description.....87
 - installing, C-series Controllers.....94
 - location.....91
 - overview.....89
 - types.....87
 - license manager
 - configuration statements.....95
 - configuring
 - SRC CLI.....95
 - license server
 - errors.....89
 - lease renewal.....91
 - license allocation.....90
 - license release.....90
 - license requests.....90
 - license switching.....91
 - SAE failover.....92
 - Lightweight Directory Access Protocol. *See* LDAP
 - load balancing
 - NIC.....37
 - local password authentication.....195
 - local properties
 - basic properties, configuring.....230
 - configuration
 - SRC CLI.....229, 230, 231, 232
 - verifying.....234
 - configuration statements.....229
 - directory connection properties, configuring.....232
 - directory location of SRC data, configuring.....231
 - logging.....118
 - See also* system log server
 - login announcements, system.....186
 - login classes
 - configuration.....177
 - configuration examples.....180
 - configuration prerequisites
 - SRC CLI.....177
 - configuration statements.....177
 - configuration verification.....179
 - default classes.....174
 - idle timeout values.....176
 - options.....170
 - overview
 - SRC CLI.....169
 - predefined.....174

privilege level options		
SRC CLI.....	170	
privilege levels		
commands.....	174	
configuration statements.....	174	
M		
maintenance permission.....	171	
manuals		
comments on.....	xxv	
messages		
broadcast messages, NTP.....	113	
multicast messages, NTP.....	114	
severity levels for logging.....	118	
MII monitor		
configuring		
SRC CLI.....	77	
Monitoring Agent		
application.....	27	
multicast		
NTP messages.....	114	
N		
NAS ID, configuring for SAE		
SRC CLI.....	148	
network		
permission.....	172	
network information collector. <i>See</i> NIC		
NIC (network information collector)		
description.....	14	
load balancing.....	37	
overview.....	14	
resolution processes.....	15	
notice icons.....	xxi	
NTP (Network Time Protocol)		
authentication		
configuration.....	112	
configuration statements	111	
authentication keys.....	112	
boot server.....	108	
client mode.....	109	
configuration.....	104	
configuration statements.....	107	
listening		
broadcast messages.....	113	
multicast messages.....	114	
modes.....	103, 104	
overview.....	103	
symmetric active mode.....	109	
O		
on-demand services.....	3, 6	
open interfaces.....	7	
operator login class.....	174	
operators, regular expression.....	175	
OSS integration.....	5	
P		
passwords		
RADIUS		
SRC CLI.....	190	
shared user.....	195	
shared user accounts.....	196	
user accounts.....	183	
permissions		
SRC CLI.....	170	
pilot license. <i>See</i> license		
policies		
management.....	6	
Policies, Services, and Subscribers CLI. <i>See</i> SRC CLI		
Policies, Services, and Subscribers tasks <i>See</i> C-Web		
interface		
policy management.....	18	
ports		
RADIUS server.....	190	
SRC-related components.....	81	
predefined login classes.....	174	
Prepaid Account Administration application.....	27	
prepaid services demonstration application.....	27	
primary directory.....	227	
privilege levels.....	174	
SRC CLI.....	170	
product features.....	5, 7	
R		
RAD-Series RADIUS Server.....	22	
RADIUS		
.....	22	
<i>See also</i> RAD-Series RADIUS Server		
address for SAE		
SRC CLI.....	148	
description.....	22	
OSS integration.....	5	
server compliant RFCs.....	22	
subscriber management.....	6	
<i>See also</i> RAD-Series RADIUS Server		
RADIUS authentication. <i>See</i> authentication		
RADIUS authorization. <i>See</i> authentication		
read-only login class.....	174	
redundancy		
directory.....	227	
references		
draft RFCs.....	248	
non-RFC software standards.....	249	
RFCs.....	247	
URLs, third-party.....	249	

regular expressions	
operators.....	175
usage guidelines.....	175
request license import master-license file-name	
command.....	94
reset permission.....	172
residential portal	
description.....	28
PDAs.....	29
resolving host names	
SRC CLI.....	123
retrieving directory changes.....	227
RFCs.....	247, 248
root account.....	186
routing permission.....	172
routing-control permission.....	172

S

SAE (service activation engine)	
configuring groups	
SRC CLI.....	146
description.....	7, 13
initial properties, overview	
SRC CLI.....	145
starting	
SRC CLI.....	149
stopping	
SRC CLI.....	149
verifying status.....	150
SAE (service activation engine), configuring initial	
properties	
SRC CLI.....	147
SAE (service activation engine), configuring NAS ID	
SRC CLI.....	148
SAE (service activation engine), configuring RADIUS	
address	
SRC CLI.....	148
sample data	
loading	
SRC CLI.....	135
overview.....	15
secondary directory.....	227
secret permission.....	172
secret-control permission.....	172
security	
digital certificates.....	197
clearing certificates.....	198, 202
clearing requests.....	201
prerequisites.....	197
requesting certificates.....	198
requesting certificates through SCEP.....	200
viewing certificates.....	198
security permission.....	172
security-control permission.....	172
serial port, C-series Controller.....	69
server license. <i>See</i> license	
service activation engine. <i>See</i> SAE	
service permission.....	172
service-control permission.....	173
services	
on demand.....	6
shared user accounts.....	196
shell permission.....	173
SNMP agent	
access control, configuring on C-series Controllers	
community strings.....	216, 217
named views.....	218
SNMP groups.....	219
VACM.....	217
configuration statements.....	206, 212
configuring	
C-series Controllers.....	207, 213
SRC CLI.....	207, 213
description.....	18
directory connection parameters, configuring	
SRC CLI.....	209
Java Runtime Environment, configuring	
SRC CLI.....	211
local properties, configuring	
SRC CLI.....	207
logging, configuring	
SRC CLI.....	211
monitoring	
SRC CLI.....	223
named views, defining	
C-series Controllers.....	218
notification targets, configuring	
C-series Controllers.....	222
SRC CLI.....	222
starting	
SRC CLI.....	223
stopping	
SRC CLI.....	223
system information, configuring	
SRC CLI.....	213
trap history, configuring	
SRC CLI.....	207
SNMP Agent	
master agent SNMP versions.....	212
snmp control permission.....	173
snmp permission.....	173
SNMP traps	
notification targets, configuring	
C-series Controllers.....	222
snmp-named-views-cli.....	218
snmp-security-names-cli.....	221
snmp-statements.....	206
software standards	
draft RFCs.....	248
non-RFC standards.....	249
RFCs.....	247

SRC CLI.....	186
directory connections	
configuration statements.....	45
configuring.....	46
verifying configuration.....	48
overview.....	45
Policies, Services, and Subscribers CLI	
password.....	49
starting.....	49
starting	
C-series platform.....	48
SRC components	
description.....	9
diagram.....	4
high availability.....	36
SRC software	
configuration prerequisites.....	39
configuring	
C-series Controllers.....	40, 41
description.....	3
features and benefits.....	5, 7
financial advantages.....	6
installing component	
C-series Controller.....	155
OSS integration.....	5
removing component	
C-series Controller.....	155
services	
description.....	3
snapshot on C-series Controller.....	152, 155
upgrading	
C-series Controller.....	152, 153, 154
SRC-ACP (SRC Admission Control Plug-In)	
overview.....	23
SRC-SG (SRC SOAP Gateway)	
description.....	18
SSH (secure shell)	
connection to remote host.....	203
standards	
draft RFCs.....	248
non-RFC software standards.....	249
RFCs.....	247
static host mapping	
configuring	
SRC CLI.....	123
overview.....	123
static routes, configuring.....	78
Steel-Belted RADIUS.....	165
Steel-Belted Radius/SPE server.....	22
subscriber	
management, description.....	6
subscriber permission.....	173
subscriber-control permission.....	173
super-user login class.....	174
support, technical <i>See</i> technical support	
symmetric active mode, NTP.....	109

system authentication. <i>See</i> authentication	
system log server	
configuration prerequisites.....	118
configuration statements.....	118
message groups.....	117
message severity levels.....	118
messages	
file locations.....	119
messages, file	
SRC CLI.....	119
messages, server	
SRC CLI.....	119
messages, user notification	
SRC CLI.....	120
overview.....	117
system login.....	186
system permission.....	173
system-control permission.....	173

T

TACACS+ authentication. <i>See</i> authentication	
tariff models.....	6
technical support	
contacting JTAC.....	xxv
Telnet connection to remote host.....	203
template authentication accounts.....	194
text conventions defined.....	xxi
third-party URLs.....	249
traffic mirroring	
administration.....	30
application.....	30
tunnel interfaces, configuring.....	72

U

UIDs.....	182
unauthorized login class.....	174
unresponsive directories.....	228
usage data.....	7
user accounts.....	169
authentication	
configuring passwords.....	184
configuring SSH authentication.....	184
root password.....	186
authentication method and password.....	183
configuration.....	181
configuration verification.....	182, 183
configuring.....	180
example.....	185
overview.....	61, 169, 183
SRC CLI.....	180
shared.....	196
<i>See also</i> login classes	
user identifiers. <i>See</i> UIDs	

user notification messages	
SRC CLI.....	120

V

view permission.....	173
view-configuration permission.....	174
virtual IP addresses, configuring.....	78

W

Web application server	
application deployment.....	163
installing Web applications inside.....	163
overview.....	157
removing Web applications from.....	163
restarting.....	164
starting.....	164
stopping.....	164
viewing statistics	
C-Web interface.....	164
SRC CLI.....	164

