



SRC-PE Software

C-Web Interface Configuration Guide

Release 3.0.x

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, California 94089
USA

408-745-2000

www.juniper.net

Part Number: 530-026639-01, 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 C-Web Configuration Guide

Release 3.0.x

Copyright © 2008, Juniper Networks, Inc.

All rights reserved. Printed in USA.

Writing: Donna O'Leary-Abkowitz, Linda Creed, Diane Florio, Justine Kangas, Sarah Lesway-Ball,

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 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 NON-INFRINGEMENT. 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

xxvii

Part 1	Configuring C-series Controllers	
Chapter 1	Configuring Remote Access to a C-series Controller (C-Web Interface)	3
Chapter 2	Configuring NTP on C-series Controllers with the C-Web Interface	11
Chapter 3	Configuring System Logging for a C-series Controller with the C-Web Interface	15
Part 2	Configuring User Access to the SRC Software	
Chapter 4	Configuring User Access with the C-Web Interface	21
Chapter 5	Authenticating Users on a C-series Controller with the C-Web Interface	25
Part 3	Managing Systems That Run the SRC Software	
Chapter 6	Configuring Static Host Mapping with the C-Web Interface	31
Chapter 7	Managing the Juniper Networks Database with the C-Web Interface	33
Chapter 8	Creating Custom SNMP Monitors (C-Web Interface)	41
Part 4	Configuring Network Components	
Chapter 9	Setting Up an SAE with the C-Web Interface	47
Chapter 10	Configuring the SAE with the C-Web Interface	51
Chapter 11	Classifying Interfaces and Subscribers (C-Web Interface)	59
Chapter 12	Configuring the SAE for a PCMM Environment (C-Web Interface)	81
Chapter 13	Configuring and Starting the SNMP Agent (C-Web Interface)	85
Chapter 14	Configuring NIC (C-Web Interface)	95
Chapter 15	Obtaining Interface Configuration for OnePopStaticRouteIp or OnePopVrflp (C-Web Interface)	103
Chapter 16	Using the C-Web Interface to Configure SRC Applications to Communicate with an SAE	107
Chapter 17	Configuring Admission Control (C-Web Interface)	111
Part 5	Integrating Network Devices	
Chapter 18	Configuring the JPS (C-Web Interface)	127
Chapter 19	Using JUNOSe Routers in the SRC Network (C-Web Interface)	137
Chapter 20	Using JUNOS Routing Platforms in the SRC Network (C-Web Interface)	149

Chapter 21	Adding Objects for CMTS Devices (C-Web Interface)	163
Chapter 22	Integrating Third-Party Network Devices into the SRC Network (C-Web Interface)	165

Part 6

Configuring Policies and Services

Chapter 23	Configuring and Managing Policies (C-Web Interface)	177
Chapter 24	Configuring Local and Global Parameters (C-Web Interface)	203
Chapter 25	Configuring Services (C-Web Interface)	205
Chapter 26	Scheduling Services (C-Web Interface)	215
Chapter 27	Managing Tiered and Premium Services with QoS on JUNOSe Routers (C-Web Interface)	231

Part 7

Configuring Subscribers and Subscriptions

Chapter 28	Configuring Subscriber-Related Properties on the SAE (C-Web Interface)	241
Chapter 29	Configuring Internal, External, and Synchronization Plug-Ins (C-Web Interface)	245
Chapter 30	Configuring Accounting and Authentication Plug-Ins (C-Web Interface)	249
Chapter 31	Configuring Subscribers and Subscriptions (C-Web Interface)	265
Chapter 32	Configuring External Subscriber Events with the C-Web Interface	273
Chapter 33	Configuring Traffic Redirection (C-Web Interface)	279

Part 8

Index

Index	289
-------	-----

Table of Contents

	About This Guide	xxvii
	SRC Guides and Release Notes	xxvii
	Audience	xxvii
	Documentation Conventions	xxvii
	Related Juniper Networks Documentation	xxix
	Obtaining Documentation	xxxi
	Documentation Feedback	xxxi
	Requesting Technical Support	xxxi
Part 1	Configuring C-series Controllers	
Chapter 1	Configuring Remote Access to a C-series Controller (C-Web Interface)	3
	Configuring External Interfaces on a C-series Controller	3
	Configuring Loopback Interfaces for IPv4 (C-Web Interface)	4
	Configuring Loopback Interfaces for IPv6 (C-Web Interface)	4
	Configuring Gigabit Ethernet Interfaces for IPv4 (C-Web Interface)	5
	Configuring Gigabit Ethernet Interfaces for IPv6 (C-Web Interface)	6
	Configuring Group Interfaces (C-Web Interface)	7
	Configuring Tunnel Interfaces (C-Web Interface)	7
	Configuring a Static Route to Devices on Other Networks (C-Web Interface)	8
	Securing Connections Between a C-series Controller and Remote Hosts	8
	Configuring a C-series Controller to Accept SSH Connections (C-Web Interface)	9
	Configuring a C-series Controller to Accept Telnet Connections (C-Web Interface)	9
	Configuring a C-series Controller to Accept NETCONF Connections (C-Web Interface)	10
Chapter 2	Configuring NTP on C-series Controllers with the C-Web Interface	11
	Specifying a Basic NTP Configuration on a C-series Controller (C-Web Interface)	11
	Configuring NTP Client Mode for a C-series Controller (C-Web Interface)	12
	Configuring an NTP Peer for a C-series Controller (C-Web Interface)	12

Configuring NTP Broadcast Mode on a C-series Controller (C-Web Interface)	13
Configuring NTP as a Multicast Client on a C-series Controller (C-Web Interface)	13
Specifying an Authentication Key for NTP on C-series Controllers (C-Web Interface)	13
Configuring NTP Authentication (C-Web Interface)	14

Chapter 3

Configuring System Logging for a C-series Controller with the C-Web Interface **15**

Overview of the C-series Controller Log Server	15
Message Groups	15
Severity Levels	16
Before You Configure System Logging (SRC CLI)	16
Saving System Log Messages to a File (C-Web Interface)	16
Sending System Log Messages to Other Servers (C-Web Interface)	17
Sending Notifications for System Log Messages to Users (C-Web Interface)	17

Part 2

Configuring User Access to the SRC Software

Chapter 4

Configuring User Access with the C-Web Interface **21**

Overview of SRC User Accounts	21
Configuring Login Classes (C-Web Interface)	21
Configuring User Accounts (C-Web Interface)	22
Configuring Authentication for SRC User Accounts (C-Web Interface)	22
Configuring a Plain Text Password	22
Configuring SSH Authentication	22
Configuring a System Login Announcement (C-Web Interface)	23

Chapter 5

Authenticating Users on a C-series Controller with the C-Web Interface **25**

Configuring RADIUS and TACACS + Authentication on a C-series Controller (C-Web Interface)	25
Configuring RADIUS Authentication (C-Web Interface)	26
Configuring TACACS + Authentication (C-Web Interface)	26
Configuring Authentication Order	26
Removing an Authentication Method from the Authentication Order	26
Using Remote Template Accounts	27
Configuring a Local User Template	27

Part 3	Managing Systems That Run the SRC Software	
Chapter 6	Configuring Static Host Mapping with the C-Web Interface	31
	Overview of Static Host Mapping	31
	Configuring Static Host Mapping with the C-Web Interface	31
Chapter 7	Managing the Juniper Networks Database with the C-Web Interface	33
	Enabling the Juniper Networks Database to Run in Standalone Mode with the C-Web Interface	33
	Configuring the Juniper Networks Database to Run in Community Mode with the C-Web Interface	34
	Securing the Juniper Networks Database with the C-Web Interface	34
	Adding a Juniper Networks Database to an Established Community with the C-Web Interface	35
	Promoting a Secondary Database to a Primary Role in a Configuration with One Primary Database with the C-Web Interface	36
	Updating Data on a Juniper Networks Database with the C-Web Interface	37
	Synchronizing Data on a Juniper Networks Database with the C-Web Interface	37
	Loading Sample Data in to a Juniper Networks Database with the C-Web Interface	37
	Securing Communications Between the Juniper Networks Database and SRC Components with the C-Web Interface	38
	Recovering Data in a Community with One Primary Database and One Secondary Database with the C-Web Interface	39
Chapter 8	Creating Custom SNMP Monitors (C-Web Interface)	41
	SNMP Monitoring on C-series Controllers	41
	Configuring SNMP Custom Monitors (C-Web Interface)	42
Part 4	Configuring Network Components	
Chapter 9	Setting Up an SAE with the C-Web Interface	47
	Initially Configuring the SAE with the C-Web Interface	47
	Creating Grouped Configurations for the SAE (SRC CLI)	48
	Configuring an SAE Group with the C-Web Interface	48
	Configuring an SAE Group	49
	Deleting Default Configurations Within an SAE Group	49
	Configuring Local Properties for the SAE with the C-Web Interface	49

Configuring the RADIUS Local IP Address and NAS ID with the C-Web Interface	50
Configuring the Directory Location for SAE Data with the C-Web Interface	50
Starting the SAE with the C-Web Interface	50
Stopping the SAE with the C-Web Interface	50

Chapter 10

Configuring the SAE with the C-Web Interface **51**

SRC Data Storage	51
Configuring LDAP Access to Directory Data with the C-Web Interface	51
Configuring Access Through LDAPS to Service and Subscriber Data	52
Configuring Access to Subscriber Data	52
Configuring Access to Service Data	53
Configuring Access to Policy Data	53
Configuring Access to the Persistent Login Cache	53
Configuring the Location of Network Device Data	53
Configuring the SAE to Manage Third-Party Devices	54
Configuring SAE Properties for Global Default SNMP Communities for Use with JUNOSe Routers and JUNOS Routing Platforms	54
Enabling Automatic Discovery of Changes in SAE Configuration Data	54
Setting the Timeout and Number of Events for SAE Directory Eventing	54
Storing Subscriber and Service Session Data	55
Session Store Files	55
Active and Passive Session Stores	55
Standby SAEs	55
Session Store File Rotation	56
Configuring the Session Store Feature on the C-Web Interface	56
Configuring Session Store Parameters for a Device Driver	56
Configuring Global Session Store Parameters (C-Web Interface)	57
Reducing the Size of Objects for the Session Store Feature	57
Configuring the Number of Threads for Sessions on the C-Web Interface	57

Chapter 11

Classifying Interfaces and Subscribers (C-Web Interface) **59**

Overview of Classification Scripts	59
How Classification Scripts Work	60
Interface Classification Scripts	60
Subscriber Classification Scripts	61
DHCP Classification Scripts	61
Overview of Configuring Classification Scripts	61
Subscriber Classifiers	61
DHCP Classifiers	62
Interface Classifiers	62

Classification Targets	62
Target Expressions	63
Classification Conditions	63
Glob Matching	63
Regular Expression Matching	64
Classifying Interfaces (C-Web Interface)	65
Interface Classification Conditions	65
Classifying Subscribers (C-Web Interface)	67
Subscriber Classification Conditions	68
Sending DHCP Options to the JUNOS Router	71
Subscriber Classification Targets	72
Classifying DHCP Subscribers (C-Web Interface)	73
Syntax for DHCP Classification Targets	74
Selecting DHCP Parameters	74
DHCP Options Supported on the SAE	75
Creating DHCP Profiles (C-Web Interface)	78

Chapter 12

Configuring the SAE for a PCMM Environment (C-Web Interface) 81

Configuring the SAE for a Cable Network Environment (C-Web Interface)	81
Configuring the SAE to Manage PCMM Devices (C-Web Interface)	82
Setting Up SAE Communities (C-Web Interface)	82
Configuring the SAE Community Manager	83
Configuring SAE Properties for the Event Notification API (C-Web Interface)	83
Configuring PCMM Record-Keeping Server Plug-Ins (C-Web Interface)	83
Configuring CMTS-Specific RKS Plug-Ins (C-Web Interface)	84
Configuring Record-Keeping Server Peers for Plug-Ins (C-Web Interface)	84

Chapter 13

Configuring and Starting the SNMP Agent (C-Web Interface) 85

Configuring the SDX SNMP Agent	86
Configuring General Properties for the SDX SNMP Agent	86
Configuring Initial Properties for the SDX SNMP Agent	86
Configuring Directory Connection Properties for the SDX SNMP Agent	87
Configuring Directory Monitoring Properties for the SDX SNMP Agent	87
Configuring Logging Destinations for the SDX SNMP Agent	87
Configuring JRE Properties	87
Configuring the SNMP Agent	88
Configuring System Information for the SNMP Agent	88
Configuring Access Control for SNMPv3 Users	88
Configuring Authentication	89
Configuring Encryption	89
Configuring Access Control for Communities	89
Configuring Access Control for the VACM	89
Associating Security Names with a Community	90
Defining Named Views	90
Defining Access Privileges for an SNMP Group	91
Assigning Security Names to Groups	91
Configuring Notification Targets	91

	Configuring Performance Traps	92
	Configuring Event Traps	92
	Starting the SDX SNMP Agent	92
	Stopping the SDX SNMP Agent	93
	Monitoring the SDX SNMP Agent	93
Chapter 14	Configuring NIC (C-Web Interface)	95
	Before You Configure the NIC	95
	Configuring the NIC (C-Web Interface)	96
	Starting the NIC (C-Web Interface)	96
	Reviewing and Changing Operating Properties for NIC (C-Web Interface)	97
	Configuring NIC Replication (C-Web Interface)	97
	Configuring a NIC Scenario (C-Web Interface)	98
	Defining the NIC Configuration (C-Web Interface)	98
	Configuring the SAE to Communicate with SAE Plug-In Agents for NIC Replication (C-Web Interface)	99
	Testing a NIC Resolution (C-Web Interface)	100
	Stopping a NIC Host on a C-series Controller (C-Web Interface)	101
	Restarting the NIC (C-Web Interface)	101
	Changing NIC Configurations (C-Web Interface)	101
Chapter 15	Obtaining Interface Configuration for OnePopStaticRoutelp or OnePopVrflp (C-Web Interface)	103
	Overview of the Network Publisher	103
	Before You Configure and Run the Network Publisher	104
	Configuring the Network Publisher (C-Web Interface)	104
	Configuring Information to Test the Network Publisher (C-Web Interface)	106
	Reviewing the Information Collected from a JUNOS Routing Platform (C-Web Interface)	106
Chapter 16	Using the C-Web Interface to Configure SRC Applications to Communicate with an SAE	107
	Before You Configure a NIC Proxy	107
	Configuring a NIC Proxy with the C-Web Interface	108
	Configuring NIC Test Data (C-Web Interface)	109
	Examples: Key Values for NIC Bindings	110
Chapter 17	Configuring Admission Control (C-Web Interface)	111
	Configuring SRC-ACP	111
	Configuring Local Properties for SRC-ACP	112
	Configuring Basic Local Properties for SRC-ACP	112
	Configuring Initial Properties for SRC-ACP	112

Configuring Directory Connection Properties for SRC-ACP	112
Configuring Initial Directory Eventing Properties for SRC-ACP	112
Configuring the SAE for SRC-ACP (C-Web Interface)	113
Configuring SRC-ACP as an External Plug-In	113
Configuring Event Publishers for SRC-ACP	113
Configuring the SAE to Monitor Interfaces for Congestion Points	113
Configuring SRC-ACP Properties	114
Configuring Logging Destinations for SRC-ACP	114
Configuring SRC-ACP Operation	115
Configuring CORBA Interfaces	117
Configuring SRC-ACP Redundancy	118
Configuring Connections to the Subscribers' Directory	118
Configuring Connections to the Services' Directory	118
Configuring SRC-ACP Scripts and Classification	118
Configuring SRC-ACP to Manage the Edge Network	118
Configuring Network Interfaces in the Directory	119
Configuring Bandwidths for Subscribers (Edge Network)	119
Assigning Network Interfaces to Subscribers	120
Configuring Bandwidths for Services	120
Configuring SRC-ACP to Manage the Backbone Network	121
Configuring Action Congestion Points	121
Configuring Congestion Points for Services	121
Configuring Congestion Points in the Directory	122
Assigning Interfaces to Congestion Points	122
Configuring Congestion Point Classification (C-Web Interface)	122
Configuring Targets and Criteria for Classification Scripts	123
Configuring Classification Script Contents for Classification Scripts	123
Defining a Congestion Point Profile	123

Part 5

Integrating Network Devices

Chapter 18

Configuring the JPS (C-Web Interface) 127

Configuring the JPS (C-Web Interface)	127
Modifying the JPS Configuration (C-Web Interface)	128
Configuring General Properties for the JPS (C-Web Interface)	128
Specifying a Policy Server Identifier in Messages (C-Web Interface)	128
Configuring Logging Destinations (C-Web Interface)	128
Specifying Connections to the Application Managers (C-Web Interface)	129
Specifying Connections to RKSs (C-Web Interface)	129
Configuring RKS Pairs (C-Web Interface)	129
Configuring Connections for RKS Pairs (C-Web Interface)	129
Configuring RKS Pairs for Associated Application Managers (C-Web Interface)	130
Specifying Connections to CMTS Devices (C-Web Interface)	130
Modifying the Subscriber Configuration (C-Web Interface)	130
Configuring Subscriber IP Pools as IP Address Ranges (C-Web Interface)	131

Configuring Subscriber IP Pools as IP Subnets (C-Web Interface)	131
Configuring the SAE to Interact with the JPS (C-Web Interface)	131
Specifying Application Managers for the Policy Server (C-Web Interface)	132
Specifying Application Manager Identifiers for Policy Servers (C-Web Interface)	132
Adding Objects for Policy Servers to the Directory (C-Web Interface)	133
Configuring Initialization Scripts (C-Web Interface)	133
Enabling State Synchronization (C-Web Interface)	134
Using the NIC Resolver in PCMM Environments	134
Managing the JPS (C-Web Interface)	135
Starting the JPS (C-Web Interface)	135
Restarting the JPS (C-Web Interface)	135
Stopping the JPS (C-Web Interface)	136
Displaying JPS Status (C-Web Interface)	136

Chapter 19

Using JUNOSe Routers in the SRC Network (C-Web Interface) 137

COPS Connection Between JUNOSe Routers and the SAE	137
Highly Available Connections to JUNOSe Routers	138
Adding JUNOSe Routers and Virtual Routers (C-Web Interface)	138
Detecting Operative JUNOSe Routers and Virtual Routers and Adding Them to the Network	138
Adding JUNOSe Routers Individually	138
Adding Virtual Routers Individually	139
Configuring the SAE to Manage JUNOSe Routers (C-Web Interface)	139
Using SNMP to Retrieve Information from JUNOSe Routers	140
How SNMP Obtains Information From Routers for the SRC Software	140
Configuring the SNMP Server on the JUNOSe Router	140
Configuring Global SNMP Communities in the SRC Software (C-Web Interface)	141
Specifying JUNOSe Router Initialization Scripts on the SAE (C-Web Interface)	141
Developing Router Initialization Scripts for JUNOSe Routers, JUNOS Routing Platforms, and Network Devices	159
Interface Object Fields	142
Required Methods	160
Example: Router Initialization Script	161
Accessing the Router CLI	144
Starting the SRC Client on a JUNOSe Router	144
Stopping the SRC Client on a JUNOSe Router	145
Monitoring Interactions Between the SAE and the JUNOSe Router	145
Troubleshooting Problems with Managing JUNOSe Routers	146
Viewing the State of JUNOSe Device Drivers (C-Web Interface)	147
Viewing Statistics for Specific JUNOSe Device Drivers (C-Web Interface)	147
Viewing Statistics for All JUNOSe Device Drivers (C-Web Interface)	147

Chapter 20	Using JUNOS Routing Platforms in the SRC Network (C-Web Interface)	149
	BEEP Connection Between JUNOS Routing Platforms and the SAE	150
	Adding JUNOS Routing Platforms and Virtual Routers (C-Web Interface)	150
	Overview of Adding JUNOS Routing Platforms and Virtual Routers	150
	Adding Operative JUNOS Routing Platforms	150
	Adding JUNOS Routers Individually	151
	Adding Virtual Routers Individually	151
	Configuring the SAE to Manage JUNOS Routing Platforms (C-Web Interface)	151
	Configuring Secure Connections Between the SAE and JUNOS Routing Platforms	152
	Manually Obtaining Digital Certificates	152
	Obtaining Digital Certificates through SCEP	154
	Adding the Server Certificate on the Routing Platform	155
	Creating a Client Certificate for the Router	156
	Adding the Client Certificate on the Router	156
	Configuring the SAE to Use TLS	157
	Configuring TLS on the SAE	157
	SAE Verification of JUNOS Configuration Changes	157
	Setting Up the SAE to Periodically Check JUNOS Configuration (C-Web Interface)	158
	Using SNMP to Retrieve Information from JUNOS Routing Platforms and Other Network Devices	158
	Developing Router Initialization Scripts for JUNOSe Routers, JUNOS Routing Platforms, and Network Devices	159
	Interface Object Fields	159
	Required Methods	160
	Example: Router Initialization Script	161
	Specifying JUNOS Router Initialization Scripts on the SAE (C-Web Interface)	161
	Troubleshooting Problems with the SRC Software Process (C-Web Interface)	161
Chapter 21	Adding Objects for CMTS Devices (C-Web Interface)	163
	Adding Objects for CMTS Devices (C-Web Interface)	163
	Creating Virtual Routers for the CMTS Device (C-Web Interface)	163
Chapter 22	Integrating Third-Party Network Devices into the SRC Network (C-Web Interface)	165
	Overview of Integrating Network Devices into the SRC Network	165
	SAE Communities	165
	Storing Session Data	166
	Using Script Services to Provision Third-Party Devices	166
	Logging In Subscribers and Creating Sessions	167
	Assigned IP Subscribers	167
	Login Interactions with Assigned IP Subscribers	168

Event Notification from an IP Address Manager	169
Login with Event Notification	169
Configuration Tasks for Integrating Third-Party Network Devices (C-Web Interface)	170
Setting Up Script Services	171
Adding Objects for Network Devices (C-Web Interface)	171
Adding a Router Object	171
Adding Virtual Router Objects	172
Setting Up SAE Communities (C-Web Interface)	172
Configuring the SAE Community Manager	172
Specifying the Community Manager in the SAE Device Driver	172
Configuring SAE Properties for the Event Notification API (C-Web Interface)	173
Specifying Initialization Scripts on the SAE	173
Using the NIC Resolver in Environments That Have Third-Party Devices (C-Web Interface)	173

Part 6

Configuring Policies and Services

Chapter 23

Configuring and Managing Policies (C-Web Interface) 177

Before You Configure SRC Policies	178
Creating a Worksheet	178
Naming Objects	178
Using the apply-groups Statement	178
Using Expressions	178
Policy Values	179
SAE to JUNOS Routing Platforms	179
SAE to JUNOSe Routers	179
Enabling the Policy Configuration on the C-Web Interface	179
Configuring Policy Folders (C-Web Interface)	180
Configuring Policy Groups (C-Web Interface)	180
Configuring Policy Lists (C-Web Interface)	180
Configuring Policy Rules (C-Web Interface)	181
Policy Management Overview	181
Adding a Policy Rule	182
Configuring Classify-Traffic Conditions (C-Web Interface)	182
Configuring Template Activation (C-Web Interface)	184
Enabling Expansion of JUNOSe Classify-Traffic Conditions (C-Web Interface)	184
Specifying the PCMM Classifier Type (C-Web Interface)	184
Specifying Port Access for Traffic Classification (C-Web Interface)	185
Creating a Classify-Traffic Condition (C-Web Interface)	186
Configuring Source Networks (C-Web Interface)	186
Configuring Source Grouped Networks (C-Web Interface)	186
Configuring Destination Networks (C-Web Interface)	186
Configuring Destination Grouped Networks (C-Web Interface)	187
Configuring Protocol Conditions (C-Web Interface)	187

Configuring Protocol Conditions with Ports (C-Web Interface)	187
Configuring Protocol Conditions with Parameters (C-Web Interface)	188
Configuring TCP Conditions (C-Web Interface)	188
Configuring ICMP Conditions (C-Web Interface)	189
Configuring IGMP Conditions (C-Web Interface)	189
Configuring IPsec Conditions (C-Web Interface)	189
Configuring ToS Byte Conditions (C-Web Interface)	189
Configuring JUNOS Filter Conditions (C-Web Interface)	189
Configuring Application Protocol Conditions (C-Web Interface)	190
Configuring QoS Conditions with the C-Web Interface with the C-Web Interface	191
Configuring Actions (C-Web Interface)	191
Configuring DOCSIS Actions (C-Web Interface)	192
Configuring Filter Actions (C-Web Interface)	192
Configuring FlowSpec Actions (C-Web Interface)	192
Configuring Forward Actions (C-Web Interface)	193
Configuring Forwarding Class Actions (C-Web Interface)	193
Configuring Gate Spec Actions (C-Web Interface)	193
Configuring Loss Priority Actions (C-Web Interface)	194
Configuring Mark Actions (C-Web Interface)	194
Configuring NAT Actions (C-Web Interface)	194
Configuring Next-Hop Actions (C-Web Interface)	195
Configuring Next-Interface Actions (C-Web Interface)	195
Configuring Next-Rule Actions (C-Web Interface)	196
Configuring Policer Actions (C-Web Interface)	196
Configuring QoS Profile Attachment Actions (C-Web Interface)	197
Configuring Rate-Limit Actions (C-Web Interface)	197
Configuring Reject Actions (C-Web Interface)	198
Configuring Routing Instance Actions (C-Web Interface)	198
Configuring Scheduler Actions (C-Web Interface)	199
Configuring Drop Profiles (C-Web Interface)	199
Configuring Service Class Name Actions (C-Web Interface)	199
Configuring Stateful Firewall Actions (C-Web Interface)	200
Configuring Traffic-Class Actions (C-Web Interface)	200
Configuring Traffic-Mirror Actions (C-Web Interface)	200
Configuring Traffic-Shape Actions (C-Web Interface)	201

Chapter 24**Configuring Local and Global Parameters (C-Web Interface) 203**

Viewing Predefined Global Parameters (C-Web Interface)	203
Configuring Global Parameters (C-Web Interface)	203
Configuring Local Parameters (C-Web Interface)	203
Viewing Runtime Parameters (C-Web Interface)	204

Chapter 25**Configuring Services (C-Web Interface) 205**

Before You Configure SRC Services	205
Enabling the Service Configuration on the C-Web Interface	205
Adding a Normal Service (C-Web Interface)	206
Setting Parameter Values for Services (C-Web Interface)	206

Configuring Service Fragments for an Aggregate Service (C-Web Interface)	206
Configuring Timers for Aggregate Services (C-Web Interface)	207
Adding an Infrastructure Service (C-Web Interface)	207
Configuring Script Services (C-Web Interface)	207
Adding a Mutex Group (C-Web Interface)	208
Configuring Service Scopes (C-Web Interface)	208
Adding Service Scopes (C-Web Interface)	208
Assigning Services and Mutex Groups to Service Scopes (C-Web Interface)	209
Assigning Service Scopes to VRs or Subscribers (C-Web Interface)	209
Example: Configuring a Limited Set of Services for Organizations (C-Web Interface)	209
Example: Customizing Generic Services to Particular Regions (C-Web Interface)	211

Chapter 26

Scheduling Services (C-Web Interface) 215

Setting the Action Threshold and Preparation Time with the C-Web Interface	215
Authorizing Scheduled Services (C-Web Interface)	216
Defining an Authorization Plug-In for a Scheduled Service in the Global Configuration (C-Web Interface)	216
Defining an Authorization Plug-In for a Scheduled Service in the Service Scope (C-Web Interface)	216
Adding a Service Schedule (C-Web Interface)	216
Adding a Service Schedule for Scopes (C-Web Interface)	217
Adding a Service Schedule for Services (C-Web Interface)	217
Adding a Service Schedule for Retailers (C-Web Interface)	218
Adding a Service Schedule for Enterprises (C-Web Interface)	219
Adding a Service Schedule for Subscribers in an Enterprise (C-Web Interface)	220
Setting the Time Schedule (C-Web Interface)	220
Setting the Action (C-Web Interface)	221
Defining Attributes for Service Activation (C-Web Interface)	222
Example: Configuring Different Service Tiers for Different Days (C-Web Interface)	222
Example: Configuring a Service to Be Active During Nonwork Hours (C-Web Interface)	225
Example: Configuring a Service to Be Available for a Specified Interval (C-Web Interface)	228

Chapter 27

Managing Tiered and Premium Services with QoS on JUNOSe Routers (C-Web Interface) 231

Overview of QoS on JUNOSe Routers	231
Dynamically Managing QoS Profiles	231
How QoS Profile Tracking Works	232
Identifying QoS Services	232
Determining the QoS Profile	233

Setting Up Policy Groups	234
Policy Group for QoS Profile Attachment Service	234
Setting Up Services	235
Reestablishing Default QoS Profile	235
Example: How QTP Activates a QoS Service	235
Configuring QoS Profile-Tracking Plug-Ins (C-Web Interface)	236
Configuring Search Filters for QoS Profile-Tracking Plug-Ins	237

Part 7

Configuring Subscribers and Subscriptions

Chapter 28

Configuring Subscriber-Related Properties on the SAE (C-Web Interface) **241**

Configuring the Length of Time That MAC Addresses Remain in SAE Cache (C-Web Interface)	241
Identifying a Profile for Unauthenticated Subscribers (C-Web Interface)	242
Configuring Interim Accounting for Services and Subscribers (C-Web Interface)	242
Avoiding Overcharges for Sessions That Time Out (C-Web Interface)	243
Allowing Multiple Logins from the Same IP Address (C-Web Interface)	243
Authenticating Registered Username/Password Pairs (C-Web Interface)	244
Configuring Timers for Session Reactivation (C-Web Interface)	244

Chapter 29

Configuring Internal, External, and Synchronization Plug-Ins (C-Web Interface) **245**

Creating Plug-In Instances (C-Web Interface)	245
Creating a Plug-In Instance for All SAE Configurations	245
Creating a Plug-In Instance for an SAE Group	246
Configuring Internal Plug-Ins (C-Web Interface)	246
Configuring the SAE for External Plug-Ins (C-Web Interface)	247
Configuring the State Synchronization Plug-In Interface (C-Web Interface)	247

Chapter 30

Configuring Accounting and Authentication Plug-Ins (C-Web Interface) **249**

Creating RADIUS Peers	249
Types of Tracking Plug-Ins	250
Configuring Flat File Accounting Plug-Ins	251
Configuring Headers for Flat File Accounting Plug-Ins	252
Configuring Basic RADIUS Accounting Plug-Ins	253
Configuring Flexible RADIUS Accounting Plug-Ins	253
Configuring Custom RADIUS Accounting-Plug-Ins	254
Types of Authentication Plug-Ins	254
Limiting Subscribers on Router Interfaces	255
Configuring Basic RADIUS Authentication Plug-Ins	256

Configuring Flexible RADIUS Authentication Plug-Ins	256
Configuring Custom RADIUS Authentication Plug-Ins	257
Configuring LDAP Authentication Plug-Ins	257
Configuring UDP Ports for RADIUS Plug-Ins (C-Web Interface)	258
Configuring Global UDP Ports	258
Overview of Flexible RADIUS Plug-Ins	258
Using Default RADIUS Templates	259
Naming RADIUS Attribute Instances	259
Defining RADIUS Attributes	260
Standard RADIUS Attributes	260
Juniper Networks VSAs	260
Configuring a RADIUS Packet Template	261
Using Flexible RADIUS Packet Definitions	262
Setting Values in Authentication Response Packets	263
Selecting IP Address Pools Using DHCP Response Packets	264
Configuring Event Publishers (C-Web Interface)	264
Configuring Global and Default Retailer Event Publishers	264

Chapter 31 Configuring Subscribers and Subscriptions (C-Web Interface) 265

Enabling the Subscriber and Subscription Configuration on the C-Web Interface	265
Adding Subscribers (C-Web Interface)	266
Adding Retailers (C-Web Interface)	266
Configuring Administrative Information for Retailers (C-Web Interface)	267
Adding Subscriber Folders (C-Web Interface)	267
Adding Residential Subscribers (C-Web Interface)	268
Configuring Administrative Information for Residential Subscribers (C-Web Interface)	268
Adding Enterprises (C-Web Interface)	268
Configuring Administrative Information for Enterprise Subscribers (C-Web Interface)	269
Adding Sites (C-Web Interface)	269
Adding Devices as Subscribers (C-Web Interface)	269
Adding Managers (C-Web Interface)	270
Configuring Subscriptions (C-Web Interface)	270
Allowing Multiple Subscriptions to the Same Service per Subscriber	271
Configuring Accesses (C-Web Interface)	271

Chapter 32 Configuring External Subscriber Events with the C-Web Interface 273

Overview of External Subscriber Monitor	273
Configuring External Subscriber Monitor	274
Configuring Basic Local Properties for External Subscriber Monitor	274
Configuring Initial Properties for External Subscriber Monitor	274
Configuring Directory Connection Properties for External Subscriber Monitor	274

Configuring Eventing Properties for External Subscriber Monitor	275
Configuring Logging Destinations for External Subscriber Monitor	275
Configuring the NIC Proxy for the Pseudo-RADIUS Server (C-Web Interface)	275
Configuring Resolution Information for a NIC Proxy	276
Changing the Configuration for the NIC Proxy Cache	276
Configuring a NIC Proxy for NIC Replication	276
Configuring the Pseudo-RADIUS Server for External Subscriber Monitor	277
Configuring the Client Secret for the External Subscriber Monitor	277
Configuring Event Notification for the External Subscriber Monitor	277
Starting External Subscriber Monitor with the C-Web Interface	277
Stopping External Subscriber Monitor with the C-Web Interface	278

Chapter 33

Configuring Traffic Redirection (C-Web Interface) 279

Configuring the Redirect Server (C-Web Interface)	279
Configuring General Properties for the Redirect Server (C-Web Interface)	280
Configuring a Connection Between the Redirect Server and the Directory with the C-Web Interface	281
Defining Traffic to Transmit to the Redirect Server (C-Web Interface)	281
Changing the Number of Requests That the Redirect Server Accepts (C-Web Interface)	282
Specifying Extensions for Files That the Redirect Server Accepts (C-Web Interface)	282
Configuring the DNS Server for the Redirect Server (C-Web Interface)	282
Configuring the Redirect Server to Support HTTP Proxies (C-Web Interface)	283
Configuring a Redundant Redirect Server (C-Web Interface)	284
Configuring Logging for the Redirect Server	284
Changing the Configuration for the Redirect Server	284
Assessing Load for Redirect Server (C-Web Interface)	284

Part 8

Index

Index	289
-------------	-----

List of Figures

Figure 1: SAE Community166

Figure 2: Login Interactions with Assigned IP Subscribers168

Figure 3: Login Interactions with Event Notification Application169

List of Tables

Table 1: Notice Icons	xxviii
Table 2: Text Conventions	xxviii
Table 3: Juniper Networks C-series and SRC Technical Publications	xxix
Table 4: Applications to Remotely Access the C-series Controller	8
Table 5: DHCP Options in UserClassificationContext Field	71
Table 6: DHCP Options Supported on the SAE	75
Table 7: Router Initialization Scripts	159
Table 8: Exported Fields	160
Table 9: Router Initialization Scripts	159
Table 10: Exported Fields	160
Table 11: Examples of Concatenated QoS Profile Input Values	233
Table 12: Settings for Filter Strings	237
Table 13: Tracking Plug-Ins	250
Table 14: Authentication Plug-Ins	255
Table 15: RADIUS Attribute Instance Names	259

About This Guide

- SRC Guides and Release Notes on page xxvii
- Audience on page xxvii
- Documentation Conventions on page xxvii
- Related Juniper Networks Documentation on page xxix
- Obtaining Documentation on page xxxi
- Documentation Feedback on page xxxi
- Requesting Technical Support on page xxxi

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 JUNOS 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 xxviii defines the notice icons used in this guide. Table 2 on page xxviii 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 xxix.

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

Configuring C-series Controllers

- Configuring Remote Access to a C-series Controller (C-Web Interface) on page 3
- Configuring NTP on C-series Controllers with the C-Web Interface on page 11
- Configuring System Logging for a C-series Controller with the C-Web Interface on page 15

Chapter 1

Configuring Remote Access to a C-series Controller (C-Web Interface)

- Configuring External Interfaces on a C-series Controller on page 3
- Configuring Loopback Interfaces for IPv4 (C-Web Interface) on page 4
- Configuring Loopback Interfaces for IPv6 (C-Web Interface) on page 4
- Configuring Gigabit Ethernet Interfaces for IPv4 (C-Web Interface) on page 5
- Configuring Gigabit Ethernet Interfaces for IPv6 (C-Web Interface) on page 6
- Configuring Group Interfaces (C-Web Interface) on page 7
- Configuring Tunnel Interfaces (C-Web Interface) on page 7
- Configuring a Static Route to Devices on Other Networks (C-Web Interface) on page 8
- Securing Connections Between a C-series Controller and Remote Hosts on page 8
- Configuring a C-series Controller to Accept SSH Connections (C-Web Interface) on page 9
- Configuring a C-series Controller to Accept Telnet Connections (C-Web Interface) on page 9
- Configuring a C-series Controller to Accept NETCONF Connections (C-Web Interface) on page 10

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 Loopback Interfaces for IPv4 (C-Web Interface)

Loopback interfaces are for private use only by software running on the C-series Controller, to communicate with other software also running on the same C-series Controller.

To configure a loopback interface for IPv4:

1. Click **Configure**, expand **Interfaces**, and then click **Interface: lo**.

The Interface:lo pane appears.

2. To specify the unit:
 - a. From the Create new list, select **Unit**.
 - b. In the dialog box, type a number for the new unit, and click **OK**.

The Unit: *< number >* appears in the side pane.

3. To specify an IPv4 address for the interface, expand **Unit: < number >**, and then expand **Family** in the side pane.
 - a. Click **Inet**.

The Inet pane appears.

- b. Click the **Create** button.
 - c. Enter information as described in the Help text in the main pane, and click **Apply**.

- Related Topics**
- Configuring Gigabit Ethernet Interfaces for IPv4 (C-Web Interface)
 - Configuring Gigabit Ethernet Interfaces for IPv6 (C-Web Interface)
 - Configuring Tunnel Interfaces (C-Web Interface)

Configuring Loopback Interfaces for IPv6 (C-Web Interface)

Loopback interfaces are for private use only by software running on the C-series Controller, to communicate with other software also running on the same C-series Controller.

To configure a loopback interface for IPv6:

1. Click **Configure**, and expand **Interfaces > Interface: lo > Unit > Family**.
2. Click **Inet6**.

The Inet6 pane appears.

3. From the Create new list, select **Address**.
4. In the dialog box, type a name for the new address, and click **OK**.

- Related Topics**
- Configuring Loopback Interfaces for IPv4 (C-Web Interface)
 - Configuring Gigabit Ethernet Interfaces for IPv4 (C-Web Interface)
 - Configuring Gigabit Ethernet Interfaces for IPv6 (C-Web Interface)
 - Configuring Tunnel Interfaces (C-Web Interface)

Configuring Gigabit Ethernet Interfaces for IPv4 (C-Web Interface)

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

To configure a Gigabit Ethernet interface for IPv4:

1. Click **Configure > Interfaces**.

The Interfaces pane appears.

2. From the Create new list, create an interface.
 - To create a new interface, select **Interface**, type a name for the new interface in the dialog box, and click **OK**.
 - To create an eth1, eth2, or eth3 interface, select **eth1**, **eth2**, or **eth3**, and click **OK**.
3. To specify the unit:
 - a. From the Create new list, select **Unit**.
 - b. In the dialog box, type a number for the new unit, and click **OK**.
4. To specify an IPv4 address for the new unit, expand **Unit: < number >**, and expand **Family** in the side pane.
 - a. In the side pane, click **Inet**.

The Interfaces pane appears.

- b. Click the **Create** button.
- c. Enter information as described in the Help text in the main pane, and click **Apply**.

- Related Topics**
- Configuring Loopback Interfaces for IPv4 (C-Web Interface)
 - Configuring Gigabit Ethernet Interfaces for IPv4 (C-Web Interface)
 - Configuring Gigabit Ethernet Interfaces for IPv6 (C-Web Interface)
 - Configuring Tunnel Interfaces (C-Web Interface)

Configuring Gigabit Ethernet Interfaces for IPv6 (C-Web Interface)

To allow remote access to the C-series Controller, you configure the Gigabit Ethernet interfaces. You can specify an IP address with mask for an interface.

To configure a Gigabit Ethernet interface for IPv6:

1. Click **Configure > Interfaces**.

The Interfaces pane appears.

2. Create an interface from the Create new list.
 - To create a new interface, select **Interface**. In the dialog box, type a name for the new interface, and click **OK**.
 - To create an eth1, eth2, or eth3 interface, select **eth1**, **eth2**, or **eth3**, and click **OK**.
3. To specify the unit:
 - a. From the Create new list, select **Unit**.
 - b. In the dialog box, type a number for the new unit, and click **OK**.
4. To specify an IPv6 address for the new unit, expand **Unit: < number >**, and expand **Family** in the side pane.
 - a. In the side pane, click **Inet6**.

The Interfaces pane appears.

- b. From the Create new list, select **Address**.
- c. In the dialog box, type a name for the new address, and click **OK**.

- Related Topics**
- Configuring Loopback Interfaces for IPv4 (C-Web Interface)
 - Configuring Loopback Interfaces for IPv6 (C-Web Interface)
 - Configuring Gigabit Ethernet Interfaces for IPv4 (C-Web Interface)
 - Configuring Tunnel Interfaces (C-Web Interface)

Configuring Group Interfaces (C-Web Interface)

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.

To configure an Ethernet group interface:

1. Click **Configure > Interfaces**.
2. In the dialog box, type the name of the new interface, and click **OK**.

The Interfaces pane appears.

3. Expand the interface, and click **Group**.
4. Click **Create**, enter information in the Group pane as described in the Help text in the main pane, and click **Apply**.
5. In the side pane, under the group click **ARP Monitoring**.

The ARP Monitoring pane appears.

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

- Related Topics**
- Configuring External Interfaces on a C-series Controller
 - Configuring Ethernet Redundancy (SRC CLI)

Configuring Tunnel Interfaces (C-Web Interface)

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

The C-series Controller supports three types of tunnel interfaces:

- GRE—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.
- IPv6 in IPv4—Encapsulates IPv6 packet in IPv4 packets.

The other endpoint for the tunnel on a JUNOS or JUNOSe router must be configured for the tunnel to be operational.

To configure tunnel interfaces:

1. Click **Configure**, expand **Interfaces**, and expand the specified interface.
2. Click **Tunnel**.

The Tunnel pane appears.

3. Click the **Create** button.
4. Enter information as described in the Help text in the main pane, and click **Apply**.

- Related Topics**
- Configuring Loopback Interfaces for IPv4 (C-Web Interface)
 - Configuring a Static Route to Devices on Other Networks (C-Web Interface)
 - Configuring Gigabit Ethernet Interfaces for IPv4 (C-Web Interface)
 - Configuring Gigabit Ethernet Interfaces for IPv6 (C-Web Interface)

Configuring a Static Route to Devices on Other Networks (C-Web Interface)

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 the IP address for a static route, include a mask.

To configure a static route to another network:

1. Click **Configure**, expand **Routing Options**, and click **Static**.

The Static pane appears.

2. From the Create new list, select **Route**.
3. In the dialog box, type a destination network/mask (using the form address/prefix length) for the new Route, and click **OK**.

The Route: <name> pane appears.

4. Enter information as described in the Help text in the main pane, and click **Apply**.

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 4 on page 8 lists the applications through which remote users can access a C-series Controller.

Table 4: 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)

Table 4: Applications to Remotely Access the C-series Controller *(continued)*

Application	Information About Access Configuration
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 (C-Web Interface)

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 C-Web interface as root.

1. Click **Configure**, expand **System > Services**, and then click **SSH**.

The SSH pane appears.

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

Configuring a C-series Controller to Accept Telnet Connections (C-Web Interface)

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.

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

1. Click **Configure**, expand **System**, and then click **Services**.

The Services pane appears.

2. Select the Telnet checkbox to accept Telnet connections. (Leave the checkbox empty to disable Telnet connections.) Refer to the information in the Help text in the main pane.

3. Click **Apply**.

Configuring a C-series Controller to Accept NETCONF Connections (C-Web Interface)

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

1. Click **Configure**, expand **System > Services**, and then click **NETCONF**.

The NETCONF pane appears.

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

Chapter 2

Configuring NTP on C-series Controllers with the C-Web Interface

- Specifying a Basic NTP Configuration on a C-series Controller (C-Web Interface) on page 11
- Configuring NTP Client Mode for a C-series Controller (C-Web Interface) on page 12
- Configuring an NTP Peer for a C-series Controller (C-Web Interface) on page 12
- Configuring NTP Broadcast Mode on a C-series Controller (C-Web Interface) on page 13
- Configuring NTP as a Multicast Client on a C-series Controller (C-Web Interface) on page 13
- Specifying an Authentication Key for NTP on C-series Controllers (C-Web Interface) on page 13
- Configuring NTP Authentication (C-Web Interface) on page 14

Specifying a Basic NTP Configuration on a C-series Controller (C-Web Interface)

We recommend that you configure NTP on C-series Controllers.

To configure NTP to operate on a C-series controller:

1. Click **Configure**, expand **System**, and then click **NTP**.

The NTP pane appears.

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



NOTE: If you do not configure a boot server, NTP cannot synchronize with a time server if the server's time is very far off the local system's time.

Related Topics ■ Configuring NTP on a C-series Controller

Configuring NTP Client Mode for a C-series Controller (C-Web Interface)

To configure an NTP server that the C-Series Controller uses for time synchronization:

1. Click **Configure**, expand **System**, and then click **NTP**.

The NTP pane appears.

2. In the Create new list, select **Server**. Type an IPV4 or IPV6 address for the server, and click **OK**.

The Server pane appears.

3. Enter information as described in the Help text in the main pane, and click **Apply**.



NOTE: If the remote system has authentication enabled, specify an authentication key and value. The system transmits the specified authentication key when transmitting packets.

Related Topics ■ NTP Support on C-series Controllers
■ Configuring NTP on a C-series Controller

Configuring an NTP Peer for a C-series Controller (C-Web Interface)

To configure NTP to operate as a peer:

1. Click **Configure**, expand **System**, and then click **NTP**.

The NTP pane appears.

2. In the Create new list, select **Peer**. Type an IPV4 or IPV6 address for the server and click **OK**.

3. Enter information as described in the Help text in the main pane, and click **Apply**.



NOTE: If the remote system has authentication enabled, specify an authentication key and value. The system transmits the specified authentication key when transmitting packets.

Related Topics ■ NTP Support on C-series Controllers
■ Configuring NTP on a C-series Controller

Configuring NTP Broadcast Mode on a C-series Controller (C-Web Interface)

To configure NTP to operate in broadcast mode:

1. Click **Configure**, expand **System**, and click **NTP**.

The NTP pane appears.

2. In the Create new list, select **Broadcast**. Type an IP address or a hostname on one of the local networks or a multicast address assigned to NTP. Click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.



NOTE: If the remote system has authentication enabled, specify an authentication key and value. The system transmits the specified authentication key when transmitting packets.

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

Configuring NTP as a Multicast Client on a C-series Controller (C-Web Interface)

To configure NTP to operate in multicast mode on a C-series controller:

1. Click **Configure**, expand **System > NTP**, and then click **Multicast Client**.

The Multicast Client pane appears.

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

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

Specifying an Authentication Key for NTP on C-series Controllers (C-Web Interface)

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.

To configure an NTP authentication key that is shared among systems that run NTP:

1. Click **Configure**, expand **System**, and then click **NTP**.

The NTP pane appears.

2. In the Create new list, select **Authentication Key**. Type the key number for the key. The key number must match on all systems using that particular key for authentication. Click **OK**.

- Related Topics**
- NTP Support on C-series Controllers
 - Configuring NTP on a C-series Controller
 - Configuring NTP Authentication (C-Web Interface)

Configuring NTP Authentication (C-Web Interface)

You can specify authentication keys for the various modes you configure for NTP.

To configure the authentication key for a mode:

- In the main pane, specify a key value for a mode.
 - Client mode—See Specifying a Basic NTP Configuration on a C-series Controller (C-Web Interface)
 - Server mode—See Configuring NTP Client Mode for a C-series Controller (C-Web Interface)
 - Broadcast mode—See Configuring NTP Broadcast Mode on a C-series Controller (C-Web Interface)
 - Symmetric active (peer) mode—See Configuring an NTP Peer for a C-series Controller (C-Web Interface)

- Related Topics**
- NTP Support on C-series Controllers
 - Configuring NTP on a C-series Controller
 - Specifying an Authentication Key for NTP on C-series Controllers (C-Web Interface)

Chapter 3

Configuring System Logging for a C-series Controller with the C-Web Interface

- Overview of the C-series Controller Log Server on page 15
- Before You Configure System Logging (SRC CLI) on page 16
- Saving System Log Messages to a File (C-Web Interface) on page 16
- Sending System Log Messages to Other Servers (C-Web Interface) on page 17
- Sending Notifications for System Log Messages to Users (C-Web Interface) on page 17

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*.

Saving System Log Messages to a File (C-Web Interface)

To save system log messages to a file:

1. Click **Configure**, expand **System**, and click **Syslog**.

The Syslog pane appears.

2. From the Create new list, select **File**.
3. Type a name for the file in the dialog box, and click **OK**.

The File pane appears.

4. To configure a message group, select the message group that you want to configure from the Create new list.

You can configure multiple message groups in the log file.

5. To configure a severity level:
 - a. In the side pane, click the log file.
 - b. From the Severity box, select the severity level that you want to track with the log file, and click **Apply**.

Sending System Log Messages to Other Servers (C-Web Interface)

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. Click **Configure**, expand **System**, and click **Syslog**.

The Syslog pane appears.

2. From the Create new list, select **Host**.
3. Type a name for the file in the dialog box, and click **OK**.

The Host pane appears.

4. To configure a message group, select the message group that you want to configure from the Create new list.

You can configure multiple message groups in the log file.

5. To configure a severity level:
 - a. In the side pane, click the log file.
 - b. From the Severity box, select the severity level that you want to track with the log file, and click **Apply**.

Sending Notifications for System Log Messages to Users (C-Web Interface)

To configure the system log server to send notifications to users:

1. Click **Configure**, expand **System**, and click **Syslog**.

The Syslog pane appears.

2. From the Create new list, select **User**.
3. Type a name for the file in the dialog box, and click **OK**.

The User pane appears.

4. To configure a message group, select the message group that you want to configure from the Create new list.

You can configure multiple message groups in the log file.

5. To configure a severity level:
 - a. In the side pane, click the log file.
 - b. From the Severity box, select the severity level that you want to track with the log file, and click **Apply**.

Part 2

Configuring User Access to the SRC Software

- Configuring User Access with the C-Web Interface on page 21
- Authenticating Users on a C-series Controller with the C-Web Interface on page 25

Chapter 4

Configuring User Access with the C-Web Interface

- Overview of SRC User Accounts on page 21
- Configuring Login Classes (C-Web Interface) on page 21
- Configuring User Accounts (C-Web Interface) on page 22
- Configuring Authentication for SRC User Accounts (C-Web Interface) on page 22
- Configuring a System Login Announcement (C-Web Interface) on page 23

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.

Configuring Login Classes (C-Web Interface)

To configure a login class:

1. Click **Configure**, expand **System**, and then click **Login**.

The Login pane appears.

2. From the Create New list, select **Class**.
3. Type a name for the login class in the dialog box, and click **OK**.

The Class pane appears.

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

Configuring User Accounts (C-Web Interface)

To configure a user account:

1. Click **Configure**, expand **System**, and then click **Login**.

The Login pane appears.

2. From the Create New list, select **User**.
3. Type a name for the user in the dialog box, and click **OK**.

The User pane appears.

4. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Authentication for SRC User Accounts (C-Web Interface)

You can configure user accounts by using the following methods:

1. Configuring a Plain Text Password on page 22
2. Configuring SSH Authentication on page 22

Configuring a Plain Text Password

To configure a plain text password for a user account:

1. Click **Configure**, expand **System**, and then click **Login**.

The Login pane appears.

2. From the side pane, expand a user account, and click **Authentication**.
3. Click **Create**, enter information as described in the Help text in the main pane, and then click **Apply**.

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. Click **Configure**, expand **System**, and then click **Login**.

The Login pane appears.

2. From the side pane, expand a user account, and click **Authentication**.
3. Click **Create**, enter information as described in the Help text in the main pane, and then click **Apply**.

Configuring a System Login Announcement (C-Web Interface)

A system login announcement appears after the user logs in. By default, no login announcement is displayed.

To configure a system login announcement:

1. Click **Configure**, expand **System**, and then click **Login**.

The Login pane appears.

2. In the Announcement box, type the system announcement.
3. Click **Apply**.

Chapter 5

Authenticating Users on a C-series Controller with the C-Web Interface

- Configuring RADIUS and TACACS + Authentication on a C-series Controller (C-Web Interface) on page 25
- Configuring RADIUS Authentication (C-Web Interface) on page 26
- Configuring TACACS + Authentication (C-Web Interface) on page 26
- Configuring Authentication Order on page 26
- Removing an Authentication Method from the Authentication Order on page 26
- Using Remote Template Accounts on page 27
- Configuring a Local User Template on page 27

Configuring RADIUS and TACACS+ Authentication on a C-series Controller (C-Web Interface)

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 (C-Web Interface).

See Configuring TACACS + Authentication (C-Web Interface).

2. Configure the authentication order.
3. Configure template accounts.

See Using Remote Template Accounts and Configuring a Local User Template.

4. (Optional) Configure individual user profiles.

See Overview of SRC User Accounts.

Configuring RADIUS Authentication (C-Web Interface)

To configure information about RADIUS servers for authentication:

1. Click **Configure > System**.

The System pane appears.

2. From the Create new list, select **RADIUS Server**.
3. Type an IPv4 address or IPv6 address in the dialog box, and click **OK**.

The RADIUS Server pane appears.

4. Enter information as described in the Help text in the main pane, and click **Apply**.

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.

Configuring Authentication Order

To configure the order in which to use authentication servers:

1. Click **Configure > System**.

The System pane appears.

2. In the Authentication Order lists, click the arrow buttons to arrange the authentication servers in the order that you want.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

If you do not configure the authentication order, users are verified based on their configured passwords.

Removing an Authentication Method from the Authentication Order

To delete an authentication method from the authentication order:

- In the System pane, select the authentication method from the Selected Values list, and click the arrow button to move the authentication method to the Suggested Values list.

Using Remote Template Accounts

To configure the remote template account and specify the privileges that you want to grant to remote users:

1. Click **Configure**, expand **System**, and then click **Login**.

The Login pane appears.

2. From the Create new list, select **User**.
3. Type **remote** in the dialog box, and click **OK**.

The User pane appears.

4. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring a Local 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:

1. Click **Configure**, expand **System**, then click **Login**.

The Login pane appears.

2. From the Create new list, select **User**.
3. Type a name for the user in the dialog box, and click **OK**.

The User pane appears.

4. Enter information in the Class, UID, and Full Name boxes as described in the Help text, and click **Apply**.

Part 3

Managing Systems That Run the SRC Software

- Configuring Static Host Mapping with the C-Web Interface on page 31
- Managing the Juniper Networks Database with the C-Web Interface on page 33
- Creating Custom SNMP Monitors (C-Web Interface) on page 41

Chapter 6

Configuring Static Host Mapping with the C-Web Interface

- Overview of Static Host Mapping on page 31
- Configuring Static Host Mapping with the C-Web Interface on page 31

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 with the C-Web Interface

To configure static host mapping:

1. Click **Configure**, expand **System**, and then click **Static Host Mapping**.

The Static Host Mapping pane appears.

2. From the Create new list, select **Static Host Mapping**.
3. Type the actual name for the static host in the dialog box, and click **OK**.

The Static Host Mapping pane appears.

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

Create button is not there; emailing Hugh (SLB)

Chapter 7

Managing the Juniper Networks Database with the C-Web Interface

- Enabling the Juniper Networks Database to Run in Standalone Mode with the C-Web Interface on page 33
- Configuring the Juniper Networks Database to Run in Community Mode with the C-Web Interface on page 34
- Securing the Juniper Networks Database with the C-Web Interface on page 34
- Adding a Juniper Networks Database to an Established Community with the C-Web Interface on page 35
- Promoting a Secondary Database to a Primary Role in a Configuration with One Primary Database with the C-Web Interface on page 36
- Updating Data on a Juniper Networks Database with the C-Web Interface on page 37
- Synchronizing Data on a Juniper Networks Database with the C-Web Interface on page 37
- Loading Sample Data in to a Juniper Networks Database with the C-Web Interface on page 37
- Securing Communications Between the Juniper Networks Database and SRC Components with the C-Web Interface on page 38
- Recovering Data in a Community with One Primary Database and One Secondary Database with the C-Web Interface on page 39

Enabling the Juniper Networks Database to Run in Standalone Mode with the C-Web Interface

When you run a Juniper Networks database in standalone mode, the database does not communicate with other Juniper Networks databases.

To enable a Juniper Networks database to run in standalone mode:

1. Click **Configure**, expand **System > LDAP**, and then click **Server**.

The Server pane appears.

2. In the Server pane, select the **Standalone** check box, and then click **Apply**.

- Related Topics**
- Configuring the Juniper Networks Database to Run in Community Mode with the C-Web Interface
 - Securing the Juniper Networks Database with the C-Web Interface

Configuring the Juniper Networks Database to Run in Community Mode with the C-Web Interface

You configure a Juniper Networks database in community mode to setup redundancy with other Juniper Networks databases.

To configure the Juniper Networks database to run in community mode:

1. Click **Configure**, expand **System > LDAP**, and then click **Server**.

The Server pane appears.

2. In the Server pane, clear the **Standalone** check box, and click **Apply**.
3. In the side pane, click **Commit**.
4. Expand **Server**, and click **Community**.

The Community pane appears.

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

- Related Topics**
- Enabling the Juniper Networks Database to Run in Standalone Mode (SRC CLI)
 - Adding a Juniper Networks Database to an Established Community with the C-Web Interface
 - Enabling the Juniper Networks Database to Run in Standalone Mode with the C-Web Interface
 - Securing the Juniper Networks Database with the C-Web Interface

Securing the Juniper Networks Database with the C-Web Interface

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. this form of security is supported only on C-series Controllers.

To secure connections to the Juniper Networks database:

1. Click **Configure**, expand **System > LDAP > Server**, and then click **Security**.

The Security pane appears.

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

Related Topics ■ Securing Communications Between the Juniper Networks Database and SRC Components (SRC CLI)

Adding a Juniper Networks Database to an Established Community with the C-Web Interface

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.



CAUTION: 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, configure the new server C-new as a primary neighbors on each of the existing servers C1 and C2:

- a. Click **Configure**, expand System **LDAP > Server**, and then click **Community**.

The Community pane appears.

- b. In the Primary Neighbors box, add the new server C-new, click **Apply**.
- c. In the side pane, click **Commit**.
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:

- a. Click **Configure**, expand System **LDAP > Server**, and then click **Community**.

The Community pane appears.

- b. If the configuration is not visible, click **Create**.
- c. In the Role box, select **Primary**.
- d. In the Primary Neighbors box, add the C1 and C2 servers, and click **Apply**.
- e. In the side pane, click **Commit**.

- Related Topics** ■ Adding a Juniper Networks Database to an Established Community(SRC CLI)
- Configuring the Juniper Networks Database to Run in Community Mode with the C-Web Interface

Promoting a Secondary Database to a Primary Role in a Configuration with One Primary Database with the C-Web Interface

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.
 - a. Click **Configure**, expand System **LDAP > Server**, and then click **Community**.
The Community pane appears.
 - b. In the Primary Neighbors box, verify whether the other database is listed as a primary neighbor. If it is not, add it.
 - c. In the Role box, select **Primary**, and click **Apply**.
 - d. In the side pane, click **Commit**.
2. On the existing database that has a primary role, remove the neighbor as secondary and add it as primary.
 - a. Click **Configure**, expand System **LDAP > Server**, and then click **Community**.
The Community pane appears.
 - b. In the Secondary Neighbors box, remove the database listed.
 - c. In the Primary Neighbors box, add the other database in the community, and click **Apply**.
 - d. In the side pane, click **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.
 - a. Click **Configure**, expand System **LDAP > Server**, and then click **Community**.
The Community pane appears.
 - b. In the Primary Neighbors box, remove the database that is to become the secondary database.
 - c. In the Secondary Neighbors box, add the database, and click **Apply**.
 - d. In the side pane, click **Commit**.

- Related Topics** ■ Adding a Juniper Networks Database to an Established Community(SRC CLI)

- Configuring the Juniper Networks Database to Run in Community Mode with the C-Web Interface

Updating Data on a Juniper Networks Database with the C-Web Interface

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 in a community of Juniper Networks databases:

1. Click **Manage > Request > System > LDAP > Community > Force Update**.

The Force Update page appears.

2. In the Neighbor box, enter the name of the neighbor to be updated.

Related Topics ■ Updating Data on a Juniper Networks Database (SRC CLI)

Synchronizing Data on a Juniper Networks Database with the C-Web Interface

You can initialize a Juniper Networks database with data from a neighbor. This process also removes any existing data in the database.

To replace data with data from a neighbor (for example, neighbor1):

1. Click **Manage > Request > System > LDAP > Community > Initialize**.

The Initialize page appears.

2. In the Neighbor box, enter the name of the neighbor to be synchronized.

Related Topics ■ Updating Data on a Juniper Networks Database with the C-Web Interface
 ■ Recovering Data in a Community with One Primary Database and One Secondary Database (SRC CLI)

Loading Sample Data in to a Juniper Networks Database with the C-Web Interface

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 in the SRC Application Library)

- Instant Virtual Extremity (IVE) Host Checker integration application (unsupported sample application in the SRC Application Library)
- Traffic-Mirroring Application (unsupported sample application in the SRC Application Library)
- Sample residential portal (unsupported sample application in the SRC Application Library)
 - Equipment registration mode
 - Internet service provider (ISP) mode

Loading sample data is not required to run the SRC software.

To load sample data from the C-Web interface:

1. Click **Manage > Request > System > LDAP > Load**.

The Load page appears.

2. In the Data box, select the component for which to load sample data, and click **OK**.

Related Topics ■ Loading Sample Data in to a Juniper Networks Database (SRC CLI)

Securing Communications Between the Juniper Networks Database and SRC Components with the C-Web Interface

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.

- License server
- NIC
- SAE
- SRC CLI
- Configuration for SRC components other than the CLI and the NIC

To change the administrative password for the Juniper Networks database:

1. Click **Manage > Request > System > LDAP > Change Admin Password**.

The Change Admin Password page appears.

2. In the New Password box, enter the new password.

To change a component password:

1. Click **Manage > Request > System > LDAP > Change Component Password**.

The Change Component Password page appears.

2. Enter information as described in the Help text in the main pane, and click **Apply**.

Related Topics ■ Securing Communications Between the Juniper Networks Database and SRC Components with the C-Web Interface

Recovering Data in a Community with One Primary Database and One Secondary Database with the C-Web Interface

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.
 - a. Click **Configure**, expand **System > LDAP > Server**, and then click **Community**.
The Community pane appears.
 - b. In the Role box, select **Primary**, click **Apply**.
 - c. In the side pane, click **Commit**.
2. On the existing database that has a primary role, remove the neighbor as secondary and add it as primary.
 - a. Click **Configure**, and expand **System > LDAP > Server > Community**.
The Community pane appears.
 - b. In the Secondary Neighbors box, remove the database that is to become the primary database.
 - c. In the Primary Neighbors box, add the database, and click **Apply**.
 - d. In the side pane, click **Commit**.

Related Topics ■ Recovering Data in a Community with One Primary Database and One Secondary Database (SRC CLI)

Chapter 8

Creating Custom SNMP Monitors (C-Web Interface)

- SNMP Monitoring on C-series Controllers on page 41
- Configuring SNMP Custom Monitors (C-Web Interface) on page 42

SNMP Monitoring on C-series Controllers

You can create custom SNMP monitors to detect changes in MIB objects. Use custom monitors to generate an alarm and take action in response to an alarm.

To configure a monitor, you define a condition that when met generates an SNMP notification. You can define a monitor for any single MIB object (of type integer) supported on a C-series Controller. These MIBs include Juniper Networks enterprise-specific objects as well as standard MIB objects.

You can configure the following for custom monitors:

- Alarms—Define an alarm condition and an event to generate in response to the alarm.

An alarm identifies the object to be monitored, the frequency with which the monitor retrieves a sample value for the object, and a condition that triggers an event.

- Events—Define the type of action (SNMP set or notification) to be taken in response to an alarm condition. If you do not define an event for an alarm, SNMP sends the notifications based on the monitor type.

The SRC software supports the following types of alarm conditions for monitors:

- Boolean test—Compares a sample value with a specified value or range of values.
- Existence test—Monitors when an object appears, disappears, or changes value.
- Threshold test—Monitors when an object's value rises above or falls below specified values.

A monitor supports only one type of alarm condition, or test, at a time. Each alarm can use one of the following sampling methods:

- Absolute value—Uses the actual value of the object.

Existence tests support only absolute values.

- Delta value—Uses the difference between two sample values.

By using the delta value sampling method, you can configure SNMP to detect a discontinuity in values to prevent false alarms caused by the value of a MIB object being reset. At the end of a polling interval before the SNMP agent calculates a delta value, SNMP checks the value of a MIB object called a discontinuity marker. If the value of the discontinuity marker changes, SNMP does not perform the test for the associated condition until the next polling interval.

For alarms that do not have a configured event, SNMP sends the following notifications that are defined in RFC 2981—Event MIB (October 2000):

- Boolean or existence test—`mteTriggerFired`
- Threshold test (rising value)—`mteTriggerRising`
- Threshold test (falling value)—`mteTriggerfalling`

The default configuration for SNMP custom monitors assesses all objects in a MIB branch based on the object identifier specified for the monitor. For this type of monitor, you can configure SNMP notification MIB objects located in the same row as the object that generates the event, as well as for a single object. You can create sophisticated monitors by monitoring an entire branch, then creating notifications for multiple objects.

Related Topics

- Configuration Statements for Customized SRC SNMP Monitors
- Configuring an SNMP Alarm on a C-series Controller (SRC CLI)
- Example: SNMP Monitoring of Multiple MIB Objects
- Configuring an SNMPv3 Security Name for SNMP Monitoring (SRC CLI)
- Overview of SNMP Traps
- Information about SRC MIBs on the Juniper Web site at <http://www.juniper.net/techpubs/software/management/src>
- Also, see information about the `disman` event MIB in RFC 2981—Event MIB (October 2000)

Configuring SNMP Custom Monitors (C-Web Interface)

You can create custom SNMP monitors to detect changes in MIB objects.

To create custom SNMP monitors:

1. Click **Configure**, expand **SNMP**, and click **Monitor**.

The Monitor pane appears.

2. From the Create new list, select **Alarm**.
3. Type a name for the new alarm in the dialog box, and click **OK**.

The alarm name appears in the side pane and the SNMP pane.

4. Enter alarm properties as described in the Help text in the Main pane, and click **OK**.
5. Configure a test condition for the alarm.
 - a. In the side pane, under the alarm you are configuring select a test condition: **Boolean test**, **Existence Test**, or **Threshold Test**.
 - b. (Optional) If you configured a boolean or threshold test, and set the sample type as delta-value, you can select **Delta Discontinuity Check** to validate delta values.
 - c. Enter test properties as described in the Help text in the Main pane, and click **OK**.
6. In the side pane, select **Monitor** again.
The Monitor pane appears.
7. From the Create new list, select **Event**.
8. Type a name for the new event in the dialog box, and click **OK**.
9. In the side pane, under the event that you created, expand the event.
10. Click **Notification** and enter notification properties as described in the Help text in the Main pane, and click **OK**.

Or

Click **SNMP Set** and enter set properties as described in the Help text in the Main pane, and click **OK**.

11. (Optional) In the left pane, select **Monitor**; then in the Main pane enter an SNMP v3 security name.

- Related Topics**
- SNMP Monitoring on C-series Controllers
 - Example: SNMP Monitoring of Multiple MIB Objects

Part 4

Configuring Network Components

- Setting Up an SAE with the C-Web Interface on page 47
- Configuring the SAE with the C-Web Interface on page 51
- Classifying Interfaces and Subscribers (C-Web Interface) on page 59
- Configuring the SAE for a PCMM Environment (C-Web Interface) on page 81
- Configuring and Starting the SNMP Agent (C-Web Interface) on page 85
- Configuring NIC (C-Web Interface) on page 95
- Obtaining Interface Configuration for OnePopStaticRouteIp or OnePopVrflp (C-Web Interface) on page 103
- Using the C-Web Interface to Configure SRC Applications to Communicate with an SAE on page 107
- Configuring Admission Control (C-Web Interface) on page 111

Chapter 9

Setting Up an SAE with the C-Web Interface

- Initially Configuring the SAE with the C-Web Interface on page 47
- Creating Grouped Configurations for the SAE (SRC CLI) on page 48
- Configuring an SAE Group with the C-Web Interface on page 48
- Configuring an SAE Group on page 49
- Deleting Default Configurations Within an SAE Group on page 49
- Configuring Local Properties for the SAE with the C-Web Interface on page 49
- Configuring the RADIUS Local IP Address and NAS ID with the C-Web Interface on page 50
- Configuring the Directory Location for SAE Data with the C-Web Interface on page 50
- Starting the SAE with the C-Web Interface on page 50
- Stopping the SAE with the C-Web Interface on page 50

Initially Configuring the SAE with the C-Web Interface

To initially configure the SAE:

- (Optional) Create a configuration group for the SAE.

See Configuring an SAE Group with the C-Web Interface
- Configure local properties for the SAE.

See Configuring Local Properties for the SAE with the C-Web Interface
- 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 with the C-Web Interface
- Configure the location of the directory that contains SAE data.

See Configuring the Directory Location for SAE Data with the C-Web Interface

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 with the C-Web Interface

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.

Related Topics ■ Deleting Default Configurations Within an SAE Group

Configuring an SAE Group

To configure an SAE group:

1. Click **Configure**, expand **Slot**, expand the slot for which you want to configure the group, and then click **SAE**.

The SAE pane appears.

2. From the Shared list, select **/SAE/**.
3. Type a name for the new group in the box below the Shared list using the **/SAE/<path>** format, and click **Add**.
4. Click **Apply**.

The group appears in the side pane.

Related Topics ■ Deleting Default Configurations Within an SAE Group
 ■ Configuring an SAE Group with the C-Web Interface

Deleting Default Configurations Within an SAE Group

If you delete a default configuration, such as a driver configuration, from an SAE group, the configuration is deleted when you commit your configuration. However, if you start the SAE, the default configuration that you deleted is added back into your configuration.

If there are multiple SAE groups, and you delete a default configuration in more than one group, the software adds the default configurations back only to the group that the SAE is currently using.

Related Topics ■ Configuring an SAE Group with the C-Web Interface

Configuring Local Properties for the SAE with the C-Web Interface

To configure local properties for the SAE:

1. Click **Configure**, and expand **Slot**.
2. Expand the slot for which you want to configure the SAE, and then click **SAE**.

The Slot SAE pane appears.

3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring the RADIUS Local IP Address and NAS ID with the C-Web Interface

To set the local RADIUS address and network access server (NAS ID):

1. Click **Configure**, and expand **Slot**.
2. Expand the slot for which you want to configure SAE, expand **SAE**, and then click **Radius**.

The Slot SAE pane appears.

3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring the Directory Location for SAE Data with the C-Web Interface

You can configure the locations for dynamic and static configuration data in the directory.

To configure the directory location for configuration data:

1. Click **Configure**, and expand **Slot**.
2. Expand the slot for which you want to configure SAE, expand **SAE**, and then click **Initial**.

The Initial pane appears.

3. Enter information as described in the Help text in the main pane, and click **Apply**.

Starting the SAE with the C-Web Interface

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:

1. Click **Manage > Enable**.

The Enable pane appears.

2. From the Component list, select **SAE**, and click **OK**.

Stopping the SAE with the C-Web Interface

To stop the SAE:

1. Click **Manage > Disable**.

The Disable pane appears.

2. From the Component list, select **SAE**, and click **OK**.

Chapter 10

Configuring the SAE with the C-Web Interface

- SRC Data Storage on page 51
- Configuring LDAP Access to Directory Data with the C-Web Interface on page 51
- Storing Subscriber and Service Session Data on page 55
- Configuring the Session Store Feature on the C-Web Interface on page 56
- Configuring the Number of Threads for Sessions on the C-Web Interface on page 57

SRC Data Storage

The SRC software stores subscriber, service, persistent login, policy, router, and cached subscriber profiles and session data in a directory. The SAE uses LDAP to store and retrieve the data.

If you do not store data in the local directory, you need to configure the LDAP connections to the directories in which the data is stored. You can also select the filter that the SAE uses to search for subscriptions in the directory and directory eventing parameters for data stored in the directory.

- Related Topics**
- Configuring LDAP Access to Directory Data with the C-Web Interface

Configuring LDAP Access to Directory Data with the C-Web Interface

The tasks to configure LDAP access to directory data are:

- Enabling Automatic Discovery of Changes in SAE Configuration Data
 - Setting the Timeout and Number of Events for SAE Directory Eventing
1. Configuring Access Through LDAPS to Service and Subscriber Data on page 52
 2. Configuring Access to Subscriber Data on page 52
 3. Configuring Access to Service Data on page 53
 4. Configuring Access to Policy Data on page 53
 5. Configuring Access to the Persistent Login Cache on page 53
 6. Configuring the Location of Network Device Data on page 53

7. Configuring the SAE to Manage Third-Party Devices on page 54
8. Configuring SAE Properties for Global Default SNMP Communities for Use with JUNOS Routers and JUNOS Routing Platforms on page 54
9. Enabling Automatic Discovery of Changes in SAE Configuration Data on page 54
10. Setting the Timeout and Number of Events for SAE Directory Eventing on page 54

Configuring Access Through LDAPS to Service and Subscriber Data

You can secure connections between a router and an external directory that contains service data or subscriber data, and you can configure the router to use LDAPS when it connects to the same data source.

To use LDAPS to secure connections between a router and an external directory:

1. Do one of the following:
 - a. To configure service data, click **Configure**, expand **Shared > SAE > LDAP**, and then click **Service Data**.

The Service Data pane appears.

- b. To configure subscriber data, click **Configure**, expand **Shared > SAE > LDAP**, and then click **Subscriber Data**.

The Subscriber Data pane appears.

2. Click **Create**.
3. Select **ldaps** from the Secured Ldap Protocol list.
4. In the router initialization script you specify the directory context.

The `/opt/UMC/sae/lib/poolPublisher.py` script and the `/opt/UMC/sae/lib/IorPublisher.py` script provide examples of how to configure a directory context. For example, from the `/opt/UMC/sae/lib/IorPublisher.py` script:

```
dirContext = Ssp.registry.get('ServiceDataSource.component').getContext()
```

In addition, you can change the directory context.

For information about how to use InitialDirContext class or the DirContext class to specify directory context, see:

<http://java.sun.com/j2se/1.4.2/docs/api/javax/naming/directory/InitialDirContext.html>

<http://java.sun.com/j2se/1.4.2/docs/api/javax/naming/directory/DirContext.html>

Configuring Access to Subscriber Data

To configure SAE access to subscriber data:

1. Click **Configure**, expand **Shared > SAE > LDAP**, and then click **Subscriber Data**.

The Subscriber Data pane appears.

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

Configuring Access to Service Data

To configure SAE access to service data:

1. Click **Configure**, expand **Shared > SAE > LDAP**, and then click **Service Data**.

The Service Data pane appears.

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

Configuring Access to Policy Data

To configure SAE access to subscriber data:

1. Click **Configure**, expand **Shared > SAE > LDAP**, and then click **Policy Data**.

The Policy Data pane appears.

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

Configuring Access to the Persistent Login Cache

To configure SAE access to persistent login cache data:

1. Click **Configure**, expand **Shared > SAE > LDAP**, and then click **Persistent Log Cache**.

The Persistent Login Cache pane appears.

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

Configuring the Location of Network Device Data

To configure SAE access to network device data:

1. Click **Configure**, expand **Shared > SAE**, and then click **Network Device Data**.

The Network Device Data pane appears.

2. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring the SAE to Manage Third-Party Devices

To configure SAE drivers for third-party devices:

1. Click **Configure**, and expand **Driver**.
2. To configure the SAE to manage AAA NAS groups, under Driver expand **Aaa**, and then click **Create**. Enter information as described in the Help text in the main pane, and then click **Apply**.
3. To configure the SAE to manage PCMM devices, under Driver expand **PCMM**, and then click **Create**. Enter information as described in the Help text in the main pane, and then click **Apply**.
4. To configure device scripts, under Driver expand **Scripts**, and then click **Create**. Enter information as described in the Help text in the main pane, and then click **Apply**.

Configuring SAE Properties for Global Default SNMP Communities for Use with JUNOS Routers and JUNOS Routing Platforms

To configure SAE properties for global default SNMP communities:

1. Click **Configure**, and expand **Driver**.
2. Under Driver expand **SNMP**, and then click **Create**. Enter information as described in the Help text in the main pane, and then click **Apply**.

Enabling Automatic Discovery of Changes in SAE Configuration Data

To enable automatic discovery of changes in SAE configuration data:

1. Click **Configure**, expand **Shared > SAE**, and then click **LDAP**.

The LDAP pane appears.

2. Click **Create**, enable the Enable Directory Eventing box as described in the Help text in the main pane, and then click **Apply**.

Setting the Timeout and Number of Events for SAE Directory Eventing

To configure the directory eventing timeout and the number of simultaneous events that the SAE can receive from the directory:

1. Click **Configure**, expand **Shared > SAE > LDAP**, and then click **Directory Eventing**.

The Directory Eventing pane appears.

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

Storing Subscriber and Service Session Data

To aid in recovering from an SAE failover, the SAE stores subscriber and service session data in flat files on the SAE host. The SRC component that controls the storage of session data on the SAE is called the session store. The session store queues data and then writes the data to session store files on the SAE host's disk. After the data has been written to disk, it can survive a server reboot.

You can configure how the SAE stores session data for JUNOSe routers, JUNOS routing platforms, simulated routers, and *PacketCable Multimedia Specification* (PCMM) devices.

Session Store Files

Session store files are numbered flat files. Session store files are located in a directory on the SAE host. You can configure the size of session store files. After the maximum size has been reached, the session store creates a new file and begins writing data to the new file.

Store operations, such as adding a session to the store (put store operations) or removing a session from the store (remove store operations), are queued in a buffer before they are written to the session store file. You can configure parameters that determine when the session store writes a queue to a session store file.

Session store files are deleted if they have not been modified and if no session activity has taken place for one week. All the data files that contain the sessions associated with a particular virtual router are deleted at the same time.

Active and Passive Session Stores

You can have a community of SAEs and duplicate session store data on each SAE in the community in case of an SAE failover. SAE communities are made up of SAEs that you configure as connected SAEs for a virtual router object.

SAEs in a community are given the role of either active SAE or passive SAE. The active SAE keeps session data up to date within the community. Each active session store opens a Transmission Control Protocol (TCP) connection to its passive SAE. The TCP connection triggers the creation of a passive session store in that SAE. When the active session store writes operations to the session store file, it passes them to passive session stores on all SAEs in the community.

When you modify a community, wait for passive session stores on the new community members to be updated before you shut down the currently active SAE. Otherwise, if you add a new member to a community, and then a failover from the current active SAE to the new member is triggered immediately, the new member's session store may not have received all data from the active SAE's session store.

Standby SAEs

In a community of SAEs, one SAE can provide redundancy for the active SAE. The redundant (standby) SAE connects to the active SAE through a COPS-PR connection.

State as well as session data is replicated from the active SAE to the standby SAE to reduce the failover time from one SAE to another.

A standby SAE can respond to SAE failures and connection failures between an SAE and a JUNOS router. Connection failures between an active SAE and a standby SAE may not be immediately detected, because each SAE continues to function for a period of time. When a standby SAE does detect that state information is different on the two SAEs, it resynchronizes data between the two.



NOTE: We recommend that you use a highly reliable and available connection between an active SAE and a standby SAE to ensure availability of the two SAEs.

Session Store File Rotation

The session store periodically rotates the session store files. During rotation, the session store copies put store operations for live sessions from the oldest file to the end of the newest file. (Live sessions are sessions that have been created but not yet deleted.) It then deletes the oldest file. Sessions are rotated in batches, and you can configure the number of sessions that are rotated at the same time, and how much disk space is used by live sessions before files are rotated. No session store activity can take place while a batch of sessions is rotated.

Configuring the Session Store Feature on the C-Web Interface

Tasks to configure the session store feature are:

- Configuring Session Store Parameters for a Device Driver on page 56
- Configuring Global Session Store Parameters (C-Web Interface) on page 57
- Reducing the Size of Objects for the Session Store Feature on page 57

Configuring Session Store Parameters for a Device Driver

To configure session store parameters within a device driver configuration:

1. Click **Configure**, expand **Shared > SAE > Configuration**, and then click **Driver**.

The Driver pane appears.

2. In the side pane, expand the type of driver that you want to configure, and then click **Session Store**.

The Session Store pane appears.

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

Configuring Global Session Store Parameters (C-Web Interface)

This section describes how to configure global session store parameters that are shared by all session store instances (active or passive) on the SAE. You can also configure session store parameters within a device driver configuration. .

To configure global session store parameters:

1. Click **Configure**, expand **Shared > SAE > Configuration > Driver**, and then click **Session Store**.

The Session Store pane appears.

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

Reducing the Size of Objects for the Session Store Feature

You can use serialized data compression to reduce the size of sessions objects that the SAE sends across the network for the session store feature. Enabling this property reduces the size of objects, but increases the CPU load on the SAE.

To specify whether or not session objects are compressed:

1. Click **Configure**, expand **Shared > SAE**, and then click **Configuration**.

The SAE Configuration pane appears.

2. Click **Create**, enable the Compress Session Data box as described in the Help text in the main pane, and then click **Apply**.

Configuring the Number of Threads for Sessions on the C-Web Interface

To configure the number of threads used to handle session-related activity:

1. Click **Configure**, expand **Shared > SAE**, and then click **Session Job Manager**.

The Session Job Manager pane appears.

2. Click **Create**, enter the number of threads as described in the Help text in the main pane, and then click **Apply**.

Chapter 11

Classifying Interfaces and Subscribers (C-Web Interface)

- Overview of Classification Scripts on page 59
- Overview of Configuring Classification Scripts on page 61
- Classifying Interfaces (C-Web Interface) on page 65
- Interface Classification Conditions on page 65
- Classifying Subscribers (C-Web Interface) on page 67
- Subscriber Classification Conditions on page 68
- Sending DHCP Options to the JUNOS Router on page 71
- Subscriber Classification Targets on page 72
- Classifying DHCP Subscribers (C-Web Interface) on page 73
- Syntax for DHCP Classification Targets on page 74
- Selecting DHCP Parameters on page 74
- DHCP Options Supported on the SAE on page 75
- Creating DHCP Profiles (C-Web Interface) on page 78

Overview of Classification Scripts

The SAE uses classification scripts to determine whether it manages router interfaces, to select default policies, to find subscriber profiles, and to choose DHCP profiles. The SAE has three classification scripts:

- Interface classification script—When a subscriber's IP interface comes up on the router, the router sends the subscriber's login and interface information to the SAE. The SAE runs the interface classification script to determine whether the SAE manages the interface and if so, what default policies to send to the router.
- Subscriber classification script—If the SAE is managing the interface, the SAE uses the login and interface information that the router sends to run the subscriber classification script to determine which subscriber profile to load into memory.
- DHCP classification script—For DHCP subscribers, the SAE runs DHCP classification scripts to choose DHCP profiles.

How Classification Scripts Work

Classification scripts consist of *targets* and *conditions*.

- A target is the result of the classification script. For example, the result of subscriber classification scripts is an LDAP search string that is used to find a unique subscriber profile. The result of interface classification scripts is a policy group.
- Conditions are match criteria. The script attempts to match conditions in the script with information sent from the router. For example, match conditions for a subscriber classification script might be login type or domain name. Match conditions for an interface classification script could be interface IP address or interface description.

Each script can have multiple targets, and each target can have multiple conditions. When an object needs classification, the script processes the targets in turn. Within each target, the script processes conditions sequentially. When it finds that the classification conditions for a target match, it returns the target to the SAE. If the script does not find any targets that can be matched, the classifier engine returns a no-match message to the SAE.

Because classification scripts examine conditions sequentially as the conditions appear in the script, you should put more specific conditions at the beginning of the script and less specific conditions at the end of the script.

Interface Classification Scripts

When a subscriber's IP interface comes up on the router, the router sends the subscriber's login and interface information to the SAE. For example, the router might send the following information:

```
IP address=0.0.0.0
Virtual router name=default@erx5_ssp58
Interface name=FastEthernet3/1.1
PPP login name (PPP)=pebbles@virneo.net
User IP address (PPP)=192.168.55.5
Interface speed=100000000
Interface description=P3/1.1
Interface alias=1st pppoe int
RADIUS class=null
```

The SAE invokes the interface classification script and provides to the script the information that it received from the router. The script engine matches the information sent from the router to the conditions in the interface classification script. The script examines each condition in sequential order to find a match.

- If it finds a match, the script processing stops, and the target for that condition is returned to the SAE. The target is the path of a policy group. This policy group is the default policy. The SAE installs the policy on the interface and begins managing the interface.

- If it does not find a match, the script sends a no-match message to the SAE. The SAE does not manage the interface; that is, the policies installed through RADIUS or the CLI remain in effect. The SAE does not install policies.

Subscriber Classification Scripts

When the SAE begins managing an interface, it determines whether a subscriber is associated with the interface by running the subscriber classification script. The SAE also runs the subscriber classification script when certain login events occur. See Login Events for a description of login event types.

To find the matching subscriber profile, the SAE uses interface information that it received from the router when the interface became operational (for example, virtual router name, interface name, interface alias). It also uses login information that it received from the router or the portal application when the subscriber attempted to log in (for example, subscriber IP address, login name, or login event type).

When the SAE runs the subscriber classification script, the script engine matches the information sent from the router to the conditions in the subscriber classification script. The script examines each condition in sequential order to find a match.

- If it finds a match, the script processing stops, and the target for the matching condition is returned to the SAE. The target is an LDAP query that uniquely identifies a subscriber profile. The SAE loads the subscriber entry and uses the entry to create a subscriber session in memory.
- If it does not find a match, the script sends a no-match message to the SAE. The SAE does not load a subscriber session onto the interface, and services cannot be activated for this session.

DHCP Classification Scripts

DHCP classification scripts choose DHCP profiles. See Assigning DHCP Addresses to Subscribers for information about how DHCP classification scripts are used.

Overview of Configuring Classification Scripts

Classification scripts are organized into rules. Each rule has a target and one or more match conditions. For example:

Subscriber Classifiers

```
subscriber-classifier {
.
.
.
rule rule-2 {
    target <-unauthenticatedUserDn->;
    condition {
        "loginType == \"ADDR\"";
        "loginType == \"AUTHADDR\"";
    }
}
```

```

    }
  }
}

```

DHCP Classifiers

```

dhcp-classifier {
.
.
.
rule rule-2 {
    target cn=default,<-dhcpProfileDN->;
    condition {
        1;
    }
}
}

```

Interface Classifiers

```

interface-classifier {
.
.
.
rule rule-5 {
    target /sample/junose/DHCP;
    condition {
        "interfaceName=\"fastEthernet*\"";
        "interfaceName=\"atm*/.*\"";
    }
}
}

```

Classification Targets

A target is the result of the classification script that gets returned to the SAE. There are two special types of targets:

- No-match targets—Targets that begin with a - (single dash) are interpreted as no match. If the conditions of this target are matched, a no-match message is returned to SAE. You can use this type of target to exclude certain patterns or to shortcut known nonmatches. To speed up processing, use this target to specify interfaces that you do not want the SAE to manage.
- Script targets—The content of the script rule is interpreted when the classifier is initially loaded. The script rule can contain definitions of custom functions, which can be called during the matching process. Because you can insert arbitrary code into a script, you can use classification scripts to perform arbitrary tasks.

Because script targets use * (asterisks), you cannot use * in other types of targets.

Target Expressions

A target can contain expressions. These expressions can refer to an object in the SAE's memory or configuration, to specific matching conditions, or to another function or script.

Suppose the classification object in a subscriber classifier contains a field called `userName`. The classifier target `uniqueId = <- userName ->` is expanded to contain the actual content of the `userName` field before it is returned to the SAE; for example, for `userName = juser`, `uniqueId = juser` is returned.

Target expressions are enclosed in angle brackets and hyphens; for example, `<-retailerDn->`. The classifier expands expressions before it returns the target to the SAE. The expression is interpreted by an embedded Python interpreter and can contain variables and Python operations. In the simplest case an expression can be a single variable that is replaced with its current contents. Available variable names are all fields of the object passed to the classifier and names created with regular expression matching.

Because a scripting interpreter interprets expressions, more complex operations are possible. Examples are:

- Indexing—`var[index]` returns the element index of a sequence. The first element is at index 0.
- Slicing—`var[start : end]` creates a substring of the variable `var` starting at index `startup` to, but not including, index `end`; for example, `var = Hello`, `var[2:4] = ll`

Classification Conditions

You can configure multiple classification conditions for a rule. For example:

```
rule rule-2 {
  target /ent/EntDefault;
  condition {
    "pppLoginName=\"\"";
    "&interfaceName!=\"fastEthernet0*\"";
    "&interfaceName!=\"null*\"";
    "&interfaceName!=\"loopback*\"";
  }
}
```

If you prefix a condition with an `&` (ampersand) character, the condition is examined only if the previous condition matches.

If you prefix a condition with a `|` (pipe) character, the condition is examined only if the previous conditions have not produced a positive match.

You can use glob or regular expression matching to configure each target's conditions.

Glob Matching

Glob matches are of the form:

```
field = match
or
field != match
```

where match is a pattern similar to UNIX filename matching. Glob matches are case insensitive. “field != match” is true, if field = match is not true.

- *—Matches any substring.
- ?—Matches any single character.
- [range]—Matches a single character in the specified range. Ranges can have the form a-z or abcd.
- [!range]—Matches a single character outside the specified range.
- C—Matches the single character c.

The available field names are described for the specific classifiers. Examples are:

- interfaceName = fastEthernet3/0 # matches the string “fastEthernet3/0” directly.
- interfaceName = fast*3/1 # matches any string that starts with “fast” and ends with “3/1”
- interfaceName = fast*3/1.* # starts with “fast”, contains “3/1.” arbitrary ending
- interfaceName = fast*3/[2-57] # starts with “fast”, contains “3/” followed by 2,3,4,5 or 7

Regular Expression Matching

Regular expression matches are of the form:

```
field =~ re
or
field !~ re
```

where field !~ re is true if field = ~ re is not true. The regular expression is *re*. For a complete description of the syntax, see: <http://www.python.org/doc/2.0/lib/re-syntax.html>

You can group regular expressions with pairs of parentheses. If such an expression matches, the contents of the groups are made available for target expressions. Group number *n* is available as G[*n*], where *n* is the number of the opening parenthesis of the group. You can also name groups by using the special notation (?P<name>...).

Examples:

```
ifAlias =~ "SSP(.*)"
# match a string starting with "SSP". The remainder is stored
# in the variable "G[1]"
ifAlias =~ (?P<dn>name=(?P<name>[^\,]*).*)
# match a string starting with "name=". The whole match is
# stored in the variable "dn". A submatch which does not
# contain any "," -characters and starts after "name="
# is stored in variable "name"
```


Classifying Interfaces (C-Web Interface)

To define interface classification scripts:

1. Click **Configure**, and expand **Shared > Network**.
2. Expand the device for which you want to configure interface classification scripts, and then click **Interface Classifier**.

The Interface Classifier pane appears.

3. From the Create new list, select **Rule**.
4. Type a name for the new rule in the dialog box, and click **OK**.

The rule appears in the side pane and the Rule pane.

5. Enter a script or a target as described in the Help text in the Main pane, and click **Apply**.
6. To configure a condition for a target:
 - a. Expand the rule in the side pane, and click **Condition**.

The Condition pane appears.

- b. From the Create new list, select **Condition**.
- c. Type the interface classification condition name, and click **OK**.

The condition appears in the side pane and the Condition pane.

Interface Classification Conditions

Use the fields in this section to define interface classification conditions.

broadcastAddr

- Interface broadcast address.
- Value—Valid broadcast address format
- Example—broadcastAddr.hostAddress = “ 255.255.255.255”

ifAlias

- Description of an interface.
- Value—Interface description that is configured on the router. For JUNOSe routers, it is the description configured with the **interface description** command.
- Example—ifAlias = “ 1st pppoe int”

ifDesc

- Alternate name of the interface that is used by SNMP. This name is a system-generated name.
- Value
 - On a JUNOSe router, the format of the description is
 `ip<slot>/<port>.<subinterface>`
 - On the JUNOS routing platform, ifDesc is the same as interfaceName.
- Example—ifDesc = “ IP3/1.1 ”

interfaceName

- Name of the interface.
- Value
 - Name of the interface in your router CLI syntax
 - FORWARDING_INTERFACE for routing instance (used by traffic mirroring)
- Example—For JUNOSe routers: interfaceName = “ fastethernet6/0.1 ”

For JUNOS routing platforms: interfaceName = “ fe-0/1/0.0 ”

For forwarding interface: interfaceName = “ FORWARDING_INTERFACE ”

ipAddress

- Interface IP address.
- Value—Valid IPv4 IP address format
- Example—ipAddress = “ 10.10.30.1 ”

ipMask

- Interface network mask.
- Value—Valid IPv4 IP network mask format
- Example—ipMask = “ 255.255.255.255 ”

mtu

- Maximum transfer unit configured on the interface.
- Value—32-integer value
- Example—mtu = “ 1492 ”

nasPortId

- Port identifier of an interface.
- Value—Includes interface name and additional layer 2 information
- Example—nasPortId = “ fastEthernet 3/1 ” (There is a space between fastEthernet and slot number 3/1 in the nasPortId.)

pppLoginName

- Login name for PPP subscribers.
- Value—Login name in the format username@domain
- Example—pppLoginName = “ pebbles@virneo.net”

radiusClass

- RADIUS class attribute.
- Value—RADIUS class name
- Example—radiusClass = “ Premium”

serviceBundle

- Content of the vendor-specific RADIUS attribute for the service bundle.
- Value—Name of a service bundle

userIpAddress

- Subscriber IP address (PPP only).
- Value—valid IPv4 address
- Example—userIpAddress = “ 192.168.30.15”

virtualRouterName

- Name of the virtual router or routing instance.
- Value—For JUNOS routers: name of the virtual router in the format vrname@hostname
For JUNOS routing platforms: name of the routing instance
- Example—virtualRouterName = “ default@erx5”

Classifying Subscribers (C-Web Interface)

To define subscriber classification scripts:

1. Click **Configure**, expand **Shared > SAE**, and then click **Subscriber Classifier**.
The Subscriber Classifier pane appears.
2. From the Create new list, select **Rule**.

3. Type a name for the new rule in the dialog box, and click **OK**.

The rule appears in the side pane and the Rule pane.

4. Enter a script or a target as described in the Help text in the Main pane, and click OK.
5. To configure a condition for a target:

- a. Expand the rule in the side pane, and click Condition.

The Condition pane appears.

- b. Type the subscriber classification condition name as described in *Classifying DHCP Subscribers (C-Web Interface)*, and click OK.

The condition appears in the side pane and the Condition pane.

Subscriber Classification Conditions

Subscriber classification conditions define match criteria that are used to find the subscriber profile. Use the fields in this section to define subscriber classification conditions.

dhcp

- DHCP options. See *Sending DHCP Options to the JUNOSe Router*.

domainName

- Domain name of the subscriber.
- Value—Valid domain name
- Example—domainName = “ isp99.com”

ifAlias

- Description of the interface.
- Value—Interface description that is configured on the router. For JUNOSe routers, it is the description configured with the **interface description** command
- Example—ifAlias = “ dhcp-subscriber12”

ifDesc

- Alternate name for the interface that is used by SNMP. This name is a system-generated name.
- Value
 - On a JUNOSe router, the format of the description is
 ip<slot>/<port>.<subinterface>

- On the JUNOS routing platform, ifDesc is the same as interfaceName.
- Example—ifDesc = “ IP3/1.1 ”

interfaceName

- Name of the interface.
- Value
 - Name of the interface in your router CLI syntax
 - FORWARDING_INTERFACE for routing instance (used by traffic mirroring)
 - Router for a JUNOSe router instance
- Example—For JUNOSe routers: interfaceName = “ fastEthernet6/0 ”

For JUNOS routing platforms: interfaceName = “ fe-0/1/0.0 ”

For forwarding interface: interfaceName = “ FORWARDING_INTERFACE ”

loginName

- Name to be used to create a loginName attribute for a subscriber session for JUNOSe interfaces that are not otherwise assigned a loginName when a session starts, such as unauthenticated DHCP addresses, unauthenticated IP interfaces (that are not using PPP connections), or core-facing interfaces.

The loginName can also be used to identify a subscriber session through the SAE CORBA remote API.

- Value—Name in the form subscriber@domain
- Guideline—The format is not defined. A loginName can be of form subscriber, domain\subscriber, subscriber@domain, or as otherwise defined by the login setup of the operator.
- < Login name >
- Example—idp@idp

loginType

- Type of subscriber session to be created.
- Value—One of the following login types:
 - ASSIGNEDIP—For assigned IP subscribers. Triggered when an application accesses a subscriber object for an assigned IP subscriber that is not currently loaded into memory. (Supported on JUNOSe routers.)
 - AUTHINTF—For authenticated interface login requests. Triggered when a login Name is reported together with the interface, such as authenticated PPP or autoconfigured ATM interface, by means of the **subscriber** command. (Supported on JUNOSe routers.)

- INTF—For unauthenticated interface login requests. Triggered when an interface comes up and the interface classification script determines that the SAE should manage the interface. (Supported on JUNOS routing platforms and JUNOSe routers.)
- ADDR—For unauthenticated address login requests. Triggered when the DHCP server in the JUNOSe router provides an unauthenticated IP address. (Supported on JUNOSe routers.)
- AUTHADDR—For authenticated address login requests. Triggered when the DHCP server in the JUNOSe router provides an authenticated IP address. (Supported on JUNOSe routers.)
- PORTAL—Triggered when the portal API is invoked to log in a subscriber. (Supported on JUNOS routing platforms and JUNOSe routers.)
- Example—loginType = “ AUTHADDR”

macAddress

- String representation of the DHCP subscriber media access control (MAC) address.
- Value—Valid MAC address
- Example—macAddress = “ 00:11:22:33:44:55”

nasPortId

- Port identifier of an interface.
- Value—Includes interface name and additional layer 2 information
- Example—nasPortId = “ fastEthernet 3/1 ” (There is a space between fastEthernet and slot number 3/1 in the nasPortId.)

radiusClass

- RADIUS class used for authorization.
- Value—RADIUS class name
- Example—radiusClass = “ Premium”

retailerDn

- DN of the retailer object. The object is found when the domain name is mapped to a retailer object in LDAP.
- Value—DN of a retailer

serviceBundle

- Content of the vendor-specific RADIUS attribute for the service bundle.
- Value—Name of a service bundle
- Example—serviceBundle = “ goldSubscriber”

unauthenticatedUserDn

- DN of the unauthenticated subscriber profile (usable for target expressions only).
- Value—DN of a subscriber profile

userName

- Name of the subscriber.
- Value—Subscriber name without the domain name
- Example—userName = “ peter”

virtualRouterName

- Name of the virtual router or routing instance.
- Value—For JUNOSe routers: name of the virtual router in the format vrname@hostname
For JUNOS routing platforms: name of the routing instance
- Example—virtualRouterName = “ default@e_series5”

Sending DHCP Options to the JUNOSe Router

Subscriber classification scripts support DHCP options conveyed through COPS. When COPS reports an address, the JUNOSe router sends DHCP options received for DHCP requests for that address. The DHCP options are available in the subscriber classification context for selecting the subscriber profile to load.

The fields in Table 5 on page 71 are in the classification context of subscriber classification scripts.

Table 5: DHCP Options in UserClassificationContext Field

DHCP Option	UserClassificationContext Field	Comments
giAddr	dhcp.giAddr	Relay agent gateway address
Option 82 data	dhcp.getOption(82)	Content is accessible with getSubOptions()
Client ID	dhcp.getOption(61).getString()	
Lease time	dhcp.getOption(51).getInt()	

Table 5: DHCP Options in UserClassificationContext Field *(continued)*

DHCP Option	UserClassificationContext Field	Comments
Client requested parameter list	dhcp.getOption(55).getBytes()	
Domain name sent to client	dhcp.getOption(12).getString() dhcp.getOption(15).getString()	12 = HostName 15 = DomainName
DNS server address(es) sent to client	dhcp.getOption(6).getIpAddresses()	
Subnet mask	dhcp.getOption(1).getIpAddress()	
NetBios name server address(es) sent to client	dhcp.getOption(44).getIpAddresses()	
NetBios node type	dhcp.getOption(46).getBytes()	
Default router address(es) sent to client	dhcp.getOption(3).getIpAddresses()	

The DHCP options are accessible to the subscriber classification script with the following syntax:

```

dhcp.giAddr = " match"

# interpret option 61 as string
dhcp[61].string = " match"

# interpret option 1 (subnet) as dotted decimal IP
dhcp[1].ipAddress = " match"

# option 82, suboption 1, interpreted as string
dhcp[82].subOptions[1].string = " match"
```

The received DHCP options are also stored in the UserSession and are available through the portal API (method User.getDhcpOptions).

Subscriber Classification Targets

The target of the subscriber classification script is an LDAP search string. The search string uses a syntax similar to an LDAP URL (see *RFC 2255—The LDAP URL Format (December 1997)*).

The syntax is:

```
" baseDN [ ? [ attributes ] [ ? [ scope ] [ ? [ filter ] ] ] ]"
```


- baseDN—Distinguished name of object where the LDAP search starts
- attributes—Can be used to override attributes in the loaded LDAP object. For example, for static IP subscribers the SAE must learn the IP address assigned to a particular subscriber. This address is defined in the ipAddress attribute of the subscriber profile. A target of the form
baseDN?ipAddress = <-function(interfaceName)-> invokes function after the subscriber profile is loaded from LDAP and sets the IP address to the return value of function. The function is defined in the subscriber classification script, and can be used for a variety of things; for example, to query an external database.



NOTE: You can use subscriber classification to override only the ipAddress, loginName, or accountingId attributes. If you configure values to override other attributes, the value is lost when the SAE recovers from a network or server failure.

- scope—Scope of search
 - base—Is the default, searches the base DN only.
 - one—Searches the direct children of the base DN.
 - sub—Searches the complete subtree below the base DN.
- filter—Is an RFC 2254-style LDAP search filter expression; for example, (uniqueId = <-userName->). See *RFC 2254—The String Representation of LDAP Search Filters (December 1997)*.

With the exception of baseDN all the fields are optional.

The result of the LDAP search must be exactly one directory object. If no object or more than one object is found, the subscriber session is terminated.

Classifying DHCP Subscribers (C-Web Interface)

A classification script can contain either a target and a condition or a script. If you do not define a script, the classifier must have both a target and a condition.

To configure DHCP classification scripts:

1. Click **Configure**, expand **Shared > SAE**, and then click **DHCP Classifier**.

The Dhcp Classifier pane appears.

2. From the Create new list, select **Rule**.
3. Type a name for the new rule in the dialog box, and click **OK**.

The rule appears in the side pane and the Rule pane.

4. Enter a script or a target as described in the Help text in the Main pane, and click **OK**.
5. To configure a condition for a target,
 - a. Expand the rule in the side pane, and click **Condition**.

The Condition pane appears.

- b. Type the DHCP classification condition name , and click OK.

The condition appears in the side pane and the Condition pane.

Syntax for DHCP Classification Targets

The target of the DHCP classification script uses a syntax similar to an LDAP URL. With the exception of baseDN, all fields are optional. The syntax is:

```
baseDN [ ? [ attributes ] [ ? [ scope ] [ ? [ filter ] ] ] ]
```

- baseDN—DN of object where search starts.
- attributes—Comma-separated list of properties, in the format attribute = <-value-> , that allow you to set specific attributes for directory objects that the script finds; see DHCP Classification Conditions.

You can use the attribute configuration to override attributes in the directory. For example, to override the IP pool name that is stored in the DHCP profile with the pool name that the authorization plug-in sends, use the attribute statement radiusFramedPool = <-poolName-> .

- scope—Scope of search in the directory
 - base—Searches the base DN only; default scope
 - one—Searches the direct subordinates of the base DN (one-level search)
 - sub—Searches all objects subordinate to the base DN
- filter—An RFC 2254-style LDAP search filter expression; for example, (uniqueId = <-userName->). See *RFC 2254—The String Representation of LDAP Search Filters (December 1997)*.

Selecting DHCP Parameters

The SAE sends a set of parameters to the DHCP server in the JUNOSe router. The DHCP server determines the IP address offered, as well as the options sent to the DHCP client. The parameters comprise IP address authorization parameters, as well as parameters stored in a DHCP profile. Parameters in the DHCP profile override authorization parameters.



NOTE: JUNOSe routers do not currently support the functionality described in this section. DHCP options and BOOTP options that the SAE sends to the JUNOSe router are ignored.

DHCP servers use DHCP options to configure DHCP clients. The DHCP local server in the JUNOSe router supports a subset of DHCP options. The SAE supports all DHCP options defined in *RFC 2132—DHCP Options and BOOTP Vendor Extensions (March*

1997) by name. It also supports other options, but you need to specify them by number and type. The DHCP options allow a flexible definition of parameters offered to DHCP subscribers. For example, they allow integration with cable modems or set-top boxes because you can configure options to control the boot sequence of these devices.

You can configure DHCP options in DHCP profiles and in DHCP classification scripts. Table 6 on page 75 lists the name, number, and type of all supported DHCP options. You can use these fields to configure DHCP options.

The following example shows how to specify an option by number and by type. The two statements identify the same option:

```
dhcp[12]
```

```
dhcp['host-name']
```

In SDX software earlier than Release 4.2, you had to include the option type in your option definition. For example:

```
dhcp[12].string = HOST
```

You can now write:

```
dhcp[12] = HOST
```

Note that the earlier method of defining options still works in Release 4.2 and later.

- Related Topics**
- Assigning DHCP Addresses to Subscribers
 - DHCP Subscriber Login and Service Activation

DHCP Options Supported on the SAE

Table 6 on page 75 lists the DHCP options are available.

Table 6: DHCP Options Supported on the SAE

Option Name	Option Number	Option Type
subnet-mask	1	ip-address
time-offset	2	int32
routers	3	ip-address
time-servers	4	ip-address
ien116-name-servers	5	ip-address
domain-name-servers	6	ip-address
log-servers	7	ip-address

Table 6: DHCP Options Supported on the SAE *(continued)*

Option Name	Option Number	Option Type
cookie-servers	8	ip-address
lpr-servers	9	ip-address
impress-servers	10	ip-address
resource-location-servers	11	ip-address
host-name	12	string
boot-size	13	int16
merit-dump	14	string
domain-name	15	string
swap-server	16	ip-address
root-path	17	string
extension-path	18	string
ip-forwarding	19	int8
non-local-source-routing	20	int8
policy-filter	21	ip-address
max-dgram-reassembly	22	int16
default-ip-ttl	23	int8
path-mtu-aging-timeout	24	int32
path-mtu-plateau-table	25	int16
interface-mtu	26	int16
all-subnets-local	27	int8
broadcast-address	28	ip-address
perform-mask-discovery	29	int8
mask-supplier	30	int8
router-discovery	31	int8
router-solicitation-address	32	ip-address
static-routes	33	ip-address
trailer-encapsulation	34	int8

Table 6: DHCP Options Supported on the SAE *(continued)*

Option Name	Option Number	Option Type
arp-cache-timeout	35	int32
ieee802-3-encapsulation	36	int8
default-tcp-ttl	37	int8
tcp-keepalive-interval	38	int32
tcp-keepalive-garbage	39	int8
nis-domain	40	string
nis-servers	41	ip-address
ntp-servers	42	ip-address
netbios-name-servers	44	ip-address
netbios-dd-server	45	ip-address
netbios-node-type	46	int8
netbios-scope	47	string
font-servers	48	ip-address
x-display-manager	49	ip-address
requested-ip-address	50	ip-address
ip-address-lease-time	51	int32
option-overload	52	int8
dhcp-msg-type	53	int8
server-identifier	54	ip-address
parameter-request-list	55	data-string
message	56	string
maximum-dhcp-msg-size	57	int16
renewal-time	58	int32
rebinding-time	59	int32
vendor-class-identifier	60	data-string
client-identifier	61	data-string
nisplus-domain	64	string

Table 6: DHCP Options Supported on the SAE *(continued)*

Option Name	Option Number	Option Type
nisplus-servers	65	ip-address
tftp-server-name	66	string
bootfile-name	67	string
mobile-ip-home-agent	68	ip-address
smtp-server	69	ip-address
pop-server	70	ip-address
nntp-server	71	ip-address
www-server	72	ip-address
finger-server	73	ip-address
irc-server	74	ip-address
streettalk-server	75	ip-address
streettalk-directory-assistance-server	76	ip-address

Creating DHCP Profiles (C-Web Interface)

When the SAE receives a DHCP discover request from the router, it uses the client's MAC address to find a DHCP profile in cache or in the directory. If it finds a DHCP profile, the SAE uses the information in the profile to create a discover decision that it returns to the router. The discover decision includes information to select an IP address and DHCP options to configure the DHCP client.

When a DHCP subscriber logs in to the SAE through a Web portal, the SAE registers the subscriber's equipment and creates a cached DHCP profile in the *o = AuthCache* directory. These profiles are keyed by the MAC address of the DHCP client device. They are created by the `grantPublicIp` or the `registerEquipment` methods.

DHCP profiles are stored in the *o = AuthCache* directory in the `dhcpProfile` object class. The `dhcpProfile` object class is subordinate to the `cachedAuthenticationProfiles` object class. Manually created profiles are keyed by the `cn` (common name) attribute.

To create a DHCP profile:

1. Click **Configure**, expand **Shared**, and then click **Auth Cache**.

The Auth Cache pane appears.

2. From the Create new list, select **Cached Dhcp Profile**.
3. Type a name for the new cached DHCP profile in the dialog box, and click **OK**.

The cached authentication profile appears in the side pane and in the Cached DHCP Profile pane.

4. Enter information as described in the Help text in the main pane, and click **Apply**.

- Related Topics** ■ For more information about how the SAE handles DHCP subscribers, see:
- Assigning DHCP Addresses to Subscribers
 - DHCP Subscriber Login and Service Activation

Chapter 12

Configuring the SAE for a PCMM Environment (C-Web Interface)

- Configuring the SAE for a Cable Network Environment (C-Web Interface) on page 81
- Configuring the SAE to Manage PCMM Devices (C-Web Interface) on page 82
- Setting Up SAE Communities (C-Web Interface) on page 82
- Configuring the SAE Community Manager on page 83
- Configuring SAE Properties for the Event Notification API (C-Web Interface) on page 83
- Configuring PCMM Record-Keeping Server Plug-Ins (C-Web Interface) on page 83
- Configuring CMTS-Specific RKS Plug-Ins (C-Web Interface) on page 84
- Configuring Record-Keeping Server Peers for Plug-Ins (C-Web Interface) on page 84

Configuring the SAE for a Cable Network Environment (C-Web Interface)

The tasks to configure the SAE for a cable network environment are:

1. Configure the SAE to manage PCMM devices.

See Configuring the SAE to Manage PCMM Devices (C-Web Interface).

2. Configure the session store.

3. Set up SAE communities.

See Setting Up SAE Communities (C-Web Interface).

4. (Optional) Configure SAE properties for the Event Notification API.

See Configuring SAE Properties for the Event Notification API (C-Web Interface) (if you are using an external address manager).

5. (Optional) Configure record-keeping server peers for plug-ins.

See Configuring Record-Keeping Server Peers for Plug-Ins (C-Web Interface) (if you are using the RKS plug-in).

6. (Optional) Configure PCMM record-keeping server plug-ins.

See Configuring PCMM Record-Keeping Server Plug-Ins (C-Web Interface) (if you are using the SAE's embedded policy server).

In addition to configuring the SAE, you need to:

1. Configure the CMTS device in the directory (if you are using the SAE's embedded policy server).

See Adding Objects for CMTS Devices (C-Web Interface) .

2. Configure the NIC (if you are using assigned IP subscribers).

See Using the NIC Resolver in PCMM Environments .

3. Enable the Common Open Policy Service (COPS) interface on the CMTS device. See the documentation for your CMTS device for information about how to do this.

Configuring the SAE to Manage PCMM Devices (C-Web Interface)

The SAE connects to the PCMM device by using a COPS over TCP connection. The PCMM device driver controls this connection.

To configure the SAE to manage PCMM devices:

1. Click **Configure**, expand **Shared > SAE > Configuration > Driver**, and then click **PCCM**.

The PCCM pane appears.

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

Related Topics ■ For information about setting up SAE groups, see Setting Up an SAE with the C-Web Interface on page 47

Setting Up SAE Communities (C-Web Interface)

You can configure the following for SAE communities:

- Define the members of an SAE community by adding the IP addresses of SAEs in the community to the virtual router object of the network device in the directory.

See Creating Virtual Routers for the CMTS Device (C-Web Interface) .

- Specify the name of the community manager.

See Configuring the SAE to Manage PCMM Devices (C-Web Interface).

- Configure parameters for the SAE community manager.

See Configuring the SAE Community Manager .

- If there is a firewall in the network, configure the firewall to allow SAE messages through.

Configuring the SAE Community Manager

To configure the SAE community manager that manages PCMM device communities:

1. Click **Configure**, expand **Shared > SAE**, and then expand the SAE group for which you want to manage PCMM devices.
2. In the side pane, expand **Configuration > External Interface Features: PCMMCommunityManager**, and then click **Community Manager**.

The Community pane appears.

3. Enter information as described in the Help text in the main pane, and click **Apply**.

Related Topics ■ For information about setting up SAE groups, see Configuring an SAE Group.

Configuring SAE Properties for the Event Notification API (C-Web Interface)

To configure properties for the event notification API:

1. Click **Configure**, expand **Shared > SAE**, and then expand the SAE group for which you want to manage devices.
2. In the side pane, expand **Configuration > External Interface Features: event**, and then click **Event API**.

The Event API pane appears.

3. Enter information as described in the Help text in the main pane, and click **Apply**.

Related Topics ■ Configuring an SAE Group

Configuring PCMM Record-Keeping Server Plug-Ins (C-Web Interface)

To configure an RKS plug-in:

1. Click **Configure**, expand **Shared > SAE**, and then expand the SAE group for which you want to create RKS plug-ins,
2. In the side pane, expand **Configuration > Plug Ins**.
3. Expand the plug-in that you created for RKS, and then click **PCMM RKS**.
4. Click **Create**, enter information as described in the Help text in the main pane, and then click **Apply**.

Related Topics ■ Configuring an SAE Group

Configuring CMTS-Specific RKS Plug-Ins (C-Web Interface)

You can configure an RKS plug-in for specific CMTS devices. When there are events for the CMTS device, the SAE sends the events to the specified plug-in.

To configure a CMTS-specific RKS plug-in:

1. Click **Configure**, expand **Shared > SAE**, > **Configuration > Driver**, and then click **PCCM**.

1. Click **Configure**, expand **Shared > SAE**, and then expand the SAE group for which you want to create CMTS-specific RKS plug-ins.

2. In the side pane, expand **Configuration > Drivers**, and then click **PCCM**.

The PCMM pane appears.

3. From the Create new list, select **CMTS Specific RKS Plug-Ins**.
4. Type a name for the new plug-in in the dialog box, and click **OK**.
5. In the side pane, click the new plug-in.
6. Click **Create**, enter information as described in the Help text in the main pane, and then click **Apply**.

Configuring Record-Keeping Server Peers for Plug-Ins (C-Web Interface)

An RKS peer is an instance of a record-keeping server. A PCMM environment has a primary RKS and optionally a secondary RKS. The primary RKS is mandatory, and you assign the RKS as primary by configuring it as the default peer in the RKS plug-in. The secondary RKS is optional, and it is an RKS peer that is not configured as the default peer. If you define multiple nondefault peers, one of them is randomly chosen to be the secondary RKS.

RKS peers are configured in the peer group for each PCMM RKS plug-in instance. To create an RKS peer group:

1. Click **Configure**, expand **Shared > SAE**, and then expand the SAE group for which you want to create RKS plug-ins.
2. In the side pane, expand **Configuration > Plug Ins**.
3. Expand the plug-in that you created for RKS, and then click **PCMM RKS**.
4. Enter information as described in the Help text in the main pane, and click **Apply**.

Chapter 13

Configuring and Starting the SNMP Agent (C-Web Interface)

- Configuring the SDX SNMP Agent on page 86
- Configuring General Properties for the SDX SNMP Agent on page 86
- Configuring Initial Properties for the SDX SNMP Agent on page 86
- Configuring Directory Connection Properties for the SDX SNMP Agent on page 87
- Configuring Directory Monitoring Properties for the SDX SNMP Agent on page 87
- Configuring Logging Destinations for the SDX SNMP Agent on page 87
- Configuring JRE Properties on page 87
- Configuring the SNMP Agent on page 88
- Configuring System Information for the SNMP Agent on page 88
- Configuring Access Control for SNMPv3 Users on page 88
- Configuring Authentication on page 89
- Configuring Encryption on page 89
- Configuring Access Control for Communities on page 89
- Configuring Access Control for the VACM on page 89
- Associating Security Names with a Community on page 90
- Defining Named Views on page 90
- Defining Access Privileges for an SNMP Group on page 91
- Assigning Security Names to Groups on page 91
- Configuring Notification Targets on page 91
- Configuring Performance Traps on page 92
- Configuring Event Traps on page 92
- Starting the SDX SNMP Agent on page 92
- Stopping the SDX SNMP Agent on page 93
- Monitoring the SDX SNMP Agent on page 93

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.

After you configure the local properties for the SDX SNMP agent, you can configure the SNMP agent. See [Configuring the SNMP Agent](#).

- Related Topics**
- [Configuring a Component to Store Log Messages in a File with SRC CLI](#)
 - [SRC-PE Monitoring and Troubleshooting Guide](#)
 - [Configuring Performance Traps](#)
 - [Configuring Event Traps](#)

Configuring General Properties for the SDX SNMP Agent

To configure properties for the SDX SNMP agent:

1. Click **Configure**, and expand **SNMP > Agent**.

The SNMP pane appears.

2. Enter information as described in the Help text in the main pane, and then click **Apply**.

Configuring Initial Properties for the SDX SNMP Agent

To configure properties for the SDX SNMP agent:

1. Click **Configure**, and expand **SNMP > Agent > Initial**.

The Initial pane appears.

2. Enter information as described in the Help text in the main pane, and then click **Apply**.

Configuring Directory Connection Properties for the SDX SNMP Agent

To configure directory connection properties:

1. Click **Configure**, and expand **SNMP > Agent > Initial > Directory Connection**.

The Directory Connection pane appears.

2. Enter information as described in the Help text in the main pane, and then click **Apply**.

Configuring Directory Monitoring Properties for the SDX SNMP Agent

To configure properties for the SDX SNMP agent:

1. Click **Configure**, and expand **SNMP > Agent > Initial > Directory Eventing**.

The Directory Eventing pane appears.

2. Enter information as described in the Help text in the main pane, and then click **Apply**.

Configuring Logging Destinations for the SDX SNMP Agent

To configure logging destinations:

1. Click **Configure**, and expand **SNMP > Agent**.
2. From the Create new list, select **Logger**.
3. Enter a name for the new Logger in the dialog box, and click **OK**.
4. For file-based logging, from the side pane, expand **File**, enter information as described in the Help text in the main pane, and then click **Create**.
5. For syslog-based logging, expand **Syslog**, enter information as described in the Help text in the main pane, and then click **Create**.

Configuring JRE Properties

To configure properties for the SDX SNMP agent:

1. Click **Configure**, and expand **SNMP > Agent > Java**.

The Java pane appears.

2. Enter information as described in the Help text in the main pane, and then click **Apply**.

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

To configure properties for the SNMP agent:

1. Click **Configure**, and expand **SNMP > Agent**.

The Agent pane appears.

2. Enter information as described in the Help text in the main pane, and then click **Apply**.

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. Click **Configure**, and expand **SNMP > V3 > USM > Local Engine**.
2. To configure MD5 authentication, from the side pane, expand the name of the user, and click Authentication MD5.
3. To configure SHA authentication, from the side pane, expand the name of the user, and click Authentication SHA.
4. Specify the authentication password as described in the Help text in the main pane, and then click **Create**.

The password must be at least eight characters.

Related Topics ■ Configuring Encryption

Configuring Encryption

Before you configure encryption, you must configure the authentication type. See [Configuring Authentication](#).

To configure encryption for SNMPv3 users:

1. Click **Configure**, and expand **SNMP > V3 > USM > Local Engine**.
2. To configure AES encryption, from the side pane, expand the name of the user, and click **Privacy AES**.
3. To configure DES encryption, from the side pane, expand the name of the user, and click **Privacy DES**.
4. Specify the authentication password as described in the Help text in the main pane, and then click **Create**.

The password must be at least eight characters.

Configuring Access Control for Communities

To configure community strings:

1. Click **Configure > SNMP**.
2. From the Create new list, select **Community**.
3. Enter a name for the new Community in the dialog box, and click **OK**.
4. From the side pane, expand the name of the community, enter information as described in the Help text in the main pane, and then click **Apply**.

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.

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.

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.

To configure the community:

1. Click **Configure > SNMP > V3**.
2. From the Create new list, select **SNMP Community**.
3. Enter a name for the new SNMP Community in the dialog box, and click **OK**.
4. From the side pane, expand the name of the SNMP community, enter information as described in the Help text in the main pane, and then click **Apply**.

Defining Named Views

To configure named views:

1. Click **Configure**, and expand **SNMP**.
2. From the Create new list, select **View**.
3. Enter a name for the new View in the dialog box, and click **OK**.
4. From the side pane, expand the name of the view,
5. From the Create new list, select **OID**.
6. Enter a name for the new OID in the dialog box, and click **OK**.

The View OID pane appears.

7. Enter information as described in the Help text in the main pane, and then click **Apply**.

Defining Access Privileges for an SNMP Group

To configure MIB views with a group for the VACM:

1. Click **Configure**, and expand **SNMP > V3 > VACM > Access**.
2. From the Create new list, select **Group**.
3. Enter a name for the new Group in the dialog box, and click **OK**.

The group name is the name for a collection of SNMP security names that belong to the same SNMP access policy.

4. From the side pane, expand the name of the group, click on **Default Context Prefix**,
5. From the Create New box, select the Security Model for access privileges.
6. From the Create New box, select the Security Level for access privileges.

The Security pane appears.

7. Enter information as described in the Help text in the main pane, and then click **Apply**.

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.

To map security names to groups for the VACM:

1. Click **Configure**, and expand **SNMP > V3 > VACM**.
2. Expand the desired **Security Model** and desired **Security Name**, enter information as described in the Help text in the main pane, and then click **Apply**.

Configuring Notification Targets

To configure notification targets:

1. Click **Configure > SNMP > Notify**.

The Notify pane appears.

2. From the Create New box, select **Target**, enter the name of the target, and click **OK**.

The Target pane appears.

3. Enter information as described in the Help text in the main pane, and then click **Apply**.

Configuring Performance Traps

To configure performance traps:

1. Click **Configure > SNMP > Notify** , and expand **Alarm** .
2. From the Create New box, select the category and associated traps, and click **OK**.

The Alarm pane appears.

3. Enter information as described in the Help text in the main pane, and then click **Apply**.

Configuring Event Traps

To configure event traps:

1. Click **Configure > SNMP > Notify** , and expand **Event** .
2. From the Create New box, select the category and the category name, and click **OK**.

The Category pane appears.

3. From the Create New box, select the event and click **OK**,

The Event pane appears.

4. Enter information as described in the Help text in the main pane, and then click **Apply**.

Starting the SDX 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.

Before you start the SDX SNMP agent:

1. Perform the initial configuration tasks on the C-series Controller.
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:

1. Click **Manage > Enable**.

2. From the Component box, select **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:

1. Click **Manage > Disable**.
2. From the Component box, select **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

To display the SDX SNMP agent status:

1. Click **Monitor > Component**.

The system responds with a status message.

Chapter 14

Configuring NIC (C-Web Interface)

- Before You Configure the NIC on page 95
- Configuring the NIC (C-Web Interface) on page 96
- Starting the NIC (C-Web Interface) on page 96
- Reviewing and Changing Operating Properties for NIC (C-Web Interface) on page 97
- Configuring NIC Replication (C-Web Interface) on page 97
- Configuring a NIC Scenario (C-Web Interface) on page 98
- Testing a NIC Resolution (C-Web Interface) on page 100
- Stopping a NIC Host on a C-series Controller (C-Web Interface) on page 101
- Restarting the NIC (C-Web Interface) on page 101
- Changing NIC Configurations (C-Web Interface) on page 101

Before You Configure the NIC

When you use NIC in a client/server configuration, you configure the NIC scenario before you configure the NIC proxies.

Before you configure NIC hosts from the CLI:

- Plan your NIC implementation:
- Choose the NIC configuration scenario to use.

The default scenario is OnePop.

For information about NIC configuration scenarios and NIC agents, see [Locating Subscriber Management Information](#).

- Ensure that the appropriate type of router initialization script is configured for the router or network device.

See [Locating Subscriber Management Information](#).

Set the editing level for the configuration application you are using, the SRC CLI or the C-Web interface to basic. This ensures that only the statements that you need to configure are visible.

To set the editing level for the C-Web interface to basic:

- Click **Preferences > Level Basic**.

Related Topics ■ Locating Subscriber Management Information

Configuring the NIC (C-Web Interface)

You configure the NIC to enable the SRC software to locate subscriber information for an application.

To configure the NIC:

1. Start the NIC component.

See Reviewing and Changing Operating Properties for NIC (C-Web Interface).

2. Review NIC operating properties, and change them if needed.

See Reviewing and Changing Operating Properties for NIC (C-Web Interface).

3. Configure NIC replication.

See Configuring NIC Replication (C-Web Interface).

4. (Optional) For the initial configuration if you plan to use a configuration scenario other than OnePop (the default), delete any data for the OnePop scenario. If you are changing from one configuration scenario to another, delete the data for the configuration scenario in use.

See Changing NIC Configurations (C-Web Interface).

5. Configure a NIC scenario.

See Configuring a NIC Scenario (C-Web Interface).

6. Verify the NIC configuration.

See Configuring Internal Plug-Ins (C-Web Interface).

Related Topics ■ Before You Configure the NIC

Starting the NIC (C-Web Interface)

Start the NIC component before you configure a NIC configuration scenario.

To start the NIC component:

1. Select **Manage > Enable**.

The Enable pane appears.

2. In the Component box, select **NIC**, and click **OK**.

Related Topics ■ Before You Configure the NIC

Reviewing and Changing Operating Properties for NIC (C-Web Interface)

Before you configure a NIC configuration scenario, review the default operating properties and change values as needed. Operating properties are configured for a slot.

To review and change the default NIC operating properties:

1. Click **Configure**, expand **Slot**, then a specified slot (for example, slot0), and then expand **NIC > Initial**. Click **Directory Connection**.

The Directory Connection pane appears.

2. Review the configuration, enter information as described in the Help text in the main pane, and then click **Apply**.
3. In the side pane, click **Directory Eventing**.

The Directory Eventing pane appears.

4. Review the configuration, enter information as described in the Help text in the main pane, and then click **Apply**.
5. In the side pane, click **NIC**.

The NIC pane appears.

6. Review the configuration, enter information as described in the Help text in the main pane, and then click **Apply**.
7. In the left pane, click **Commit**.

Related Topics ■ Locating Subscriber Management Information
 ■ Configuring the NIC (C-Web Interface)
 ■ Configuring NIC Replication (C-Web Interface)

Configuring NIC Replication (C-Web Interface)

You configure NIC replication to keep the NIC configuration highly available.

Before you configure NIC replication:

- Make sure that you understand how NIC groups are used.
 See Locating Subscriber Management Information.
- Identify which NIC hosts are to provide redundancy for each other.
- Specify a name for a group for each of these hosts.

To configure NIC replication:

1. Click **Configure > Slot**, then a specified slot (for example, slot0), and then **NIC**.

The NIC pane appears.

2. Specify a group for NIC replication in the **Runtime Group** box, as described in the Help text; for example, group1.
3. Click **Apply**.
4. In the left pane, click **Commit**.

- Related Topics**
- Locating Subscriber Management Information
 - Configuring the NIC (C-Web Interface)
 - Reviewing and Changing Operating Properties for NIC (C-Web Interface)

Configuring a NIC Scenario (C-Web Interface)

The following topics provide the procedures for configuring a NIC scenario with the C-Web Interface:

- Defining the NIC Configuration (C-Web Interface) on page 98
- Configuring the SAE to Communicate with SAE Plug-In Agents for NIC Replication (C-Web Interface) on page 99

Defining the NIC Configuration (C-Web Interface)

To use the NIC to locate subscriber configuration, you must configure one of the NIC configuration scenarios provided with the SRC software. Which agents you configure depends on the NIC configuration scenario that you use.

The OnePop configuration scenario is the default configuration for the NIC. If you want to use another configuration scenario, you first clear data for the configuration scenario. Anytime you change the configuration scenario, you first clear data for the configuration scenario in use. See *Changing NIC Configurations (C-Web Interface)*.

When you select a NIC configuration scenario, the software adds the default configuration for most properties. You can modify the NIC properties, including those for agents.



NOTE: We recommend that you change only those statements visible at the basic editing level. Contact Juniper Professional Services or Juniper Customer Support before you change any of the NIC statements not visible at the basic editing level.



NOTE: By default, the CORBA naming server on a C-series platform uses port 2809. The NIC host is configured to communicate with this naming server.

To configure a NIC configuration scenario:

1. Click **Configure**, expand **Shared > NIC**, and click the configuration scenario that you want to configure; for example, **Scenario: OnePop**.
2. In the left pane, expand **Agents**.
3. For each directory agent that the NIC configuration scenario includes, review and if needed update NIC agent configuration to define properties specific to your environment, such as server identification and authentication information. For example, for the OnePop configuration scenario:
 - a. Click **Agents**, then a specific agent such as Agent:PoolVr, and then **Configuration > Directory**.

The Directory pane appears.

- b. Enter information as described in the Help text in the main pane, and click **Apply**.
4. For each SAE plug-in agent that the NIC configuration scenario includes, review and if needed update the NIC agent configuration to define properties specific to your environment, such as the event filter and the number of events that the SAE sends to the agent at one time during state synchronization. For example, for the OnePopLogin configuration scenario:
 - a. Click **Agents**, then a specific agent such as Agent:LoginNameVr, and then **Configuration > SAE Plug-In**.

The SAE Plug-In pane appears.

If you plan to change the event filter for the agent, make sure that you are familiar with:

- Plug-in attributes and values

See Configuring Internal Plug-Ins.

- Filter syntax

See the documentation for the SAE CORBA Remote API in the SAE Core API documentation on the Juniper Networks Web site at:

<http://www.juniper.net/techpubs/software/management/src/api-index.html>

- b. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring the SAE to Communicate with SAE Plug-In Agents for NIC Replication (C-Web Interface)

For each NIC host that uses SAE plug-in agents, configure a corresponding external plug-in for the SAE. By default, the SAE plug-in agents share events with the single SAE plug-in. You must also configure the SAE to communicate with the SAE plug-in agent in each NIC host that you use in the NIC replication.

To configure an external plug-in:

1. Configure an SAE external plug-in.

See Configuring the SAE for External Plug-Ins.

2. Specify the following values for the plug-in:

- CORBA object reference that has the following syntax:

host : *port-number* /NameService# *plugInName*

where:

- *host* —IP address or name of the machine on which you installed the NIC host that supports the agent

For local host, use the IP address 127.0.0.1.

- *port-number* —Port on which the name server runs

The default port number is 2809.

- *plugInName* —Name under which the agent is registered in the naming service

Use the format `nicssae_ groupname /saePort`, where *groupname* is the name of the replication group. (When replication is not used, the format is `nicssae/saePort`.)

For example: `corbaname::127.0.0.1:2809/NameService#nicssae/saePort`

- Attributes that are sent to the external plug-in for a NIC host. Because the SAE plug-in agents share the event by default, you configure only one for a NIC host.

Specify the plug-in options that the agent uses. You must specify the options `session-id` and `router-name`, and other options that you specified for the agent's network data types and the agent's event filter. Specify attributes options of the PAT_OPAQUE attribute type, such as the option `dhcp-packet`, only if you are using IPv6 addressing.



NOTE: Do not include attributes that are not needed.

- NIC reference as a subscriber tracking plug-in.

Testing a NIC Resolution (C-Web Interface)

To test a NIC resolution:

1. Click **Diagnose > NIC > Resolve**.
2. Enter information as described in the Help text in the main pane, and click **OK**.

Related Topics ■ Configuring a NIC Scenario (C-Web Interface)

Stopping a NIC Host on a C-series Controller (C-Web Interface)

If you run the NIC in client/server mode, you can stop the NIC host independently of the NIC proxy.

To stop a NIC host:

1. Click **Manage > Disable**.
2. In the Component list in the main pane, select **NIC**, and click **OK**.

Related Topics ■ Restarting the NIC (C-Web Interface)

Restarting the NIC (C-Web Interface)

To restart a NIC host:

1. Click **Manage > Restart**.
2. In the Component list in the main pane, select **NIC**, and click **OK**.

Related Topics ■ Stopping a NIC Host on a C-series Controller (C-Web Interface)

Changing NIC Configurations (C-Web Interface)

If you change the type of NIC resolution that you use in your network (for example, from the OnePop configuration scenario to the OnePopAllRealms configuration scenario), delete any existing data and specify a static DN that identifies the DN for the new NIC configuration scenario; otherwise, the new NIC configuration may not perform resolutions correctly.

To change the type of NIC resolution that you use in your network:

1. Disable the NIC:
 - a. Click **Manage > Disable**.
 - b. In the Component list in the main pane, select **NIC**, and click **OK**.
2. Delete the NIC configuration data for the existing configuration scenario from the directory.
 - a. Click **Manage > Request > NIC > Clear > Scenario Data**.

The Scenario Data pane appears.

- b. In the **Slot** box, enter the number of the slot that contains the NIC scenario configuration (typically, slot 0), and click **OK**.
3. Restart the NIC host:

- a. Click **Manage > Restart**.
 - b. In the Component list in the main pane, select **NIC**, and click **OK**.
4. Configure the new NIC scenario.

Related Topics ■ Configuring a NIC Scenario (C-Web Interface)

Chapter 15

Obtaining Interface Configuration for OnePopStaticRouteIp or OnePopVrflp (C-Web Interface)

- Overview of the Network Publisher on page 103
- Before You Configure and Run the Network Publisher on page 104
- Configuring the Network Publisher (C-Web Interface) on page 104
- Configuring Information to Test the Network Publisher (C-Web Interface) on page 106
- Reviewing the Information Collected from a JUNOS Routing Platform (C-Web Interface) on page 106

Overview of the Network Publisher

The network publisher is a NIC component that connects to JUNOS routing platforms and collects information, such as information about system interfaces and VPNs, from IPv4 and IPv6 routing tables. After collecting the information, the network publisher stores this information in the Juniper Networks database for access by the NIC.

Use the network publisher to collect information from JUNOS routing tables for the following configuration scenarios:

- OnePopStaticRouteIp—Resolves an IP address for a subscriber whose traffic enters the network through a JUNOS interface to a reference for the SAE that manages the interface. The Threat Mitigation Application Portal demonstration application relies on this scenario.
- OnePopVrflp—Resolves an IP address for a subscriber whose traffic enters the network through a VPN configured on a JUNOS interface. This scenario provides support for multiple VPNs that have overlapping IP pools.

You run the network publisher whenever you want to get routing table information from one or more routers; the network publisher does not automatically update configuration information in the directory.

- Related Topics**
- NIC Document That Maps Subscriber IP Addresses to a JUNOS Interface
 - Overview of Files to Test Network Publisher

- Before You Configure and Run the Network Publisher
- Configuration Statements for the Network Publisher

Before You Configure and Run the Network Publisher

Before you configure and run the network publisher:

- Verify the version of the JUNOS software that is running on each JUNOS routing platform.

Typically, all the JUNOS routing platforms should run the same version of the JUNOS software.

- Verify that the C-series Controller can connect to the SAE-managed JUNOS routing platforms.
- Make sure that an SSH (recommended) or a Telnet service is enabled on each router from which the network publisher is to collect interface information.

When you run the network publisher, it connects to a number of JUNOS routing platforms through the configured protocol.

- Identify the routing tables and elements in the routing tables from which you want the network publisher to collect information. Which tables and elements you select depends on the application to use the NIC OnePopStaticRouteIp or the OnePopVrflp configuration scenario.
- Before you run the network publisher, make sure that the NIC is enabled.

Related Topics

- Overview of the Network Publisher
- Configuration Statements for the Network Publisher
- Configuring the Network Publisher
- Configuring the Network Publisher (C-Web Interface)
- Starting the NIC (SRC CLI)

Configuring the Network Publisher (C-Web Interface)

Before you configure and run the network publisher, see Before You Configure and Run the Network Publisher.

To configure the network publisher:

1. Click **Configure**, expand **Slot**, expand the slot for which you want to configure the network publisher, and then click **Network Publisher**.
2. Under Network Publisher, click **Directory**.

The Directory pane appears.

3. In the main pane, review the configuration and make changes as needed.
4. Click logger entries, and configure logging as you would for any component.

5. Click **Routers**, and in the Main pane, specify the release number of the JUNOS software.
6. Under Routers, click **Authentication**.

The Authentication pane appears.

7. Enter authentication properties as described in the Help text in the Main pane, and click **Apply**.
8. Under Routers, click **Select**.

The Select pane appears.

9. Define the routing tables and elements in those routing tables from which the network publisher collects information.
10. (Optional) Configure a specific router from which the network publisher collects routing table information. The network publisher uses the router-specific properties for specified routers, and applies the general routers properties to all other routers.
 - a. In the Routers pane, select **Router** in the Create new list.
 - b. Type a name for the new router in the dialog box, and click **OK**.

The router name appears in the side pane and the Routers pane.

- c. Enter router properties as described in the Help text in the Main pane, and click **Apply**.
- d. Under the router, click **Authentication**.

The Authentication pane appears.

- e. Enter authentication properties as described in the Help text in the Main pane, and click **Apply**.
- f. Under the router, click **Select**.

The Select pane appears.

- g. Define the routing tables and elements in those routing tables from which the network publisher collects information.

After you configure the network publisher, run it to collect routing table information.

- Related Topics**
- Overview of the Network Publisher
 - Running the Network Publisher

Configuring Information to Test the Network Publisher (C-Web Interface)

You can use an input file to verify that the network publisher is collecting information as configured or to set up a demonstration for an application.

To configure the network publisher to use an input file:

- Click **Configure**, expand **Slot**, expand the slot for which you want to configure the network publisher, and then expand **Network Publisher > Routers > Test Mode**.

Or

Click **Configure**, expand **Slot**, expand the slot for which you want to configure the network publisher, and then expand **Network Publisher > Routers > *specific-router* > Test Mode**.

The Test Mode pane appears.

- Select **Enable Input File**.

Related Topics

- Overview of the Network Publisher
- Troubleshooting Network Publisher Operations

Reviewing the Information Collected from a JUNOS Routing Platform (C-Web Interface)

Purpose Review information that the network publisher collects from a JUNOS routing platform.

Action To configure the network publisher to use an input file:

- Click **Configure**, expand **Slot**, expand the slot for which you want to configure the network publisher, and then expand **Network Publisher > Routers > Test Mode**.

Or

Click **Configure**, expand **Slot**, expand the slot for which you want to configure the network publisher, and then expand **Network Publisher > Routers > *specific-router* > Test Mode**.

The Test Mode pane appears.

- Select **Enable Output File**.
- Run the network publisher.

See Running the Network Publisher.

Related Topics

- Overview of the Network Publisher
- Troubleshooting Network Publisher Operations

Chapter 16

Using the C-Web Interface to Configure SRC Applications to Communicate with an SAE

You can use the C-Web interface to configure SRC applications to communicate with network information collector (NIC) hosts. This chapter describes how to configure a NIC proxy from the C-Web interface that runs on a C-series Controller. Topics include:

- Before You Configure a NIC Proxy on page 107
- Configuring a NIC Proxy with the C-Web Interface on page 108
- Configuring NIC Test Data (C-Web Interface) on page 109
- Examples: Key Values for NIC Bindings on page 110

Before You Configure a NIC Proxy

Before you configure a NIC proxy, you should have a good understanding of:

- NIC resolution
- NIC data types
- How NIC proxies work

See Locating Subscriber Management Information, Overview of the NIC Resolution Process, and Overview of NIC Proxy Configuration.



NOTE: You cannot configure a local NIC host when the NIC is running on a C-series Controller.

The values that you configure for a NIC proxy depend on the particular application; for example, you must specify the type of data used for the key and the type of data used for the value for each application.

Before you configure a NIC proxy for an application, obtain the following information from the system manager who maintains the NIC configuration for NIC hosts:

- The name of the resolver that the application uses.
- The type of key the application will provide to the NIC host.
- The type of value the NIC host is to return.
- Whether or not the application will use a local NIC host.
- If the application does not use a local NIC host:
 - The size of the NIC proxy cache.
 - The groups to be listed for NIC host selection. These groups provide NIC replication.

Configuring a NIC Proxy with the C-Web Interface

To have an application communicate with the NIC, you configure the type of resolution used by a NIC proxy.

To configure resolution information for a NIC proxy.

1. Click **Configure**, expand **Shared > SAE**, and then click **Configuration**.

The Configuration pane appears.

2. From the Create new list, select **NIC Proxy Configuration**. Type a name for the new NIC proxy in the dialog box, and click **OK**.

The new NIC proxy configuration appears in the side pane.

3. Expand the NIC proxy configuration.
4. To configure resolution information, in the side pane click **Resolution**.

The Resolution pane appears.

5. Click **Create**, enter information as described in the Help text, and click **Apply**.
6. To optimize resolution performance, in the side pane click **Cache**.

The Cache pane appears.

The cache options are available at the Advanced and Expert editing levels.

7. Click **Create**, enter information as described in the Help text, and click **Apply**.
8. To keep the NIC highly available, configure NIC host selection, and define how the NIC proxy handles NIC hosts to which it cannot connect.

The NIC Host Selection options are available at the Advanced and Expert editing levels.

- a. In the side pane, click **NIC Host Selection**.

The NIC Host Selection pane appears.

- b. Click **Create**, enter information as described in the Help text, and then click **Apply**.

- c. Expand **NIC Host Selection**, and click **Blacklisting**.

The Blacklisting pane appears.

- d. Click **Create**, enter information as described in the Help text, and click **Apply**.

- Related Topics**
- Changing NIC Configurations (SRC CLI)
 - Configuring NIC Test Data (C-Web Interface)

Configuring NIC Test Data (C-Web Interface)

To test a resolution without NIC, you can configure a NIC proxy stub to take the place of the NIC. The NIC proxy stub comprises a set of explicit mappings of data keys and values in the NIC proxy configuration. When the SAE (or another SRC component configured to use a NIC proxy stub) passes a specified key to the NIC proxy stub, the NIC proxy stub returns the corresponding value. When you use a NIC proxy stub, no NIC infrastructure is required.

For example, you can specify a subscriber's IP address that is associated with a particular SAE. When the SRC component passes this IP address to the NIC proxy stub, the NIC proxy stub returns the corresponding SAE.

To use the NIC proxy stub for the SAE:

1. Click **Configure**, and expand **Shared > SAE**, and then click **Configuration**.

The Configuration pane appears.

2. From the Create new list, select **NIC Proxy Configuration**. Type a name for the new NIC proxy in the dialog box, and click **OK**.

The new NIC proxy configuration appears in the side pane.

3. In the side pane, expand the new NIC proxy configuration, and click **Test NIC Bindings**.

The Test NIC Bindings pane appears.

4. Click **Create**, select the **Use Test Bindings** check box, and then click **Apply**.
5. In the side pane, expand **Test NIC Bindings**, and click **Key Values**.
6. From the Create new list, select Key Values. Type a name in the dialog box for the key that indicates the NIC data value for the proxy, and click **OK**.

The Key Values *name* pane appears in the side pane and in the Key Values pane.

7. Enter a value for the key that specifies a value for the NIC data type.
8. Click **Apply**.

Examples: Key Values for NIC Bindings

To set up a login name-to-IP mapping for login name `jane@virneo.com` to the IP address `192.0.2.30`:

1. In the side pane, expand the new NIC proxy configuration, and click **Test NIC Bindings**.

The Test NIC Bindings pane appears.

2. Click **Create**, select the **Use Test Bindings** check box, and then click **Apply**.
3. In the side pane, expand **Test NIC Bindings**, and click **Key Values**.
4. From the Create new list, select **Key Values**. Type the IP address **192.0.2.30** in the dialog box, and click **OK**.

The Key Values pane appears.

5. In the Value box, enter the value `jane@virneo.com`.
6. Click **Apply**.

To set up an IP-to-SAE ID mapping for IP address `190.0.2.30` to an SAE ID identified by the URL for the CORBA IOR `corbaloc::10.227.7.145:8801/SAE`:

1. In the side pane, expand the new NIC proxy configuration, and click **Test NIC Bindings**.

The Test NIC Bindings pane appears.

2. Click **Create**, select the **Use Test Bindings** check box, and click **Apply**.
3. In the side pane, expand **Test NIC Bindings**, and click **Key Values**.
4. From the Create new list, select **Key Values**. Type the IP address **192.0.2.30** in the dialog box, and click **OK**.



NOTE: The SAE writes the value of the CORBA IOR to the `var/run` directory. The IP address in the corbaloc URL can be adjusted to the IP address or DNS name of the SAE.

You can use the key **ANY-KEY** to match any key for any key type. For example, if you want all IP addresses to resolve to the same SAE, type **ANY-KEY** for the name in the Key Values box.

The Key Values pane appears.

5. In the Value box, enter the value `corbaloc::10.20.7.145:8801/SAE`.
6. Click **Apply**.

Related Topics ■ Configuring a NIC Proxy with the C-Web Interface

Chapter 17

Configuring Admission Control (C-Web Interface)

- Configuring SRC-ACP on page 111
- Configuring Local Properties for SRC-ACP on page 112
- Configuring the SAE for SRC-ACP (C-Web Interface) on page 113
- Configuring SRC-ACP Properties on page 114
- Configuring SRC-ACP to Manage the Edge Network on page 118
- Configuring SRC-ACP to Manage the Backbone Network on page 121
- Configuring Action Congestion Points on page 121
- Configuring Congestion Points for Services on page 121
- Configuring Congestion Points in the Directory on page 122
- Assigning Interfaces to Congestion Points on page 122
- Configuring Congestion Point Classification (C-Web Interface) on page 122
- Defining a Congestion Point Profile on page 123

Configuring SRC-ACP

To use SRC-ACP in the SRC network, you must perform some configuration. For information about these configuration procedures, see:

1. (Optional) Configure a grouped configuration for SRC-ACP.
2. Configuring Local Properties for SRC-ACP
3. Configuring the SAE for SRC-ACP (C-Web Interface)
4. Configuring SRC-ACP Properties
5. (Edge and dual mode only) Configuring SRC-ACP to Manage the Edge Network
6. (Backbone and dual mode only) Configuring SRC-ACP to Manage the Backbone Network

You can automate and scale the configuration of congestion points using congestion point classification. For more information, see [Configuring NIC Test Data \(SRC CLI\)](#) and [Configuring Congestion Point Classification \(C-Web Interface\)](#).

Configuring Local Properties for SRC-ACP

To configure the local properties for SRC-ACP:

1. Configuring Basic Local Properties for SRC-ACP on page 112
2. Configuring Initial Properties for SRC-ACP on page 112
3. Configuring Directory Connection Properties for SRC-ACP on page 112
4. Configuring Initial Directory Eventing Properties for SRC-ACP on page 112

Configuring Basic Local Properties for SRC-ACP

To configure basic local properties:

1. Click **Configure > Slot > Slot:0 > ACP**.
2. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Initial Properties for SRC-ACP

To configure initial properties for SRC-ACP:

1. Click **Configure > Slot > Slot:0 > ACP > Initial**.
2. If desired, specify the properties for ACP as described in the Help text in the main pane, and click **Apply**.

Configuring Directory Connection Properties for SRC-ACP

To configure directory connection properties:

1. Click **Configure > Slot > Slot:0 > ACP > Initial > Directory Connection**.

The Directory Connection pane appears.

2. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Initial Directory Eventing Properties for SRC-ACP

To configure initial directory eventing properties:

1. Click **Configure > Slot > Slot:0 > ACP > Initial > Directory Eventing**.

The Directory Eventing pane appears.

2. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring the SAE for SRC-ACP (C-Web Interface)

To configure the SAE to recognize SRC-ACP by adding information about SRC-ACP to the SAE properties:

1. Configuring SRC-ACP as an External Plug-In on page 113
2. Configuring Event Publishers for SRC-ACP on page 113
3. Configuring the SAE to Monitor Interfaces for Congestion Points on page 113

Configuring SRC-ACP as an External Plug-In

To configure SRC-ACP as an external plug-in for the SAE:

1. Click **Configure > Shared > SAE**, and then expand the SAE group for which you want to configure a plug-in.

The Group pane appears.

2. From the side pane, expand **Configuration > Plug Ins**.

The Plug Ins pane appears.

3. In the Create new list, select **Name**.
4. Type a name for the new plug-in in the dialog box, and click **OK**.

The plug-in appears in the side pane and in the Plug In pane.

5. From the side pane, expand the new plug-in, and then click **External**.

The External pane appears.

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

Configuring Event Publishers for SRC-ACP

Configure the SAE to publish the following types of events to SRC-ACP:

- (Edge and dual mode only) Global subscriber tracking
- Global service authorization
- Global service tracking

Configuring the SAE to Monitor Interfaces for Congestion Points



NOTE: Configure this feature only if SRC-ACP is in backbone or dual mode.

The SAE uses a hosted internal plug-in to monitor the state of interfaces on a VR for backbone congestion points. If a subscriber tries to activate a service on an interface that is unavailable, the SAE denies the request. The plug-in also monitors the directory for new backbone congestion points.

When this plug-in initializes, it reads all the backbone services from the directory and generates a list of the DNs (network interfaces) of the backbone congestion points. The SAE sends interface tracking events, which contain the names of the interfaces, VRs, and routers to this plug-in. For this feature to work correctly, the interface, VR, and router must be configured (see Configuring Network Interfaces in the Directory).

To configure the ACP interface listener as an internal plug-in for the SAE:

1. Click **Configure > Shared > SAE**, and then expand the SAE group for which you want to configure RADIUS plug-ins.

The Group pane appears.

2. From the side pane, expand **Configuration > Plug-Ins**.
3. Expand the plug-in that you created for file accounting, and then click **ACP Interface Listener**.

The ACP Interface Listener pane appears.

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

Configuring SRC-ACP Properties

- Configuring Logging Destinations for SRC-ACP on page 114
- Configuring SRC-ACP Operation on page 115
- Configuring CORBA Interfaces on page 117
- Configuring SRC-ACP Redundancy on page 118
- Configuring Connections to the Subscribers' Directory on page 118
- Configuring Connections to the Services' Directory on page 118
- Configuring SRC-ACP Scripts and Classification on page 118

Configuring Logging Destinations for SRC-ACP

SRC-ACP groups contain default file logging configurations. You can modify an existing configuration or create a new one.

To modify logging destinations that store log messages in a file:

1. Click **Configure > Shared > ACP**, expand the group for which you want to configure logging and expand **Configuration**.

Several Logger:file configurations appear.

2. In the Create new list, select **Logger**.
3. Type a name for the new logger in the dialog box, and click **OK**.

The logger appears in the side pane.

4. Select the configuration that you want to modify, enter information as described in the Help text in the main pane, and click **Apply**.

To create logging destinations to store log messages in a file:

1. Click **Configure > Shared > ACP**, and expand the group for which you want to configure logging destinations and expand **Configuration**.
2. From the Create new list, select **Logger**.
3. Type a name for the new logging configuration, and click **OK**.

The logger appears in the side pane.

4. Expand the new logging configuration, select **File**, and enter information as described in the Help text in the main pane, and click **Apply**.

You can configure logging destinations to send log messages to the system logging facility. SRC-ACP groups contain default system logging configurations. You can modify an existing configuration or create a new one.

To modify an existing system logging configuration:

1. Click **Configure > Shared > ACP**, expand the group for which you want to modify an existing configuration, and expand **Configuration**.

Several Logger:syslog configurations appear.

2. Select the configuration that you want to modify, enter information as described in the Help text in the main pane, and click **Apply**.

To create a configuration that causes logging destinations to send log messages to the system logging facility:

1. Click **Configure > Shared > ACP**, and expand the group for which you want to modify an existing configuration.
2. In the Create new list, select **Logger**. Type a name for the new logging configuration, and click **OK**.

The logger appears in the side pane.

3. Expand the new logging configuration, select **Syslog**, and enter information as described in the Help text in the main pane, and click **Apply**.

Configuring SRC-ACP Operation

To configure SRC-ACP operation:

1. Click **Configure > Shared > ACP**, expand the group for which you want to modify an existing configuration, and expand **Configuration**.
2. Click **ACP Options**, enter information as described in the Help text in the main pane, and click **Create**.

3. In the Remote Update Database Index Keys box, specify the values to look for in the configuration data. Specifying index keys can improve performance by filtering the data.
 - The value is a list of attributes, separated by commas. An attribute is one of the following text strings:
 - accountingId—Value of directory attribute accountingUserId.
 - dhcpPacket—Content of the DHCP discover request.
 - hostname— Name of the host on which the SAE is installed.
 - ifIndex—SNMP index of the interface. This attribute is not supported on JUNOS routing platforms.
 - ifRadiusClass—RADIUS class attribute on the JUNOS interface. This attribute is not supported on JUNOS routing platforms.
 - ifSessionId—Identifier for RADIUS accounting on the JUNOS interface. This attribute is not supported on JUNOS routing platforms.
 - interfaceAlias—Alias of the interface; that is, the IP description in the interface configuration.
 - interfaceDescr—SNMP description of the interface.
 - interfaceName—Name of the interface.
 - loginName—Subscriber's login name.
 - nasInetAddress—IP address of the router; using a byte array instead of an integer.
 - nasPort—NAS port used by the router to identify the interface to RADIUS.
 - portId—Identifier of VLAN or virtual circuit. For a virtual circuit, use the format `<VPI> / <VCI>`. This attribute is not supported on JUNOS routing platforms.
 - `<VPI>` —Virtual path identifier
 - `<VCI>` —Virtual connection identifier
 - primaryUserName—PPP login name or the public DHCP username. This attribute is not supported on JUNOS routing platforms.
 - routerName—Name of the virtual router in the format `<virtualRouter> @ <router>`.
 - `<virtualRouter>` —Virtual router name
 - `<router>` —Router name
 - routerType—Type of router driver.
 - userInetAddress—IP address of the subscriber that uses a byte array instead of an integer.

- userMacAddress—MAC address of the DHCP subscriber. This attribute is not supported on JUNOS routing platforms.
 - userRadiusClass—RADIUS class attribute of the subscriber session for a service. This attribute can occur multiple times and can be returned by an authorization plug-in.
 - userType—Type of subscriber.
4. In the Interface Tracking Filter box, specify the interface tracking events that the SRC-ACP ignores.

The value is filter strings in the format of a list of < attribute > = < value > pairs. The filter strings can be contained within query operations.

- < attribute > —Name of an attribute for an interface tracking event.
- < value > —Filtering string of the following types:
 - *—Any value
 - Explicit string—Any value matching the specified string (not case-sensitive)
 - String containing an asterisk—Any value containing the specified string (not case-sensitive)
- To perform query operations on filter strings, you can use the following values in your filter strings:
 - ()—Match no objects.
 - (*)—Match all objects.
 - (& < filter > < filter > ...)—Performs logical AND operation on filter strings; true if all filter strings match.
 - (| < filter > < filter > ...)—Performs logical OR operation on filter strings; true if at least one filter string matches.
 - (! < filter >)—Performs logical NOT operation on filter string; true if the filter string does not match.

Configuring CORBA Interfaces

To configure CORBA interfaces:

1. Click **Configure > Shared > ACP > Configuration** , and then click **CORBA**.

The CORBA pane appears.

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

Configuring SRC-ACP Redundancy

To configure SRC-ACP redundancy and state synchronization with the SAE:

1. Click **Configure > Shared > ACP > Redundancy**.

The Redundancy pane appears.

2. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Connections to the Subscribers' Directory

To configure how SRC-ACP connects to the directory that stores subscriber information:

1. Click **Configure > Shared > ACP > LDAP**, and expand **Subscriber Data**.

The Subscriber Data pane appears.

2. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Connections to the Services' Directory

To configure how SRC-ACP connects to the directory that stores service information:

1. Click **Configure > Shared > ACP > LDAP**, and expand **Service Data**.

The Service Data pane appears.

2. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring SRC-ACP Scripts and Classification

To configure SRC-ACP scripts and classification:

1. Click **Configure > Shared > ACP > Configuration** and then expand **Scripts and Classification**.

The Scripts and Classification pane appears.

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

Configuring SRC-ACP to Manage the Edge Network

To configure SRC-ACP to manage the edge network, you must:

1. Configuring Network Interfaces in the Directory on page 119
2. Configuring Bandwidths for Subscribers (Edge Network) on page 119

3. Assigning Network Interfaces to Subscribers on page 120
4. Configuring Bandwidths for Services on page 120

Configuring Network Interfaces in the Directory

How you add network interfaces to the directory depends on the network type:

- Edge networks—Specify the network interfaces of the routers and the switches in the access network between subscribers and the SRC network.
- Backbone congestion points—Add only VRs and their interfaces.

To configure the network interfaces of the routers and the switches in the access network:

1. Click **Configure > Shared > Admission Control**, expand the desired device.
2. If the device does not exist, from the Create new list, select **Device**. Type a name for the new device in the dialog box, and click **OK**.

The Device pane appears.

3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Bandwidths for Subscribers (Edge Network)

You must configure bandwidths for subscribers that SRC-ACP manages in the edge region of the network.

If congestion points cannot be derived from network access information, you must provide the following information for each subscriber.

- Provisioned downstream bandwidth
- Provisioned upstream bandwidth
- Actual downstream bandwidth for the current subscriber session
- Actual upstream bandwidth for the current subscriber session
- List of DNs of interfaces associated with congestion points

For further information, see *SRC-PE Network Guide*.

To configure bandwidths for subscribers:

1. Click **Configure > Subscribers**.
2. In the side pane, expand the desired retailer, expand the desired subscriber folder, and expand the desired subscriber.

The Admission Control pane appears.

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

Assigning Network Interfaces to Subscribers

You must assign to the subscriber object interfaces (including the router interfaces) for all congestion points between the subscriber and the router.



NOTE: You must define the interface in the directory before you can assign it to a residential subscriber (see *Configuring Network Interfaces in the Directory*).

To assign an interface:

1. Click **Configure > Subscribers**.
2. In the side pane, expand the desired retailer, and then click the desired subscriber folder.

The Admission Control pane appears.

3. Enter information in the Congestion Points box as described in the Help text in the main pane, and click **Apply**.

Configuring Bandwidths for Services

Upstream and downstream bandwidths must be specified for services that SRC-ACP manages. You can obtain bandwidths for services in two ways:

- Provide static values through the directory.
- Allow the values to be provided through the SAE core API.

For example, a business partner may need to specify the required values for a particular piece of content through the SAE core API.

To configure values for services:

1. For global configuration, click **Configure > Services > Global** and expand **Service**.
2. For scope configuration, click **Configure > Services > Scope** and expand **Service**.
3. In the side pane, expand the desired service and click **Admission Control**.

The Admission Control pane appears.

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

Related Topics

- For more information about configuring residential subscribers, see *Adding Subscribers (SRC CLI)*.
- For more information about configuring services, see *Adding a Normal Service (SRC CLI)*.

Configuring SRC-ACP to Manage the Backbone Network

To configure SRC-ACP to manage the backbone network:

1. Configuring Network Interfaces in the Directory
2. (Optional) Configure an action congestion point.
3. Configure guaranteed bandwidths for services.
4. Assign network interfaces to services.
5. Create congestion points in the directory.
6. Assign interfaces to congestion points.

Related Topics ■ *SRC-PE Network Guide*

Configuring Action Congestion Points

You can define an application in a backbone congestion point so that SRC-ACP can execute it in a predefined manner. Backbone congestion points that are configured to run an application are called action congestion points. If you want to use an action congestion point to execute an application that requires real-time congestion point status, you must enable SRC-ACP state synchronization with the SAE.

Before you configure an action congestion point, make sure that you know the location of the application file.

To configure an action congestion point:

1. Click **Configure > Shared**, and expand **Service**.
2. In the side pane, expand the desired retailer, and then click the desired subscriber folder.

The Admission Control pane appears.

3. Enter information in the Congestion Points box as described in the Help text in the main pane, and click **Apply**.

Related Topics ■ *SRC-PE Network Guide*

Configuring Congestion Points for Services

You must assign a congestion point to each service that SRC-ACP manages.

To configure values for services:

1. For global configuration, click **Configure > Services > Global** and expand **Service**.
2. For scope configuration, click **Configure > Services > Scope** and expand **Service**.
3. **In the side pane, expand the desired service, and click Admission Control.**

The Admission Control pane appears.

4. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Congestion Points in the Directory

To configure individual backbone congestion points:

1. Click **Configure > Shared > Congestion Points**.

The Congestion Points pane appears.

2. In the Create new list, select **Profile**. Type a name for the new profile in the dialog box, and click **OK**.

The Congestion Point Profile screen appears.

3. Enter information as described in the Help text in the main pane, and click **Apply**.

Assigning Interfaces to Congestion Points

You must assign interfaces either to VRs or to individual services under the VRs. Services inherit interface assignments from the associated VR unless you assign an interface to the individual service. This network interface lists the DNS of interfaces associated with backbone congestion points.

To assign interfaces to congestion points:

1. Click **Configure > Shared > Congestion Points**.
2. In the side pane, expand the desired profile.

The Profile pane appears.

3. Enter information as described in the Help text in the main pane, and click **Apply**.

Related Topics ■ For more information about configuring services, see [Adding a Normal Service with the SRC CLI](#).

Configuring Congestion Point Classification (C-Web Interface)

Congestion point classification allows you to automate and scale the configuration of congestion points. SRC-ACP uses classification scripts to determine which congestion point to load for a subscriber. SRC-ACP can select the congestion point from congestion point profiles or subscriber profiles.

To configure congestion point classification scripts:

- [Configuring Targets and Criteria for Classification Scripts on page 123](#)
- [Configuring Classification Script Contents for Classification Scripts on page 123](#)

Configuring Targets and Criteria for Classification Scripts

To define a target and criteria for the congestion point classification script:

1. Click **Configure > Shared > ACP > Configuration > Scripts and Classification**.

The Scripts and Classification pane appears.

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

Configuring Classification Script Contents for Classification Scripts

To use the contents of a classification script to point to another object for the congestion point classification script:

1. Click **Configure > Shared > ACP**, expand the desired group, and click **Congestion Point Classifier**.

The Congestion Point Classifier pane appears.

2. In the Create new list, select **Rule**.
3. Type a name for the new rule, and click **OK**.
4. In the side pane, expand the new rule, enter information for the script as described in the Help text in the main pane, and click **Apply**.

Defining a Congestion Point Profile

You can create a congestion point profile that automatically performs congestion point classification. This profile supports only edge mode and dual mode for SRC-ACP.

To define a congestion point profile:

1. Click **Configure > Shared > Congestion Points**.

The Congestion Point Profile pane appears.

2. In the Create new list, select **Profile**. Type a name for the new profile in the dialog box, and click **OK**.

The Profile screen appears.

3. Enter information as described in the Help text in the main pane, and click **Apply**.

- Related Topics**
- Congestion Point Expressions
 - Classifying Interfaces (SRC CLI).

Part 5

Integrating Network Devices

- Configuring the JPS (C-Web Interface) on page 127
- Using JUNOSe Routers in the SRC Network (C-Web Interface) on page 137
- Using JUNOS Routing Platforms in the SRC Network (C-Web Interface) on page 149
- Adding Objects for CMTS Devices (C-Web Interface) on page 163
- Integrating Third-Party Network Devices into the SRC Network (C-Web Interface) on page 165

Chapter 18

Configuring the JPS (C-Web Interface)

- Configuring the JPS (C-Web Interface) on page 127
- Modifying the JPS Configuration (C-Web Interface) on page 128
- Configuring RKS Pairs (C-Web Interface) on page 129
- Modifying the Subscriber Configuration (C-Web Interface) on page 130
- Configuring Subscriber IP Pools as IP Address Ranges (C-Web Interface) on page 131
- Configuring Subscriber IP Pools as IP Subnets (C-Web Interface) on page 131
- Configuring the SAE to Interact with the JPS (C-Web Interface) on page 131
- Specifying Application Managers for the Policy Server (C-Web Interface) on page 132
- Specifying Application Manager Identifiers for Policy Servers (C-Web Interface) on page 132
- Adding Objects for Policy Servers to the Directory (C-Web Interface) on page 133
- Configuring Initialization Scripts (C-Web Interface) on page 133
- Enabling State Synchronization (C-Web Interface) on page 134
- Using the NIC Resolver in PCMM Environments on page 134
- Managing the JPS (C-Web Interface) on page 135

Configuring the JPS (C-Web Interface)

You can modify the JPS configuration, which includes configuring the logging destinations and connections to the JPS interfaces. Any configuration changes will be applied within 15 seconds.

You can configure the subscriber, which maps a subscriber address to the CMTS address.

The tasks to configure the JPS for a cable network environment are:

1. Modifying the JPS Configuration (C-Web Interface)
2. Modifying the Subscriber Configuration (C-Web Interface)

In addition to configuring the JPS, you might need to perform these tasks:

1. Configuring the SAE to Interact with the JPS (C-Web Interface) .

2. Using the NIC Resolver in PCMM Environments.

- Related Topics**
- Overview of the JPS.
 - Configuring the JPS

Modifying the JPS Configuration (C-Web Interface)

Tasks to modify the current JPS configuration are:

1. Configuring General Properties for the JPS (C-Web Interface) on page 128
2. Specifying a Policy Server Identifier in Messages (C-Web Interface) on page 128
3. Configuring Logging Destinations (C-Web Interface) on page 128
4. Specifying Connections to the Application Managers (C-Web Interface) on page 129
5. Specifying Connections to RKs (C-Web Interface) on page 129

Configuring General Properties for the JPS (C-Web Interface)

To configure general properties for the JPS:

1. Click **Configure**, and expand **Slot > Slot: 0**, and then click **JPS**.

The JPS pane appears.

2. Enter the information in the main pane as described in the Help text, and click **Apply**.

Specifying a Policy Server Identifier in Messages (C-Web Interface)

To configure a policy server identifier for the JPS:

1. Click **Configure**, expand **Slot > Slot: 0**, and then click **JPS**.

The JPS pane appears.

2. In the Policy Server ID box, enter a value as described in the Help text in the main pane.
3. Enter information in the remaining boxes as described in the Help text in the main pane, and click **Apply**.

Configuring Logging Destinations (C-Web Interface)

You can configure the logging destination to store messages in a file, or to a system logging facility (Syslog)

You can create or modify loggers. By default, the JPS has four logging destinations (log1, log2, log3, and log4).

Specifying Connections to the Application Managers (C-Web Interface)

This section describes how to configure the application manager-to-policy server interface (PKT-MM3) so that the policy server can communicate with application managers.

To configure the connections to the application managers:

1. Click **Configure**, expand **Slot > Slot: 0 > JPS**, and then click **AM Interface**.

The AM Interface pane appears.

2. Enter the information in the main pane as described in the Help text, and click **Apply**.

Specifying Connections to RKSs (C-Web Interface)

To configure the policy server-to-RKS interface (PKT-MM4) so that policy events can be sent to the RKS, you can configure RKS pairs and their associated application managers.

To configure the policy server-to-RKS interface:

1. Click **Configure**, expand **Slot > Slot: 0 > JPS**, and then click **RKS Interface**.

The RKS Interface pane appears.

2. Enter the information in the main pane as described in the Help text, and click **Apply**.

Configuring RKS Pairs (C-Web Interface)

- Configuring Connections for RKS Pairs (C-Web Interface) on page 129
- Configuring RKS Pairs for Associated Application Managers (C-Web Interface) on page 130
- Specifying Connections to CMTS Devices (C-Web Interface) on page 130

Configuring Connections for RKS Pairs (C-Web Interface)

By default, the JPS has four RKS pairs. All parameters that share the same RKS pair name configure the connection to that RKS pair. Any configured RKS pair can be used as the value for the default RKS pair or the RKS pair associated with a specific application manager.



NOTE: When running more than one JPS in a group to provide redundancy, all the JPSs in that group must have the same RKS pair configuration (including the default RKS pair and any configured RKS pairs associated with a specific application manager).

To configure the RKS pair:

1. Click **Configure**, and expand **Slot > Slot: 0 > JPS > RKS Interface**.
2. Click the specified RKS pair (for example, pair 1).

The RKS Pair:pair 1 pane appears.

3. Enter the information in the main pane as described in the Help text, and click **Apply**.

Configuring RKS Pairs for Associated Application Managers (C-Web Interface)

By default, the JPS has four associated application managers. All parameters that share the same application manager name configure the RKS pair to which events associated with a specific application manager are sent.

To configure the associated application manager:

1. Click **Configure**, and expand **Slot > Slot: 0 > JPS > RKS Interface**.
2. Click the specified AM (for example, AM:1).

The RKS Interface/AM:1 pane appears.

3. Enter the information in the main pane as described in the Help text, and click **Apply**.

Specifying Connections to CMTS Devices (C-Web Interface)

To configure the policy server-to-CMTS interface (PKT-MM2) so that the policy server can communicate with CMTS devices:

1. Click **Configure**, expand **Slot > Slot: 0 > JPS**, and then click **CMTS Interface**.

The CMTS Interface pane appears.

2. Enter the information in the main pane as described in the Help text, and click **Apply**.

Modifying the Subscriber Configuration (C-Web Interface)

To locate the CMTS device associated with a subscriber, the JPS maps the subscriber IP address in a message to the CMTS IP address to which the message must be delivered. This mapping specifies the subscriber IP pools associated with CMTS devices.

The tasks to configure a CMTS device to which the JPS can connect and the pools of subscriber IP addresses that are managed by that CMTS device are:

1. Configuring Subscriber IP Pools as IP Address Ranges (C-Web Interface)
2. Configuring Subscriber IP Pools as IP Subnets (C-Web Interface)

Configuring Subscriber IP Pools as IP Address Ranges (C-Web Interface)

To configure subscriber IP pools that are managed by the CMTS device as IP address ranges:

1. Click **Configure**, expand **Slot > Slot: 0 > JPS**, and then click **CMTS Registry**.

The CMTS Registry pane appears.

2. From the Create new list, select **CMTS**.
3. In the dialog box, type an IPv4 or IPv6 address for the new CMTS, and click **OK**.

The CMTS: *< ip address >* pane appears.

4. From the Create new list, select **Range Pool**.
5. In the dialog box, enter a number for the new Range Pool, and click **OK**.

The Range Pool: *< number >* pane appears.

6. Enter the information in the main pane as described in the Help text, and click **Apply**.

Configuring Subscriber IP Pools as IP Subnets (C-Web Interface)

To configure subscriber IP pools that are managed by the CMTS device as IP subnets:

1. Click **Configure**, expand **Slot > Slot: 0 > JPS**, and then click **CMTS Registry**.

The CMTS Registry pane appears.

2. From the Create new list, select **CMTS**.
3. In the dialog box, type an IPv4 or IPv6 address for the new CMTS, and click **OK**.

The CMTS: *< ip address >* pane appears.

4. From the Create new list, select **Subnet Pool**.
5. In the dialog box, enter a network IP address/mask for the new Subnet Pool, and click **OK**.

The Subnet Pool: *< ip address/mask >* pane appears.

6. Enter the information in the main pane as described in the Help text, and click **Apply**.

Configuring the SAE to Interact with the JPS (C-Web Interface)

You must configure the SAE as an application manager to allow it to interact with PCMM-compliant policy servers. The policy server acts as a policy decision point that manages the relationships between application managers and CMTS devices. Policy servers that manage the same group of CMTS devices are grouped together and are simultaneously active. The policy server group provides a way for the SAE to communicate with any CMTS device that is managed by a policy server in the policy

server group. To provide redundancy, the SAEs are grouped in an SAE community that connects to a policy server group. Only one of the SAEs in the SAE community is active. The active SAE establishes connections to all the policy servers in the policy server group. The active SAE will fail over to a redundant SAE only when it loses the connection to all the policy servers in the policy server group. State synchronization enables the SAE to synchronize its state with all the CMTS devices connected to a policy server group.

The tasks to configure the SAE as an application manager are:

- Specifying Application Managers for the Policy Server (C-Web Interface)
- Specifying Application Manager Identifiers for Policy Servers (C-Web Interface)
- Adding Objects for Policy Servers to the Directory (C-Web Interface)
- Configuring Initialization Scripts (C-Web Interface)
- Enabling State Synchronization (C-Web Interface)

Specifying Application Managers for the Policy Server (C-Web Interface)

To specify the SAE community that connects to a policy server group, you need to add an application manager group object to the directory.

To specify the application manager for the policy server:

1. Click **Configure**, expand **Shared**, and then click **Network**.

The Network pane appears.

2. From the Create new list, select **Application Manager Group**.
3. In the dialog box, enter a name for the new Application Manager Group, and click **OK**.

The Application Manager Group: <name> pane appears.

4. Enter the information in the main pane as described in the Help text, and click **Apply**.

- Related Topics**
- Adding Objects for Policy Servers to the Directory (C-Web Interface)
 - Configuring Initialization Scripts (C-Web Interface).

Specifying Application Manager Identifiers for Policy Servers (C-Web Interface)

The application manager identifier (AMID) identifies the application manager (such as the SAE) in messages sent to and from the policy server. The SAE constructs the AMID value by concatenating two fields: Application Manager Tag and Application Type.

The Application Manager Tag value is obtained from the specification of application managers for policy servers.

The Application Type value is obtained during service activation from the specification of the PCMM Application Type value when you configure normal services.

Related Topics ■ Specifying Application Manager Identifiers for Policy Servers (C-Web Interface)

Adding Objects for Policy Servers to the Directory (C-Web Interface)

To communicate with policy servers, the SAE creates and manages pseudointerfaces that it associates with a policy decision point object in the directory. Each policy server in the SRC network must appear in the directory as a policy decision point object.

To add a policy server to the directory:

1. Click **Configure**, expand **Shared**, and then click **Network**.

The Network pane appears.

2. From the Create new list, select **Policy Decision Point**.
3. In the dialog box, enter a name for the new Policy Decision Point, and click **OK**.

The Policy Decision Point: <name> pane appears.

4. Enter the information in the main pane as described in the Help text, and click **Apply**.

Related Topics ■ Specifying Application Manager Identifiers for Policy Servers (C-Web Interface)

Configuring Initialization Scripts (C-Web Interface)

When the SAE establishes a connection with a policy server, it runs an initialization script to customize the setup of the connection.

To configure initialization scripts for the SAE:

1. Click **Configure**, expand **Shared > SAE > Configuration > Driver**, and then click **Scripts**.

The Scripts pane appears.

2. Click the **Create** button.
3. In the Pcmbox, enter the information as described in the Help text in the main pane, and click **Apply**. For the JPS, we recommend setting this value to **amlorPublisher**.

The script is run when the connection between a policy server and the SAE is established and again when the connection is dropped.

Enabling State Synchronization (C-Web Interface)

State synchronization is achieved when the SAE is configured to communicate with the policy server over the COPS connection.

To enable state synchronization with policy servers:

1. Click **Configure**, expand **Shared > SAE > Configuration > Driver**, and then click **Pcmm**.

The Pcmm pane appears.

2. Click the **Create** button.
3. Clear the **Disable Full Sync** checkbox to enable full synchronization.
4. If the policy server or devices do not support policies defined in PCMM-I03, make sure the **Disable PCMM I03** checkbox is selected and that the correct value is displayed in the **Session Recovery Retry Interval** box. Refer to the Help text in the main pane as needed.
5. Click **Apply**.

Using the NIC Resolver in PCMM Environments

If you are using the NIC to map the subscriber IP address to the SAE, you need to configure a NIC host. The NIC system uses IP address pools to map IP addresses to SAEs. You configure the local address pools in the application manager configuration for a policy server group. These pools are published in the NIC. The NIC maps subscriber IP addresses in requests received through the portal or Advanced Services Gateway to the policy server group that currently manages that CMTS device.

The OnePopPcmm sample configuration data supports this scenario for a PCMM environment in which you use the assigned IP subscriber method to log in subscribers and in which you use the NIC to determine the subscriber's SAE. The OnePopPcmm configuration supports one point of presence (POP). NIC replication can be used to provide high availability. The realm for this configuration accommodates the situation in which IP pools are configured locally on each application manager group object.

The resolution process takes a subscriber's IP address as the key and returns a reference to the SAE managing this subscriber as the value.

The following agents collect information for resolvers in this realm:

- Directory agent PoolVr collects and publishes information about the mappings of IP pools to the policy server group.
- Directory agent VrSaeld collects and publishes information about the mappings of policy server groups to SAEs.

Related Topics ■ Specifying Application Manager Identifiers for Policy Servers (C-Web Interface)

Managing the JPS (C-Web Interface)

After you have installed the JPS and applied the local configuration of the JPS, you can perform these tasks:

- Starting the JPS (C-Web Interface) on page 135
- Restarting the JPS (C-Web Interface) on page 135
- Stopping the JPS (C-Web Interface) on page 136
- Displaying JPS Status (C-Web Interface) on page 136

Starting the JPS (C-Web Interface)

You must start the JPS when you install the JPS without rebooting the JPS host.

To start the JPS:

1. Click **Manage > Enable**.

The Enable pane appears.

2. From the **Component** list, select **JPS**, and click **OK**.

The system responds with a start message. If the JPS is already running, the system responds with a warning message.

Related Topics ■ Restarting the JPS (C-Web Interface)
 ■ Stopping the JPS (C-Web Interface)
 ■ Monitoring the SDX SNMP Agent

Restarting the JPS (C-Web Interface)

To restart the JPS:

1. Click **Manage > Restart**.

The Restart pane appears.

2. From the **Component** list, select **JPS**, and click **OK**.

The system responds with a start message. If the JPS is already running, the system responds with a shutdown message and then a start message.

Related Topics ■ Starting the JPS (C-Web Interface)
 ■ Stopping the JPS (C-Web Interface)
 ■ Displaying JPS Status (C-Web Interface)

Stopping the JPS (C-Web Interface)

To stop the JPS:

1. Click **Manage > Disable**.

The Disable pane appears.

2. From the **Component** list, select **JPS**, and click **OK**.

The system responds with a shutdown message. If the JPS is not running when you issue the command, the system responds with a status message.

- Related Topics**
- Starting the JPS (C-Web Interface)
 - Restarting the JPS (C-Web Interface)
 - Monitoring the SDX SNMP Agent

Displaying JPS Status (C-Web Interface)

To display the JPS status:

1. Click **Monitor > Component**.

The Installed Components pane appears.

2. Locate jps in the Name column. The Version and Status columns display the JPS status.

- Related Topics**
- Starting the JPS (C-Web Interface)
 - Restarting the JPS (C-Web Interface)
 - Stopping the JPS (C-Web Interface)
 - Modifying the JPS Configuration (C-Web Interface)
 - *SRC-PE Monitoring and Troubleshooting Guide*

Chapter 19

Using JUNOSe Routers in the SRC Network (C-Web Interface)

This chapter describes how to use the C-Web interface to set up the SRC software and how to set up a JUNOSe router so that the router can be used in the SRC network. It also shows how to monitor the interactions between the SAE and the JUNOSe router and how to troubleshoot SRC problems on the router.

Topics in this chapter include:

- COPS Connection Between JUNOSe Routers and the SAE on page 137
- Adding JUNOSe Routers and Virtual Routers (C-Web Interface) on page 138
- Configuring the SAE to Manage JUNOSe Routers (C-Web Interface) on page 139
- Using SNMP to Retrieve Information from JUNOSe Routers on page 140
- Specifying JUNOSe Router Initialization Scripts on the SAE (C-Web Interface) on page 141
- Developing Router Initialization Scripts for JUNOSe Routers, JUNOS Routing Platforms, and Network Devices on page 159
- Accessing the Router CLI on page 144
- Starting the SRC Client on a JUNOSe Router on page 144
- Stopping the SRC Client on a JUNOSe Router on page 145
- Monitoring Interactions Between the SAE and the JUNOSe Router on page 145
- Troubleshooting Problems with Managing JUNOSe Routers on page 146
- Viewing the State of JUNOSe Device Drivers (C-Web Interface) on page 147
- Viewing Statistics for Specific JUNOSe Device Drivers (C-Web Interface) on page 147
- Viewing Statistics for All JUNOSe Device Drivers (C-Web Interface) on page 147

COPS Connection Between JUNOSe Routers and the SAE

Configuring the SRC client on a JUNOSe router opens a Common Open Policy Service (COPS) protocol layer connection to the SAE. When the SRC client software establishes a TCP/IP connection to the SAE, the SAE starts to manage the JUNOSe router. Subsequently, the SRC client sends configuration changes made on the JUNOSe router to the SAE, and the SAE updates SRC configurations for services and policies accordingly.

The SAE supports two versions of COPS:

- COPS usage for policy provisioning (COPS-PR)
- COPS External Data Representation Standard (COPS-XDR)

The version of COPS that you use depends on the version of COPS that your JUNOSe router supports. When you set up your JUNOSe router to work with the SAE, you enable either COPS-PR mode or COPS-XDR mode.

Highly Available Connections to JUNOSe Routers

JUNOSe routers maintain state information, a feature that allows an active, managing SAE to reconnect to a JUNOSe router without performing a data resynchronization in the following instances:

- The network connection between the SAE and the JUNOSe router is disrupted, and the router reconnects to the SAE
- For JUNOSe routers with high availability configured, when the secondary SRP module takes control from a failed SRP it can reconnect to the SAE

Adding JUNOSe Routers and Virtual Routers (C-Web Interface)

The SAE uses router and virtual router objects to manage interfaces on JUNOSe virtual routers. Each JUNOSe router in the SRC network and its virtual routers (VRs) must have a configuration.

There are several ways to add routers:

1. Detecting Operative JUNOSe Routers and Virtual Routers and Adding Them to the Network on page 138
2. Adding JUNOSe Routers Individually on page 138
3. Adding Virtual Routers Individually on page 139

Detecting Operative JUNOSe Routers and Virtual Routers and Adding Them to the Network

If you add a router using the discover network feature, the software adds the IP address of the first SNMP agent on the router to respond to the discover request.

To add routers and JUNOSe VRs that are currently operative and have an operating SNMP agent:

1. Click **Manage > Request > Network > Discovery**.
2. Enter information as described in the Help text in the main pane, and click **Apply**.

Adding JUNOSe Routers Individually

To add a router:

1. Click **Configure**, expand **Shared**, and then click **Network**.

The Shared Network pane appears.

2. From the Create new list, select **Device**.
3. Type a name for the new device in the dialog box, and click **OK**.

The Device pane appears.

4. From the Device Type list, select **JUNOSe**.
5. Enter information as described in the Help text in the main pane, and click **Apply**.

Adding Virtual Routers Individually

To add a virtual router to an existing router:

1. Click **Configure**, expand **Shared > Network**, and then click a JUNOSe router.

The Device pane appears.

2. From the Create new list, select **Virtual Router**.
3. Type a name for the new device in the dialog box, and click **OK**.

The Virtual Router pane appears.

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

Configuring the SAE to Manage JUNOSe Routers (C-Web Interface)

To set up the SAE to manage JUNOSe routers, configure a router driver that specifies a COPS server that can accept COPS connections from the COPS client in JUNOSe routers.

To configure the SAE to manage JUNOSe routers:

1. Click **Configure**, expand **Shared > SAE > Configuration > Driver**, and then click **JUNOSe**.

The JUNOSe pane appears.

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

Using SNMP to Retrieve Information from JUNOSe Routers

You can use SNMP to retrieve information for the SRC software from JUNOSe routers. Topics include:

- How SNMP Obtains Information From Routers for the SRC Software on page 140
- Configuring the SNMP Server on the JUNOSe Router on page 140
- Configuring Global SNMP Communities in the SRC Software (C-Web Interface) on page 141

How SNMP Obtains Information From Routers for the SRC Software

Some scripts in the SRC software use SNMP to get information from the router. For example, the **poolPublisher** router initialization script uses SNMP to read the IP pools.

- On the router, you can configure access to the router's SNMP server. See *Configuring the SNMP Server on the JUNOSe Router*.
- On the SAE, you can configure global default SNMP communities that are used for read and write access to the router.
- You can specify SNMP communities for each virtual router. We recommend that you specify communities for each virtual router instead of configuring global communities. See *Adding JUNOSe Routers and Virtual Routers with the CLI*.

Configuring the SNMP Server on the JUNOSe Router

Access to the SNMP server on the router by an SNMP client is governed by a proprietary SNMP community table. This table identifies communities that have read-only, read-write, or administrative permission to the SNMP Management Information Base (MIB) stored on a particular server.

When an SNMP server receives a request, the server extracts the client's IP address and the community name. The SNMP server searches the community table for a matching community.

- If a match is found, its access list name is used to validate the IP address.
 - If the access list name is null, the IP address is accepted.
 - If an invalid IP address results, an SNMP authentication error is sent to the SNMP client.
- If a match is not found, an SNMP authentication error results.

To configure the SNMP agent on the JUNOSe router:

1. Switch to the virtual router for which you want to create an SRC client.

```
host1#(config)virtual-router <vrName>
```

2. Enable the SNMP agent.

```
host1:<vrName>#(config)snmp-server
```

3. Configure at least one authorized SNMP read-write community (SNMPv1/v2c), which provides SNMP client access.

```
host1:<vrName>(config)#snmp-server community boston rw
```

4. (Optional) Configure a read-only community.
5. host1: < vrName > #(config)snmp-server public ro

Configuring Global SNMP Communities in the SRC Software (C-Web Interface)

You can configure global default SNMP communities that are used if a VR does not exist on the router or if the community strings have not been configured for the VR.

To configure global default SNMP communities:

1. Click **Configure**, expand **Shared > SAE > Configuration > Driver**, and then click **SNMP**.

The SNMP pane appears.

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

Specifying JUNOSe Router Initialization Scripts on the SAE (C-Web Interface)

To configure router initialization scripts for JUNOSe routers:

1. Click **Configure**, expand **Shared > SAE > Configuration > Driver**, and then click **Scripts**.

The Scripts pane appears.

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

Developing Router Initialization Scripts for JUNOSe Routers, JUNOS Routing Platforms, and Network Devices

When the SAE establishes a connection with a router or network device, it can run an initialization script to customize the setup of the connection. These initialization scripts are run when the connection between a router or network device and the SAE is established and again when the connection is dropped.

We provide the `IorPublisher` script in the `/opt/UMC/sae/lib` folder. The `IorPublisher` script publishes the interoperable object reference (IOR) of the SAE in the directory so that a NIC can associate a router with an SAE.

For JUNOSe VRs that supply IP addresses from a local pool, a router initialization script is provided that identifies which VR supplies each IP pool and writes the

information to the configuration. The SAE runs the script only when a COPS connection is established to the JUNOS router. Consequently, if you modify information about IP pools on a VR after the COPS connection is established, the SAE will not automatically register the changes, and you must update the configuration.

Table 7 on page 159 describes the router initialization scripts that we provide with the SRC software in the `/opt/UMC/sae/lib` folder.

Table 7: Router Initialization Scripts

Script Name	Function	When to Use Script
iorPublisher	Publishes the IOR of the SAE into an internal part of the shared configuration so that a NIC can associate a router with an SAE.	Use with JUNOS routers that do not supply IP addresses from local pools, and with JUNOS routing platforms. Use with all JUNOS routing platforms. Use with third-party network devices.
poolPublisher	Publishes the IOR of the SAE and local IP address pools in the directory so that a NIC can associate a router with an SAE and resolve the IP-to-SAE mapping.	Use with JUNOS virtual routers that supply IP addresses from local pools.

Interface Object Fields

Router initialization scripts are written in the Python programming language (www.python.org) and executed in the Jython environment (www.jython.org).

Router initialization scripts interact with the SAE through an interface object called `Ssp`. The SAE exports a number of fields through the interface object to the script and expects the script to provide the entry point to the SAE.

Table 8 on page 160 describes the fields that the SAE exports.

Table 8: Exported Fields

Ssp Attribute	Description
<code>Ssp.properties</code>	System properties object (class: <code>java.util.Properties</code>)—The properties should be treated as read-only by the script.
<code>Ssp.errorLog</code>	Error logger—Use the <code>Ssp.errorLog.println (message)</code> to send error messages to the log.
<code>Ssp.infoLog</code>	Info logger—Use the <code>Ssp.infoLog.println (message)</code> to send informational messages to the log.
<code>Ssp.debugLog</code>	Debug logger—Use the <code>Ssp.debugLog.println (message)</code> to send debug messages to the log.

The router initialization script must set the field `Ssp.routerInit` to a factory function that instantiates a router initialization object:

- `<VRName>` —Name of the virtual router in which the COPS client has been configured, format: `virtualRouterName@RouterName`
- `<virtualIp>` —Virtual IP address of the SAE (string, dotted decimal; for example: 192.168.254.1)
- `<realIp>` —Real IP address of the SAE (string, dotted decimal; for example, 192.168.1.20)
- `<VRIp>` —IP address of the virtual router (string, dotted decimal)
- `<transportVR>` —Name of the virtual router used for routing the COPS connection, or `None`, if the COPS client is directly connected

The factory function must implement the following interface:

```
Ssp.routerInit(VRName,
virtualIp,
realIp,
VRIp,
transportVR)
```

The factory function returns an interface object that is used to set up and tear down a connection for a given COPS server. A common case of a factory function is the constructor of a class.

The factory function is called directly after a COPS server connection is established. In case of problems, an exception should be raised that leads to the termination of the COPS connection.

Required Methods

Instances of the interface object must implement the following methods:

- `setup()`—Is called when the COPS server connection is established and is operational. In case of problems, an exception should be raised that leads to the termination of the COPS connection.
- `shutdown()`—Is called when the COPS server connection to the virtual router is terminated. This method should not raise any exceptions in case of problems.

Example: Router Initialization Script

The following script defines a router initialization class named *SillyRouterInit*. The interface class does not implement any useful functionality. The interface class just writes messages to the `infoLog` when the router connection is created or terminated.

```
class SillyRouterInit:
    def __init__(self, vrName, virtualIp, realIp, vrIp, transportVr):
        """ initialize router initialization object """
        self.vrName = vrName
        Ssp.infoLog.println("SillyRouterInit created")
```

```

def setup(self):
    """ initialize connection to router """
    Ssp.infoLog.println("Setup connection to VR %(vrName)s" %
        vars(self))
def shutdown(self):
    """ shutdown connection to router """
    Ssp.infoLog.println("Shutdown connection to VR %(vrName)s" %
        vars(self))
#
# publish interface object to Ssp core
#
Ssp.routerInit = SillyRouterInit

```

Accessing the Router CLI

You can access the CLIs of Juniper Networks routers through a Telnet or secure shell connection.

- To open a Telnet session to a router, use the **telnet** operational mode command. For example:

```
user@host> telnet 10.10.10.3
```

- To open a secure shell connection, use the **ssh** operational command. For example:

```
user@host> ssh host 10.10.10.3
```

Starting the SRC Client on a JUNOSe Router

JUNOSe routers use an SRC client to interact with the SAE. See *JUNOSe Broadband Access Configuration Guide* for complete information about configuring the SRC client on a JUNOSe router.

To start the SRC client:

1. Access the router CLI.
2. Access Global configuration mode.

```
host1#configure terminal
```

3. Switch to the virtual router for which you want to create an SRC client.

```
host1(config)#virtual-router <vrName>
```

4. Enable the SRC client.

To enable COPS-PR mode:

```
host1:<vrName>(config)#sscc enable cops-pr
```

To enable COPS-XDR mode:


```
host1:<vrName>(config)#sscc enable
```

5. Set the primary address from the configuration directory.

```
host1:<vrName>(config)#sscc primary address <ipAddress> port 3288
```

Stopping the SRC Client on a JUNOSe Router

JUNOSe routers use an SRC client to interact with the SAE. See *JUNOSe Broadband Access Configuration Guide* for complete information about configuring the SRC client on the JUNOSe router.

To stop the SRC client:

1. Access the router CLI.

See Accessing the Router CLI.

2. Access Global configuration mode.

```
host1#configure terminal
```

3. Switch to the virtual router for which you want to stop an SRC client.

```
host1(config)#virtual-router <vrName>
```

4. Disable the SRC client.

```
host1:<vrName>(config)#no sscc enable
```

Monitoring Interactions Between the SAE and the JUNOSe Router

Purpose Monitor connection between the SAE and a JUNOSe router.

Action To monitor the connection between the router and the SAE:

- Use the **show sscc info** command on the JUNOSe router

To display the version number of the SRC client:

- Use the **show sscc version** command on the JUNOSe router.

See the *JUNOSe Command Reference Guide* for details about these commands.

You can also monitor the interactions between the SRC software and the router in the log files for the SAE and in the log files generated by the JUNOSe router.

- For information about configuring logging on JUNOSe routers, see *JUNOSe System Event Logging Reference Guide*.

Troubleshooting Problems with Managing JUNOSe Routers

Problem SRC client or JUNOSe router is not working as expected.

Solution You can troubleshoot problems with the SRC client on JUNOSe routers and with managed JUNOSe routers, interfaces, and services on the SAE.

To troubleshoot SRC problems on the router:

1. Look at the log files for the SAE and the log files generated by the SRC client on the JUNOSe router.
 - If the log files indicate a problem with specific interfaces on the router, review the configuration of the associated policies in the SRC software, and fix any errors.
 - If the log files indicate a problem with a specific service or its associated policy rules, review the configuration of the service or policies in the SRC software, and fix any errors.
 - If the log files indicate only that the SRC client is not responding, ensure that the values in the SAE configuration match the values in the SRC client configuration on the router.
2. Restart the SRC client on the JUNOSe router.

When you restart the SRC client, the SRC client removes all policies that were installed by the SRC software and reports all interfaces again.



NOTE: DHCP addresses that were managed are not reported again, so we recommend that you do not restart the SRC client if you are managing DHCP sessions.

To restart the SRC client in COPS-PR mode, enter the following commands:

```
host1:<vrName>(config)#no sssc enable
host1:<vrName>(config)#sscc enable cops-pr
```

To restart the SRC client in COPS-XDR mode, enter the following commands:

```
host1:<vrName>(config)#no sssc enable
host1:<vrName>(config)#sscc enable
```

If restarting the SRC client does not resolve the problem, rebuild the router configuration and restart the client.

Viewing the State of JUNOSe Device Drivers (C-Web Interface)

Purpose If the log files indicate a problem with a specific driver, review the configuration of the associated with the JUNOSe router driver with the C-Web interface.

- Action**
1. Click **Monitor > SAE > Drivers**.

The Drivers pane appears.
 2. Enter information as described in the Help text in the main pane, and click **OK**.

The Drivers pane displays information about the JUNOSe device driver.

Viewing Statistics for Specific JUNOSe Device Drivers (C-Web Interface)

Purpose To view SNMP statistics about a specific JUNOSe device driver:

- Action**
1. Click **Monitor > SAE > Statistics > Device**.

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

For JUNOSe router drivers, use the format:

< virtual router name > @ < router name >
 3. Enter information as described in the Help text in the main pane, and click **OK**.

The Device pane displays statistics for a specific JUNOSe device driver.

Viewing Statistics for All JUNOSe Device Drivers (C-Web Interface)

Purpose To view SNMP statistics for all JUNOSe device driver:

- Action**
1. Click **Monitor > SAE > Statistics > Device > Common**.

The Common pane appears.
 2. Enter information as described in the Help text in the main pane, and click **OK**.

The Common pane displays statistics for the JUNOSe device driver.

Chapter 20

Using JUNOS Routing Platforms in the SRC Network (C-Web Interface)

This chapter describes how to use the C-Web interface to set up the SRC software and how to set up JUNOS routing platforms so that the routing platforms can be used in the SRC network. It also shows how to monitor the interactions between the SAE and JUNOS routing platforms and how to troubleshoot SRC problems on JUNOS routing platforms.

Topics in this chapter include:

- BEEP Connection Between JUNOS Routing Platforms and the SAE on page 150
- Adding JUNOS Routing Platforms and Virtual Routers (C-Web Interface) on page 150
- Configuring the SAE to Manage JUNOS Routing Platforms (C-Web Interface) on page 151
- Configuring Secure Connections Between the SAE and JUNOS Routing Platforms on page 152
- Manually Obtaining Digital Certificates on page 152
- Obtaining Digital Certificates through SCEP on page 154
- Adding the Server Certificate on the Routing Platform on page 155
- Creating a Client Certificate for the Router on page 156
- Adding the Client Certificate on the Router on page 156
- Configuring the SAE to Use TLS on page 157
- Configuring TLS on the SAE on page 157
- SAE Verification of JUNOS Configuration Changes on page 157
- Setting Up the SAE to Periodically Check JUNOS Configuration (C-Web Interface) on page 158
- Using SNMP to Retrieve Information from JUNOS Routing Platforms and Other Network Devices on page 158
- Developing Router Initialization Scripts for JUNOSe Routers, JUNOS Routing Platforms, and Network Devices on page 159

- Specifying JUNOS Router Initialization Scripts on the SAE (C-Web Interface) on page 161
- Troubleshooting Problems with the SRC Software Process (C-Web Interface) on page 161

BEEP Connection Between JUNOS Routing Platforms and the SAE

For information about which JUNOS routing platforms and releases a particular SRC release supports, see the SRC *Release Notes*.

The SAE interacts with a JUNOS software process, referred to as the SRC software process in this documentation, on the JUNOS routing platform. The SAE and the SRC software process communicate using the Blocks Extensible Exchange Protocol (BEEP). You can secure the BEEP connection by using Transport Layer Security (TLS).

When the SRC software process establishes a BEEP session for the SAE, the SAE configures an interface on the JUNOS routing platform. The SAE builds the configuration for an interface using the policies stored in the directory. If the policies are subsequently modified, the SAE builds a new configuration and reconfigures the interface on the JUNOS routing platform. The JUNOS routing platform stores data about interfaces and services that the SAE manages in a configuration group called *sdx*. You must create this configuration group on the JUNOS routing platform.

Adding JUNOS Routing Platforms and Virtual Routers (C-Web Interface)

- Overview of Adding JUNOS Routing Platforms and Virtual Routers on page 150
- Adding Operative JUNOS Routing Platforms on page 150
- Adding JUNOS Routers Individually on page 151
- Adding Virtual Routers Individually on page 151

Overview of Adding JUNOS Routing Platforms and Virtual Routers

On JUNOS routing platforms, the SAE manages interfaces. The SRC software associates a virtual router called *default* with each JUNOS routing platform. Each JUNOS routing platform in the SRC network and its associated virtual router (VR) called *default* must appear in the directory. The VRs are not actually configured on the JUNOS routing platform; the VR in the directory provides a way for the SAE to manage the interfaces on the JUNOS routing platform.

There are two ways to add routers:

- Detect operative routers and configured JUNOS VRs in the SRC network and add them to the configuration.
- Add each router and VR individually.

Adding Operative JUNOS Routing Platforms

To add to the directory routers and JUNOS VRs that are currently operative and have an operating SNMP agent:

1. Click **Manage > Request > Network > Discovery**.
2. Enter information as described in the Help text in the main pane, and click **Apply**.

If you add a router using the discover network feature, the software adds the IP address of the first SNMP agent on the router to respond to the discover request.

Adding JUNOS Routers Individually

To add a router:

1. Click **Configure**, expand **Shared**, and then click **Network**.

The Shared Network pane appears.

2. From the Create new list, select **Device**.
3. Type a name for the new device in the dialog box, and click **OK**.

The Device pane appears.

4. From the Device Type list, select **JUNOS**.
5. Enter information as described in the Help text in the main pane, and click **Apply**.

Adding Virtual Routers Individually

To add a virtual router to an existing router:

1. Click **Configure**, expand **Shared > Network**, and then click a JUNOS router.

The Device pane appears.

2. From the Create new list, select **Virtual Router**.
3. Type a name for the new device in the dialog box, and click **OK**.

The Virtual Router pane appears.

4. Enter information as described in the Help text in the main pane, and click **Apply**.

Related Topics ■ For information about service scopes, see [Configuring Service Scopes](#)

Configuring the SAE to Manage JUNOS Routing Platforms (C-Web Interface)

A JUNOS routing platform interacts with the SAE by using a JUNOS software process called `sdx`. When the `sdx` process establishes a TCP/IP connection to the SAE, the SAE begins to manage the router. The JUNOS router driver configuration defines parameters related to the interactions between the SAE and the `sdx` process.

To configure the SAE to manage JUNOS routers:

1. Click **Configure**, expand **Shared > SAE > Configuration > Driver**, and then click **JUNOS**.

The JUNOS pane appears.

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

Configuring Secure Connections Between the SAE and JUNOS Routing Platforms

You can use TLS to protect communication between the SAE and JUNOS routing platforms.

To complete the handshaking protocol for the TLS connection, the client (JUNOS routing platform) and the server (SAE) must exchange and verify certificates. You need to create a client certificate and a server certificate. Both certificates must be signed by a certificate authority (CA). JUNOS software supports VeriSign, Inc. (<http://www.verisign.com>). You must then install both certificates on the SAE and on the JUNOS routing platform.

You can use the C-Web interface 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.

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

Adding the Server Certificate on the Routing Platform

The TLS client (JUNOS routing platform) needs a copy of the certificate that was used to sign the SAE certificate so that it can verify the SAE certificate. To install the SAE certificate on the JUNOS routing platform:

1. Include the following statements at the [edit security certificates certificate-authority] hierarchy level.

```
[edit security certificates certificate-authority]
security{
  certificates{
    certificate-authority SAE Cert{
      file /var/db/certs/cert.pem;
    }
  }
}
```

2. Include the following statements at the [system services service-deployment] hierarchy level.

```
system{
  services{
    service-deployment{
      servers {
        server-address port port-number{
          security-options {
            tls;
          }
        }
      }
    }
  }
}
```

Creating a Client Certificate for the Router

For information about how to obtain a certificate for the router from a certificate authority, see *Obtaining a Certificate from a Certificate Authority* in the *JUNOS System Basics Configuration Guide*.

Adding the Client Certificate on the Router

To install the client (router) certificate on the JUNOS routing platform:

1. Include the following statements at the [edit security certificates certificate-authority] hierarchy level.

```
[edit security certificates certificate-authority]
security{
  certificates{
  }
}
```

2. Include the following statements at the [system services service-deployment] hierarchy level.

```
system{
```

```

services{
  service-deployment{
    local-certificate clientCert;
  }
}

```

Configuring the SAE to Use TLS

To configure the SAE to accept TLS connections:

1. Click **Configure**, expand **Shared > Network**, and then click a JUNOS router.

The Device pane appears.

2. Type a port number in the Beep Server Port box, and click **Apply**.

Configuring TLS on the SAE

To configure TLS on the SAE:

1. Click **Configure**, expand **Shared > SAE > Configuration > Driver > JUNOS**, and then click **Security**.

The Security pane appears.

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

SAE Verification of JUNOS Configuration Changes

The SAE can check the configuration of a JUNOS routing platform under its control to detect whether the configuration has changed by a means other than through the SAE. If the SAE finds a disparity between the router and the SAE configurations, it can take several actions. The SAE checks the configuration installed on the router against the state of the SAE session layer (subscriber, service, and interface sessions). While the check is occurring, the SAE does not handle jobs from the router, and all provisioning activity is blocked, including event notifications.

The SAE can take the following actions if it finds a disparity between the router and SAE configurations:

- The SAE takes the state of the session layer on the router to be correct and updates its local state to be consistent with the router. The SAE then sends stop events for all sessions where the corresponding provisioning in the router has been removed.
- The SAE takes its local state to be the correct state and updates the router to be consistent with its local state.
- The SAE does not solve the state discrepancy. It reports disparities through the SAE device driver event trap called `routerConfOutOfSynch` and through the info log.

Note that it is not possible to check the consistency of individual objects that the SAE provisions. Therefore, modifications to a provisioning object while the SAE is disconnected from the router cannot be detected.

Setting Up the SAE to Periodically Check JUNOS Configuration (C-Web Interface)

Use the following configuration statements to configure the SAE to periodically check the configuration of the JUNOS routing platform:

To configure the SAE to periodically check the configuration of the JUNOS routing platform:

1. Click **Configure**, expand **Shared > SAE > Configuration > Driver > JUNOS**, and then click **Configuration Checking**.

The Configuration Checking pane appears.

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

Using SNMP to Retrieve Information from JUNOS Routing Platforms and Other Network Devices

Although procedure the same in other topics - intro is different

You can use SNMP to retrieve information from a JUNOS router or a network device. For example, if you create a router initialization script that uses SNMP, you need to specify the SNMP communities that are on the router.

We recommend that you specify SNMP communities for each virtual router. You can also configure global default SNMP communities.

You can configure global default SNMP communities that are used if a VR does not exist on the router or if the community strings have not been configured for the VR.

To configure global default SNMP communities:

1. Click **Configure**, expand **Shared > SAE > Configuration > Driver**, and then click **SNMP**.

The SNMP pane appears.

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

Related Topics ■ Adding Virtual Routers Individually

Developing Router Initialization Scripts for JUNOSe Routers, JUNOS Routing Platforms, and Network Devices

When the SAE establishes a connection with a router or network device, it can run an initialization script to customize the setup of the connection. These initialization scripts are run when the connection between a router or network device and the SAE is established and again when the connection is dropped.

We provide the `IorPublisher` script in the `/opt/UMC/sae/lib` folder. The `IorPublisher` script publishes the interoperable object reference (IOR) of the SAE in the directory so that a NIC can associate a router with an SAE.

For JUNOSe VRs that supply IP addresses from a local pool, a router initialization script is provided that identifies which VR supplies each IP pool and writes the information to the configuration. The SAE runs the script only when a COPS connection is established to the JUNOSe router. Consequently, if you modify information about IP pools on a VR after the COPS connection is established, the SAE will not automatically register the changes, and you must update the configuration.

Table 7 on page 159 describes the router initialization scripts that we provide with the SRC software in the `/opt/UMC/sae/lib` folder.

Table 9: Router Initialization Scripts

Script Name	Function	When to Use Script
iorPublisher	Publishes the IOR of the SAE into an internal part of the shared configuration so that a NIC can associate a router with an SAE.	Use with JUNOSe routers that do not supply IP addresses from local pools, and with JUNOS routing platforms.
		Use with all JUNOS routing platforms.
		Use with third-party network devices.
poolPublisher	Publishes the IOR of the SAE and local IP address pools in the directory so that a NIC can associate a router with an SAE and resolve the IP-to-SAE mapping.	Use with JUNOSe virtual routers that supply IP addresses from local pools.

Interface Object Fields

Router initialization scripts are written in the Python programming language (www.python.org) and executed in the Jython environment (www.jython.org).

Router initialization scripts interact with the SAE through an interface object called `Ssp`. The SAE exports a number of fields through the interface object to the script and expects the script to provide the entry point to the SAE.

Table 8 on page 160 describes the fields that the SAE exports.

Table 10: Exported Fields

Ssp Attribute	Description
Ssp.properties	System properties object (class: java.util.Properties)—The properties should be treated as read-only by the script.
Ssp.errorLog	Error logger—Use the SsperrorLog.println (message) to send error messages to the log.
Ssp.infoLog	Info logger—Use the Ssp.infoLog.println (message) to send informational messages to the log.
Ssp.debugLog	Debug logger—Use the Ssp.debugLog.println (message) to send debug messages to the log.

The router initialization script must set the field Ssp.routerInit to a factory function that instantiates a router initialization object:

- <VRName> —Name of the virtual router in which the COPS client has been configured, format: virtualRouterName@RouterName
- <virtualIp> —Virtual IP address of the SAE (string, dotted decimal; for example: 192.168.254.1)
- <realIp> —Real IP address of the SAE (string, dotted decimal; for example, 192.168.1.20)
- <VRIp> —IP address of the virtual router (string, dotted decimal)
- <transportVR> —Name of the virtual router used for routing the COPS connection, or None, if the COPS client is directly connected

The factory function must implement the following interface:

```
Ssp.routerInit(VRName,
virtualIp,
realIp,
VRIp,
transportVR)
```

The factory function returns an interface object that is used to set up and tear down a connection for a given COPS server. A common case of a factory function is the constructor of a class.

The factory function is called directly after a COPS server connection is established. In case of problems, an exception should be raised that leads to the termination of the COPS connection.

Required Methods

Instances of the interface object must implement the following methods:

- *setup()*—Is called when the COPS server connection is established and is operational. In case of problems, an exception should be raised that leads to the termination of the COPS connection.
- *shutdown()*—Is called when the COPS server connection to the virtual router is terminated. This method should not raise any exceptions in case of problems.

Example: Router Initialization Script

The following script defines a router initialization class named *SillyRouterInit*. The interface class does not implement any useful functionality. The interface class just writes messages to the infoLog when the router connection is created or terminated.

```
class SillyRouterInit:
    def __init__(self, vrName, virtualIp, realIp, vrIp, transportVr):
        """ initialize router initialization object """
        self.vrName = vrName
        Ssp.infoLog.println("SillyRouterInit created")
    def setup(self):
        """ initialize connection to router """
        Ssp.infoLog.println("Setup connection to VR %(vrName)s" %
                             vars(self))
    def shutdown(self):
        """ shutdown connection to router """
        Ssp.infoLog.println("Shutdown connection to VR %(vrName)s" %
                             vars(self))
#
# publish interface object to Ssp core
#
Ssp.routerInit = SillyRouterInit
```

Specifying JUNOS Router Initialization Scripts on the SAE (C-Web Interface)

To configure router initialization scripts for JUNOS routing platforms:

1. Click **Configure**, expand **Shared > SAE > Configuration > Driver**, and then click **Scripts**.

The Scripts pane appears.

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

Troubleshooting Problems with the SRC Software Process (C-Web Interface)

To troubleshoot SRC problems on the JUNOS routing platform, review the log files for the SAE and the log files generated by the SRC software process on the router. If the log files indicate that the SRC software process on the JUNOS routing platform is not responding:

1. Look at the status of the process on the JUNOS routing platform.

```
root@ui1>show system services service-deployment
```

```
Connected to 172.17.20.151 port 3333 since 2004-02-06 14:50:31 PST
Keepalive settings: Interval 15 seconds
Keepalives sent: 100, Last sent: 6 seconds ago
Notifications sent: 0
Last update from peer: 00:00:06 ago
```

2. If you see the message “ error: the service-deployment subsystem is not running,” reenable the SRC software process.
3. If the process is already enabled, review the configurations of the router and the SAE in the directory, and fix any problems.
4. Restart the SRC software process on the router.

```
root@ui1>restart service-deployment
```

The SAE synchronizes with the SRC software process and deletes unnecessary data from the router.

Chapter 21

Adding Objects for CMTS Devices (C-Web Interface)

This chapter describes how to configure objects for cable modem termination system (CMTS) devices with the C-Web interface. You can also use the SRC CLI to add objects for CMTS devices:

Topics in this chapter include:

- Adding Objects for CMTS Devices (C-Web Interface) on page 163
- Creating Virtual Routers for the CMTS Device (C-Web Interface) on page 163

Adding Objects for CMTS Devices (C-Web Interface)

To manage CMTS devices, the SAE creates and manages pseudointerfaces that it associates with a virtual router object. Each CMTS device in the SRC network must appear in the configuration as a router object, and it must be associated with a virtual router object called default. The router and virtual router are not actually configured on the CMTS device; the router and virtual router provide a way for the SAE to manage the CMTS device by using the SAE's embedded policy server.

To add a router:

1. Click **Configure**, expand **Shared**, and then click **Network**.

The Shared Network pane appears.

2. From the Create new list, select **Device**.
3. Type a name for the new device in the dialog box, and click **OK**.

The Device pane appears.

4. From the Device Type list, select **pccm**.
5. Enter information as described in the Help text in the main pane, and click **Apply**.

Creating Virtual Routers for the CMTS Device (C-Web Interface)

You need to add a virtual router object called default to the CMTS device.

To add a virtual router to an existing router:

1. Click **Configure**, expand **Shared > Network**, and then click a CMTS device.

The Device pane appears.

2. From the Create new list, select **Virtual Router**.
3. Type a name for the new device in the dialog box, and click **OK**.

The Virtual Router pane appears.

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

Chapter 22

Integrating Third-Party Network Devices into the SRC Network (C-Web Interface)

This chapter describes how to use the C-Web interface to integrate third-party network devices into the SRC network. You can use the C-Web interface to configure the SRC software on a C-series Controller.

Topics in this chapter include:

- Overview of Integrating Network Devices into the SRC Network on page 165
- Logging In Subscribers and Creating Sessions on page 167
- Configuration Tasks for Integrating Third-Party Network Devices (C-Web Interface) on page 170
- Setting Up Script Services on page 171
- Adding Objects for Network Devices (C-Web Interface) on page 171
- Setting Up SAE Communities (C-Web Interface) on page 172
- Using the NIC Resolver in Environments That Have Third-Party Devices (C-Web Interface) on page 173

Overview of Integrating Network Devices into the SRC Network

You can integrate third-party routers and other network devices into your SRC network. The SAE provides a driver that you can use to integrate the SAE with a third-party device. This device driver uses the session store to store and replicate subscriber and service session data within a community of SAEs.

To log in subscribers to the SAE, you use assigned IP subscribers or event notification from an IP address manager.

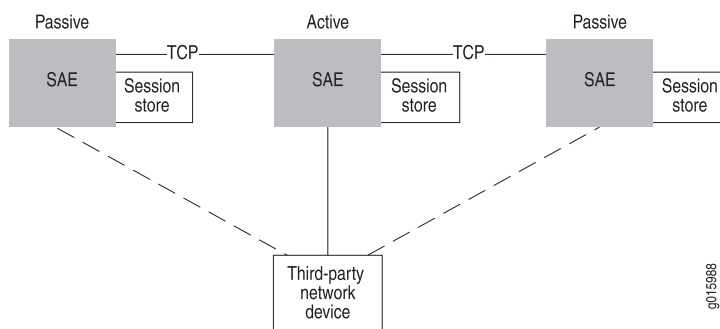
To activate services and provision policies on the device, you use script services. You can also activate aggregate services for subscribers. However, you cannot activate normal services that require policies to be provisioned on the device.

SAE Communities

For SAE redundancy in an SRC network, you can have a community of two or more SAEs. SAEs in a community are given the role of either active SAE or passive SAE. The active SAE manages the connection to the network device and keeps session

data up to date within the community. Figure 1 on page 166 shows a typical SAE community.

Figure 1: SAE Community



When an SAE starts, it negotiates with other SAEs to determine which SAE controls the network device. The SAE community manager and members of the community select the active SAE.

A passive SAE needs to take over as active SAE in any of the following cases:

- The active SAE shuts down. In this case, the active SAE notifies the passive SAEs, and one of the passive SAEs takes over as active SAE.
- A passive SAE does not receive a keepalive message from the active SAE within the keepalive interval. In this case, the passive SAE attempts to become the active SAE.

Storing Session Data

To aid in recovering from an SAE failover, the SAE stores subscriber and service session data. When the SAE manages a network device, session data is stored in the SAE host's file system. The SRC component that controls the storage of session data on the SAE is called the session store. The session store queues data and then writes the data to session store files on the SAE host's disk. Once the data is written to disk, it can survive a server reboot.

For more information, see *Storing Subscriber and Service Session Data*.

Using Script Services to Provision Third-Party Devices

You use script services to activate services and provision policies on third-party network devices. A script service is a service into which you can insert or reference a script. You write a script that will activate services and provision policies on the third-party device, and then you insert the script into the script service or reference the script in the service. When the SAE activates a service, it runs the script. The script provisions policies on the device using a means that the device supports. You can also include an interface in the script that causes the SAE to send authentication and tracking events when it activates, modifies, or deactivates a script service session.

The SAE core API includes two interfaces for creating a script:

- **ScriptService**—Defines a service provider interface (SPI) that the script service must implement. The implementation of the ScriptService interface activates, modifies, or deactivates the service.
- **ServiceSessionInfo**—Provides a callback interface into the SAE and provides information about the service session to the script service.

For information about the ScriptService interface and the ServiceSessionInfo interface, see the script service documentation in the SAE core API documentation on the Juniper Networks Web site at <http://www.juniper.net/techpubs/software/management/src/api-index.html>

You can write the script in Java or Jython.

- Related Topics**
- Configuration Tasks for Integrating Third-Party Network Devices
 - Logging In Subscribers and Creating Sessions

Logging In Subscribers and Creating Sessions

You can use two mechanisms to obtain subscriber address requests and other information and to set up a pseudointerface on the network device. (You must choose one mechanism; you cannot mix them.)

1. **Assigned IP subscriber.** The SAE learns about a subscriber through subscriber-initiated activities, such as activating a service through the portal or through the SRC SOAP Gateway (SRC-SG).

With this method, you use the assigned IP subscriber login type along with the network interface collector (NIC) to map IP addresses to the SAE.

2. **Event notification from an IP address manager.** The SAE learns about subscribers through notifications from an external IP address manager, such as a DHCP server or a RADIUS server.

With this method, you use the event notification application programming interface (API). The API provides an interface to the IP address manager, and lets the IP address manager notify the SAE of events such as IP address assignments.

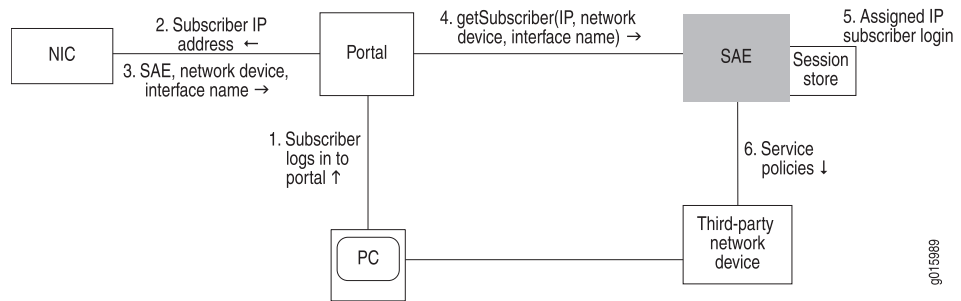
Assigned IP Subscribers

With the assigned IP subscriber method of logging in subscribers and creating sessions, the SRC software uses IP address pools along with network information collector (NIC) resolvers to provide mapping of IP addresses to SAEs. You configure the static address pools or dynamically discovered address pools in the virtual router configuration for a network device. These pools are published in the NIC. The NIC maps subscriber IP addresses in requests received through the portal or SRC-SG to the SAE that currently manages that network device.

Login Interactions with Assigned IP Subscribers

This section describes login interactions for assigned IP subscribers. In the example shown in Figure 2 on page 168, the subscriber activates a service through a portal. You could also have the subscriber activate a service through the SRC-SG.

Figure 2: Login Interactions with Assigned IP Subscribers



The sequence of events for logging in and creating sessions for assigned IP subscribers is:

1. The subscriber logs in to the portal.
2. The portal sends the subscriber's IP address to the NIC.
3. Based on the IP address, the NIC looks up the subscriber's SAE, network device, and interface name, and returns this information to the portal.
4. The portal sends a `getSubscriber` message to the SAE. The message includes the subscriber's IP address, network device, and interface name.
5. The SAE creates an assigned IP subscriber and performs a subscriber login. Specifically, it:
 - a. Runs the subscriber classification script with the IP address of the subscriber. (Use the `ASSIGNEDIP` login type in subscriber classification scripts.)
 - b. Loads the subscriber profile.
 - c. Runs the subscriber authorization plug-ins.
 - d. Runs the subscriber tracking plug-ins.
 - e. Creates a subscriber session and stores the session data in the session store file.
6. The SAE pushes service policies for the subscriber session to the network device.

Because the SAE is not notified when the subscriber logs out, the assigned IP idle timer begins when no service is active. The SAE removes the interface subscriber session when the timeout period ends.

Event Notification from an IP Address Manager

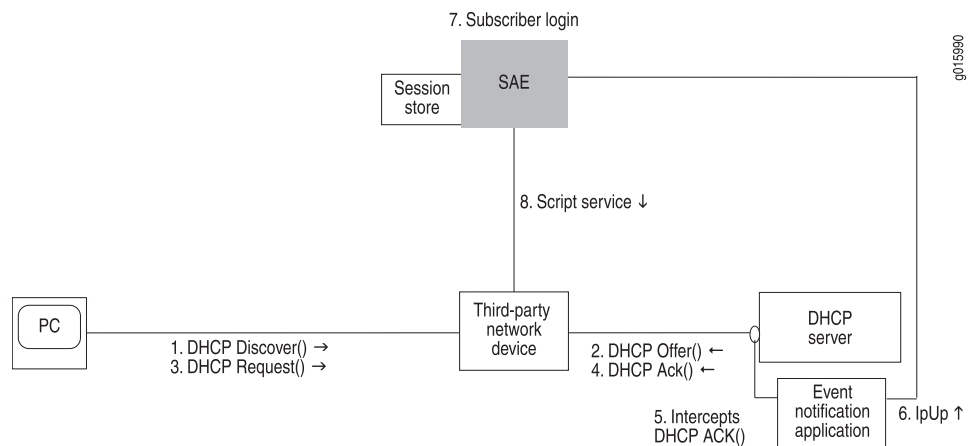
With the event notification method of logging in subscribers and creating subscriber sessions, the subscriber logs in to the network device and obtains an IP address through an address server, usually a DHCP server. The SAE receives notifications about the subscriber, such as the subscriber's IP address, from an event notification application that is installed on the DHCP server.

To use this method of logging in subscribers, you can use the event notification API to create the application that notifies the SAE when events occur between the DHCP server and the network device. You can also use Monitoring Agent, a sample application that was created with the event notification API and that monitors DHCP or RADIUS messages for DHCP or RADIUS servers. See the *SRC-PE Sample Applications Guide*.

Login with Event Notification

This section describes login interactions by means of event notifications.

Figure 3: Login Interactions with Event Notification Application



The sequence of events for logging in subscribers and creating sessions is:

1. The DHCP client in the subscriber's computer sends a DHCP discover request to the DHCP server.
2. The DHCP server sends a DHCP offer to the subscriber's DHCP client.
3. The DHCP client sends a DHCP request to the DHCP server.
4. The DHCP server acknowledges the request by sending a DHCP Ack message to the DHCP client.
5. The event notification application that is running on the DHCP server intercepts the DHCP Ack message.
6. The event notification application sends an ipUp message to the SAE that notifies the SAE that an IP address is up.
7. The SAE performs a subscriber login. Specifically, it:

- a. Runs the subscriber classification script.
 - b. Loads the subscriber profile.
 - c. Runs the subscriber authorization plug-ins.
 - d. Runs the subscriber tracking plug-ins.
 - e. Creates a subscriber session and stores the session in the session store file.
8. The SAE can start script services.

The ipUp event should be sent with a timeout set to the DHCP lease time. The DHCP server sends an ipUp event for each Ack message sent to the client. The SAE restarts the timeout each time it receives an ipUp event.

If the client explicitly releases the DHCP address (that is, it sends a DHCP release event), the DHCP server sends an ipDown event. If the client does not renew the address, the lease expires on the DHCP server and the timeout expires on the SAE.

- Related Topics**
- Overview of Integrating Network Devices into the SRC Network
 - Configuration Tasks for Integrating Third-Party Network Devices

Configuration Tasks for Integrating Third-Party Network Devices (C-Web Interface)

To integrate third-party devices into your SRC network, complete the following tasks:

- Write a script and add a script service that references the script.
- Add objects for the devices.

See [Adding Objects for Network Devices \(C-Web Interface\)](#) .

- Configure an SAE community.

See [Setting Up SAE Communities \(C-Web Interface\)](#) .

- (Optional) Configure SAE properties for the event notification API if you are using the event notification method to log in subscribers.
- Configure the session store.
- If you are using the event notification method to log in subscribers, integrate the SAE with an IP address manager. There are two ways to do so:

- Use the event notification API to create an application that notifies the SAE when events occur between the DHCP server and the network device.

See the event notification API documentation in the SAE CORBA remote API documentation on the Juniper Networks Web site at

<http://www.juniper.net/techpubs/software/management/src/api-index.html>

- Use Monitoring Agent, an application that was created with the event notification API and that monitors DHCP or RADIUS messages for DHCP or RADIUS servers.

See the *SRC Sample Applications Guide*.

Setting Up Script Services

To set up script services:

1. Write a script that implements the ScriptService interface, a service provider interface (SPI) for the SAE.

See Customizing Service Implementations.

See the script service documentation in the SAE core API documentation on the Juniper Networks Web site at

<http://www.juniper.net/techpubs/software/management/src/api-index.html>

2. Add a script service that references the script.

See Overview of SRC Script Services.

- Related Topics**
- Configuration Tasks for Integrating Third-Party Network Devices
 - Overview of Integrating Network Devices into the SRC Network
 - Logging In Subscribers and Creating Sessions

Adding Objects for Network Devices (C-Web Interface)

For each network device that the SAE manages, add a router object and virtual router object.

- Adding a Router Object on page 171
- Adding Virtual Router Objects on page 172

Adding a Router Object

To add a router object:

1. Click **Configure**, expand **Shared**, and then click **Network**.

The Shared Network pane appears.

2. From the Create new list, select **Device**.
3. Type a name for the new device in the dialog box, and click **OK**.

The Device pane appears.

4. Enter information as described in the Help text in the main pane, and click **Apply**.

Adding Virtual Router Objects

To add a virtual router to an existing router object:

1. Click **Configure**, expand **Shared > Network**, and then click an existing device.

The Device pane appears.

2. From the Create new list, select **Virtual Router**.
3. Type a name for the new device in the dialog box, and click **OK**.

The Virtual Router pane appears.

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

Setting Up SAE Communities (C-Web Interface)

Tasks to configure SAE communities are:

- Configuring the SAE Community Manager on page 172
- Specifying the Community Manager in the SAE Device Driver on page 172
- Configuring SAE Properties for the Event Notification API (C-Web Interface) on page 173
- Specifying Initialization Scripts on the SAE on page 173

Configuring the SAE Community Manager

To configure the SAE community manager that manages third-party device communities:

1. Click **Configure**, expand **Shared > SAE**, and then click the SAE group for which you want to manage third-party devices.

The Group pane appears.

2. In the side pane, expand **Configuration > External Interface Features: PCMMCommunityManager**, and then click **Community Manager**.

The Community Manager pane appears.

3. Enter information as described in the Help text in the main pane, and click **Apply**.

Specifying the Community Manager in the SAE Device Driver

To specify the community manager in the SAE device driver:

1. Click **Configure**, expand **Shared > SAE > Configuration > Driver**, and then click **Third Party**.

The Third Party pane appears.

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

Configuring SAE Properties for the Event Notification API (C-Web Interface)

Although procedure is similar for topics with different titles, keep this topic separate.

To configure properties for the event notification API:

1. Click **Configure**, expand **Shared > SAE**, and then click the SAE group for which you want to manage devices.

The Group pane appears.

2. In the side pane, expand **Configuration > External Interface Features: Event**, and then click **Event API**.

The Event API pane appears.

3. Enter information as described in the Help text in the main pane, and click **Apply**.

Specifying Initialization Scripts on the SAE

To configure initialization scripts for third-party devices:

1. Click **Configure**, expand **Shared > SAE > Configuration > Driver**, and then click **Scripts**.

The Scripts pane appears.

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

Using the NIC Resolver in Environments That Have Third-Party Devices (C-Web Interface)

If you are using the assigned IP subscriber method of logging in subscribers, and you are using the NIC to determine the subscriber's SAE, you need to configure a resolver on the NIC. The OnePopDynamicIp sample configuration data supports this scenario. The OnePopDynamicIp configuration supports one point of presence (POP) and provides no redundancy. The realm for this configuration accommodates the situation in which IP pools are configured locally on each virtual router object.

You can access the OnePopDynamicIp configuration in the SRC CLI.

Related Topics Locating Subscriber Management Information

Part 6

Configuring Policies and Services

- Configuring and Managing Policies (C-Web Interface) on page 177
- Configuring Local and Global Parameters (C-Web Interface) on page 203
- Configuring Services (C-Web Interface) on page 205
- Scheduling Services (C-Web Interface) on page 215
- Managing Tiered and Premium Services with QoS on JUNOS Routers (C-Web Interface) on page 231

Chapter 23

Configuring and Managing Policies (C-Web Interface)

This chapter describes how to use the C-Web interface to configure and manage policies.

Topics include:

- Before You Configure SRC Policies on page 178
- Enabling the Policy Configuration on the C-Web Interface on page 179
- Configuring Policy Folders (C-Web Interface) on page 180
- Configuring Policy Groups (C-Web Interface) on page 180
- Configuring Policy Lists (C-Web Interface) on page 180
- Configuring Policy Rules (C-Web Interface) on page 181
- Enabling Expansion of JUNOS Classify-Traffic Conditions (C-Web Interface) on page 184
- Specifying the PCMM Classifier Type (C-Web Interface) on page 184
- Specifying Port Access for Traffic Classification (C-Web Interface) on page 185
- Creating a Classify-Traffic Condition (C-Web Interface) on page 186
- Configuring Source Networks (C-Web Interface) on page 186
- Configuring Source Grouped Networks (C-Web Interface) on page 186
- Configuring Destination Networks (C-Web Interface) on page 186
- Configuring Destination Grouped Networks (C-Web Interface) on page 187
- Configuring Protocol Conditions (C-Web Interface) on page 187
- Configuring Protocol Conditions with Ports (C-Web Interface) on page 187
- Configuring Protocol Conditions with Parameters (C-Web Interface) on page 188
- Configuring TCP Conditions (C-Web Interface) on page 188
- Configuring ICMP Conditions (C-Web Interface) on page 189
- Configuring IGMP Conditions (C-Web Interface) on page 189
- Configuring IPSec Conditions (C-Web Interface) on page 189
- Configuring ToS Byte Conditions (C-Web Interface) on page 189
- Configuring JUNOS Filter Conditions (C-Web Interface) on page 189

- Configuring Application Protocol Conditions (C-Web Interface) on page 190
- Configuring QoS Conditions with the C-Web Interface with the C-Web Interface on page 191
- Configuring Actions (C-Web Interface) on page 191

Before You Configure SRC Policies

Building policies is a top-down operation. For example, before you can add a subordinate to the policy group, the policy group itself must exist.

Creating a Worksheet

Before you configure policies, you must determine what information you want to enter and where it will go. It is best to create a worksheet where you can record such things as names, priorities, addresses, and so on.

To create a worksheet:

1. Determine the policy requirements for your system.
2. Consider information that contains (at a minimum) names and parameters for:
 - Policy group
 - Policy list
 - Policy rules
 - Conditions
 - Actions
 - Record the policy information about the worksheet.

Naming Objects

Object names must be unique and must conform to LDAP distinguished name (DN) constraints.

Using the `apply-groups` Statement

When you use the `apply-groups` statement on the JUNOS routing platform to apply a configuration group to a hierarchy level in a configuration, you need to make sure that the SAE configuration group (default name is `sdx`) is in the first position in the `apply-groups` statement.

Using Expressions

Many of the policy options can take expressions in addition to literal values. If you can enter an expression for an option, the expression type is noted in the

documentation for the command. For information about using and formatting expressions, see Expressions in Parameters.

Policy Values

As you are planning your policy configuration, you need to understand how invalid values in policies are handled on JUNOS routing platforms and JUNOSe routers.

SAE to JUNOS Routing Platforms

When the SAE sends policies to JUNOS routing platforms, it uses JUNOScript on the Blocks Extensible Exchange Protocol (BEEP), which is an XML-based protocol. Many of the configuration values in JUNOScript are strings in which the value is a number. If you enter an integer value that is too large, the policy software flags the entry as invalid, but the value is still sent to the router because JUNOScript on BEEP allows for its transmission. The router is the authority that decides whether values are valid for the particular version of the JUNOS software and the routing platform. If the value is too large, the router sends an error message to the SAE.

For example, the valid range for the burst size limit in a policer action is 1,500 to 100,000,000. If you specify a value greater than 100,000,000, it is flagged as invalid. However, as usual, the SRC software attempts to activate the service, but the activation will fail because the burst size is an invalid value on the router.

SAE to JUNOSe Routers

When the SAE sends policies to JUNOSe routers, it uses the Common Open Policy Service (COPS) protocol with specific standard Policy Information Bases (PIBs) and private PIBs. Many of the configuration values in the PIBs are not strings in which the value is a number. Sometimes the numeric range in the PIB is larger than the valid range of values on the router. For integer values in policies, the eventual policy on the router has only the portion of a value that can be converted to an integer in the usable range.

The example below for ToS byte is such a case. From the JUNOSe-IP-PIB:

```
JunoselpolicyClacRuleEntry ::= SEQUENCE {
    junoselpolicyClacRuleTosByte Integer32,
    junoselpolicyClacRuleTosMask Integer32,
}
```

If a policy has a literal ToS byte value of 300, the high bits are ignored (or a mask of 255 is used) so that the value used for the ToS byte is 44; that is, 300 minus 256.

Enabling the Policy Configuration on the C-Web Interface

Before you can configure policies with the C-Web interface, you must enable the policy, service, and subscriber editor. To do so:

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

3. Click **OK**.

Configuring Policy Folders (C-Web Interface)

You use policy folders to organize policy groups.

To create a policy folder:

1. Click **Configure > Policies**.
2. From the Create new list, select **Folder**. Type a name for the new folder, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Policy Groups (C-Web Interface)

Policy groups hold policy lists. You can create policy groups at the Policies level or within policy folders.

To create a policy group:

1. Click **Configure > Policies**. You can add the policy group at the Policies level, or you can expand **Policies** and select a folder for which you want to add the group.
2. From the Create new list, select **Group**. Type a name for the new group, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Policy Lists (C-Web Interface)

When you add a policy list, you specify whether the policy list is for JUNOS routing platforms, JUNOSe routers (junose-ipv4 or junose-ipv6), or a CMTS device (pcmm). The type of policy list that you add controls the type of policy rules that you can add to the policy list.

You create policy lists within policy groups.

To add a policy list:

1. Click **Configure > Policies**.
2. Expand **Policies**, and expand the policy group for which you want to add the list.
3. From the Create new list, select **List**. Type a name for the new list, and click **OK**.
4. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Policy Rules (C-Web Interface)

You can configure policy rules from the C-Web interface. Topics include:

- Policy Management Overview on page 181
- Adding a Policy Rule on page 182
- Configuring Classify-Traffic Conditions (C-Web Interface) on page 182
- Configuring Template Activation (C-Web Interface) on page 184

Policy Management Overview

This chapter introduces policy-based routing management on E-series routers. Policy management enables you to configure, manage, and monitor policies that selectively cause packets to take different paths without requiring a routing table lookup. The JUNOS software's packet mirroring feature uses secure policies.

Policy management enables network service providers to configure services that customize the treatment of individual packet flows received on a subscriber's interface. The main tool for implementing policy management is a policy list. A policy list is a set of rules, each of which specifies a policy action. A rule is a policy action optionally combined with a classification.

Packets are sorted at ingress or egress into packet flows based on attributes defined in classifier control lists (CLACLs). You can apply policy lists to packets arriving and leaving an interface. You can use policy management on ATM, Frame Relay, generic routing encapsulation (GRE), IP, IPv6, Layer 2 Tunneling Protocol (L2TP), Multiprotocol Label Switching (MPLS), and virtual local area network (VLAN) traffic.

Policy management provides:

- Policy routing—Predefines a classified packet flow to a destination port or IP address. The router does not perform a routing table lookup on the packet. This provides superior performance for real-time applications.
- Bandwidth management—Rate-limits a classified packet flow at ingress to enforce ingress data rates below the physical line rate of a port. A rate-limit profile with a policy rate-limit profile rule provides this capability. You can construct policies to provide rate limiting for individual packet flows or for the aggregate of multiple packet flows. E-series router rate limits are calculated based on the layer 2 packet size. To configure rate limiting, you first create a rate-limit profile, which is a set of bandwidth attributes and associated actions. You next create a policy list with a rule that has rate limit as the action and associate a rate-limit profile with this rule. You can configure rate-limit profiles to provide a variety of services, including tiered bandwidth service where traffic conforming to configured bandwidth levels is treated differently than traffic that exceeds the configured values, and a hard-limit service where a fixed bandwidth limit is applied to a traffic flow. Finally, you can configure rate-limit profiles to provide a TCP-friendly rate-limiting service that works in conjunction with TCP's native flow-control functionality.
- Security—Provides a level of network security by using policy rules that selectively forward or filter packet flows. You can use a filter rule to stop a denial-of-service attack. You can use secure policies to mirror packets and send them to an analyzer.

- RADIUS policy support—Enables you to create and attach a policy to an interface through RADIUS.
- Packet tagging—Enables the traffic-class rule in policies to tag a packet flow so that the Quality of Service (QoS) application can provide traffic-class queuing. Policies can perform both in-band and out-of-band packet tagging.
- Packet forwarding—Allows forwarding of packets in a packet flow.
- Packet filtering—Drops packets in a packet flow.
- Packet mirroring—Uses secure policies to mirror packets and send them to an analyzer.
- Packet logging—Logs packets in a packet flow.

Policy management gives you the CLI tools to build databases, which can then be drawn from to implement a policy. Each database contains global traffic specifications. When building a policy, you specify input from one or more of these databases and then attach the policy to an interface. By combining the information from the various databases into policies, you can deploy a wide variety of services.

Adding a Policy Rule

You create policy rules within policy lists.

To add a policy rule:

1. In the side pane, select a policy list that has already been created and configured.
2. From the Create new list, select **Rule**. Type a name for the new rule, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Classify-Traffic Conditions (C-Web Interface)

You create classify-traffic conditions in JUNOS policy rules, in JUNOS ASP and JUNOS filter policy rules, and in PCMM policy rules.

The available configuration statements change depending on the type of policy rule that holds the condition and on the type of protocol that you specify.

To configure a classify-traffic condition, do the following:

1. Create a classify-traffic condition. See:
 - See Creating a Classify-Traffic Condition (C-Web Interface).
2. Configure source networks. You can configure source networks in one of two formats. See:
 - Configuring Source Networks (C-Web Interface)
 - Configuring Source Grouped Networks (C-Web Interface)

3. Configure destination networks. You can configure destination networks in one of two formats. See:
 - [Configuring Destination Networks \(C-Web Interface\)](#)
 - [Configuring Destination Grouped Networks \(C-Web Interface\)](#)
4. Configure protocol conditions. The type of protocol condition that you use depends on your configuration.
 - To configure protocol conditions that do not include ports, see:
 - [Configuring Protocol Conditions \(C-Web Interface\)](#)
 - To configure protocol conditions that include ports, see:
 - [Configuring Protocol Conditions with Ports \(C-Web Interface\)](#)
 - To configure protocol conditions in which the protocol that you specify is a parameter, see:
 - [Configuring Protocol Conditions with Parameters \(C-Web Interface\)](#)
 - To configure protocol conditions in which the protocol is TCP, see:
 - [Configuring TCP Conditions \(C-Web Interface\)](#)
 - To configure protocol conditions in which the protocol is ICMP, see:
 - [Configuring ICMP Conditions \(C-Web Interface\)](#)
 - To configure protocol conditions in which the protocol is IGMP, see:
 - [Configuring IGMP Conditions \(C-Web Interface\)](#)
 - To configure protocol conditions in which the protocol is IPSec, see:
 - [Configuring IPSec Conditions \(C-Web Interface\)](#)
 - To configure a ToS byte condition, see:
 - [Configuring IGMP Conditions \(C-Web Interface\)](#)
5. For JUNOS filter policies, configure a JUNOS filter condition. See:
 - [Configuring JUNOS Filter Conditions \(C-Web Interface\)](#)
6. For the stateful firewall and NAT policies, configure an application protocol condition. See:

- Configuring Application Protocol Conditions (C-Web Interface)



NOTE: PCMM classifiers support only the following classifiers:

- Source and destination IP addresses
- Network protocol
- Source or destination port
- Type-of-service (ToS) byte and ToS mask

The policy engine ignores all other values.

Configuring Template Activation (C-Web Interface)

Use this action to activate templates for RADIUS-enabled devices. You can configure template activation actions for AAA policy rules.

To configure template activation:

1. Configure a policy group, and specify the following configuration values:
 - List role—aaa
 - Rule type—aaa
2. In the Rule pane, in the Create new list, select **Template Activation**.
The Template Activation pane for the policy rule appears.
3. Enter information as described in the Help text in the Main pane, and click **Apply**.

Related Topics ■ Configuring Policy Groups (C-Web Interface)

Enabling Expansion of JUNOSe Classify-Traffic Conditions (C-Web Interface)

For information about expanded classifiers, see Policy Management Overview.

To specify whether or not the SAE expands the JUNOSe classify-traffic conditions into multiple classifiers before it installs the policy on the router:

1. Select **Configure**, and expand **Shared > SAE > Configuration > Policy Management Configuration**.
2. Check or clear the **Enable JUNOSe Classifier Expansion** box, and click **Apply**.

Specifying the PCMM Classifier Type (C-Web Interface)

To specify whether or not the SAE sends to the router classifiers that comply with PCMM I03:

1. Select **Configure**, expand **Shared > SAE > Configuration > Driver**, and select **pcmm**.
2. Check or clear the **Disable PCMM I03 Policy** box, and click **Apply**.

Specifying Port Access for Traffic Classification (C-Web Interface)

In the SRC software, the way that you specify a range of port numbers greater than or less than a specific value in a traffic classifier is different from the way you define a range in the configuration on JUNOS routers.

In the C-Web interface, you specify ranges by setting values in the Port Operation boxes.

To specify a range of port numbers greater or less than a specified value, you can:

- Define the full set of port numbers in the range to be allowed.
- Define the full set of port numbers in the range not allowed.

To configure port numbers greater than a defined value by specifying which values are allowed:

1. From the Port Operation list, select **eq**.
2. In the From Port box, enter the range of ports allowed.

For example, to specify access to all port numbers greater than 10, specify **11..65535**.

To configure port numbers greater than a defined value by specifying which values are not allowed:

1. From the Port Operation list, select **neq**.
2. In the From Port box, enter the range of ports not allowed.

For example, to specify access to all port numbers greater than 10, specify **1..9**.

To configure port numbers less than a defined value by specifying which values are allowed:

1. From the Port Operation list, select **eq**.
2. In the From Port box, enter the range of ports.

For example, to specify access to all port numbers less than 10, specify **1..9**.

To configure port numbers less than a defined value by specifying which values are not allowed:

1. From the Port Operation list, select **neq**.
2. In the From Port box, enter the range of ports.

For example, to specify access to all port numbers less than 10, specify **11..65535**.

Creating a Classify-Traffic Condition (C-Web Interface)

You create classify-traffic conditions within policy rules.

To add a classify-traffic condition:

1. In the side pane, select a policy rule.
2. From the Create new list, select **Traffic Condition**. Type a name for the traffic condition, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Source Networks (C-Web Interface)

To configure a source network in a classify-traffic condition:

1. In the side pane, expand a traffic condition, expand **Source Network**, and select **Network**.
2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Source Grouped Networks (C-Web Interface)

You can configure source networks in grouped format. For JUNOS ASP policy rules, you must enter source networks in grouped format.

To configure a grouped source network in a classify-traffic condition:

1. In the side pane, expand a traffic condition, expand **Source Network**, and select **Group Network**.
2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Destination Networks (C-Web Interface)

To configure a destination network in a classify-traffic condition:

1. In the side pane, expand a traffic condition, expand **Destination Network**, and select **Network**.
2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Destination Grouped Networks (C-Web Interface)

You can configure destination networks in grouped format. For JUNOS ASP policies rules, you must enter destination networks in grouped format.

To configure a grouped destination network in a classify-traffic condition:

1. In the side pane, expand a traffic condition, expand **Destination Network**, and select **Group Network**.
2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Protocol Conditions (C-Web Interface)

The procedure in this sections shows how to configure general protocol conditions.

- If your condition includes port numbers, use the procedure in Configuring Protocol Conditions with Ports (C-Web Interface).
- If your condition consists of a protocol that is assigned with a parameter value, use the procedure in Configuring Protocol Conditions with Parameters (C-Web Interface).

To configure general protocol conditions in a classify-traffic condition:

1. In the side pane, expand a traffic condition, and select **Protocol Condition**.
2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Protocol Conditions with Ports (C-Web Interface)

To configure general protocol conditions with ports in a classify-traffic condition:

1. In the side pane, expand a traffic condition, and select **Protocol Port Condition**.
2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

To configure source and destination ports for protocol conditions:

1. In the side pane, expand **Protocol Port Condition > Source Port**, and select **Port**.
2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.
3. In the side pane, expand **Protocol Port Condition > Destination Port**, and select **Port**.
4. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Protocol Conditions with Parameters (C-Web Interface)

Before you assign a parameter for the protocol, you must create a parameter of type protocol and commit the parameter configuration.

To configure a protocol condition that contains a parameter value for the protocol:

1. In the side pane, select a policy rule.
2. From the Create new list, expand a traffic condition, and select **Parameter Protocol Condition**.
3. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.
4. (Optional) To configure protocol attributes:
 - a. In the side pane, expand **Parameter Protocol Condition**, and select **Proto Attr**.
 - b. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

To configure source and destination ports:

1. In the side pane, expand **Proto Attr > Source Port**, and select **Port**.
2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.
3. In the side pane, expand **Proto Attr > Destination Port**, and select **Port**.
4. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring TCP Conditions (C-Web Interface)

To configure TCP conditions:

1. In the side pane, expand a traffic condition, and select **TCP Condition**.
2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

To configure source and destination ports for TCP conditions:

1. In the side pane, expand **TCP Condition > Source Port**, and select **Port**.
2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.
3. In the side pane, expand **TCP Condition > Destination Port**, and select **Port**.
4. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring ICMP Conditions (C-Web Interface)

To configure ICMP conditions:

1. In the side pane, expand a traffic condition, and select **Icmp Condition**.
2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring IGMP Conditions (C-Web Interface)

To configure IGMP conditions:

1. In the side pane, expand a traffic condition, and select **Igmp Condition**.
2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring IPSec Conditions (C-Web Interface)

You can configure IPSec conditions for JUNOS policy rules.

To configure IPSec conditions:

1. In the side pane, expand a JUNOS traffic condition, and select **Ipssec**.
2. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring ToS Byte Conditions (C-Web Interface)

Use this condition to define a particular traffic flow to the service's network for the DA IP field in the IP packet.

The CoS feature on JUNOS routing platforms supports DiffServ as well as six-bit IP header ToS byte settings. The DiffServ protocol uses the ToS byte in the IP header. The most significant six bits of this byte form the Differentiated Services code point (DSCP). The CoS feature uses DSCPs to determine the forwarding class associated with each packet. It also uses the ToS byte and ToS byte mask to determine IP precedence.

To configure ToS byte conditions in a classify-traffic condition:

1. In the side pane, expand a traffic condition, and select **ToS**.
2. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring JUNOS Filter Conditions (C-Web Interface)

To configure traffic match conditions in JUNOS filter policy rules:

1. In the side pane, select a JUNOS filter policy rule.
2. From the Create new list, select **Traffic Condition**. Type a name for the traffic condition, and click **OK**.
3. In the side pane, expand the traffic condition, and select **Traffic Match Condition**.
4. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Application Protocol Conditions (C-Web Interface)

You can define application protocols for the stateful firewall and NAT services to use in match condition rules. An application protocol defines application parameters by using information from network layer 3 and above. Examples of such applications are FTP and H.323.

To create and configure an application protocol condition:

1. In the side pane, select an ASP policy rule.
2. From the Create new list, select **Traffic Condition**. Type a name for the traffic condition, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.
4. From the Create new list, select Application Protocol Condition. Type a name for the application protocol condition, and click **OK**.
5. Enter information as described in the Help text in the main pane, and click **Apply**.
6. (Optional) To configure protocol attributes:
 - a. In the side pane, expand the application protocol condition, and select **Proto Attr**.
 - b. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.
7. (Optional) To configure source ports:
 - a. In the side pane, expand **Proto Attr > Destination Port**, and select **Port**.
 - b. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.
8. (Optional) To configure destination ports:
 - a. In the side pane, expand **Proto Attr > Source Port**, and select **Port**.
 - b. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring QoS Conditions with the C-Web Interface with the C-Web Interface

You can create QoS conditions within JUNOS scheduler policy rules.

To create a QoS condition:

1. In the side pane, select a JUNOS scheduler policy rule.
2. From the Create new list, select **Qos Condition**. Type a name for the QoS condition, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Actions (C-Web Interface)

Actions define the action taken on packets that match conditions in a policy rule. You create actions within policy rules. The type of action that you can create depends on the type of policy rule. See [Policy Management Overview](#).

Configure the action as described in the following sections:

- Configuring DOCSIS Actions (C-Web Interface) on page 192
- Configuring Filter Actions (C-Web Interface) on page 192
- Configuring FlowSpec Actions (C-Web Interface) on page 192
- Configuring Forward Actions (C-Web Interface) on page 193
- Configuring Forwarding Class Actions (C-Web Interface) on page 193
- Configuring Gate Spec Actions (C-Web Interface) on page 193
- Configuring Loss Priority Actions (C-Web Interface) on page 194
- Configuring Mark Actions (C-Web Interface) on page 194
- Configuring NAT Actions (C-Web Interface) on page 194
- Configuring Next-Hop Actions (C-Web Interface) on page 195
- Configuring Next-Interface Actions (C-Web Interface) on page 195
- Configuring Next-Rule Actions (C-Web Interface) on page 196
- Configuring Policer Actions (C-Web Interface) on page 196
- Configuring QoS Profile Attachment Actions (C-Web Interface) on page 197
- Configuring Rate-Limit Actions (C-Web Interface) on page 197
- Configuring Reject Actions (C-Web Interface) on page 198
- Configuring Routing Instance Actions (C-Web Interface) on page 198
- Configuring Scheduler Actions (C-Web Interface) on page 199
- Configuring Drop Profiles (C-Web Interface) on page 199
- Configuring Service Class Name Actions (C-Web Interface) on page 199
- Configuring Stateful Firewall Actions (C-Web Interface) on page 200
- Configuring Traffic-Class Actions (C-Web Interface) on page 200

- Configuring Traffic-Mirror Actions (C-Web Interface) on page 200
- Configuring Traffic-Shape Actions (C-Web Interface) on page 201

Configuring DOCSIS Actions (C-Web Interface)

You can configure Data over Cable Service Interface Specifications (DOCSIS) actions for *PacketCable Multimedia Specification* (PCMM) policy rules.

The types of DOCSIS actions that you can create are:

- Best effort
- Downstream
- Non-real-time polling service
- Real-time polling service
- Unsolicited grant service
- Unsolicited grant service with activity detection
- Parameter—This is a DOCSIS action with the service flow scheduling type set to a `trafficProfileType` parameter. You must enter a `trafficProfileType` parameter that has been created and committed.

To configure a DOCSIS action:

1. In the side pane, select a PCMM policy rule.
2. From the Create new list, select the type of DOCSIS action that you want to create. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Filter Actions (C-Web Interface)

Use this action to discard packets. You can configure filter actions for JUNOS filters and JUNOSe policy rules.

To configure a filter action:

1. In the side pane, select a JUNOS filter or JUNOSe policy rule.
2. From the Create new list, select **Filter**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring FlowSpec Actions (C-Web Interface)

A FlowSpec is made up of two parts, a traffic specification (TSpec) and a service request specification (RSpec). The TSpec describes the traffic requirements for the flow, and the RSpec specifies resource requirements for the desired service. You can configure FlowSpec actions for PCMM policy rules.

To configure a FlowSpec action:

1. In the side pane, select a PCMM policy rule.
2. From the Create new list, select **Flow Spec**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Forward Actions (C-Web Interface)

Use this action to forward packets, such as packets that are sent by means of a routing table. You can configure forward actions for JUNOS filters and JUNOS policy rules.

To configure a forward action:

1. In the side pane, select a JUNOS filter or JUNOS policy rule.
2. From the Create new list, select Forward. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Forwarding Class Actions (C-Web Interface)

You can configure forwarding class actions for JUNOS filter policy rules. The forwarding class action causes the router to assign a forwarding class to packets that match the associated classify-traffic condition.

To configure a forwarding class action:

1. In the side pane, select a JUNOS filter policy rule.
2. From the Create new list, select **Forwarding Class**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Gate Spec Actions (C-Web Interface)

You can configure GateSpec actions for PCMM policy rules. See Policy Management Overview for more information.

To configure a Gate Spec action:

1. In the side pane, select a PCMM policy rule.
2. From the Create new list, select **Gate Spec**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Loss Priority Actions (C-Web Interface)

You can configure loss priority actions for JUNOS filter policy rules. The loss priority action causes the router to assign a packet loss priority to packets that match the associated classify-traffic condition.

To configure a loss priority action:

1. In the side pane, select a JUNOS filter rule.
2. From the Create new list, select **Loss Priority**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Mark Actions (C-Web Interface)

Use this action to mark packets. You can configure mark actions for JUNOSe and PCMM policy rules.

To configure a mark action:

1. In the side pane, select a JUNOSe or PCMM policy rule.
2. From the Create new list, select **Mark**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.
4. Expand the mark action, and select **Info**.
5. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring NAT Actions (C-Web Interface)

You can configure NAT actions for JUNOS ASP policy rules. To configure a NAT action:

1. In the side pane, select a JUNOS ASP policy rule.
2. From the Create new list, select **NAT**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.
4. To configure the port range to restrict port translation when the NAT translation type is configured in dynamic-source mode:
 - a. In the side pane, select **Port**.
 - b. Click create, and enter information as described in the Help text in the main pane, and click **Apply**.
5. To configure the IP address ranges.
 - a. In the side pane, select **IP Network**.
 - b. In the main pane, click **Create**.

- c. In the side pane, expand **IP Network**, and select **Group Network**.
- d. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Next-Hop Actions (C-Web Interface)

Use this action for the ingress side of the interface to specify the next IP address where the classified packets should go. You can configure next-hop actions for JUNOS filters and JUNOS policy rules.

The captive portal feature is used to intercept HTTP requests from a subscriber to an unauthorized Web resource and redirect the requests to a dedicated Web page, the captive portal page. See Overview of Traffic Redirection.

In a captive portal environment, you would typically set up a next-hop action on a subscriber's interface that forwards traffic to the redirect engine. In this case, you would set the next-hop address to the address of the redirect server.

When you set up redirect server redundancy, both the active and redundant redirect servers share a virtual IP address so that subscribers can always reach the active redirect server. Subscribers send requests to the virtual IP address, and the router automatically sends the request to the active redirect server by means of a static route. In this case, you would set the next-hop address to the virtual IP address.

To configure a next-hop action:

1. In the side pane, select a JUNOS filters or JUNOS policy rules.
2. From the Create new list, select **Next Hop**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Next-Interface Actions (C-Web Interface)

Use this action to forward packets to a particular interface and/or a next-hop address. You can configure next-interface actions for JUNOS filters and JUNOS policy rules. On JUNOS routers, you can use this action for both ingress and egress parts of the interface.

To configure a next-interface action:

1. In the side pane, select a JUNOS filter or JUNOS policy rule.
2. From the Create new list, select **Next Interface**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Next-Rule Actions (C-Web Interface)

You can configure next-rule actions for JUNOS filter policy rules. If a packet matches the classify-traffic condition, the next-rule action causes the router to continue to the next rule in the policy list for evaluation.

To configure a next-rule action:

1. In the side pane, select a JUNOS filter policy rule.
2. From the Create new list, select **Next Rule**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Policer Actions (C-Web Interface)

The policer action specifies rate and burst size limits and the action taken if a packet exceeds those limits. You can create policer actions in JUNOS policer and JUNOS filter policy rules.

Each policer action has a packet action. The packet action specifies the action taken on a packet that exceeds its rate limits. You configure packet actions within policer actions. There are four types of actions that you can configure:

- Filter—Packets are discarded.
- Forwarding class—Packets are assigned to the forwarding class that you specify.
- Loss priority—Packets are assigned the loss priority that you specify.
- Parameter—The action specified by the parameter is applied. Before you assign a parameter, you must create a parameter of type packetOperation and commit the parameter configuration.

To configure a policer action:

1. In the side pane, select a JUNOS policer or JUNOS filter policy rule.
2. From the Create new list, select **Policer**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.
4. From the Create new list for the policer action, select **Packet Action**. Type a name for the action, and click **OK**.
5. Expand the packet action, and click on the type of packet action that you want to configure for this policer action.
6. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring QoS Profile Attachment Actions (C-Web Interface)

Use this action to specify the name of the QoS profile to attach to the router interface when this action is taken. You can configure QoS actions for JUNOS policy rules.

The router allows only one QoS profile to be attached to an interface at one time. Therefore, as a subscriber activates and deactivates different services, the QoS profile running on the interface needs to change. The SRC software provides a QoS-tracking plug-in (QTP) that you can use to ensure that as a subscriber activates and deactivates services, the required QoS profile is attached to the subscriber interface. See *Dynamically Managing QoS Profiles*.

To configure a QoS profile attachment action:

1. In the side pane, select a JUNOS policy rule.
2. From the Create new list, select **Qos Attach**. Type a name for the QoS profile attachment action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Rate-Limit Actions (C-Web Interface)

Use this action to define the quality of service. You can configure rate-limit actions for JUNOS policy rules.

To configure a rate-limit action:

1. In the side pane, select a JUNOS policy rule.
2. From the Create new list, select **Rate Limit**. Type a name for the rate-limit action, and click **OK**.
3. From the **Type** list, select the type of rate-limit action, either `one_rate` or `two_rate`, and click **Apply**.

The screen changes to display the parameters that you can configure for the type of rate-limit action that you selected.

Under the rate-limit action, there are three types of actions that you can configure:

- Committed action—Takes action on traffic flows that do not exceed the committed rate.
- Conformed action—Takes action on traffic flows that exceed the committed rate but remain below the peak rate.
- Exceed action—Takes action on traffic flows that exceed the peak rate.

For each committed, conformed, and exceed action, you can select one action to configure—filter, forward, mark, or parameter.

To configure an action for rate-limit actions:

1. Expand the rate-limit action, and expand the action that you want to configure.
2. To set an action to filter, in the side pane select **Filter**, and then click **Create** in the main pane.
3. To set an action to forward, in the side pane select **Forward**, and then click **Create** in the main pane.
4. To set an action to mark:
 - a. In the side pane, expand **Mark** and select **Mark Info**.
 - b. In the main pane, click **Create**.
 - c. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.
5. To set an action to parameter:
 - a. Make sure that you have a packetOperation parameter configured.
 - b. In the side pane, select **Parameter**, and then click **Create** in the main pane.
 - c. In the **Action** list, select a parameter.
 - d. Click **Apply**.

Configuring Reject Actions (C-Web Interface)

You can configure reject actions for JUNOS filter policy rules. The reject action causes the router to discard a packet and send an ICMP destination unreachable message.

To configure a reject action:

1. In the side pane, select a JUNOS filter policy rule.
2. From the Create new list, select **Reject**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Routing Instance Actions (C-Web Interface)

You can configure routing instance actions for JUNOS filter policy rules. Use routing instance actions for filter-based forwarding to direct traffic to a specific routing instance configured on the router.

To configure a routing instance action:

1. In the side pane, select a JUNOS filter policy rule.
2. From the Create new list, select **Routing Instance**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Scheduler Actions (C-Web Interface)

You use scheduler actions along with QoS conditions and traffic-shape actions to configure transmission scheduling and rate control. Schedulers define the priority, bandwidth, delay buffer size, rate control status, and random early detection (RED) drop profiles to be applied to a particular class of traffic. You can create scheduler actions in JUNOS scheduler policy rules.

To configure a scheduler action:

1. In the side pane, select a JUNOS schedule policy rule.
2. From the Create new list, select **Scheduler Action**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Drop Profiles (C-Web Interface)

You configure drop profiles within scheduler actions. Drop profiles support the RED process by defining the drop probabilities across the range of delay-buffer occupancy. For a packet to be dropped, it must match the drop profile. When a packet arrives, RED checks the queue fill level. If the fill level corresponds to a nonzero drop probability, the RED algorithm determines whether to drop the arriving packet. Depending on the drop probabilities, RED might drop packets aggressively long before the buffer becomes full, or it might drop only a few packets even if the buffer is almost full.

In drop profiles you configure the queue threshold and drop probability as paired values. The values can be either percentage values (segmented) or data points (interpolated). These two alternatives enable you to configure each drop probability at up to 64 fill-level/drop-probability paired values, or to configure a profile represented as a series of line segments. For more information about configuring fill level and drop probabilities, see the JUNOS routing platform documentation.

To configure drop profiles:

1. In the side pane, select a scheduler action.
2. From the Create new list, select **Drop Profile**. Type a name for the drop profile, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Service Class Name Actions (C-Web Interface)

You can configure service class name actions for PCMM policy rules.

To configure a service class name action:

1. In the side pane, select a PCMM policy rule.

2. From the Create new list, select **Service Class Name**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Stateful Firewall Actions (C-Web Interface)

You can configure stateful firewall actions for JUNOS ASP policy rules. Stateful firewall actions specify the action to take on packets that match the classify-traffic condition.

1. In the side pane, select a JUNOS ASP policy rule.
2. From the Create new list, select **Stateful Firewalls**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.
4. Expand the policy list and expand **Packet Action**.

A list of actions that can be taken on a packet appears in the side pane. You can configure one type of action.

5. Select the action that you want to configure for the stateful firewall, and click **Create**.
6. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Traffic-Class Actions (C-Web Interface)

Use this action to put packets in a particular traffic class. You can configure traffic-class actions for JUNOSe policy rules.

To configure a traffic-class action:

1. In the side pane, select a JUNOSe policy rule.
2. From the Create new list, select **Traffic Class**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Traffic-Mirror Actions (C-Web Interface)

Use this action to mirror traffic from a destination to a source or from a source to a destination. You can configure traffic-mirror actions for JUNOS filter input policy rules.

Before you use traffic-mirror actions, you must configure forwarding options on JUNOS routing platforms for port mirroring and next-hop group. For information about how these features work on the router, see the JUNOS Policy Framework Configuration Guide.

The rule containing a traffic-mirror action must comply with these conditions:

- It must be combined with forward actions in the same rule. One of the forward actions must accept the traffic if the source and/or destination IP addresses do not match the conditions.
- It contains either no classify-traffic condition or only one classify-traffic condition.
- It can be marked for accounting.

To configure a traffic-mirror action:

1. In the side pane, select a JUNOS filter policy rule.
2. From the Create new list, select **Traffic Mirror**. Type a name for the action, and click **OK**.
3. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Traffic-Shape Actions (C-Web Interface)

Traffic-shape actions specify the maximum rate of traffic transmitted on an interface. You can create traffic-shape actions in JUNOS shaping policy rules.

To configure a traffic-shape action:

1. In the side pane, select a JUNOS shaping policy rule.
2. From the Create new list, select **Traffic Shape**. Type a name for the action, and click **OK**.
3. To create a new value for the Rate parameter, enter a value in the box, and click **Add**.
4. Enter information as described in the Help text in the main pane, and click **Apply**.

Chapter 24

Configuring Local and Global Parameters (C-Web Interface)

This chapter describes how to configure global and local parameters with the C-Web Interface. You can also use the following to configure parameters:

Topics in this chapter include:

- Viewing Predefined Global Parameters (C-Web Interface) on page 203
- Configuring Global Parameters (C-Web Interface) on page 203
- Configuring Local Parameters (C-Web Interface) on page 203
- Viewing Runtime Parameters (C-Web Interface) on page 204

Viewing Predefined Global Parameters (C-Web Interface)

Purpose View predefined global parameters.

Action 1. Click **Configure > Policies**, and then expand **Global Parameters**.

Configuring Global Parameters (C-Web Interface)

If you change global variables for policies, the change takes effect the next time a service is activated; the change does not take effect for active service sessions.

To create a global parameter:

1. Click **Configure > Policies**, and select **Global Parameters**.
2. In the Create new list, select **Parameter**. Type a name for the new parameter, and click **OK**.
3. Enter information as described in the help text in the main pane, and click **Apply**.

Related Topics For valid values of each parameter type, see Overview of Global and Local Parameters.

Configuring Local Parameters (C-Web Interface)

You create local parameters within a policy group.

To configure local parameters:

1. In the side pane, expand a policy group, and select **Local Parameters**.
2. In the Create new list, select **Parameter**. Type a name for the new parameter, and click **OK**.
3. Enter information as described in the help text in the main pane, and click **Apply**.

Related Topics For valid values of each parameter type, see Overview of Global and Local Parameters.

Viewing Runtime Parameters (C-Web Interface)

Purpose Runtime parameters are parameters that are filled in with an actual value from the running system when the policy is installed. The SRC software comes with many predefined runtime parameters.

- Action** To view runtime parameters:
1. Click **Configure > Policies > Global Parameters > Runtime Parameters**.
 2. In the side pane, select the runtime parameter that you want to view.

Chapter 25

Configuring Services (C-Web Interface)

- Before You Configure SRC Services on page 205
- Enabling the Service Configuration on the C-Web Interface on page 205
- Adding a Normal Service (C-Web Interface) on page 206
- Setting Parameter Values for Services (C-Web Interface) on page 206
- Configuring Service Fragments for an Aggregate Service (C-Web Interface) on page 206
- Configuring Timers for Aggregate Services (C-Web Interface) on page 207
- Adding an Infrastructure Service (C-Web Interface) on page 207
- Configuring Script Services (C-Web Interface) on page 207
- Adding a Mutex Group (C-Web Interface) on page 208
- Configuring Service Scopes (C-Web Interface) on page 208
- Example: Configuring a Limited Set of Services for Organizations (C-Web Interface) on page 209
- Example: Customizing Generic Services to Particular Regions (C-Web Interface) on page 211

Before You Configure SRC Services

Before you configure services:

- Plan the services that you want to make available to subscribers.
- Configure the policies for a service to use. For information about configuring policies, see [Configuring Policy Groups](#) and [Configuring Policy Lists](#).

Enabling the Service Configuration on the C-Web Interface

Before you can configure services with the C-Web interface, you must enable the policy, service, and subscriber editor on the C-Web interface. To do so:

1. Click **Manage > Enable**.

The Enable pane appears.

2. From the Component list, select **editor**, and click **OK**.

Adding a Normal Service (C-Web Interface)

To add a normal service:

1. Click **Configure**, and expand **Services**.
2. You can add a normal service to the global service scope or to a service scope.
 - To add a normal service to the global service scope, click **Global**.
 - To add a normal service to the service scope, click the specified scope.
3. In the Create new list, select **Service**.
4. In the dialog box, type a name for the new Service. and click **OK**.

The Service: *<name>* pane appears.

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

Setting Parameter Values for Services (C-Web Interface)

Using parameters, you can define general settings in one SRC object and provide specific values for that setting in another object. For example, you can define the general settings for a rate limiter in a policy, insert a parameter for a rate in the policy, and provide specific values for the rate in each service that uses this policy.

To configure parameters for services:

1. Click **Configure**, and expand **Services**.
2. You can configure a parameter for services in the global service scope or in a service scope.
 - To configure a parameter for services in the global service scope, expand **Global**, and then expand the specified service.
 - To configure a parameter for services in the service scope, expand the specified scope and service.
3. Click **Parameter**.

The Parameter pane appears.

4. Enter information as described in the Help text in the main pane, and click **Apply**.

Related Topics ■ *SRC-PE Services and Policies Guide*

Configuring Service Fragments for an Aggregate Service (C-Web Interface)

To configure service fragments for an aggregate service:

1. Click **Configure**, and expand **Services**.

2. You can configure service fragments for an aggregate service in the global service scope or in a service scope.
 - To configure service fragments for an aggregate service in the global service scope, expand **Global**, and then expand the specified service.
 - To configure service fragments for an aggregate service in the service scope, expand the specified scope and service.

Related Topics ■ Configuring Service Fragments for an Aggregate Service (SRC CLI)

Configuring Timers for Aggregate Services (C-Web Interface)

You can change the values for several timers to specify the intervals associated with monitoring and activating aggregate sessions.

To configure timers used by aggregate services:

1. Click **Configure**, and expand **Shared > SAE > Configuration**.
2. Click **Aggregate Services**.

The Aggregate Services pane appears.

3. Click the **Create** button.

The Aggregate Services pane reappears.

4. Enter information as described in the Help text in the main pane, and click **Apply**.

Related Topics ■ Configuring Service Fragments for an Aggregate Service (SRC CLI)

Adding an Infrastructure Service (C-Web Interface)

To add an infrastructure service:

- Add the service to be shared, as described in Adding a Normal Service (C-Web Interface).
 - a. When entering information in the Services pane, select **Infrastructure** from the Type list.
 - b. Type a name in the RADIUS Class box to configure the name of the service to be shared.

Related Topics ■ *SRC-PE Services and Policies Guide*

Configuring Script Services (C-Web Interface)

Before you configure a script service, make sure that you know the location of the script file that the service will reference.

To configure a script service:

1. Add a service as described in Adding a Normal Service (C-Web Interface).
2. When entering information in the Services pane, select **Script** from the Type list.

Related Topics ■ *SRC-PE Services and Policies Guide*

Adding a Mutex Group (C-Web Interface)

You can add a mutex group in the global service scope or in a service scope.

To add a mutex group:

1. Click **Configure**, and expand **Services**.
2. To add a mutex group in the global service scope:
 - a. Click **Global**.
 - b. From the Create new list, select **Mutex Group**.
 - c. Type a name for the new mutex group in the dialog box, and click **OK**.
3. To add a mutex group in the service scope:
 - a. Click the specified scope.
 - b. From the Create new list, select **Mutex Group**.
 - c. Type a name for the new mutex group in the dialog box, and click **OK**.
4. The Mutex Group: *< name >* pane appears.
5. Enter information as described in the Help text in the main pane, and click **Apply**.

Related Topics ■ *SRC-PE Services and Policies Guide*

Configuring Service Scopes (C-Web Interface)

The tasks to configure a service scope are:

1. Adding Service Scopes (C-Web Interface) on page 208
2. Assigning Services and Mutex Groups to Service Scopes (C-Web Interface) on page 209
3. Assigning Service Scopes to VRs or Subscribers (C-Web Interface) on page 209

Adding Service Scopes (C-Web Interface)

To add a service scope:

1. Click **Configure > Services**.

The Services pane appears.

2. From the Create new list, select **Scope**.
3. Enter a name for the new Scope, and click **OK**.

The Scope: *< name >* pane appears.

4. Enter information as described in the Help text in the main pane, and click **Apply**.

Assigning Services and Mutex Groups to Service Scopes (C-Web Interface)

To assign services and mutex groups to a scope:

1. Click **Configure**, and expand **Services**.
2. Click the specified scope.

The Scope: *< name >* pane appears.

3. From the Create new list, select **Mutex Group** or **Service**.
4. In the dialog box, type a name for the new mutex group or service, and click **OK**.

Assigning Service Scopes to VRs or Subscribers (C-Web Interface)

You can assign multiple service scopes to a VR or subscriber, and you can assign a service scope to multiple VRs and subscribers.

To assign a service scope:

1. Click **Configure**, and expand **Shared**.
2. Expand **Network** and the specified device.
3. Click the specified virtual router.

The Virtual Router: *< name >* pane appears.

4. In the **Scope** box, select a virtual router as described in the Help text in the main pane, and click **Apply**.

Example: Configuring a Limited Set of Services for Organizations (C-Web Interface)

You can use service scopes to create a limited set of services to be made available to specified organizations. For enterprise users, you can define a set of services available on the JUNOS routing platform.

To deliver a small set of services to specified enterprises:

1. Create a scope for the services to be made available. For example, see the EntJunos scope in the sample data. For information about loading the sample

data, see Loading Sample Data in to a Juniper Networks Database with the C-Web Interface.

To display the sample data:

- a. Click **Configure**, and expand **Services**.
- b. Click **EntJUNOS**.

The EntJUNOS pane appears.

2. Add services to the scope, such as those in the sample data in the EntJunos scope.
 - a. Expand **EntJunos** to view the list of services in the sample data.
 - b. To add services to the scope:
 - From the Create new list, select **Service**.
 - In the dialog box, type a name for the new service, and click **OK**.

The Service pane appears.

- Enter information as described in the Help text in the main pane, and click **Apply**.

3. Assign the scope to one or more enterprise subscribers. For example, assign the EntJunos scope to the Acme enterprise.

To assign the EntJunos scope to the Acme enterprise:

- a. Click **Configure > Subscribers**.

The Subscribers pane appears.

- b. From the Create new list, select **Retailer**.
- c. In the dialog box, type **ENT**, and click **OK**.
- d. In the side pane, click **Ent**.

The Subscribers pane appears.

- e. From the Create new list, select **Subscriber Folder**.
- f. In the dialog box, type **entAcme**, and click **OK**.
- g. In the side pane, click **entAcme**.

The Subscriber pane appears.

- h. From the Create new list, select **Enterprise**.
- i. In the dialog box, type **Acme**, and click **OK**.
- j. From the Scope box in the main pane, select **EntJunos**, and click **Apply**.

If you use a portal to manage enterprises, you see only the services for the specified scope from the portal. Other services are not visible to the IT managers

who manage services and subscriptions from the enterprise service portal. For example, you can see the services available to Acme in Enterprise Manager Portal.

Example: Customizing Generic Services to Particular Regions (C-Web Interface)

You can use service scopes to customize a generic audio service called Audio-Bronze on a regional basis. This example assumes that the network is configured so that VR boston serves the Boston subnet and VR chicago serves the Chicago subnet.

When the network starts operating, the SAE substitutes the parameters you specified in the service scope definition for the corresponding fields in the service subordinate to that scope.

May want to add line drawing of configuration.

To customize the new service Audio-Bronze for the Boston and Chicago subnets:

1. Add the Audio-Bronze service within a service scope called boston, and configure the IP address and mask used by VR boston in the parameter configuration.

This IP address and mask determine an access point to the service provider's equipment.

- a. Click **Configure**, and expand **Services**.
- b. Click **POP-Boston**.
- c. From the Create new list, select **Service**.
- d. In the dialog box, enter **Audio-Bronze**, and click **OK**.
- e. In the side pane, expand **Audio-Bronze**, and click **Parameter**.

The Parameter pane appears.

- f. Click the **Create** button.
- g. In the Service IP Address box, type **10.10.40.33**.
- h. In the Service IP Mask box, type **255.255.255.255**, and click **Apply**.
2. Add another Audio-Bronze service within a service scope called chicago, and specify the IP address and mask used by VR chicago.

To do this:

- a. Click **Services**.

The Services pane appears.

- b. From the Create new list, select **Scope**.
- c. In the dialog box, enter **chicago**.
- d. In the side pane, click **chicago**.

- e. From the Create new list, select **Service**.
 - f. In the dialog box, enter **Audio-Bronze**, and click **OK**.
 - g. In the side pane, expand **Audio-Bronze**, and click **Parameter**.
The Parameter pane appears.
 - h. Click the **Create** button.
 - i. In the Service IP Address box, type **10.10.55.1**.
 - j. In the Service IP Mask box, type **255.255.255.255**, and click **Apply**.
3. Assign service scope boston to virtual router boston.
To do this:
 - a. In the side pane, expand **Shared**, and click **Network**.
The Network pane appears.
 - b. From the Create new list, select **Device**.
 - c. In the dialog box, type **BostonRouter**, and click **OK**.
 - d. In the side pane, click **BostonRouter**.
The Device: BostonRouter pane appears.
 - e. From the Create new list, select **Virtual Router**.
 - f. In the dialog box, type **multimedia**, and click **OK**.
 - g. In the side pane, click **multimedia**.
The Virtual Router: multimedia pane appears.
 - h. In the Scope box, type **multimedia**.
 4. Assign service scope chicago to virtual router chicago.
 - a. Expand **Shared**, and click **Network**.
The Network pane appears.
 - b. From the Create new list, select **Device**.
 - c. In the dialog box, type **ChicagoRouter**, and click **OK**.
 - d. In the side pane, click **ChicagoRouter**.
The Device:ChicagoRouter pane appears.
 - e. From the Create new list, select **Virtual Router**.
 - f. In the dialog box, enter **chicago**, and click **OK**.
 - g. In the side pane, click **chicago**.

The Virtual Router: **chicago** pane appears.

- h. In the Scope box, select **chicago**, and click **Apply**.

Chapter 26

Scheduling Services (C-Web Interface)

This chapter describes how to create and manage schedules for services with the C-Web interface.

Topics in this chapter include:

- Setting the Action Threshold and Preparation Time with the C-Web Interface on page 215
- Authorizing Scheduled Services (C-Web Interface) on page 216
- Adding a Service Schedule (C-Web Interface) on page 216
- Example: Configuring Different Service Tiers for Different Days (C-Web Interface) on page 222
- Example: Configuring a Service to Be Active During Nonwork Hours (C-Web Interface) on page 225
- Example: Configuring a Service to Be Available for a Specified Interval (C-Web Interface) on page 228

Setting the Action Threshold and Preparation Time with the C-Web Interface

You can set the action threshold and preparation time for all schedules; you cannot set these values for individual schedules.

To set the action threshold and preparation time for an SAE:

1. Click **Configure**, expand **Shared > SAE > Configuration**, and click **Time Based Policies**.

The Time Based Policies pane appears.

2. Click the **Create** button.
3. Enter the information as described in the Help text in the main pane, and click **Apply**.

Authorizing Scheduled Services (C-Web Interface)

You can configure an authorization plug-in to authorize a scheduled service in the following ways:

1. Defining an Authorization Plug-In for a Scheduled Service in the Global Configuration (C-Web Interface) on page 216
2. Defining an Authorization Plug-In for a Scheduled Service in the Service Scope (C-Web Interface) on page 216

Defining an Authorization Plug-In for a Scheduled Service in the Global Configuration (C-Web Interface)

To define an authorization plug-in for a scheduled service in the global configuration:

1. Click **Configure**, and expand **Services > Global**.

The Global pane appears.

2. Click the specified **Service**.

The Service: *< name >* pane appears.

3. In the Authorization Plug In box, select the name of the authorization plug-in that will authorize the schedule for this service. For example, select **scheduleAuth** in the Suggested values box, and click the right arrow to move it to the Selected values box.
4. Click **Apply**.

Defining an Authorization Plug-In for a Scheduled Service in the Service Scope (C-Web Interface)

To define an authorization plug-in for a scheduled service in the service scope:

1. Click **Configure**, and expand **Services** and the specified scope.
2. Click the specified service.

The Service: *< name >* pane appears.

3. In the Authorization Plug In box, select the name of the authorization plug-in that will authorize the schedule for this service. For example, select **scheduleAuth** in the Suggested values box, and click the right arrow to move it to the Selected values box.
4. Click **Apply**.

Adding a Service Schedule (C-Web Interface)

The following tasks describe how to create service schedules for SRC objects:

1. Adding a Service Schedule for Scopes (C-Web Interface) on page 217
2. Adding a Service Schedule for Services (C-Web Interface) on page 217

3. Adding a Service Schedule for Retailers (C-Web Interface) on page 218
4. Adding a Service Schedule for Enterprises (C-Web Interface) on page 219
5. Adding a Service Schedule for Subscribers in an Enterprise (C-Web Interface) on page 220
6. Setting the Time Schedule (C-Web Interface) on page 220
7. Setting the Action (C-Web Interface) on page 221
8. Defining Attributes for Service Activation (C-Web Interface) on page 222

Adding a Service Schedule for Scopes (C-Web Interface)

To add a service schedule for scopes:

1. Click **Configure**, expand **Services**, and click the specified scope.

The Scope: *< name >* pane appears.

2. From the Create new list, select **Schedule**.
3. In the dialog box, enter a name for the new Schedule, and click **OK**.

The Schedule: *< name >* pane appears.

4. In the Description box, type a unique name for the service schedule, and click **Apply**.
5. A number of schedule events, or rules, constitute each service schedule. To create schedule events for the service schedule:
 - a. From the Create new list, select **Event**.
 - b. In the dialog box, type a name for the new Event, and click **OK**.

An event consists of the schedule time, any excluded times, and a list of actions.

- To specify the time schedule, see Setting the Time Schedule (C-Web Interface).
- To specify the actions, see Setting the Action (C-Web Interface).



NOTE: If you change or remove the name of a service that is referenced by a schedule, the SRC software treats this case like one in which no subscribers have a subscription to this service. In both cases, the action for the service is not taken. The software does not regard either case as an error in the schedule; a failure is not reported.

Adding a Service Schedule for Services (C-Web Interface)

To add a service schedule for services:

1. Click **Configure**, expand **Services**, and click **Global**.

The Global pane appears.

2. From the Create new list, select **Schedule**.
3. In the dialog box, enter a name for the new Schedule, and click **OK**.

The Schedule: *<name>* pane appears.

4. In the Description box, type a name for the service schedule, and click **Apply**.
5. A number of schedule events, or rules, constitute each service schedule. To create schedule events for the service schedule:
 - a. From the Create new list, select **Event**.
 - b. In the dialog box, type a name for the new Event, and click **OK**.

An event consists of the schedule time, any excluded times, and a list of actions.

- To specify the time schedule, see Setting the Time Schedule (C-Web Interface).
- To specify the actions, see Setting the Action (C-Web Interface).



NOTE: If you change or remove the name of a service that is referenced by a schedule, the SRC software treats this case like one in which no subscribers have a subscription to this service. In both cases, the action for the service is not taken. The software does not regard either case as an error in the schedule; a failure is not reported.

Adding a Service Schedule for Retailers (C-Web Interface)

To add a service schedule for retailers:

1. Click **Configure**, expand **Subscribers**, and click a specified retailer.

The Retailer: *<name>* pane appears.

2. From the Create new list, select **Schedule**.
3. In the dialog box, enter a name for the new Schedule, and click **OK**.

The Schedule: *<name>* pane appears.

4. In the Description box, type a name for the service schedule, and click **Apply**.
5. A number of schedule events, or rules, constitute each service schedule. To create schedule events for the service schedule:
 - a. From the Create new list, select **Event**.
 - b. In the dialog box, type a name for the new Event, and click **OK**.

An event consists of the schedule time, any excluded times, and a list of actions.

- To specify the time schedule, see Setting the Time Schedule (C-Web Interface).
- To specify the actions, see Setting the Action (C-Web Interface).



NOTE: If you change or remove the name of a service that is referenced by a schedule, the SRC software treats this case like one in which no subscribers have a subscription to this service. In both cases, the action for the service is not taken. The software does not regard either case as an error in the schedule; a failure is not reported.

Adding a Service Schedule for Enterprises (C-Web Interface)

To add a service schedule for enterprises:

1. Click **Configure**, and expand **Subscribers**.
2. Navigate to the enterprise for which you want to configure a schedule. For example, expand the following specified folders:
retailer > subscriber folder > enterprise > schedule.

The Schedule: < *name* > pane appears.

3. From the Create new list, select **Schedule**.
4. In the dialog box, enter a name for the new Schedule, and click **OK**.

The Schedule: < *name* > pane appears.

5. In the Description box, type a name for the service schedule, and click **Apply**.
6. A number of schedule events, or rules, constitute each service schedule. To create schedule events for the service schedule:
 - a. From the Create new list, select **Event**.
 - b. In the dialog box, type a name for the new Event, and click **OK**.

An event consists of the schedule time, any excluded times, and a list of actions.

- To specify the time schedule, see Setting the Time Schedule (C-Web Interface).
- To specify the actions, see Setting the Action (C-Web Interface).



NOTE: If you change or remove the name of a service that is referenced by a schedule, the SRC software treats this case like one in which no subscribers have a subscription to this service. In both cases, the action for the service is not taken. The software does not regard either case as an error in the schedule; a failure is not reported.

Adding a Service Schedule for Subscribers in an Enterprise (C-Web Interface)

To add a service schedule for subscribers in an enterprise:

1. Click **Configure**, and expand **Subscribers**.
2. Navigate to the schedule configuration for the specified schedule. For example, expand the following specified folders:
retailer > subscriber folder > subscriber > schedule.

The Schedule: <name> pane appears.

3. From the Create new list, select **Schedule**.
4. In the dialog box, enter a name for the new Schedule, and click **OK**.

The Schedule: <name> pane appears.

5. In the Description box, type a description for the service schedule, and click **Apply**.
6. A number of schedule events, or rules, constitute each service schedule. To create schedule events for the service schedule:
 - a. From the Create new list, select **Event**.
 - b. In the dialog box, type a name for the new Event, and click **OK**.

An event consists of the schedule time, any excluded times, and a list of actions.

- To specify the time schedule, see Setting the Time Schedule (C-Web Interface).
- To specify the actions, see Setting the Action (C-Web Interface).



NOTE: If you change or remove the name of a service that is referenced by a schedule, the SRC software treats this case like one in which no subscribers have a subscription to this service. In both cases, the action for the service is not taken. The software does not regard either case as an error in the schedule; a failure is not reported.

Setting the Time Schedule (C-Web Interface)

Before you configure the time schedule, create the schedule.

When you set up a time schedule for an event, you specify:

- For event schedules—Time at which an action is to occur; the from date and time information
- For schedules for services that have authorization configured—Beginning and end of the interval; the to date and time information
- For exclusions—Times to be excluded from that schedule

To configure the time schedule:

1. Click **Configure**, and navigate to the specified service schedule.
2. From the Create new list, select **Except** (to set an exclusion).
3. In the dialog box, type a name for the new Except. The specified name is not stored as an identifier, so the arbitrary value can be as simple as a number.
4. Click **From** in the side pane.

The From pane appears.

5. Click the **Create** button.

The From pane reappears. This pane allows you to specify the effective period in which to schedule the event. This period is the interval after the associated from or to time during which the scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

6. Enter the information as described in the Help text in the main pane, and click **Apply**.
7. Click **To** in the side pane.

The To pane appears.

8. Click the **Create** button.

The To pane reappears. This pane allows you to specify the effective period in which to schedule the event. This period is the interval after the associated from or to time during which the scheduled action can be initiated by a subscriber who is logging in to a subscriber session.

9. Enter the information as described in the Help text in the main pane, and click **Apply**.

Setting the Action (C-Web Interface)

Before you configure the time schedule, create the schedule.

To configure the actions for the service schedule:

1. Click **Configure**, and navigate to the specified service schedule.
2. Click **Event** in the side pane.

The Event: *< name >* pane appears.

3. From the Create new list:
 - a. Select **Action**.
 - b. In the dialog box, type a name for the new Action, and click **OK**. The specified name is not stored as an identifier, so the arbitrary value can be as simple as a number.

The Action: *< name >* pane appears.

4. Enter the information as described in the Help text in the main pane, and click **Apply**.

- The Type values (deny and deny-deactivate) apply only to services that have an authorization plug-in configured. For more information, see *Authorizing Scheduled Services (C-Web Interface)* .
- For more information about the Substitution box, see the `activateService` method of the SAE external interface in the SAE CORBA remote API documentation on the Juniper Networks Web site at

<http://www.juniper.net/techpubs/software/management/src/api-index.html>

Defining Attributes for Service Activation (C-Web Interface)

To define the attributes for service activation:

1. Click **Configure** and access the service schedule for the objects for which you can create a service schedule. The following example provides steps for defining attributes for service activation for a subscriber action.
2. Expand **Subscribers** and expand the following specified folders: `retailer > subscriber folder > subscriber > schedule > event > action`.
3. Click **Attribute**.

The Attribute pane appears.

4. From the Create new list, select the attribute to set before the service is activated.

The Attribute `< name >` pane appears.

5. In the dialog box, type a value as described in the Help text in the main pane, and click **Apply**.

Subscription attributes apply only to service activations.

Example: Configuring Different Service Tiers for Different Days (C-Web Interface)

This example shows how to configure a schedule for an audio service to provide:

- Gold level of service on weekends
- Bronze level of service on weekdays

The sample schedule:

- Uses the Audio-Gold and Audio-Bronze services in the sample data.
- Activates the Audio-Gold service and denies the Audio-Bronze service on Saturday.
- Activates the Audio-Bronze service and denies and deactivates the Audio-Gold service on Monday.
- Does not have a preparation time configured for the SAE.

For demonstration purposes, the sample schedule is configured in the global configuration to make the service schedule available to all subscribers to the two

audio services. It is assumed that subscribers are continuously logged in to the system to access the audio services.

To configure a schedule to make the Audio-Gold service available on Saturday and Sunday and the Audio-Bronze service available for the rest of the week:

1. Enter a unique name for the service schedule (for example, audioSchedule):
 - a. Click **Configure**, expand **Services**, and Click **Global**.
The Global pane appears.
 - b. From the Create new list, select **Schedule**.
 - c. In the dialog box, type **audioSchedule** as the name of the new Schedule, and click **OK**.
The Schedule: audioSchedule pane appears.
 - d. In the Description box, type a description of the service schedule, and click **Apply**.
2. Enter a name for the schedule event (for example, audioTime1):
 - a. From the Create new list, select **Event**.
 - b. In the dialog box, type **audioTime1** as the name of the new Event, and click **OK**.
 - c. From the Create new list, select **Action**.
 - d. In the dialog box, type **action-1**, and click **OK**.
The Action: action-1 pane appears.
 - From the Service list, select **Audio-Gold**.
 - From the Type list, select **activate**, and click **Apply**.
 - e. In the side pane, click **From** under the **Event: audioTime1** folder.
The From pane appears.
 - f. Click the **Create** button.
The From pane reappears.
3. For the time, specify the day of the week as Saturday, and for the actions, specify activate for the Audio-Gold Service and deny-deactivate for the Audio-Bronze service:
 - a. In the Day Of Week box, type **6** (specifying Saturday), and click **Apply**.
 - b. In the side pane, click **Event: audioTime1**.
The Event: audioTime1 pane appears.
 - c. From the Create new list, select **Action**.
 - d. In the dialog box, type **action-2**, and click **OK**.

The Action: action-2 pane appears.

- From the Service list, select **Audio-Bronze**.
- From the Type list, select **deny-deactivate**, and click **Apply**.

4. Enter a name for the schedule event (for example, audioTime2):

- a. In the side pane, click **Schedule: audioSchedule**.

The Schedule: audioSchedule pane appears.

- b. From the Create new list, select **Event**.
- c. In the dialog box, type **audioTime2** as the name of the new Event, and click **OK**.
- d. From the Create new list, select **Action**.
- e. In the dialog box, type **action-1**, and click **OK**.

The Action: action-1 pane appears.

- From the Service list, select **Audio-Bronze**.
- From the Type list, select **activate**, and click **Apply**.

- f. In the side pane, click **From** under the **Event: audioTime2** folder.

The From pane appears.

- g. Click the **Create** button.

The From pane reappears.

5. For the time, specify the day of the week as Monday, and for the actions, specify activate for the Audio-Bronze service and deny-deactivate for the Audio-Gold service:

- a. In the Day Of Week box, type **1** (specifying Monday), and click **Apply**.
- b. In the side pane, click **Event: audioTime2**.

The Event: audioTime2 pane appears.

- c. From the Create new list, select **Action**.
- d. In the dialog box, type **action-2**, and click **OK**.

The Action: action-2 pane appears.

- From the Service list, select **Audio-Gold**.
- From the Type list, select **deny-deactivate**, and click **Apply**.

Example: Configuring a Service to Be Active During Nonwork Hours (C-Web Interface)

This example shows how to configure a schedule for the Internet-Gold service in the sample data to be active:

- Monday–Friday outside the 8:30 AM to 4:30 PM work day
- January 1 of the following year—All day

The sample schedule:

- Deactivates the Internet-Gold service from 8:30 AM through 4:29 PM.
- Activates the service at 4:30 PM.
- Does not have a preparation time configured for the SAE.

This configuration avoids schedule overlap.

For demonstration purposes, the sample schedule is configured in the global configuration to make the service schedule available to all subscribers to the Internet-Gold service.

To configure a schedule to make a service available outside work hours and on January 1:

1. Specify the default schedule authorization plug-in for the Internet-Gold service:
 - a. Click **Configure**, expand **Services > Global**, and click **Service: Internet-Gold**.

The Service: Internet-Gold pane appears.

- b. In the Authorization Plug In box:
 - Type **scheduleAuth** in the Optionally, add a new value box, and click **Add**.

ScheduleAuth displays in the Selected values box.

- In the Selected values box, select **scheduleAuth** and click **Apply**.

2. Enter a unique name for the service schedule (for example, afterHours):

- a. Click **Global**.

The Global pane appears.

- b. From the Create new box, select **Schedule**.
 - c. In the dialog box, type **afterHours** as the name of the new Schedule, and click **OK**.

The Schedule: afterHours pane appears.

- d. In the Description box, enter a description for the schedule, and click **Apply**.

3. Enter a name for the schedule event (for example, goldTime):

- a. From the Create new list, select **Event**.
 - b. In the dialog box, type **goldTime** as the name of the new Event, and click **OK**.
4. For the time, specify the day of the week as Monday through Friday, and the schedule starting at 8:30 AM and ending at 4:29 PM (16:29) each day:
 - a. In the side pane, expand **Event: goldTime**, and click **From**.
 The From pane appears.
 - b. Click the **Create** button, and enter these values in the following boxes:
 - Day Of Week: 1
 - Hour: 8
 - Minute: 30
 - c. Click **Apply**.
 - d. In the side pane, click **To** under the **Event: goldTime** folder.
 The To pane appears.
 - e. Click the **Create** button, and enter these values in the following boxes:
 - Day Of Week: 5
 - Hour: 16
 - Minute: 29
 - f. Click **Apply**.
5. Enter a name for the exclusion (for example, exclude-1), and specify a one-time exclusion for January 1:
 - a. In the side pane, click **Event: goldTime**.
 - b. From the Create new box, select **Except**.
 - c. In the dialog box, type **exclude-1**
 - d. In the side pane, click **From** under the **Except: exclude-1** folder.
 The From pane appears.
 - e. Enter these values in the following boxes:
 - Day of Month: 1
 - Month: 1

By excluding January 1 from the schedule, the Internet-Gold service is active all day.
 - f. Click **Apply**.

6. Enter a name for the action (for example, action-1), and specify deny-deactivate for the Internet-Gold service:

- a. In the side pane, click **Event: goldTime**.

The Event: goldTime pane appears.

- b. From the Create new list, select **Action**.

- c. In the dialog box, type **action-1** as the name of the new Action, and click **OK**.

The Action: action-1 pane appears.

- In the Service list, select **Internet-Gold**.

- In the Type list, select **deny-deactivate**, and click **Apply**.

7. Enter a name for the schedule event (for example, goldTime2):

- a. In the side pane, click **Schedule: afterHours**.

The Schedule: afterHours pane appears.

- b. In the Create new list, select **Event**.

- c. In the dialog box, type **goldTime2**, and click **OK**.

8. Specify the time schedule as 4:30 PM (that is, 16:30):

- a. In the side pane, expand **Event: goldTime2**, and click **From**.

The From pane appears.

- b. Click the **Create** button.

The From pane reappears.

- c. Enter these values in the following boxes:

- Hour: 16

- Minute: 30

- d. Click **Apply**.

9. Enter a name for the exclusion (for example, exclude-2), and specify a one-time exclusion for January 1:

- a. In the side pane, click **Event: goldTime2**.

- b. From the Create new box, select **Except**.

- c. In the dialog box, type **exclude-2**, and click **OK**.

- d. In the side pane, click **From** under the **Except: exclude-2** folder.

The From pane appears.

- e. Enter these values in the following boxes:

- Set Month: 1
- Set Day-Of-Month: 1

By excluding January 1 from the schedule, the Internet-Gold service is active all day.

- f. Click **Apply**.
10. Enter a name for the action (for example, action-2), and specify activate for the Internet-Gold service:
 - a. In the side pane, click **Event: goldTime2**.

The Event: goldTime pane appears.
 - b. From the Create new list, select **Action**.
 - c. In the dialog box, type **action-2** as the name of the new Action, and click **OK**.

The Action: action-2 pane appears.
 - In the Service list, select **Internet-Gold**.
 - In the Type list, select **activate**, and click **Apply**.

Example: Configuring a Service to Be Available for a Specified Interval (C-Web Interface)

You can use an effective period for a schedule to make a service available to subscribers who log in during a specified time period. The following example shows how to configure a schedule to make a service available from 8 AM until 4 PM.

To make a specified service available from 8 AM until 4 PM:

1. Enter a unique name for the service schedule (for example, effectiveHours):
 - a. Click **Configure**, expand **Services**, and click **Global**.

The Global pane appears.
 - b. From the Create new list, select **Schedule**.
 - c. In the dialog box, type **effectiveHours**, and click **OK**.

The Schedule: effectiveHours pane appears.
 - d. In the Description box, enter a description for the schedule, and click **Apply**.
2. Enter a name for the schedule event (for example, availableTime):
 - a. From the Create new list, select **Event**.
 - b. In the dialog box, type **availableTime** as the name of the new Event, and click **OK**.

3. For the time, specify when the service is first available — 8:00 AM — and for how long the service is to be available — 480 minutes:
 - a. In the side pane, expand **Event: availableTime**, and click **From**.
 The From pane appears.
 - b. Click the **Create** button and enter these values in the following boxes:
 - Hour: 8
 - Effective: 480
 - c. Click **Apply**.
4. Enter a name for the action (for example, action-1), and specify activate for the Internet-Gold service:
 - a. In the side pane, click **Event: availableTime**.
 The Event: availableTime pane appears.
 - b. From the Create new list, select **Action**.
 - c. In the dialog box, type **action-1** as the name of the new Action, and click **OK**.
 The Action: action-1 pane appears.
 - In the Service list, select **Internet-Gold**.
 - In the Type list, select **activate**, and click **Apply**.

Chapter 27

Managing Tiered and Premium Services with QoS on JUNOSe Routers (C-Web Interface)

- Overview of QoS on JUNOSe Routers on page 231
- Dynamically Managing QoS Profiles on page 231
- Configuring QoS Profile-Tracking Plug-Ins (C-Web Interface) on page 236
- Configuring Search Filters for QoS Profile-Tracking Plug-Ins on page 237

Overview of QoS on JUNOSe Routers

Tiered Internet access and premium services such as video on demand, gaming, or videoconferencing require QoS profiles to be running on the subscriber interface on the JUNOSe router. The router allows only one QoS profile to be attached to an interface at one time. Therefore, as a subscriber activates and deactivates different services, the QoS profile running on the interface needs to change. Also, as subscribers activate services, they may have multiple QoS services running at the same time; for example, internet-gold with videoconferencing.

With the SRC software, you can:

- Dynamically manage QoS profiles on the JUNOSe router to control a combination of services that require QoS.
- Update the directory with a list of QoS profiles that are currently configured on a JUNOSe router.
- Search the directory for QoS policy information.

Dynamically Managing QoS Profiles

The SAE provides a QoS-tracking plug-in (QTP) that you can use to ensure that, as a subscriber activates and deactivates services, the required QoS profile is attached to the subscriber interface. With the QTP, the QoS profile selected is based on the activation state of an aggregation of services, not just one service.

For example, a subscriber activates a QoS service on a subscriber interface that requires a QoS profile that supports 512 best effort. The subscriber then activates a faster service (for example, 1024 best effort), as well as video on demand, and now

has two QoS services running on an interface. The subscriber now needs a QoS profile to be attached to the interface that supports both video on demand and 1024 best-effort service. The QTP can determine which QoS profile the subscriber needs, and can cause the existing QoS profile to be removed from the subscriber interface and the new QoS profile to be attached to the interface.

Note that if a profile is installed on a subscriber interface and the QTP installs a new profile, the new profile is based on QoS services that are currently active. The new profile does not combine the functionality of the previous profile with the new profile. For example, if a subscriber has a default policy with QoS profile be-512 installed on the subscriber interface, and the subscriber activates a video-on-demand service, the QTP does not combine the functionality of be-512 with the profile that supports video on demand.

How QoS Profile Tracking Works

The SAE manages policies on router interfaces through service sessions. Service session configurations contain the policy that needs to be installed on an interface when a service is activated. The policy definition can include the name of a QoS profile to attach to the interface when the policy is installed.

When you set up the QTP, you create a QoS profile attachment service. The purpose of this service is to attach the required QoS profile to an interface. This service is hidden from subscribers and is under only QTP control.

Because profiles need to be changed only when QoS services are activated or deactivated, the QTP tracks services and reacts to service state changes by adjusting the QoS profile attachment as needed by deactivating and activating the QoS profile attachment service.

Subscribers who need their services managed by the QTP are subscribed to the QoS profile attachment service.

Identifying QoS Services

When you set up a service, you identify the service as a QoS service in one of the fields in the service definition. For example, you can assign a service name or category to indicate that the service is a QoS service, or you could assign the QTP instance name in the Tracking Plugin field.

When the SAE notifies the QTP that a service has been activated or deactivated, the QTP determines whether it is a QoS service by searching attributes in the service object. The QTP uses a search filter that you set up to search an attribute for the information that you assigned to the service to indicate that it is a QoS service.

For example, suppose you enter myqtp in the tracking plug-in field of QoS services to indicate that the service is a QoS service. You would set up the search filter to search tracking plug-in attributes for any service that contains myqtp:

```
(attribute.trackPlug=*myqtp*)
```


Or you might configure the category to indicate that a service is a QoS service. The following filter searches service category attributes for any entry that contains ultra, video on demand, or video telephony:

```
((serviceCategory=*ultra*)((serviceCategory=*video on
demand*)(serviceCategory=*video telephony*)))
```

To obtain a list of attribute names for the sspService object class, see the LDAP schema documentation in `SDK+AppSupport+Demos+Samples.tar.gz` file in the folder `SDK/doc/ldap` or on the Juniper Networks Web site at

<http://www.juniper.net/techpubs/software/management/src>

Determining the QoS Profile

After the QTP determines that a service is a QoS service, it needs to obtain the name of the QoS profile for the service. The QTP generates a QoS profile name based on active QoS services as follows:

1. Obtains QoS profile input values.

The QTP obtains these values by taking the value of an attribute in the service definition. You specify which attribute that you want the QTP to use as the input value. For example, you can specify the service name, the category, or the contents of the design and graphics attribute.

2. Compiles a list of the QoS profile input values.
3. Removes duplicate values from the list.
4. Sorts the remaining list by using a case-sensitive alphanumeric comparison.
5. Concatenates the values with a separator. The default value for the separator is a hyphen (-). You can specify a different separator.

Table 11 on page 233 shows how lists of QoS profile input values are sorted and then concatenated.

Table 11: Examples of Concatenated QoS Profile Input Values

Input – QoS Profile Input Values	Output – Concatenated Name
be512, vod	be512-vod
game, be1024, vod	be1024-game-vod
be128	be128

6. Adds a prefix to the resulting name. The default prefix is qos-profile. (You can specify a different value.) The output from our examples now looks like this:
 - qos-profile-be512-vod
 - qos-profile-be1024-game-vod

- qos-profile-be128

The names that result from this process are the QoS profile names.

As you can see from this process, you need to design services and configure the QTP so that the resulting QoS profile names match the names of the QoS profiles configured on the JUNOS router.

Typically, a QoS designer creates a number of QoS profiles that support all the services that are expected to be used. This design results in various QoS profiles that need to be configured on each router. If a required QoS profile is not configured on the router, the hidden QoS profile attachment service cannot be activated. Services are still activated for the subscriber, but the services will not provide the expected traffic requirements. When this happens, the SAE logs the error but does not send an error message to the subscriber.

Setting Up Policy Groups

You need to create two types of policy groups in your QTP configuration. The QoS profile attachment service needs a policy group that attaches the required QoS profile to the subscriber interface when the attachment service is activated. QoS services need policy groups that classify traffic and specify the action to take on traffic that matches the classifier. (You can set up traffic classifiers to match any traffic.)

Policy Group for QoS Profile Attachment Service

The policy group for the hidden QoS profile attachment service must have an egress policy list with only one policy rule that contains a QoS profile attachment action. The QoS profile attachment action must have a variable parameter in the QoS profile field.



NOTE: The policy group for the QoS profile attachment service must contain only one egress policy list and must contain one and only one QoS profile attachment action. Otherwise, the SRC software will require a license for the hidden service.

When the profile attachment service is activated, the QTP substitutes the QoS profile attribute in the policy with the QoS profile name that it determined. The service then loads the policy.

The following example creates a policy group for the QoS profile attachment service. This policy group does not match any traffic.

1. Create a policy group called Pg-qos-attach, and add an egress policy list.
2. In the egress policy list, create a policy rule that has a classify-traffic condition that will not match any real traffic. For example, set both the source and destination addresses to 0.0.0.0/32.
3. In the egress policy list, create a policy rule that has a QoS profile attachment action with QoS profile qpName.

By default, the QTP looks for qpName as the variable parameter.

When the QTP determines the required QoS profile name, it substitutes qpName with the value that it acquired.

Setting Up Services

You need to set up a QoS profile attachment service and QoS services. Both types of services are value-added (SSP) services.

In the QoS profile attachment service, assign the policy group that you configured for the service. For example, policyGroupName = Pg-qos-attach, ou = ent, o = Policies, o = umc.

In QoS services, assign the policy group that you configured for the service.

Subscribe subscribers to the QoS profile attachment service and to the appropriate QoS services.

Reestablishing Default QoS Profile

A default QoS profile may be installed on the subscriber interface before the QTP installs QoS profiles in response to the activation of QoS services. For example, a profile may have been attached to the subscriber interface when the default policy was installed. Once QoS services are no longer active on the interface, the QTP can reestablish the QoS profile that was installed on the interface before the QTP began tracking services and installing profiles on the interface.

Example: How QTP Activates a QoS Service

The following example shows the process that QTP uses when a subscriber activates a QoS service. In this example, QoS profile input values are taken from the service name attribute. The hidden QoS profile attachment service is named svc-qos-attach. The svc-qos-attach service contains a policy that has the variable parameter qpName assigned as the QoS profile name.

1. The subscriber does not have any active services.
2. The subscriber activates service be512, which is a QoS service.
 - a. The SAE sends a Service Session Start event to the QTP.
 - b. The QTP searches an attribute in the service definition and determines that the service is a QoS service.
 - c. Using the SAE Common Object Request Broker Architecture (CORBA) remote application programming interface (API), the QTP gets a list of the subscriber's active QoS services.

The list contains only service be512 because that is the only service that the subscriber has activated.

- d. The QTP adds the default prefix to the QoS profile input value to obtain the QoS profile name. The result is:

qos-profile-be512

- e. The QTP deactivates the hidden svc-qos-attach service. Because this svc-qos-attach service was not active before, this operation does not have any effect.
 - f. The QTP activates the hidden svc-qos-attach service, and it substitutes variable parameter qpName with '\$qos-profile-be512' as the QoS profile name in the policy.
 - g. The policy loads qos-profile-be512 on the subscriber interface.
3. The subscriber activates service vod, which is a QoS service.
- a. The SAE sends a Service Session Start event to the QTP.
 - b. QTP searches attributes in active service definitions and determines that the service is a QoS service.
 - c. The QTP gets a list of the subscriber's active QoS services. The result is:
be512, vod
 - d. The QTP sorts the list and concatenates the QoS profile input values with the separator. The result is:
be512-vod
 - e. The QTP adds the default prefix to the concatenated name to obtain the QoS profile name. The result is:
qos-profile-be512-vod.
 - f. The QTP deactivates the hidden svc-qos-attach service.
 - g. The QTP activates the hidden svc-qos-attach service, and it substitutes variable parameter qpName with '\$qos-profile-be512-vod' as the QoS profile name in the policy.
 - h. The policy loads qos-profile-be512-vod.
4. The subscriber deactivates service vod.
- a. The QTP follows the same procedure as in Step 2 above and determines that the QoS profile name is qos-profile-vod.
 - b. The QTP deactivates the hidden svc-qos-attach service.
 - c. The QTP reactivates the hidden svc-qos-attach service, and it substitutes variable parameter qpName with '\$qos-profile-be512' as the QoS profile name in the policy.
 - d. The policy loads qos-profile-be512.

Configuring QoS Profile-Tracking Plug-Ins (C-Web Interface)

To configure the QoS profile-tracking plug-in with the C-Web interface:

1. Click **Configure**, expand **Shared > SAE**, and then expand the SAE group for which you want to configure a QoS tracking plug-in.
2. From the side pane, click **Configuration > Plug Ins**.
3. Click the plug-in for which you want to configure QoS tracking, and then click **QoS Profile Tracking**.

The QoS Profile Tracking pane appears.

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

For additional information, see the following sources:

Configuring Search Filters for QoS Profile-Tracking Plug-Ins

The SAE uses a search filter to search service objects in the directory to find QoS services. You can set up the filter to search the values of any attribute in the service object, such as service name, category, or tracking plug-in. The search is successful when a value matches the filter.

For information about obtaining a list of attribute names for the sspService object class, see the documentation for the LDAP schema on the Juniper Networks Web site at

<http://www.juniper.net/techpubs/software/management/src>

Configure the search filter in a format similar to the LDAP search filter. Table 12 on page 237 lists the values that you can use for filters. Each filter string `<filter>` contains a simplified LDAP query.

Table 12: Settings for Filter Strings

Filter String	Action
()	Matches no objects
(*)	Matches all objects
List of <code><attribute> = <value></code> pairs <code><attribute></code> —Name of a property or attribute <code><ldapAttributeName></code> <code><value></code> —One of the following <ul style="list-style-type: none"> ■ * (asterisk) ■ Explicit string ■ String that contains an * <p>Note: To define a special character (* & , ! \) in a string, precede it with the backslash symbol (\).</p>	<ul style="list-style-type: none"> ■ If <code><value></code> is *, checks for any value. ■ If <code><value></code> is an explicit string, checks whether any value of the property matches the string, regardless of case. ■ If <code><value></code> is a string that contains a *, checks whether any value of the property contains the string, regardless of case.
(<code>&</code> <code><filter></code> <code><filter></code> ...)	True if all filters match

Table 12: Settings for Filter Strings *(continued)*

Filter String	Action
(< filter > < filter > ...)	True if at least one filter matches
(! < filter >)	True if the filter does not match

- Default—(attribute.trackPlug =); note that you need to add a search value after the equal sign
- Examples
 - To search tracking plug-in attributes for any entry that contains qtp:
 (attribute.trackPlug=*qtp*)
 - To search service category attributes for any entry that contains ultra, video on demand, or video telephony:
 (|(serviceCategory=*ultra*)(|(serviceCategory=*video on demand*)(serviceCategory=*video telephony*)))

Part 7

Configuring Subscribers and Subscriptions

- Configuring Subscriber-Related Properties on the SAE (C-Web Interface) on page 241
- Configuring Internal, External, and Synchronization Plug-Ins (C-Web Interface) on page 245
- Configuring Accounting and Authentication Plug-Ins (C-Web Interface) on page 249
- Configuring Subscribers and Subscriptions (C-Web Interface) on page 265
- Configuring External Subscriber Events with the C-Web Interface on page 273
- Configuring Traffic Redirection (C-Web Interface) on page 279

Chapter 28

Configuring Subscriber-Related Properties on the SAE (C-Web Interface)

This chapter describes how to use the C-Web interface to configure subscriber-related properties on the SAE.

Topics in this chapter include:

- Configuring the Length of Time That MAC Addresses Remain in SAE Cache (C-Web Interface) on page 241
- Identifying a Profile for Unauthenticated Subscribers (C-Web Interface) on page 242
- Configuring Interim Accounting for Services and Subscribers (C-Web Interface) on page 242
- Avoiding Overcharges for Sessions That Time Out (C-Web Interface) on page 243
- Allowing Multiple Logins from the Same IP Address (C-Web Interface) on page 243
- Authenticating Registered Username/Password Pairs (C-Web Interface) on page 244
- Configuring Timers for Session Reactivation (C-Web Interface) on page 244

Configuring the Length of Time That MAC Addresses Remain in SAE Cache (C-Web Interface)

When a DHCP subscriber transitions from an authenticated IP address to an unauthenticated IP address or vice-versa, the SAE:

1. Logs out the subscriber associated with the original IP address.
2. Caches the subscriber profile in the in-memory cache, indexed by the DHCP subscriber's MAC address.
3. Waits until the DHCP subscriber with the cached MAC address obtains its new IP address, and then logs in the subscriber and associates it with the new IP address.

The period during which the subscriber profile remains in the in-memory cache can last until the DHCP lease time for the original address. If something happens during this period—for example, the subscriber turns off the client computer—the subscriber profile remains in the SAE's in-memory cache forever. When a new IP address is assigned to the same DHCP client, problems can occur. To avoid such problems, entries in the in-memory cache are removed after a configurable amount of time.

Configure the amount of time that entries remain in cache to be greater than the time required for a DHCP subscriber to transition from an unauthenticated IP address to an authenticated IP address or vice versa. The time required for a DHCP subscriber to transition from one IP address to another depends on the lease times configured on the JUNOS router and the instructions given to the subscriber on the Web portal, such as reboot your PC now.

To configure the amount of time that subscriber profiles remain in the SAE's in-memory cache:

1. Click **Configure**, expand **Shared > SAE**, and then click **Driver**.

The Driver pane appears.

2. Click **Create**, specify the amount of time that subscriber profiles remain in the SAE's cache as described in the Help text in the Main pane, and then click **Apply**.

Identifying a Profile for Unauthenticated Subscribers (C-Web Interface)

The SAE uses an unauthenticated subscriber profile as a transitional profile for subscribers who are not logged in to the SAE. For example, if a subscriber logs out of the SAE using the API method `Subscriber.logout()`, an unauthenticated subscriber session is created. The unauthenticated subscriber profile must exist and can be subscribed to services available for unauthenticated subscribers. The portal implementation determines whether unauthenticated (anonymous) subscribers can access the portal.

To specify an unauthenticated subscriber profile:

1. Click **Configure**, expand **Shared > SAE**, and then click **Driver**.

The Driver pane appears.

2. Click **Create**, specify a subscriber profile for unauthenticated access to the portal as described in the Help text, and then click **Apply**.

Configuring Interim Accounting for Services and Subscribers (C-Web Interface)

You can enable and disable interim accounting and set intervals between interim accounting messages for services and subscribers. These settings apply to all subscriber sessions and service sessions unless you override these settings for specific services by configuring an accounting interim interval in the value-added service configuration.

To set up interim accounting:

1. Click **Configure**, expand **Shared > SAE**, and then click **Interim Accounting**.

The Interim Accounting pane appears.

2. Click **Create**.
3. (Optional) Enable service interim accounting as described in the Help text.

4. Specify the interval between service interim accounting messages as described in the Help text.
5. (Optional) Enable interim accounting for subscribers as described in the Help text.
6. Specify the interval between subscriber interim accounting messages as described in the Help text.
7. Click **Apply**.

Avoiding Overcharges for Sessions That Time Out (C-Web Interface)

When an idle timeout terminates a session, you can set up the SAE to reduce the session time reported in the accounting stop message by the idle time. This way the session time is accurately reported; the report avoids overcharges for the session.

To adjust the session time:

1. Click **Configure**, expand **Shared > SAE**, and then click **Idle Timeout**.

The Idle Timeout pane appears.

2. Enable when an idle timeout terminates a session as described in the Help text.

The session time reported in the accounting stop message is reduced by the idle time.

3. Click **Apply**.

Allowing Multiple Logins from the Same IP Address (C-Web Interface)

You can specify whether the SAE allows a login from the same IP address without requiring that the previous session log out first.

- If you enable this setting, the SAE logs in the new subscriber session and automatically logs out the previous session.
- If you disable this setting, the SAE denies login requests if a subscriber session for an IP address is active.

To specify whether the SAE allows a login from the same IP address without requiring that the previous session log out first:

1. Click **Configure**, expand **Shared > SAE**, and then click **Subscriber Sessions**.

The Subscriber Sessions pane appears.

2. Enable or disable whether the SAE allows a login from the same IP address without requiring that the previous session log out first, as described in the Help text.
3. Click **Apply**.

Authenticating Registered Username/Password Pairs (C-Web Interface)

You can specify whether the application programming interface (API) method `registerLoginCredentials` authenticates the registered username/password or creates the registration without authentication. Enable this setting if your authentication server does not allow authentication while a session for the authenticated username is active.

To specify whether or not registered username/password pairs are authenticated:

1. Click **Configure**, expand **Shared > SAE**, and then click **Login Registration**.

The Login Registration pane appears.

2. Enable or disable whether registered username/password pairs are authenticated, as described in the Help text.
3. Click **Apply**.

Configuring Timers for Session Reactivation (C-Web Interface)

If a service session fails unexpectedly, the SAE tries to start the session again in the background. You can change how many times the SAE tries to activate the session and the interval between these attempts. In most instances, you do not need to change the default values.

To configure session reactivation behavior:

1. Click **Configure**, expand **Shared > SAE**, and then click **Service Activation**.

The Service Activation pane appears.

2. Configure the number of times the SAE tries to activate a service session if activation fails or to deactivate a service session if deactivation fails, as described in the Help text.
3. Configure the time between attempts to activate a service session if activation fails or to deactivate a service session if deactivation fails, as described in the Help text.
4. Click **Apply**.

Chapter 29

Configuring Internal, External, and Synchronization Plug-Ins (C-Web Interface)

This chapter describes how to use the C-Web interface to configure internal, external, and state synchronization plug-ins.

Topics in this chapter include:

- Creating Plug-In Instances (C-Web Interface) on page 245
- Creating a Plug-In Instance for All SAE Configurations on page 245
- Creating a Plug-In Instance for an SAE Group on page 246
- Configuring Internal Plug-Ins (C-Web Interface) on page 246
- Configuring the SAE for External Plug-Ins (C-Web Interface) on page 247
- Configuring the State Synchronization Plug-In Interface (C-Web Interface) on page 247

Creating Plug-In Instances (C-Web Interface)

You can use the C-Web interface to create a plug-in instance and choose the type of plug-in that you want to create. You can create plug-ins for all SAE configurations or for groups.



NOTE: When you create a plug-in instance and specify a plug-in type, all the other available types are removed from the side pane when you commit the configuration. To change the type, create a new plug-in.

Creating a Plug-In Instance for All SAE Configurations

To create a plug-in instance for all SAE configurations:

1. Click **Configure**, expand **Shared > SAE > Configuration**, and then click **Plug Ins**.
2. From the Create new list, select **Name**.
3. Type a name for the new plug-in in the dialog box, and click **OK**.

The plug-in appears in the side pane and in the Plug In pane.

4. From the side pane, expand the plug-in, and select the type of plug-in that you want to configure.

Creating a Plug-In Instance for an SAE Group

To create a plug-in instance for an SAE group:

1. Click **Configure > Shared > SAE**, and then expand the SAE group for which you want to configure a plug-in.
2. From the side pane, expand **Configuration**, and click **Plug Ins**.

The Plug Ins pane appears.

3. From the Create new list, select **Name**.
4. Type a name for the new plug-in in the dialog box, and click **OK**.

The plug-in appears in the side pane and in the Plug In pane.

5. From the side pane, expand the plug-in, and select the type of plug-in that you want to configure.

Configuring Internal Plug-Ins (C-Web Interface)

To configure an internal plug-in:

1. Click **Configure**, expand **Shared > SAE**, and then expand the SAE group for which you want to configure a plug-in.
2. From the side pane, expand **Configuration**, and click **Plug Ins**.

The Plug Ins pane appears.

3. From the Create new list, select **Name**.
4. Type a name for the new plug-in in the dialog box, and click **OK**.

The plug-in appears in the side pane and in the Plug In pane.

5. In the side pane, expand the new plug-in, and then click **Internal**.

The Internal pane appears.

6. Enter information as described in the Help text in the main pane, and click **Apply**.
7. To configure properties for the plug-in:
 - a. In the side pane, expand the plug-in, and then click **Internal > Properties**.
 - b. From the Create new list, select **Properties**.

The new property appears in the side pane and in the Properties pane.

- Related Topics** ■ For information about creating a plug-in instance for a group, see *Creating Plug-In Instances (C-Web Interface)*.

Configuring the SAE for External Plug-Ins (C-Web Interface)

You need to configure SAE external plug-ins for SAE plug-in agents in the NIC, for Admission Control Plug-Ins, and for custom plug-ins developed in Common Object Request Broker Architecture (CORBA). For information about external plug-ins, see *SRC-PE Network Guide*.

When you use an external plug-in, you need to export its object reference to the SAE. When the SAE sends the first event to a registered plug-in, it resolves the object reference. In case of a failure, the SAE resolves the object reference again. In this case, if a plug-in restarts and instantiates a different object (that is, a different object reference), the SAE learns about the new object through the naming service or the file reference.

You can configure the SAE to resolve the object reference and specify which attributes to send to the external plug-in.

To configure an external plug-in:

1. Click **Configure**, expand **Shared > SAE**, and then expand the SAE group for which you want to configure a plug-in.
2. From the side pane, expand **Configuration**, and click **Plug Ins**.

The Plug Ins pane appears.

3. From the Create new list, select **Name**.
4. Type a name for the new plug-in in the dialog box, and click **OK**.

The plug-in appears in the side pane and in the Plug In pane.

5. From the side pane, expand the new plug-in, and then click **External**.
6. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

- Related Topics** ■ For information about creating a plug-in instance for a group, see *Creating Plug-In Instances (C-Web Interface)*.

Configuring the State Synchronization Plug-In Interface (C-Web Interface)

Some external plug-ins, such as the Admission Control Plug-In (ACP) application and the SAE plug-in agent for the NIC, support state synchronization with the SAE. The state synchronization plug-in interface allows external plug-ins to maintain the state of active subscriber, service, and interface sessions without having to store intermediate versions of the state locally.

To configure the state synchronization plug-in interface:

1. To configure the state synchronization plug-in interface:
 - a. Click **Configure**, expand **Shared > SAE**, and then expand the SAE group for which you want to configure a plug-in.
 - b. In the side pane, expand **Configuration > Plug Ins**, and then click **State Synchronization**.

The State Synchronization pane appears.
 - c. Enter information as described in the Help text in the main pane, and click **Apply**.
2. To configure the number of threads:
 - a. Click **Configure**, expand **Shared > SAE**, and then expand the SAE group for which you want to configure a plug-in.
 - b. In the side pane, expand **Configuration > Plug Ins**, and then click **Manager**.
 - c. Enter information as described in the Help text in the main pane, and click **Apply**.

Related Topics ■ For information about creating a plug-in instance for a group, see [Creating Plug-In Instances \(C-Web Interface\)](#).

Chapter 30

Configuring Accounting and Authentication Plug-Ins (C-Web Interface)

This chapter describes how to configure authentication and accounting plug-ins with the C-Web interface. It also describes how to configure global and default retailer event publishers.

Topics in this chapter include:

- Creating RADIUS Peers on page 249
- Types of Tracking Plug-Ins on page 250
- Configuring Flat File Accounting Plug-Ins on page 251
- Configuring Headers for Flat File Accounting Plug-Ins on page 252
- Configuring Basic RADIUS Accounting Plug-Ins on page 253
- Configuring Flexible RADIUS Accounting Plug-Ins on page 253
- Configuring Custom RADIUS Accounting-Plug-Ins on page 254
- Types of Authentication Plug-Ins on page 254
- Limiting Subscribers on Router Interfaces on page 255
- Configuring Basic RADIUS Authentication Plug-Ins on page 256
- Configuring Flexible RADIUS Authentication Plug-Ins on page 256
- Configuring Custom RADIUS Authentication Plug-Ins on page 257
- Configuring LDAP Authentication Plug-Ins on page 257
- Configuring UDP Ports for RADIUS Plug-Ins (C-Web Interface) on page 258
- Configuring Global UDP Ports on page 258
- Overview of Flexible RADIUS Plug-Ins on page 258
- Configuring a RADIUS Packet Template on page 261
- Using Flexible RADIUS Packet Definitions on page 262
- Configuring Event Publishers (C-Web Interface) on page 264

Creating RADIUS Peers

RADIUS peers are instances of RADIUS servers. If you define multiple servers, the SAE uses them in cases of failover or as alternate routers for load-balancing purposes.

Each RADIUS plug-in requires a default peer. Configure a RADIUS peer before you configure the plug-in.

RADIUS peers are configured in the peer group for each RADIUS plug-in.

To create a RADIUS peer:

1. Click **Configure**, expand **Shared > SAE**, and then expand the SAE group for which you want to configure RADIUS plug-ins.
2. In the side pane, expand **Configuration > Plug Ins**.
3. Expand the plug-in that you created for RADIUS accounting and authentication, and click one of the following:
 - **Custom RADIUS Accounting**
 - **Custom RADIUS Authentication**
 - **Flex RADIUS Accounting**
 - **Flex RADIUS Accounting**
 - **RADIUS Accounting**
 - **RADIUS Authentication**
4. Click **Create**, enter information as described in the Help text in the main pane, and then click **Apply**.

Types of Tracking Plug-Ins

You can configure the tracking plug-ins described in Table 13 on page 250.

By default, the fileAcct plug-in instance tracks all subscriber and service sessions and writes all available attributes to a file. You can use this plug-in instance or create new one.



NOTE: When you use the NAS-Port attribute in tracking plug-ins, the SAE calculates the NAS-Port value based on the NAS-Port-Id value that it receives from the JUNOS software. You can change the NAS-Port format in the JUNOS software. However, because the SAE has no indication of which format is configured on the JUNOS router, the calculation of the NAS-Port attribute is correct only if the router uses the default configuration.

Table 13: Tracking Plug-Ins

Plug-In	Description
Basic RADIUS accounting	Sends accounting information to an external RADIUS accounting server or a group of redundant servers. Java class name—net.juniper.smgmt.sae.plugin.RadiusTrackingPluginEventListener

Table 13: Tracking Plug-Ins (continued)

Plug-In	Description
Custom RADIUS accounting	Provides customized functions that can also be found in the flexible RADIUS accounting plug-ins. Custom plug-ins are internal plug-ins that are designed to deliver better system performance than the flexible RADIUS plug-ins. You can extend this plug-in by using the RADIUS client library. Java class name— <code>net.juniper.smgmt.sae.plugin.CustomRadiusAccounting</code>
Flat file accounting	Writes tracking information to a file in comma-separated format. Java class name— <code>net.juniper.smgmt.sae.plugin.FileTrackingPluginEventListener</code>
Flexible RADIUS accounting	Performs the same functions as the basic RADIUS accounting plug-in, but also lets you customize RADIUS accounting packets that the SAE sends to RADIUS servers. You can specify which fields are included in RADIUS accounting packets and what information is contained in the fields. Java class name— <code>net.juniper.smgmt.sae.plugin.FlexibleRadiusTrackingPluginEventListener</code>
PCMM record-keeping server plug-in	Sends accounting information to an external PCMM record-keeping server (RKS). See <i>Configuring PCMM Record-Keeping Server Plug-Ins with SRC CLI</i> . Java class name— <code>net.juniper.smgmt.sae.plugin.RksEventListener</code>
QoS profile tracking	Ensures that as a subscriber activates and deactivates services, the correct QoS profile is attached to the subscriber interface. See <i>Dynamically Managing QoS Profiles</i> . Java class name— <code>net.juniper.smgmt.sae.plugin.qtp.QosProfileTrackingPluginEventListener</code>

Configuring Flat File Accounting Plug-Ins

Flat file accounting plug-ins write information to a file in a comma-separated format. The SRC software has a default flat file accounting plug-in instance called `fileAcct`. The `fileAcct` instance logs all possible attributes for 24-hour periods in the file `var/acct/log`.

Another item that you can configure for flat files is the names of the headers that appear in the file.

To create flat-file accounting plug-ins:

1. Click **Configure**, expand **Shared > SAE**, and then expand the SAE group for which you want to configure RADIUS plug-ins.
2. In the side pane, expand **Configuration > Plug-Ins**.
3. Expand the plug-in that you created for file accounting, and then click **File Accounting**.

The File Accounting pane appears.

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

Configuring Headers for Flat File Accounting Plug-Ins

When the SAE writes data to a flat file, it writes into the first line the headers that identify the attributes in the file. For example, in the following accounting file, the first line lists headers for all attribute fields in the file, and the following lines list the actual data in each field:

```
Accounting Status,NAS ID,SSP Host,Router Name,Interface Name,Interface
Alias,Interface Description,NAS port ID,User IP Address,User ID,User Accounting
ID,User Authentication ID,INTF Radius Class,INTF,SessionId, Service Name,Radius
Class,Timestamp,SessionId, Terminate Cause,Session Time,Input Octets,Output
Octets,Input Packets,Output Packets,NAS IP,User Mac address,Service Session
Name,Service Session Tag,User Session Type,User Session Radius Class,User
Session ID
start,SSP.uelmo,uelmo,default@erx7_ssp57,FastEthernet1/1.1,,IP1/1.1,default@erx7_ssp57
FastEthernet1/1:65535, 10.10.10.20,pebbles@virneo.net,,,erx fastEthernet
1/1:0001048619,Video-Gold,Video-Gold,Fri Jan 30 14:23:29 EDT 2004,
VideoGold:null:1064946209182, 0,0,0,0,0,0, 10.10.7.17,,,PPP,,
pebbles:1064946144841
```

You can assign your own names to the headers that appear in the file. To do so, define the header names in a template, and then set up file accounting plug-in instances to use the template. The default template, FileAccounting.std, defines header names for all possible attributes. You can use the default template or create your own templates.

To set up a file accounting template:

- Click **Configure**, expand **Shared > SAE**, and then expand the SAE group for which you want to configure RADIUS plug-ins.

To set up a file accounting template from the default template:

1. In the side pane, expand **Configuration > File Accounting Template:std > Attributes**.

The Attributes pane appears.

2. In the side pane, click one of the attributes, enter information as described in the Help text in the main pane, and then click **Apply**.

To create a new file accounting template and add attributes:

1. In the side pane, click **Configuration**.

The Configuration pane appears.

2. From the Create new list, select **File Accounting Template**.
3. In the dialog box, type a name for the template, and click **OK**.

The new template appears in the side pane and in the File Accounting pane.

4. To add attributes to your template, expand the template in the side pane, and click **Attributes**.

The Attributes pane appears.

5. From the Create new list, select the attribute that you want to create.
6. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Basic RADIUS Accounting Plug-Ins

You can use basic RADIUS accounting plug-ins to send accounting information to an external RADIUS accounting server or to a group of redundant servers. To communicate with nonredundant servers, you need to create multiple instances of the plug-in.

To set up basic RADIUS accounting plug-ins:

1. Click **Configure**, expand **Shared > SAE**, and then expand the SAE group for which you want to configure RADIUS plug-ins.
2. In the side pane, expand **Configuration > Plug Ins**.
3. Expand the plug-in that you created for basic RADIUS accounting, and then click **RADIUS Accounting**.

The RADIUS Accounting pane appears.

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

Related Topics ■ For information about setting up default peers, see [Creating RADIUS Peers](#).

Configuring Flexible RADIUS Accounting Plug-Ins

Flexible RADIUS accounting plug-ins provide the same features as basic RADIUS accounting plug-ins. In addition, they allow you to customize RADIUS accounting packets that the SAE sends to RADIUS servers. You can specify which fields are included in the RADIUS accounting packets and what information is contained in the fields.

To set up flexible RADIUS accounting plug-ins:

1. Click **Configure**, expand **Shared > SAE**, and then expand the SAE group for which you want to configure RADIUS plug-ins.
2. In the side pane, expand **Configuration > Plug Ins**.
3. Expand the plug-in that you created for flexible RADIUS accounting, and then click **Flex RADIUS Accounting**.

The Flex RADIUS Accounting pane appears.

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

Related Topics ■ For information about setting up default peers, see Creating RADIUS Peers.

Configuring Custom RADIUS Accounting-Plug-Ins

The custom RADIUS accounting plug-ins provide the same functions as the flexible RADIUS accounting plug-ins, but are designed to deliver better system performance. To use a custom plug-in, you must provide a Java class that implements the service provider interface (SPI) defined in the RADIUS client library. Use this SPI to specify which fields and field values to include in RADIUS accounting packets. The RADIUS client library is part of the SAE core application programming interface (API).

See the documentation for the RADIUS client library in the SAE core API documentation on the Juniper Networks Web site at

<http://www.juniper.net/techpubs/software/management/src/api-index.html>

For a sample implementation, see the following directory in the `SDK+AppSupport+Demos+Samples.tar.gz` file:

`SDK/plugin/java/src/net/juniper/smg/sample/radiuslib/RadiusPacketHandlerImpl.java..`
You can download the `SDK+AppSupport+Demos+Samples.tar.gz` from the Juniper Networks Web site at: <https://www.juniper.net/support/csc/swdist-erx/src.html>.

To set up custom RADIUS accounting plug-ins:

1. Click **Configure**, expand **Shared > SAE**, and then expand the SAE group for which you want to configure RADIUS plug-ins.
2. In the side pane, expand **Configuration > Plug Ins**.
3. Expand the plug-in that you created for custom RADIUS accounting, and then click **Custom RADIUS Accounting**.

The Custom RADIUS Accounting pane appears.

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

Related Topics ■ For information about setting up default peers, see Creating RADIUS Peers.

Types of Authentication Plug-Ins

This section shows how to configure the authentication plug-ins described in Table 14 on page 255. Because authentication and authorization are similar, the plug-in user interface does not distinguish between them. However, when you configure plug-ins, you need to set them up to perform the correct behavior, either authentication or authorization.

You can configure multiple authentication plug-ins. The plug-ins are called in an arbitrary order, and each plug-in can return authorization values. (If multiple plug-ins return a session-timeout value, the smallest value is used.) Authentication or authorization succeeds if all plug-in calls succeed.

Table 14: Authentication Plug-Ins

Plug-In	Description
Basic RADIUS authentication	<p>Sends authentication information to an external RADIUS authentication server or a group of redundant servers.</p> <p>Java class name—<code>net.juniper.smgmt.sae.plugin.RadiusAuthPluginEventListener</code></p>
Custom RADIUS authentication	<p>Provides customized functions that can also be found in the flexible RADIUS authentication plug-ins. Custom plug-ins are internal plug-ins that are designed to deliver better system performance than the flexible RADIUS plug-ins. You can extend this plug-in by using the RADIUS client library.</p> <p>Java class name—<code>net.juniper.smgmt.sae.plugin.CustomRadiusAuth</code></p>
Flexible RADIUS authentication	<p>Performs the same functions as the basic RADIUS authentication plug-in, but also lets you customize RADIUS authentication packets that the SAE sends to RADIUS servers. You can specify which fields are included in RADIUS authentication packets and what information is contained in the fields.</p> <p>Java class name—<code>net.juniper.smgmt.sae.plugin.FlexibleRadiusAuthPluginEventListener</code></p>
LDAP authentication	<p>Performs authentication against different directories using different authentication methods. There are two LDAP authentication plug-ins: one authenticates subscribers, and the second authenticates SRC administrators so that they can access the SAE Web Admin application.</p> <p>Java class name of the subscriber authentication plug-in—<code>net.juniper.smgmt.sae.plugin.LdapAuthenticator</code></p> <p>Java class name of the administrator authentication plug-in—<code>net.juniper.smgmt.sae.plugin.adminLdap</code></p>
Limiting subscribers	<p>Limits the number of authenticated subscribers who connect to an IP interface on the router.</p> <p>Java class name—<code>net.juniper.smgmt.sae.plugin.LimitNumSubscriberPerIntfAuthPluginListener</code></p>

Limiting Subscribers on Router Interfaces

You can limit the number of authenticated subscribers who connect to an IP interface on the router. This plug-in does not limit the number of unauthenticated subscribers who connect to an IP interface, and does not limit the number of subscribers who connect to a physical or link-layer interface. In the case of subscriber interfaces, the plug-in limits the number of authenticated subscribers on the subscriber interface but not on the underlying primary IP interface.

To set up a plug-in that limits the number of subscribers on interfaces:

1. Click **Configure**, expand **Shared > SAE**, and then expand the SAE group for which you want to configure subscriber limits.
2. In the side pane, expand **Configuration > Plug Ins**.
3. Expand the plug-in that you created for limiting subscribers, and then click **Interface Subscriber Limit**.

The Interface Subscriber Limit pane appears.

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

Configuring Basic RADIUS Authentication Plug-Ins

You can use basic RADIUS authentication plug-ins to send authentication information to an external RADIUS accounting server or a group of redundant servers. To communicate with nonredundant servers, you need to create additional instances of the plug-in.

To set up basic RADIUS authentication plug-ins:

1. Click **Configure**, expand **Shared > SAE**, and then expand the SAE group for which you want to configure RADIUS plug-ins.
2. In the side pane, expand **Configuration > Plug Ins**.
3. Expand the plug-in that you created for basic RADIUS authentication, and then click **RADIUS Authentication**.

The RADIUS Authentication pane appears.

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

Related Topics ■ For information about setting up default peers, see [Creating RADIUS Peers](#).

Configuring Flexible RADIUS Authentication Plug-Ins

Flexible RADIUS authentication plug-ins provide the same features as basic RADIUS authentication plug-ins. In addition, they allow you to customize RADIUS authentication packets that the system sends to RADIUS servers and specify which fields are included in the RADIUS authentication packets and what information is contained in the fields.

To set up flexible RADIUS authentication plug-ins:

1. Click **Configure**, expand **Shared > SAE**, and then expand the SAE group for which you want to configure RADIUS plug-ins.
2. In the side pane, expand **Configuration > Plug Ins**.
3. Expand the plug-in that you created for flexible RADIUS authentication, and then click **Flex RADIUS Authentication**.

The Flex RADIUS Authentication pane appears.

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

Related Topics ■ For information about setting up default peers, see Creating RADIUS Peers.

Configuring Custom RADIUS Authentication Plug-Ins

The custom RADIUS authentication plug-ins provide the same functions as the flexible RADIUS authentication plug-ins, but are designed to deliver better system performance. To use a custom plug-in, you must provide a Java class that implements the SPI defined in the RADIUS client library. Use this SPI to specify which fields and field values to include in RADIUS accounting packets. The RADIUS client library is part of the SAE core API.

See the documentation for the RADIUS client library in the folder *SDK/doc/sae/net/juniper/smg/sae/radiuslib* in the *SDK+AppSupport+Demos+Samples.tar.gz* on the Juniper Networks Web site at: <https://www.juniper.net/support/csc/swdist-erx/src.html>. You can also view the SAE core API documentation on the Juniper Networks Web site at <http://www.juniper.net/techpubs/software/management/src/api-index.html>.

For a sample implementation, see the following directory in the *SDK+AppSupport+Demos+Samples.tar.gz* file:
SDK/plugin/java/src/net/juniper/smg/sample/radiuslib/RadiusPacketHandlerImpl.java.

To set up custom RADIUS authentication plug-ins:

1. Click **Configure**, expand **Shared > SAE**, and then expand the SAE group for which you want to configure RADIUS plug-ins.
2. In the side pane, expand **Configuration > Plug Ins**.
3. Expand the plug-in that you created for custom RADIUS authentication, and then click **Custom RADIUS Authentication**.

The Custom RADIUS Authentication pane appears.

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

Related Topics ■ For information about setting up default peers, see Creating RADIUS Peers.

Configuring LDAP Authentication Plug-Ins

To create LDAP authentication plug-ins:

1. Click **Configure**, expand **Shared > SAE**, and then expand the SAE group for which you want to configure LDAP authentication plug-ins.
2. In the side pane, expand **Configuration > Plug Ins**.

- Expand the plug-in that you created for LDAP authentication, and then click **LDAP Authentication**.

The LDAP Authentication pane appears.

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

Configuring UDP Ports for RADIUS Plug-Ins (C-Web Interface)

In RADIUS packets that RADIUS plug-ins send to a RADIUS server, the plug-in uses an identifier field to match requests to replies. This field provides for a maximum of 256 identifiers. Once all identifiers are used, the plug-in cannot send any more requests until it receives replies that match the requests already sent. In high-load systems, this limit can slow performance.

To overcome this limitation, you can configure a pool of UDP ports for RADIUS plug-ins. Having a pool of ports allows RADIUS plug-ins to create one queue per port to wait for RADIUS replies. Each queue can wait for 256 RADIUS packets. The RADIUS plug-ins send RADIUS packets through the pool of ports in a round-robin mode.

You can configure a global source UDP port or pool of ports that RADIUS plug-ins use to communicate with RADIUS servers. You can also configure UDP ports for each plug-in instance. If you do not configure a UDP port for a plug-in instance, the plug-in uses the global UDP port.

Configuring Global UDP Ports

To configure global UDP ports:

- Click **Configure**, expand **Shared > SAE**, and then expand the SAE group for which you want to configure global UDP ports.
- In the side pane, expand **Configuration**, and then click **Global RADIUS UDP Port**.

The Global RADIUS UDP Port pane appears.

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

Overview of Flexible RADIUS Plug-Ins

Flexible RADIUS accounting and authentication plug-ins allow you to define the content of RADIUS packets that the SAE sends to RADIUS servers. You can specify which attributes are included in different types of RADIUS packets (for example, session start or stop requests, or accounting on or off requests). You can also specify what information is contained in the attribute fields.

A RADIUS attribute configuration consists of RADIUS attribute instances. Each instance defines attributes for a specific type of packet—For example, start requests or accounting off requests.

Within each attribute instance, you define individual RADIUS attributes. The following is a RADIUS attribute instance for authentication requests:

```
radius-attributes auth {
  attributes {
    User-Name loginId;
    User-Password password;
    NAS-Identifier localNasId;
    NAS-IP-Address localNasIp;
    NAS-Port nasPort;
  }
}
```

Each RADIUS packet template can consist of multiple RADIUS attribute instances.

Using Default RADIUS Templates

The SRC software comes with two default templates:

- **stdAcct**—Defines RADIUS accounting packets and is used in the default RADIUS flexible accounting plug-in instance `flexRadiusAcct`.
- **stdAuth**—Defines RADIUS authentication packets and is used in the default RADIUS flexible authentication plug-in instance `flexRadiusAuth`.

Naming RADIUS Attribute Instances

Attribute instances define attributes for a specific type of RADIUS packet. The name that you assign to an attribute instance specifies the type of packet to which the attribute definition is applied. Table 15 on page 259 lists the available packet types.

Table 15: RADIUS Attribute Instance Names

Attribute Instance (Packet-Type)	Type of RADIUS Packet to Which Attribute Definition Is Applied
acct	Any accounting request
auth	Any authentication request
authresp	Any authorization response
dhcprsp	DHCP response
off	Accounting-Off requests
on	Accounting-On requests
onoff	Accounting-On or Accounting-Off requests
start	Start requests
startstop	Start, Stop, or Interim Update requests
stop	Stop or Interim Update requests

Table 15: RADIUS Attribute Instance Names *(continued)*

Attribute Instance (Packet-Type)	Type of RADIUS Packet to Which Attribute Definition Is Applied
svcacct	Service Session Start, Stop, or Interim requests
svcrep	Any service authorization response
svcstart	Service Session Start requests
svcstop	Service Session Stop or Interim requests
useracct	Subscriber Session Start, Stop, or Interim requests
userrep	Any subscriber authorization response
userstart	Subscriber Session Start requests
userstop	Subscriber Session Stop, or Interim requests

Defining RADIUS Attributes

RADIUS attribute definitions consist of a RADIUS attribute and a value for the RADIUS attribute.

You can define values for standard RADIUS attributes or JUNOS vendor-specific attributes (VSAs).

Standard RADIUS Attributes

For standard RADIUS attributes, use a name or number as defined in *RFC 2865—Remote Authentication Dial In User Service (RADIUS) (June 2000)*, *RFC 2866—RADIUS Accounting (June 2000)*, or *RFC 2869—RADIUS Extensions (June 2000)*. For a full list, see www.iana.org/assignments/radius-types.

Juniper Networks VSAs

For Juniper Networks VSAs, use one of the following formats:

- Vendor-Specific.4874. <vsa#> . <type>
- 26.4874. <vsa#> . <type>

where <type> is one of the following:

- text—Indicates that the value is 1–253 octets containing UTF-8 encoded characters
- string—Indicates that the value is 1–253 octets containing binary data
- address—Indicates that the value is a 32-bit value

- integer—Indicates that the value is a 32-bit unsigned value
- time—Indicates that the value is a 32-bit unsigned value, seconds since 00:00:00 UTC, January 1, 1970

The following is an example of RADIUS attribute instances that define RADIUS VSAs.

```
radius-attributes svcresp {
  attributes {
    Session-Timeout setSessionTimeout(ATTR);
    Idle-Timeout setIdleTimeout(ATTR);
    vendor-specific.Juniper.Sdx-Session-Volume-Quota setSessionVolumeQuota(ATTR);
    vendor-specific.WISPr.Redirection-URL "setProperty(\"startURL=%s\" % ATTR)";
    vendor-specific.WISPr.Bandwidth-Min-Up "setSubstitution(\"min_up_rate=%s\" % ATTR)";
    vendor-specific.WISPr.Bandwidth-Min-Down "setSubstitution(\"min_down_rate=%s\" % ATTR)";
    vendor-specific.WISPr.Bandwidth-Max-Up "setSubstitution(\"max_up_rate=%s\" % ATTR)";
    vendor-specific.WISPr.Bandwidth-Max-Down "setSubstitution(\"max_down_rate=%s\" % ATTR)";
  }
}
radius-attributes dhcpreisp {
  attributes {
    Framed-Pool setPoolName(ATTR);
    Framed-IP-Address setUserIpAddress(ATTR);
    26.4874.1.text setAuthVirtualRouterName(ATTR);
    26.4874.2.text setPoolName(ATTR);
    26.4874.31.text setServiceBundle(ATTR);
  }
}
```

Configuring a RADIUS Packet Template

There are two ways to define RADIUS packets for flexible RADIUS accounting and authentication plug-ins:

- Define attributes in a template, and then apply the template to flexible RADIUS accounting and authentication plug-ins.
- Define attributes in the packet definition configuration of a flexible plug-in instance. These definitions override definitions in packet templates.

To configure attributes in a template:

1. Click **Configure**, expand **Shared > SAE**, and then expand the SAE group for which you want to configure a RADIUS template.
2. To configure a new RADIUS accounting template:
 - a. In the side pane, expand **Configuration**, and then click **RADIUS Packet Template: stdAcct**.

The RADIUS Packet Template: stdAcct pane appears.

- b. From the Create new list, select **RADIUS Attributes**, type the RADIUS attribute name in the dialog box, and click **OK**.

The new RADIUS accounting template appears in the side pane.

3. To configure a new RADIUS authentication template:
 - a. In the side pane, expand **Configuration**, and then click **RADIUS Packet Template: stdAuth**.

The RADIUS Packet Template: stdAuth pane appears.

- b. From the Create new list, select **RADIUS Attributes**, type the RADIUS attribute name in the dialog box, and click **OK**.

The new RADIUS authentication template appears in the side pane.

Using Flexible RADIUS Packet Definitions

This topic shows some of the ways you can use flexible RADIUS packet definitions. Remember that the name of the attribute instance determines the type of RADIUS packet in which the packet definition is used.

- To use the Challenge Handshake Authentication Protocol (CHAP) to authenticate subscribers, include the Chap-Password and optionally the Chap-Challenge attributes in authentication requests. (We recommend that you use Chap-Password only. Use Chap-Challenge only if required.) To use a CHAP password, include the following in attribute instance auth:

Chap-Password = password

- To cause the Calling-Station-Id attribute to use the subscriber's MAC address:

Calling-Station-Id = userMacAddress

- To set the value to prefix N followed by the service name and the prefix S followed by the service session name:

'N'+serviceName, 'S'+serviceSessionName

- To construct a value for the Nas-Port-Id attribute by concatenating the value of routerName, a space, and the Nas-Port-ID on the router:

Nas-Port-Id=routerName + " " + portId

For example, the constructed value might be:

default@phoenix FastEthernet 4/2

- The following example sets the User-Name attribute as follows:
- Sets the value to accountingId, or
- If accountingId is empty, sets the value to loginName, or
- If loginName is also empty, sets the value to NN

User-Name = accountingId or loginName or " NN"

- To extract the lower 32 bits of the 64-bit inOctet counter:

Acct-Input-Octets = lowWord(inOctets)

- To set the counter fields in the RADIUS packet to the appropriate 32-bit values:

Acct-Input-Octets = lowWord(inOctets)
Acct-Output-Octets = lowWord(outOctets)
Acct-Input-Packets = inPackets
Acct-Output-Packets = outPackets

Acct-Input-Gigawords = highWord(inOctets)
Acct-Output-Gigawords = highWord(outOctets)

- The inOctets and outOctets are 64-bit values and must be split into lower 32-bit (Acct-*-Octets) and upper 32-bit (Acct-*-Gigawords) values.
- The inPacket and outPacket counters are 32-bit values and can be assigned directly.

Setting Values in Authentication Response Packets

You can use some special attribute values to set values in authentication response packets. For example:

- setRadiusClass(ATTR)
- setSessionTimeout(ATTR)
- setSessionVolumeQuota(ATTR)

[Unresolved xref] lists the type of packets (authresp, userresp, or svcresp) in which you can use these values.

When the RADIUS client finds one of these attribute values in an authentication response, it binds ATTR to the current attribute and executes the defined expression. The expression calls one of the available set methods to set the value in the plug-in event.

Below are some examples.

- To set a session timeout:

Session-Timeout = setSessionTimeout(ATTR)

- To set the RADIUS class:

Class = setRadiusClass(ATTR)

- To set the service bundle in VSA 31:

26.4874.31.text = setServiceBundle(ATTR)

- To set the session volume quota:

26.4874.50.text = setSessionVolumeQuota(ATTR)

Selecting IP Address Pools Using DHCP Response Packets

For DHCP subscribers, you can set up RADIUS authorization plug-ins to return to the router attributes that can be used to select a DHCP address such as framed IP address and pool. You can also set up the name of the virtual router on which the address pool is located and select a fixed address for each subscriber.

- Framed IP address—Selects the pool from which the address is allocated; if the framed IP address is not available, the DHCP server allocates the next available address in the pool; use the setUserIpAddress value.
- Framed IP pool—Name of the address pool on the router from which an IP address is assigned; use the setPoolName value.
- Virtual router name—Name of the virtual router on which the address pool is located; use the setAuthVirtualRouterName value.

You can also select a fixed address for each subscriber. If you identify subscribers by port information (for example, NAS-IP and NAS-Port), the authorization response can select a fixed IP address for each subscriber.



NOTE: Parameters set in the DHCP profile override parameters set by DHCP authorization plug-ins.

Configuring Event Publishers (C-Web Interface)

- Configuring Global and Default Retailer Event Publishers on page 264

Configuring Global and Default Retailer Event Publishers

To configure global and default retailer event publishers:

1. Click **Configure**, expand **Shared > SAE**, and then expand the SAE group for which you want to configure a event publisher.
2. In the side pane, expand **Plug Ins**, and then click **Event Publishers**.

The Event Publishers pane appears.

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

Chapter 31

Configuring Subscribers and Subscriptions (C-Web Interface)

This chapter describes how to use the C-Web interface to configure subscribers and managers and to configure subscriptions to services.

Topics in this chapter include:

- Enabling the Subscriber and Subscription Configuration on the C-Web Interface on page 265
- Adding Subscribers (C-Web Interface) on page 266
- Adding Retailers (C-Web Interface) on page 266
- Configuring Administrative Information for Retailers (C-Web Interface) on page 267
- Adding Subscriber Folders (C-Web Interface) on page 267
- Adding Residential Subscribers (C-Web Interface) on page 268
- Configuring Administrative Information for Residential Subscribers (C-Web Interface) on page 268
- Adding Enterprises (C-Web Interface) on page 268
- Configuring Administrative Information for Enterprise Subscribers (C-Web Interface) on page 269
- Adding Sites (C-Web Interface) on page 269
- Adding Devices as Subscribers (C-Web Interface) on page 269
- Adding Managers (C-Web Interface) on page 270
- Configuring Subscriptions (C-Web Interface) on page 270
- Allowing Multiple Subscriptions to the Same Service per Subscriber on page 271
- Configuring Accesses (C-Web Interface) on page 271

Enabling the Subscriber and Subscription Configuration on the C-Web Interface

Before you can configure subscribers and subscriptions with the C-Web interface, you must enable the policy, service, and subscriber editor on the C-Web interface. To do so :

1. Click **Manage > Enable**.

The Enable pane appears.

2. From the Component list, select **Editor**, and click **OK**.

If you are using multiple C-series Controllers, we recommend that you enable the policy, service, and subscriber editor on only one C-series Controller on your network.



CAUTION: If you enable the editor on multiple platforms, there is a risk that configuration changes will conflict. In this case, the second edit that is committed to the platform is lost.

Adding Subscribers (C-Web Interface)

This section describes how to add and configure subscribers with the C-Web interface.

The tasks to configure subscribers are:

- Add retailers.

See Adding Retailers (C-Web Interface).

- Add subscriber folders.

See Adding Subscriber Folders (C-Web Interface).

The subscriber hierarchy requires that the objects immediately subordinate to retailers be subscriber folders. You can, however, use subscriber folders subordinate to other subscriber objects to organize groups of subscribers.

- Add residential subscribers.

See Adding Residential Subscribers (C-Web Interface).

- Add enterprises.

See Adding Enterprises (C-Web Interface) .

- Add sites.

See Adding Sites (C-Web Interface).

- Add devices as subscribers.

See Adding Devices as Subscribers (C-Web Interface).

Related Topics

- Adding Managers (C-Web Interface)
- Configuring Subscriptions (C-Web Interface) .

Adding Retailers (C-Web Interface)

If you customize the SRC software for only one Internet service provider (ISP), use the retailer called *default* that is provided in the sample data. If the SRC software will manage multiple ISPs, add a retailer for each ISP.

To add a retailer:

1. Click **Configure > Subscribers**.

The Subscribers pane appears.

2. From the Create new list, select **Retailer**.
3. In the dialog box, type a name for the new Retailer (for example, retailer-one), and click **OK**.

The Retailer: *< name >* pane appears.

4. Enter information as described in the Help text in the main pane, and click **Apply**.

Related Topics ■ Configuring Administrative Information for Retailers (C-Web Interface)

Configuring Administrative Information for Retailers (C-Web Interface)

To add administrative information about retailers:

1. Click **Configure**, and expand **Subscribers**.
2. Expand the specified retailer, and click **Info**.

The Info pane appears.

3. Click the **Create** button.

The Info pane reappears.

4. Enter information as described in the Help text in the main pane, and click **Apply**.

Related Topics ■ Adding Retailers (C-Web Interface)

Adding Subscriber Folders (C-Web Interface)

You can create subscriber folders for retailers, existing subscriber folders, enterprises, and sites. You must create a subscriber folder in a retailer object before you can add other types of subscribers.

To create a subscriber folder:

1. Click **Configure**, and expand **Subscribers**.
2. Click the specified retailer.
3. From the Create new list, select **Subscriber Folder**.
4. In the dialog box, enter a name for the new Subscriber Folder, and click **OK**.

The Subscriber Folder: *< name >* pane appears.

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

Adding Residential Subscribers (C-Web Interface)

To add a residential subscriber:

1. Click **Configure**, and expand **Subscribers**.
2. Expand the specified retailer, and the specified subscriber folder.
3. Click the specified subscriber.

The Subscriber: *< name >* pane appears.

4. From the Create new list, select **Subscriber**.
5. In the dialog box enter a name for the new Subscriber, and click **OK**.

The Subscriber: *< name >* pane appears.

6. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Administrative Information for Residential Subscribers (C-Web Interface)

To add administrative information about residential subscribers:

1. Click **Configure**, and expand **Subscribers**.
2. Expand the specified retailer and the specified subscriber folder.
3. Expand the specified subscriber, and click **Info**.

The Info pane appears.

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

Adding Enterprises (C-Web Interface)

To add an enterprise subscriber:

1. Click **Configure**, and expand **Subscribers**.
2. Expand the specified retailer, and then click the specified subscriber folder.

The Subscriber Folder: *< name >* pane appears.

3. From the Create new list, select **Enterprise**.
4. In the dialog box, enter a name for the new Enterprise, and click **OK**.

The Enterprise: *< name >* pane appears.

5. Enter information as described in the Help text in the main pane, and click **Apply**.
6. Configure an access subscription for the enterprise. (See Configuring Accesses (C-Web Interface).)

Configuring Administrative Information for Enterprise Subscribers (C-Web Interface)

To add administrative information about enterprise subscribers:

1. Click **Configure**, and expand **Subscribers**.
2. Expand the specified retailer and subscriber folder.
3. Expand the specified enterprise, and click **Info**.

The Info pane appears.

4. Click the **Create** button.

The Info pane reappears.

5. Enter information as described in the Help text in the main pane, and then click **Apply**.

Adding Sites (C-Web Interface)

To add a site:

1. Click **Configure**, and expand **Subscribers**.
2. Expand the specified retailer and the subscriber folder.
3. Click the specified enterprise.

The Enterprise: *< name >* pane appears.

4. From the Create new list, select **Site**.
5. In the dialog box, enter a name for the new Site, and click **OK**.

The Site: *< name >* pane appears.

6. Enter information as described in the Help text in the main pane, and click **Apply**.
7. Configure an access for the site. (See Configuring Accesses (C-Web Interface).)

Adding Devices as Subscribers (C-Web Interface)

You can configure a device subscriber for subscriber sessions that manage the forwarding interface on JUNOS routing platforms and the router pseudo-subscriber on JUNOSe routers.

You can add devices as subscribers to subscriber folders, enterprises, and sites.

To add a device as a subscriber:

1. Click **Configure**, and expand **Subscribers** and the specified retailer.
2. Click the specified subscriber folder.

The Subscriber Folder: *< name >* pane appears.

3. From the Create new list, select **Device**.
4. In the dialog box, enter a name for the new Device, and click **OK**.

The Device: *< name >* pane appears.

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

Adding Managers (C-Web Interface)

To add a manager:

1. Click **Configure**, and expand **Subscribers**.
2. Expand the specified retailer and subscriber folder.
3. Click the specified enterprise.

The Enterprise: *< name >* pane appears.

4. From the Create new List, select **Manager**.
5. In the dialog box, enter a name for the new Manager, and click **OK**.

The Manager: *< name >* pane appears.

6. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Subscriptions (C-Web Interface)

After you add subscribers, you configure subscriptions for the subscribers. Residential or enterprise subscribers may also be able to configure subscriptions through the portal, and managers assigned to a subscriber object may be able to configure subscriptions for that object.

You must add a service to the directory before you can specify that service for subscribers.

After you configure a subscription to a service, the service is available to the subscriber through the portal. Depending on the configuration, the subscriber may need to activate the service. You can configure schedules to define when services are available to subscribers.

To configure a subscription to a service:

1. Click **Configure**, and expand **Subscribers** and the specified retailer.
2. Click the specified subscriber folder.

The Subscriber Folder: *<name>* pane appears.
3. From the Create new list, select the type of subscription that you want to configure.

The Subscription: *<name>* pane appears.
4. Enter information as described in the Help text in the main pane, and click **Apply**.

Allowing Multiple Subscriptions to the Same Service per Subscriber

To allow a subscriber to have multiple subscriptions to the same service, each subscription:

- Must have its own parameter substitutions.
- Can be activated or deactivated independently.

An object for each subscription is created in the directory. The name of the object has the following format:

<ServiceName>%<SubscriptionId>

- *<ServiceName>* —Name of the service
- *<SubscriptionId>* —Name of the subscription

Other than the naming convention, multiple subscriptions are identical to regular subscriptions.

Configuring Accesses (C-Web Interface)

You must configure an access for an enterprise or a site. An access determines the way that the enterprise or site accesses Internet services, and specifies a set of services that are available to the particular access.

Subscriber classification scripts can use access subscription properties to match the interface in the network with an access in the directory. Typically, the interface alias, interface description, interface name, unique ID, NAS port ID, and router name are used to match an interface to an access.

You can specify multiple accesses; for example, you might want to specify primary and backup services for Internet access.

To configure a subscription to an access service:

1. Click **Configure**, and expand **Subscribers**.
2. Expand the specified retailer and the subscriber folder.

3. Click the specified enterprise.

The Enterprise: *< name >* pane appears.

4. From the Create new list, select **Access**.
5. In the dialog box, enter a name for the new Access, and click **OK**.

The Access: *< name >* pane appears.

6. Enter information as described in the Help text in the main pane, and click **Apply**.

Chapter 32

Configuring External Subscriber Events with the C-Web Interface

This chapter describes how you can integrate IP address managers into an SRC-managed network so that the SAE is notified about subscriber events. Topics include:

- Overview of External Subscriber Monitor on page 273
- Configuring External Subscriber Monitor on page 274
- Configuring the NIC Proxy for the Pseudo-RADIUS Server (C-Web Interface) on page 275
- Configuring the Pseudo-RADIUS Server for External Subscriber Monitor on page 277
- Configuring the Client Secret for the External Subscriber Monitor on page 277
- Configuring Event Notification for the External Subscriber Monitor on page 277
- Starting External Subscriber Monitor with the C-Web Interface on page 277
- Stopping External Subscriber Monitor with the C-Web Interface on page 278

Overview of External Subscriber Monitor

You use the External Subscriber Monitor application with the event notification method of logging in subscribers and creating subscriber sessions. You can use event notification when you integrate devices into the SRC network that do not notify the SAE about subscriber events, such as when a subscriber logs in or when the address assignment is terminated.

For information about event notification with other third-party network devices, see *Logging In Subscribers and Creating Sessions*.

External Subscriber Monitor must view all RADIUS accounting messages associated with subscriber sessions. External Subscriber Monitor is stateless and cannot synchronize the current set of subscribers when there is a failure. If events are missed because of a software or network failure, the overall state recovers when RADIUS interim updates are sent. For example, missed ipUp events become effective when the next interim update is sent, and missed ipDown events time out after the configured RADIUS time to live.

External Subscriber Monitor is configured as a pseudo-RADIUS server and acts as a RADIUS accounting server. Configure the router or RADIUS server to duplicate

accounting packets to External Subscriber Monitor. When External Subscriber Monitor is the pseudo-RADIUS server, it handles software failures more robustly. The pseudo-RADIUS server does not acknowledge failed accounting requests and gives the RADIUS client the option to retransmit the accounting packet to a backup External Subscriber Monitor.

Configuring External Subscriber Monitor

Configure initial properties, including directory connection and directory eventing properties.

Tasks to configure External Subscriber Monitor are:

1. Configuring Basic Local Properties for External Subscriber Monitor on page 274
2. Configuring Initial Properties for External Subscriber Monitor on page 274
3. Configuring Directory Connection Properties for External Subscriber Monitor on page 274
4. Configuring Eventing Properties for External Subscriber Monitor on page 275
5. Configuring Logging Destinations for External Subscriber Monitor on page 275

Configuring Basic Local Properties for External Subscriber Monitor

To configure basic local properties:

1. Click **Configure > Slot**, then a specified slot (for example, slot0), and then **External Subscriber Monitor**.

The External Subscriber Monitor pane appears.

2. From the Create new list, select **Logger**. Type a name for the new logger in the dialog box, and click **OK**.
3. Enter the maximum java heap size in the **Java Heap Size** box, as described in the Help text.
4. Click **Apply**.

Configuring Initial Properties for External Subscriber Monitor

To configure initial properties:

1. Click **Configure > Slot**, then a specified slot (for example, slot0).
2. Expand **External Subscriber Monitor**.
3. Click **Initial**.

The Initial pane appears.

Configuring Directory Connection Properties for External Subscriber Monitor

To configure directory connection properties:

1. Click **Configure > Slot**, then a specified slot (for example, slot0).
2. Expand **External Subscriber Monitor**.
3. Expand **Initial**, then click **Directory Connection**.

The Directory Connection pane appears.

4. Enter the information as described in the Help text box.
5. Click **Apply**.

Configuring Eventing Properties for External Subscriber Monitor

To configure eventing properties:

1. Click **Configure > Slot**, then a specified slot (for example, slot0).
2. Expand **External Subscriber Monitor**.
3. Expand **Initial**, and then click **Directory Eventing**.

The Directory Eventing pane appears.

4. Enter the information as described in the Help text box.
5. Click **Apply**.

Configuring Logging Destinations for External Subscriber Monitor

You can configure the logging destination to store messages in a file or a system logging facility (Syslog). You can create or modify loggers.

To configure logging destinations to store log messages:

1. Click **Configure > Slot**, then a specified slot (for example, slot0).
2. Expand **External Subscriber Monitor**.
3. From the Create new list, select **Logger**.
4. In the dialog box, type a name for the new logger, and click **OK**.

The name of the logger appears in the side pane and the Logger pane.

5. Expand the logger in the side pane, and then click **File** or **Syslog**.
6. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring the NIC Proxy for the Pseudo-RADIUS Server (C-Web Interface)

Tasks to configure the NIC proxy are:

1. Configuring Resolution Information for a NIC Proxy on page 276
2. Changing the Configuration for the NIC Proxy Cache on page 276
3. Configuring a NIC Proxy for NIC Replication on page 276

Configuring Resolution Information for a NIC Proxy

To configure resolution information for a NIC proxy:

1. Click **Configure > Slot**, then a specified slot (for example, slot0),
2. Expand **External Subscriber Monitor**.
3. Click **NIC Proxy Configuration**.

The NIC Proxy Configuration pane appears.

Changing the Configuration for the NIC Proxy Cache

You can modify cache properties for the NIC proxy to optimize the resolution performance for your network configuration and system resources. Typically, you can use the default settings for the cache properties.

1. Click **Configure > Slot**, then a specified slot (for example, slot0).
2. Expand **External Subscriber Monitor**.
3. Expand **NIC Proxy Configuration**, and then expand **RADIUS Accounting NIC**.
4. Click **Resolution**.

The Resolution pane appears.

5. Enter the information as described in the Help text.
6. Click **Apply**.

Configuring a NIC Proxy for NIC Replication

Typically, you configure NIC replication to keep the NIC highly available. You configure NIC host selection to specify the groups of NIC hosts to be contacted to resolve a request and to define how the NIC proxy handles NIC hosts that the proxy is unable to contact.

To configure a NIC proxy to use NIC replication:

1. Click **Configure > Slot**, then a specified slot (for example, slot0).
2. Expand **External Subscriber Monitor**.
3. Expand **NIC Proxy Configuration**, and then expand **RADIUS Authorization NIC**.
4. Click **Resolution**.

The Resolution pane appears.

5. Enter the information as described in the Help text.
6. Click **Apply**.

Configuring the Pseudo-RADIUS Server for External Subscriber Monitor

To configure the RADIUS accounting server:

1. Click **Configure > Slot**, then a specified slot (for example, slot0).
2. Expand **External Subscriber Monitor**.
3. Click **Radius Accounting**.

The RADIUS Accounting pane appears.

4. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring the Client Secret for the External Subscriber Monitor

To configure trusted clients for External Subscriber Monitor:

1. Click **Configure > Slot**, then a specified slot (for example, slot0).
2. Expand **External Subscriber Monitor**.
3. Expand **Radius Accounting**, and click **Client**.

The Client pane appears.

4. Enter information as described in the Help text in the main pane, and click **Apply**.

Configuring Event Notification for the External Subscriber Monitor

To configure event notification for External Subscriber Monitor:

1. Click **Configure > Slot**, then a specified slot (for example, slot0).
2. Expand **External Subscriber Monitor**, and then click **Event Notification**.

The Event Notification pane appears.

3. Enter information as described in the Help text in the main pane, and click **Apply**.

Starting External Subscriber Monitor with the C-Web Interface

To start the External Subscriber Monitor:

1. Click **Manage > Enable**.

The Enable pane appears.

2. From the Component list, select **exsubmonr**, and click **OK**.

Stopping External Subscriber Monitor with the C-Web Interface

To stop the External Subscriber Monitor:

1. Click **Manage > Disable**.

The Disable pane appears.

2. From the Component list, select **exsubmonr**, and click **OK**.

Chapter 33

Configuring Traffic Redirection (C-Web Interface)

This chapter describes how to use the C-Web interface to configure the redirect server for a C-series Controller.

Topics in this chapter include:

- Configuring the Redirect Server (C-Web Interface) on page 279
- Configuring General Properties for the Redirect Server (C-Web Interface) on page 280
- Configuring a Connection Between the Redirect Server and the Directory with the C-Web Interface on page 281
- Defining Traffic to Transmit to the Redirect Server (C-Web Interface) on page 281
- Changing the Number of Requests That the Redirect Server Accepts (C-Web Interface) on page 282
- Specifying Extensions for Files That the Redirect Server Accepts (C-Web Interface) on page 282
- Configuring the DNS Server for the Redirect Server (C-Web Interface) on page 282
- Configuring the Redirect Server to Support HTTP Proxies (C-Web Interface) on page 283
- Configuring a Redundant Redirect Server (C-Web Interface) on page 284
- Configuring Logging for the Redirect Server on page 284
- Changing the Configuration for the Redirect Server on page 284
- Assessing Load for Redirect Server (C-Web Interface) on page 284

Configuring the Redirect Server (C-Web Interface)

Configure the redirect server on a C-series Controller to manage IP layer redirection.

< Add procedure for Callisto additions - see CLI chapter >

To configure the redirect server:

1. Configure general properties for the redirect server.

See [Configuring General Properties for the Redirect Server \(C-Web Interface\)](#) .

2. Configure a connection from the redirect server to the directory.

See [Configuring a Connection Between the Redirect Server and the Directory with the C-Web Interface](#) .

3. (Optional) Define traffic to be forwarded to the redirect server. In most cases you can accept the default values—traffic destined for port 80 (Web requests) and forwarded from all interface on a C-series Controller.

See [Defining Traffic to Transmit to the Redirect Server \(C-Web Interface\)](#) .

4. (Optional) Configure the number of requests that the redirect server accepts.

See [Changing the Number of Requests That the Redirect Server Accepts \(C-Web Interface\)](#).

5. (Optional) Configure the types of files for which the redirect server accepts requests.

See [Specifying Extensions for Files That the Redirect Server Accepts \(C-Web Interface\)](#).

6. (Optional) For a configuration to support HTTP proxies, configure DNS. You can configure the DNS server included with the redirect server, or another DNS server on your network. If you use another DNS server, you do not need to configure the DNS server included with the redirect server.

For information about configuring the DNS server included with the redirect server, see [Configuring the DNS Server for the Redirect Server \(C-Web Interface\)](#).

7. (Optional) Configure support for HTTP proxies.

See [Configuring the Redirect Server to Support HTTP Proxies \(C-Web Interface\)](#).

8. (Optional) Configure a redundant redirect server.

See [Configuring a Redundant Redirect Server \(C-Web Interface\)](#).

- Related Topics**
- [Overview of Traffic Redirection](#)
 - [Redirect Server Redundancy](#)
 - [Configuring the Redirect Server \(SRC CLI\)](#)

Configuring General Properties for the Redirect Server (C-Web Interface)

To configure general properties for the redirect server:

1. Click **Configure > Redirect Server**.

The Redirect Server pane appears.

2. Enter information as described in the Help text in the main pane, and click **Apply**.

- Related Topics**
- Overview of Traffic Redirection
 - Configuring the Redirect Server (C-Web Interface)

Configuring a Connection Between the Redirect Server and the Directory with the C-Web Interface

To configure a connection between the redirect server and the directory:

1. Click **Configure**, expand **Redirect Server**, then click **Ldap**.

The Ldap pane appears.

2. Enter information as described in the Help text in the main pane, and click **Apply** to trigger an automatic commit.

- Related Topics**
- Overview of Traffic Redirection
 - Configuring the Redirect Server (C-Web Interface)

Defining Traffic to Transmit to the Redirect Server (C-Web Interface)

You can define traffic to be forwarded to the redirect server by identifying the destination port number (typically, port 80 for Web requests) for packets and the physical interface on a C-series Controller from which subscriber traffic is forwarded to the redirect server. In most cases you can accept the default values for configuration for IP redirection. If you do not specify an interface, traffic is accepted on all interfaces.

To change the values of the port for traffic and/or the C-series interface on which traffic is forwarded to the redirect server:

1. Click **Configure**, expand **Redirect Server**, and then click **IP Redirect**.

The IP Redirect pane appears.

2. Click the **Create** button.

The IP Redirect pane reappears.

3. Enter the information as described in the Help text in the main pane, and click **Apply**.

- Related Topics**
- Overview of Traffic Redirection
 - Configuring the Redirect Server (C-Web Interface)

Changing the Number of Requests That the Redirect Server Accepts (C-Web Interface)

If you want to change the number of redirection requests that the redirect server accepts, change the values for the request rates and the client rates.

To configure the number of redirection requests that the redirect server can accept:

1. Click **Configure > Redirect Server**.

The Redirect Server pane appears.

2. Change the values in the following boxes as described in the Help text in the main pane:
 - Request Rate
 - Request Burst Size
 - Client Rate
 - Client Burst Size
3. Click **Apply**.

- Related Topics**
- Overview of Traffic Redirection
 - Configuring the Redirect Server (C-Web Interface)

Specifying Extensions for Files That the Redirect Server Accepts (C-Web Interface)

If you do not specify the types of files that the redirect server accepts, the redirect server accepts all file types. You can identify file types by specifying the file extensions for the files that the redirect server is to accept.

To specify the extensions for the types of files accepted by the redirect server:

1. Click **Configure > Redirect Server**.

The Redirect Server pane appears.

2. To enable or disable checking file extensions, clear or select the Check File Extensions box as described in the Help Text in the main pane.
3. Click **Apply**.

- Related Topics**
- Overview of Traffic Redirection
 - Configuring the Redirect Server (C-Web Interface)

Configuring the DNS Server for the Redirect Server (C-Web Interface)

A DNS server is required to support HTTP proxies to resolve the name of any HTTP proxy, even if the name is valid only in the private domain of the client. You can use

an external DNS or the DNS server that is included with the redirect server for this purpose.



NOTE: If you plan to use an external DNS server, do not follow this procedure.

The following procedure describes how to configure the DNS server that is included with the redirect server.

Proxy support must be enabled before configuring the DNS server. See [Configuring the Redirect Server to Support HTTP Proxies \(C-Web Interface\)](#).

To configure the DNS server that is included with the redirect server:

1. Click **Configure**, expand **Redirect Server**, and click **DNS**.

The DNS pane appears.

2. Enter information as described in the Help text in the main pane, and click **Apply**.

- Related Topics**
- Overview of Traffic Redirection
 - Configuring the Redirect Server (C-Web Interface)

Configuring the Redirect Server to Support HTTP Proxies (C-Web Interface)

Support for proxy requests is an optional feature of the redirect server. If you configure proxy support, you must also have DNS configured. You can use DNS servers already installed on your network, or use the server included with the SRC software.

To configure the redirect server to support HTTP proxies:

1. Click **Configure > Redirect Server**.

The Redirect Server pane appears.

2. Clear the Proxy Support checkbox box to disenable HTTP proxy support. Select the checkbox to enable HTTP proxy support. Refer to the information in the Help text in the main pane.
3. In the Destination Url box, type the URL sent as a response to proxy requests.
4. Click **Apply**.

- Related Topics**
- Overview of Traffic Redirection
 - Configuring the Redirect Server (C-Web Interface)
 - For information about configuring the DNS server included with the SRC software, see [Configuring the DNS Server for the Redirect Server \(C-Web Interface\)](#)

Configuring a Redundant Redirect Server (C-Web Interface)

Although configuration of a redundant redirect server is optional, we recommend that you configure redundancy to maintain high availability for the server.

Before you configure the redirect server, review configuration prerequisites. See [Before You Configure Redundancy for a Redirect Server](#).

To configure redundancy for the redirect server:

1. Click **Configure > Redirect Server**.

The Redirect Server pane appears.

2. To enable or disable redundancy for the redirect server, clear (or select) the Redundancy checkbox as described in the Help text in the main pane.

- Related Topics**
- Overview of Traffic Redirection
 - Redirect Server Redundancy
 - Configuring the Redirect Server (C-Web Interface)
 - Configuring a Redundant Redirect Server (SRC CLI)

Configuring Logging for the Redirect Server

The redirect server logs incoming HTTP requests through syslog with a priority of INFO and log facility of LOCAL7.

- Related Topics**
- Configuring a Component to Store Log Messages in a File with SRC CLI
 - Configuring System Logging with SRC CLI

Changing the Configuration for the Redirect Server

When you change the configuration for the redirect server and commit that configuration, the redirect server is automatically restarted.

- Related Topics**
- Configuring the Redirect Server (SRC CLI)

Assessing Load for Redirect Server (C-Web Interface)

Purpose View the number of requests sent to the redirect server, and whether the requests reach the configured limit for the server and for server users. You can then use this information to fine-tune the properties for redirect server.

- Action**
1. Click **Monitor > Redirect Server > Statistics**.
- The Redirect Server Statistics pane appears.
2. From the Output Style list, select an output style as described in the Help text in the main pane.

3. Click **OK**. The Redirect Server pane displays the following statistics:

- Uptime
- Accepted requests
- Rejected requests
- Number of user-limit leaky buckets
- Number of user limits reached
- Number of global limits reached

You can also obtain statistics for redirect server through SNMP. The name of the MIB for redirect server is Juniper-SDX-REDIRECTOR-MIB.

Related Topics

- Overview of Traffic Redirection
- Configuring General Properties for the Redirect Server (SRC CLI)
- Viewing Statistics for the Redirect Server (C-Web Interface)
- Viewing Information About Filtered Traffic (C-Web Interface)

Part 8

Index

- Index on page 289

Index

A

- accesses
 - configuring subscriptions
 - C-Web interface.....270, 271
- accounting
 - basic RADIUS accounting plug-in.....250
 - custom RADIUS accounting plug-ins.....251
 - flat file accounting plug-ins.....251
 - flexible RADIUS accounting plug-ins.....251
- action congestion points
 - configuring with C-Web interface.....121
- action threshold, service schedules
 - setting
 - C-Web interface.....215
- aggregate services
 - adding
 - C-Web interface.....206
 - timers, configuring
 - C-Web interface.....207
- announcements at system login.....23
- apply-groups statement, JUNOS routing
 - platforms.....178
- assigned IP subscribers
 - third-party devices.....167
 - IP address pools.....167
- assigning
 - edge congestion points to subscribers with C-Web
 - interface.....120
 - interfaces to backbone congestion points with
 - C-Web interface.....122
 - interfaces to subscribers with C-Web
 - interface.....120
- authentication
 - NTP authentication keys.....13, 14
 - RADIUS
 - configuring.....25
 - configuring with C-Web interface.....26
 - shared user accounts.....27

- TACACS+, configuring with C-Web
 - interface.....25, 26
- template accounts
 - configuring local user with C-Web
 - interface.....27
 - configuring remote users with C-Web
 - interface.....27
- authentication order
 - configuring with C-Web interface.....26
 - removing authentication method.....26
- authentication plug-ins
 - configuring
 - SRC CLI.....254
- authorization plug-ins
 - configuring
 - SRC CLI.....254

B

- backbone congestion points.....113
 - configuring for services with C-Web
 - interface.....121
 - configuring with C-Web interface.....121, 122
 - running applications from.....121
- backbone network.....121
- backbone network management with SRC-ACP
 - configuring with C-Web interface.....121
- backbone network with SRC-ACP
 - managing with C-Web interface.....121
- bandwidth
 - configuring
 - for services with C-Web interface.....120
 - for subscribers with C-Web interface.....119
- bandwidths and congestion points for subscribers with
 - C-Web interface
 - configuring.....119
- basic RADIUS accounting plug-in.....250
 - configuring
 - SRC CLI.....253
- basic RADIUS authentication plug-in.....255
 - configuring
 - SRC CLI.....256
- BEEP, JUNOS routing platforms
 - connection.....150

C

C-series Controllers	
interfaces.....	3
C-series platform, configuring to accept SSH connections with the C-Web interface.....	9
C-series platform, configuring to accept telnet connections with the C-Web interface.....	9
captive portal	
using with next-hop action	
C-Web interface.....	195
certificate authority (CA).....	152
classification scripts	
conditions.....	59
glob matching.....	61
joining.....	61
regular expression matching.....	64
configuring	
SRC CLI.....	61
descriptions.....	59
DHCP classification, C-series controller	
description.....	59
targets.....	74
DHCP subscriber classification, C-series platform	
C-Web interface.....	73
interface classification, C-series controller	
conditions.....	65
description.....	59
examples.....	65
how it works.....	59
targets.....	65
interface classification, C-series platform	
C-Web interface.....	65
targets.....	65
structure	
SRC CLI.....	61
subscriber classification, C-series controller	
condition.....	68
description.....	59
DHCP options.....	71
how it works.....	59
targets.....	72
target, C-series controller	
definition.....	59
expressions.....	61
types.....	61
classify-traffic condition	
application protocol	
defining, C-Web interface.....	190
configuring	
C-Web interface.....	182
destination grouped network, configuring	
C-Web interface.....	187
destination network, configuring	
C-Web interface.....	186
expanded classifiers	
configuring, C-Web interface.....	184
extended classifiers	
configuring, C-Web interface.....	184
ICMP conditions, setting	
C-Web interface.....	189
IGMP conditions, setting	
C-Web interface.....	189
IPSec conditions, setting	
C-Web interface.....	189
JUNOS filter conditions, setting	
C-Web interface.....	189
PCMM I02 and I03	
configuring, C-Web interface.....	184
protocol conditions with parameters, setting	
C-Web interface.....	188
protocol conditions with ports, setting	
C-Web interface.....	187
protocol conditions, setting	
C-Web interface.....	187
source grouped network, configuring	
C-Web interface.....	186
source network, setting	
C-Web interface.....	186
TCP conditions, setting	
C-Web interface.....	188
CMTS devices	
adding objects to directory	
C-Web interface.....	163
adding virtual router objects to directory	
SRC CLI.....	163
configuration statements.....	163
community manager	
configuring, third-party devices	
C-Web interface.....	172
configuration group, JUNOS routing platforms.....	150
congestion points	
configuring.....	119
conventions	
notice icons.....	xxvii
text.....	xxvii
COPS (Common Open Policy Service)	
connection with JUNOSe routers.....	137
configuring SAE, C-Web interface.....	139
disabling on router.....	145
enabling on router.....	144
CORBA (Common Object Request Broker Architecture)	
IOR location.....	110
CORBA interfaces	
SRC-ACP.....	117
custom RADIUS accounting plug-ins.....	251
configuring	
SRC CLI.....	254
custom RADIUS authentication plug-ins.....	255
configuring	
SRC CLI.....	257
customer support.....	xxxix
contacting JTAC.....	xxxix

D

- data recovery
 - Juniper Networks database.....39
- Data-over-Cable Service Interface Specifications. *See* DOCSIS
- device drivers
 - JUNOS
 - configuring, C-Web interface.....151
 - JUNOSe
 - configuring, C-Web interface.....139
 - configuring, SRC CLI.....151
 - viewing state, C-Web interface.....141
 - viewing statistics, C-Web interface.....141
- DHCP (Dynamic Host Configuration Protocol)
 - classification scripts. *See* classification scripts
 - options.....75
 - profiles
 - C-Web interface.....78
- directory
 - services for SRC-ACP.....118
 - subscribers for SRC-ACP.....118
- DOCSIS policy actions
 - configuring
 - C-Web interface. 192, 193, 194, 195, 196, 197, 198, 199, 200, 201
- documentation set
 - comments on.....xxxi
- drop profile maps
 - configuring
 - C-Web interface.....199
 - drop probability, setting
 - C-Web interface.....199
 - fill level, setting
 - C-Web interface.....199

E

- edge congestion points
 - assigning to subscribers with C-Web interface.....120
- edge network.....118
- edge network management, configuring with C-Web interface.....118
- enterprise subscribers
 - adding
 - C-Web interface.....268
- event notification, PCMM network
 - configuration statements.....83
 - properties, configuring
 - SRC CLI.....83
- event notification, third-party devices
 - configuring properties
 - C-Web interface.....173
 - description.....168

- event publishers
 - configuring
 - SRC CLI.....264
- events, publishing.....113
- example-simple.....110, 209, 211, 222, 225, 228
- exclusions to service schedule
 - defining
 - C-Web interface.....220
- expanded classifiers
 - configuring
 - C-Web interface.....184
- extended classifiers, PCMM
 - configuring
 - C-Web interface.....184
- external plug-ins
 - configuring
 - C-Web interface.....247
- External Subscriber Monitor
 - acting as pseudo RADIUS server, C-Web interface.....273
 - changing configuration for NIC proxy cache, C-Web interface.....276
 - configuring basic local properties, C-Web interface.....274
 - configuring directory connection properties, C-Web interface.....274
 - configuring event notification, C-Web interface.....277
 - configuring eventing properties, C-Web interface.....275
 - configuring initial properties, C-Web interface.....274
 - configuring, for C-Web interface.....274
 - configuring, NIC proxy for NIC replication, C-Web interface.....276
 - configuring, NIC proxy for pseudo-RADIUS server, C-Web interface.....275
 - configuring, NIC proxy for pseudo-RADIUS server, C-Web interface.....276
 - IP address manager
 - C-Web Interface.....273
 - overview, C-Web interface.....273
 - starting
 - C-Web interface.....277
 - stopping
 - C-Web interface.....278

F

- filter actions
 - configuring
 - C-Web interface.....192

flat file accounting plug-ins.....	251
configuring	
SRC CLI.....	251
configuring headers	
SRC CLI.....	252
flexible RADIUS accounting plug-ins.....	251
attributes, defining	
SRC CLI.....	258
configuring.....	253
flexible RADIUS authentication plug-ins.....	255
attributes, defining	
examples.....	262
SRC CLI.....	258
configuring	
SRC CLI.....	256
setting responses	
SRC CLI.....	262
FlowSpec actions	
configuring	
C-Web interface.....	192
forward actions	
configuring	
C-Web interface.....	193
forwarding class actions	
configuring	
C-Web interface.....	193

G

gateSpec actions	
configuring	
C-Web interface.....	193
Gigabit Ethernet interfaces for IPv4, configuring with the C-Web interface.....	5
Gigabit Ethernet interfaces for IPv6, configuring with the C-Web interface.....	6
global parameters	
configuring	
C-Web.....	203
predefined	
viewing with C-Web.....	203
GRE tunnel interfaces.....	7

H

hosted internal plug-in.....	113
------------------------------	-----

1

- infrastructure services.....207
- interface classification scripts. *See* classification scripts
- interfaces
 - C-series Controllers.....3
 - Gigabit Ethernet, configuring.....5, 6
 - group.....7

loopback, configuring.....	4
tunnel, configuring.....	7
interfaces, assigning to backbone congestion points	
with C-Web interface.....	122
interim accounting, configuring on SAE.....	242
internal plug-ins	
configuring	
C-Web interface.....	246
IOR	
router initialization scripts.....	142, 159
IP-over-IP tunnel interfaces.....	7
IPv6 in IPv4 tunnel interfaces.....	7

J

JPS (Juniper Policy Server)	
application manager-to-policy server interface, configuring	
C-Web interface.....	129
monitoring	
C-Web interface.....	136
operational status.....	136
policy server-to-CMTS interface, configuring	
C-Web interface.....	130
starting	
C-Web interface.....	135
stopping	
C-Web interface.....	136
subscriber address mappings, configuring	
C-Web interface.....	130
subscriber configuration, modifying	
C-Web interface.....	130
Juniper Networks database	
community mode, adding Juniper Networks database	
C-Web interface.....	35
community mode, configuring	
C-Web interface.....	34
data recovery	
C-Web interface.....	39
initialize date	
C-Web interface.....	37
loading sample data.....	37
roles,changing secondary to primary	
C-Web interface.....	36
security configuration	
C-Web interface.....	34, 38
standalone mode.....	33
updating data	
C-Web interface.....	37

JUNOS ASP policy rules	
NAT actions	
configuring, C-Web interface.....	194
network, specifying	
C-Web interface.....	186, 187
stateful firewall actions, configuring	
C-Web interface.....	200
JUNOS filter policy rules	
conditions, setting	
C-Web interface.....	189
JUNOS policer policy rules	
policer actions	
configuring, C-Web interface.....	196
JUNOS routing platforms	
configuration groups.....	150
default virtual router	
adding with C-Web interface.....	150
router objects, adding	
SRC CLI.....	151
SRC software process.....	150
troubleshooting.....	161
VR objects, adding individually	
C-Web interface.....	151
JUNOS scheduler policy rules.....	199
actions	
configuring, C-Web interface.....	199
QoS conditions, configuring	
C-Web interface.....	191
<i>See also</i> drop profile maps	
JUNOSe routers	
accessing router CLI.....	144
COPS connection	
configuring, C-Web interface.....	139
integration overview.....	137
monitoring interactions with SAE.....	145
router objects, adding	
C-Web interface.....	138
SNMP communities, configuring	
C-Web interface.....	141
SNMP server	
configuring on router.....	140
SRC client.....	137
starting.....	144
stopping.....	145
troubleshooting.....	146
VR objects	
adding individually, C-Web interface.....	139
discovering, C-Web interface.....	138
L	
LDAP access. <i>See</i> SAE (service activation engine), configuring	
LDAP authentication plug-in.....	255
configuring	
SRC CLI.....	257

limiting subscribers plug-in.....	255
configuring	
SRC CLI.....	255
local parameters	
configuring	
C-Web interface.....	203
local password authentication.....	27
logging.....	16
redirect server.....	284
<i>See also</i> system log server	
logging properties	
configuring for SRC-ACP with C-Web interface.....	114
login announcements, system.....	23
login classes	
configuration.....	21
login process	
assigned IP subscribers, third-party devices.....	168
event notification method, third-party devices.....	169
login registration	
configuring	
SRC CLI.....	244
loopback interfaces for IPv4, configuring with the C-Web interface.....	4
loopback interfaces for IPv6, configuring with the C-Web interface.....	4
loss priority actions	
configuring	
C-Web interface.....	194

M

managers	
configuring	
C-Web interface.....	270
managing	
edge network with SRC-ACP.....	118
manuals	
comments on.....	xxxi
mark actions	
configuring	
C-Web interface.....	194
messages	
severity levels for logging.....	16
monitoring	
backbone congestion points with C-Web interface.....	113
mutex group	
adding	
SRC CLI.....	207

N

NAS ID, configuring for SAE	
C-Web interface.....	50

NAT (Network Address Translation) policies	
actions	
configuring, C-Web interface.....	194
application protocol condition	
defining, C-Web interface.....	190
network interfaces.....	119
network publisher <i>See</i> NIC	
next-hop actions	
captive portal feature	
C-Web interface.....	195
configuring	
C-Web interface.....	195
next-interface actions	
configuring	
C-Web interface.....	195
next-rule actions	
configuring	
C-Web interface.....	196
NIC (network information collector)	
configuration overview.....	96
configuration prerequisites	
C-series controllers.....	95
configuration, changing	
C-Web interface.....	101
network publisher	
overview.....	103
prerequisites.....	104
test information.....	106
operating properties.....	97
replication	
configuring with C-Web interface.....	97
SAE plug-in agents.....	99
restarting	
C-Web interface.....	101
starting	
C-Web interface.....	96
testing	
any key.....	109
test data.....	109
testing resolution	
C-Web interface.....	100
NIC configuration scenarios	
changing	
C-Web interface.....	101
configuring	
C-Web interface.....	98
OnePopStaticRouteIp.....	103
OnePopVrflp.....	103
NIC hosts	
configuration prerequisites.....	95
stopping	
C-Web interface.....	101
NIC proxies	
configuration prerequisites.....	107
prerequisites.....	107
notice icons.....	xxvii

notification targets	
configuring with C-Web interface.....	91
NTP (Network Time Protocol)	
authentication key configuration	
C-Web interface.....	13
broadcast mode	
C-Web interface.....	13
configuration	
C-Web interface.....	11
multicast client configuration	
C-web interface.....	13
peer configuration	
C-Web interface.....	12
server configuration	
C-Web interface.....	12

O

operation	
SRC-ACP, configuring with C-Web interface.....	115

P

PacketCable Multimedia Specifications. <i>See</i> PCMM	
parameter values, setting in services.....	206
parameters	
global. <i>See</i> global parameters	
local. <i>See</i> local parameters	
runtime. <i>See</i> runtime parameters	
passwords	
RADIUS.....	26
shared user.....	27
PCMM (PacketCable Multimedia)	
configuring SAE	
C-Web interface.....	81
PCMM device driver	
configuration statements.....	82
configuring	
C-Web interface.....	82
PCMM policies	
DOCSIS parameters	
configuring, C-Web	
interface. 192, 193, 194, 195, 196, 197, 198, 199, 200, 201	
extended classifiers	
configuring, C-Web interface.....	184
FlowSpec parameters	
configuring, C-Web interface.....	192
gateSpec parameters, configuring	
C-Web interface.....	193
I02 and I03 classifiers	
configuring, C-Web interface.....	184
service class name	
configuring, C-Web interface.....	199

- PCMM record-keeping server plug-in
 - configuration statements.....83
 - configuring
 - C-Web interface.....83
- plug-ins
 - authentication
 - configuring, SRC CLI.....254
 - authorization
 - configuring, SRC CLI.....254
 - basic RADIUS accounting.....250
 - configuring, SRC CLI.....253
 - basic RADIUS authentication.....255
 - configuring, SRC CLI.....256
 - custom RADIUS accounting.....251
 - configuring, SRC CLI.....254
 - custom RADIUS authentication.....255
 - configuring, SRC CLI.....257
 - external
 - configuring, C-Web interface.....247
 - flat file accounting.....251
 - configuring, SRC CLI.....251
 - flexible RADIUS accounting.....251
 - configuring.....253
 - flexible RADIUS authentication.....255
 - configuring, SRC CLI.....256
 - hosted internal plug-in.....113
 - internal
 - configuring RADIUS peers, SRC CLI.....249
 - configuring, C-Web interface.....246
 - RADIUS attributes, SRC CLI.....258
 - LDAP authentication.....255
 - configuring, SRC CLI.....257
 - limiting subscribers.....255
 - configuring, SRC CLI.....255
 - state synchronization
 - configuring, C-Web interface.....247
 - tracking
 - configuring, SRC CLI.....250
- policer actions
 - configuring
 - C-Web interface.....196
- policy actions
 - configuring
 - C-Web interface.....191
- DOCSIS
 - configuring, C-Web interface. 192, 193, 194, 195, 196, 197, 198, 199, 200, 201
- filter
 - configuring, C-Web interface.....192
- FlowSpec
 - configuring, C-Web interface.....192
- forward
 - configuring, C-Web interface.....193
- forwarding class
 - configuring, C-Web interface.....193
- gateSpec
 - configuring, C-Web interface.....193
- loss priority
 - configuring, C-Web interface.....194
- mark
 - configuring, C-Web interface.....194
- NAT
 - configuring, C-Web interface.....194
- next hop
 - configuring, C-Web interface.....195
- next interface
 - configuring, C-Web interface.....195
- next rule
 - configuring, C-Web interface.....196
- policer
 - configuring, C-Web interface.....196
- QoS profile attachment
 - configuring, C-Web interface.....197
- rate limit
 - configuring, C-Web interface.....197
- reject
 - configuring, C-Web interface.....198
- routing instance
 - configuring, C-Web interface.....198
- scheduler
 - configuring, C-Web interface.....199
- service class name
 - configuring, C-Web interface.....199
- stateful firewall
 - configuring, C-Web interface.....200
- traffic class
 - configuring, C-Web interface.....200
- traffic mirror
 - configuring, C-Web interface.....200
- traffic-shape
 - configuring, C-Web interface.....201
- policy folders
 - configuring
 - C-Web interface.....180
- policy groups
 - configuring
 - C-Web interface.....180
- policy lists
 - configuring
 - C-Web interface.....180
- policy management
 - bandwidth management.....181
 - overview.....181
 - packet logging.....182
 - packet mirroring.....181
 - packet tagging.....181
 - policy routing.....181
 - QoS classification and marking.....181
 - RADIUS support.....181
 - security.....181

policy rules	
configuring	
C-Web interface.....	181
policy servers	
adding application manager groups	
C-Web interface.....	132
adding objects to directory	
C-Web interface.....	133
specifying application managers	
C-Web interface.....	132
specifying SAE communities	
C-Web interface.....	132
ports	
RADIUS server.....	26
preparation time, service schedules	
setting	
C-Web interface.....	215
properties	
SRC-ACP.....	114
pseudo-RADIUS server	
configuring External Subscriber Monitor, C-Web	
interface.....	277
publishing events.....	113

Q

QoS (quality of service)	
condition	
configuring, C-Web interface.....	191
QoS profile attachment actions	
configuring, C-Web interface.....	197
QoS profile, configuring	
C-Web interface.....	197
QoS profile-tracking plug-in	
description.....	231
QoS profiles, JUNOSe routers	
how tracking works.....	231
managing dynamically.....	231
QoS tracking plug-in.....	251
quality of service. <i>See</i> QoS	

R

RADIUS	
address for SAE	
C-Web interface.....	50
RADIUS attributes	
defining in RADIUS plug-ins	
SRC CLI.....	258
examples, defining in RADIUS plug-ins	
SRC CLI.....	262
RADIUS authentication. <i>See</i> authentication	
RADIUS authorization. <i>See</i> authentication	
RADIUS peers	
configuring in plug-ins	
SRC CLI.....	249

RADIUS plug-ins.....	250
authentication.....	255
UDP port.....	258
<i>See also</i> plug-ins	
rate-limit actions	
configuring	
C-Web interface.....	197
redirect server	
assessing load	
C-Web interface.....	284
changing request accepted, C-Web interface.....	282
configuring	
C-series platform	279
C-Web interface.....	279
configuring connection with C-Web	
interface.....	281
configuring DNS server for	
C-Web interface	282
configuring general properties with C-Web	
interface.....	280
configuring redundant	
C-Web interface.....	284
configuring to support HTTP proxies	
C-Web interface.....	283
defining traffic	
C-Web interface.....	281
defining traffic to transmit.....	281
logging	
SRC CLI.....	284
number of requests.....	282
specifying extensions for files	
C-Web interface.....	282
redundant redirect server, configuring.....	284
reject actions	
configuring	
C-Web interface.....	198
residential subscribers	
adding	
C-Web interface.....	268
resolving host names	
SRC CLI.....	31
retailers	
subscribers	
adding, C-Web interface.....	266
RKS (record-keeping server)	
peers, configuration statements.....	84
peers, configuring in plug-ins	
C-Web interface.....	84
plug-in, configuring	
C-Web interface.....	83
router initialization scripts	
iorPublisher.....	142, 159
JUNOS	
configuring location, SRC CLI.....	161

JUNOSe.....	141, 159
configuring location, C-Web interface.....	141
example.....	143, 161
poolPublisher.....	142, 159
router subscribers	
adding	
C-Web interface.....	269
routers	
accessing router CLI.....	144
adding JUNOS routing platforms	
SRC CLI.....	150
adding JUNOSe	
C-Web interface.....	138
integrating JUNOS routing platform.....	150
integrating JUNOSe.....	137
routing instance actions	
configuring	
C-Web interface.....	198
RTPS (real-time polling service)	
configuring.....	192
runtime parameters	
viewing with C-Web.....	204

S

SAE (service activation engine)	
classification scripts. <i>See</i> classification scripts	
configuring as an application manager	
C-Web interface.....	131
configuring for SRC-ACP with C-Web	
interface.....	113
configuring groups	
C-Web.....	48
SRC CLI.....	48
configuring initial properties	
C-Web interface.....	49
configuring to monitor backbone congestion	
points with C-Web interface.....	113
initial properties, overview	
C-Web interface.....	47
monitoring interactions	
JUNOSe routers.....	145
NIC replication, configuring	
C-Web interface.....	99
router initialization scripts. <i>See</i> router	
initialization scripts	
session store	
C-series controllers.....	55
starting	
SRC CLI.....	50
SRC client on JUNOSe router.....	144
stopping	
SRC CLI.....	50
SRC client on JUNOSe router.....	145
SAE (service activation engine), configuring	
community manager	
SRC CLI.....	83
COPS connection	
C-Web interface.....	139
directory eventing, SAE configuration data	
C-Web interface.....	54
event notification API properties	
SRC CLI.....	83
interim accounting	
C-Web interface.....	242
LDAP access, C-Web interface	
device data.....	53
directory data.....	51
persistent login cache data.....	53
policy data.....	53
service data.....	53
subscriber data.....	52
login registration	
C-Web interface.....	244
multiple logins from same IP address	
C-Web interface.....	243
PCMM device driver	
C-Web interface.....	82
SRC CLI.....	82
reduce reported session time	
C-Web interface.....	243
router initialization script location	
SRC CLI.....	161
serialized data compression	
C-Web interface.....	57
session job manager	
C-Web interface.....	57
session reactivation timers	
C-Web interface.....	244
session store	
C-Web interface.....	56
SNMP communities	
C-series platforms.....	140
time for MAC address in cache	
C-Web interface.....	241
unauthenticated user DN	
C-Web interface.....	242
SAE (service activation engine), configuring directory	
location for SAE data	
C-Web interface.....	50
SAE (service activation engine), configuring groups	
C-Web interface.....	49
SAE (service activation engine), configuring NAS ID	
C-Web interface.....	50
SAE (service activation engine), configuring RADIUS	
address	
C-Web interface.....	50
SAE (service activation engine), configuring router	
initialization script location	
C-Web interface.....	141

SAE communities	
configuration overview	
SRC CLI.....	82
configuration statements.....	83
configuring manager	
SRC CLI.....	83
description, third-party devices.....	165
sample data, loading	
Juniper Networks database, C-Web interface.....	37
scheduler actions.....	199
configuring	
C-Web interface.....	199
<i>See also</i> drop profile maps	
script services	
adding	
SRC CLI.....	207
for third-party devices.....	166
security	
digital certificates	
requesting certificates.....	152
requesting certificates through SCEP.....	154
serial port, C-series Controller.....	3
serialized data compression, configuring	
C-Web interface.....	57
service class name actions	
configuring	
C-Web interface.....	199
service schedules	
action threshold, setting	
C-Web interface.....	215
configuring	
C-Web interface.....	216
examples	
C-Web interface.....	222, 225, 228
exclusions, defining	
C-Web interface.....	220
preparation time, setting	
C-Web interface.....	215
service scopes	
adding	
C-Web interface.....	208
assigning services and Mutex groups	
C-Web interface.....	209
assigning to VRs or subscribers	
C-Web interface.....	209
configuring	
C-Web interface.....	208
example	
SRC CLI.....	211
services	
adding aggregate	
C-Web interface.....	206
adding infrastructure	
C-Web interface.....	207
adding Mutex group	
C-Web interface.....	208
adding normal	
SRC CLI.....	206
adding script services	
C-Web interface.....	207
configuring bandwidth for with C-Web	
interface.....	120
setting parameter values.....	206
C-Web interface.....	206
session job manager, configuring	
C-Web interface.....	57
session store	
C-series controllers.....	55
configuring, C-Web interface	
device driver.....	56
global parameters.....	57
configuring, SRC CLI	
compressing session objects.....	57
in third-party networks.....	166
setting parameter values	
C-Web interface.....	206
shared user accounts.....	27
sites	
subscriber	
adding, C-Web interface.....	269
SNMP agent	
access control, configuring on C-series Controllers	
with C-Web interface	
VACM.....	89
configuring	
C-series Controllers.....	88
C-series Controllers with C-Web	
interface.....	86
C-Web interface.....	88
configuring with C-Web interface	
SRC CLI.....	86
description.....	85
directory connection parameters, configuring	
C-Web interface.....	87
local properties, configuring	
with C-Web interface.....	86
monitoring	
C-Web interface.....	93
starting	
C-Web interface.....	92
stopping	
C-Web interface.....	93
SNMP communities	
configuring on SAE	
SRC CLI.....	140
SNMP monitors	
overview.....	41
SNMP server	
configuring on JUNOSe router.....	140

- SRC client, JUNOS routers
 - configuring.....137
 - starting.....144
 - stopping.....145
- SRC software process, JUNOS routing platforms.....150
- SRC-ACP (SRC Admission Control Plug-In).....118
 - backbone network management, configuring with C-Web interface.....121
 - classification scripts
 - configuring with C-Web interface.....118
 - configuring with C-Web interface.....111
 - congestion points.....113
 - connections to services directory, configuring with C-Web interface.....118
 - connections to subscribers' directory, configuring with C-Web interface.....118
 - CORBA interfaces, configuring with C-Web interface.....117
 - event publishers, configuring with C-Web interface.....113
 - logging properties, configuring with C-Web interface.....114
 - operation, configuring with C-Web interface.....115
 - properties.....114
 - redundancy
 - configuring with C-Web interface.....118
 - SAE, configuring with C-Web interface.....113
 - state synchronization
 - configuring with C-Web interface.....118
- state synchronization plug-in interface
 - configuring C-Web interface.....247
- stateful firewall policies
 - actions
 - configuring, C-Web interface.....200
 - application protocol conditions
 - defining, C-Web interface.....190
- static host mapping
 - configuring C-Web interface.....31
 - overview.....31
- static route, configuring to devices on other networks with the C-Web interface.....8
- subscriber classification scripts. *See* classification scripts
- subscriber folders
 - adding C-Web interface.....267
- subscribers
 - adding C-Web interface.....266
 - assigning interfaces to with C-Web interface.....120
 - configuring bandwidths and congestion points
 - for.....119
 - with C-Web interface.....119

- enterprise
 - adding, C-Web interface.....268
- residential
 - adding, C-Web interface.....268
- retailer
 - adding, C-Web interface.....266
- router
 - adding, C-Web interface.....269
- sites
 - adding, C-Web interface.....269
- subscriptions
 - access, configuring C-Web interface.....271
 - configuring C-Web interface.....270
 - enabling C-Web interface.....265
 - multiple per subscriber.....271
- support, technical *See* technical support
- system log server
 - configuration prerequisites.....16
 - message groups.....15
 - message severity levels.....16
 - messages, file
 - C-Web interface.....16
 - messages, server
 - C-Web interface.....17
 - messages, user notification
 - C-Web interface.....17
 - overview.....15
- system login
 - C-Web interface.....23

T

- TACACS+ authentication. *See* authentication
- targets. *See* classification scripts
- task-topic.....140
- technical support
 - contacting JTAC.....xxxi
- text conventions defined.....xxvii
- third-party devices
 - creating sessions.....167
 - integrating into SRC network
 - SRC CLI.....165
 - logging in subscribers
 - assigned IP method.....167
 - overview.....167
 - provisioning with script services.....166
 - SAE communities.....165
 - VR objects, adding C-Web interface.....172
- tracking plug-ins
 - configuring SRC CLI.....250

traffic mirror actions	
configuring	
C-Web interface.....	200
traffic shape actions	
configuring	
C-Web interface.....	201
traffic-class actions	
configuring	
C-Web interface.....	200
troubleshooting	
JUNOS routing platforms.....	161
JUNOSe routers.....	146
tunnel interfaces, configuring with the C-Web	
interface.....	7

U

UDP ports	
RADIUS plug-ins.....	258
UGS (unsolicited grant service)	
configuring	
C-Web interface.....	192
UGS-AD (unsolicited grant service with activity	
detection)	
configuring	
C-Web interface.....	192
user accounts.....	21
authentication	
configuring passwords.....	22
configuring SSH authentication.....	22
configuring with C-Web interface.....	22
overview.....	21
shared.....	27
<i>See also</i> login classes	
User Datagram Protocol. <i>See</i> UDP	
user notification messages.....	17

V

virtual routers	
adding for third-party devices	
C-Web interface.....	172
adding individually for JUNOS routing	
platforms.....	151
adding individually for JUNOSe routers	
C-Web interface.....	139
adding operative VRs.....	150
C-Web interface.....	138