



SRC-PE Software

Subscribers and Subscriptions Guide

Release 1.0.x

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089

USA

408-745-2000

www.juniper.net

Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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

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.

Products made or sold by Juniper Networks (including the ERX-310, ERX-705, ERX-710, ERX-1410, ERX-1440, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, and T320 routers, T640 routing node, and the JUNOS, JUNOSe, and SDX-300 software) 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.

Copyright © 2007, Juniper Networks, Inc.
All rights reserved. Printed in USA.

SRC-PE Software Subscribers and Subscriptions Guide, Release 1.0.x
Writing: Linda Creed, Justine Kangas, Betty Lew, Helen Shaw
Editing: Fran Mues
Illustration: Nathaniel Woodward
Cover Design: Edmonds Design

Revision History
6 April 2007—Revision 1

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

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)).

Table of Contents

About This Guide	xix
Objectives	xix
Audience	xix
Documentation Conventions.....	xx
Related Juniper Networks Documentation.....	xxi
Obtaining Documentation.....	xxiii
Documentation Feedback	xxiii
Requesting Support.....	xxiv

Part 1

Managing Subscribers and Subscriptions

Chapter 1	Overview of Subscribers and Subscriptions on a C-series Platform	3
	Overview of Subscribers	3
	Overview of Subscriptions	4
	Enterprise Subscriber and Subscription Hierarchy	4
	Enterprise Subscription Hierarchy	5
	Overview of Managers	6
	Read Privileges	6
	Management Privileges.....	6
	Managers That Control All Retailers.....	7
Chapter 2	Overview of Subscribers and Subscriptions on a Solaris Platform	9
	Overview of Subscribers	9
	Overview of Subscriptions	10
	Enterprise Subscriber and Subscription Hierarchy	11
	Enterprise Subscription Hierarchy	12
	Overview of Operators.....	12
	Operator Read Privileges	12
	Operator Management Privileges.....	13
Chapter 3	Subscriber Logins and Service Activation	15
	Overview of Login Events and Processes	15
	Login Events	16
	Summary of the Login Process	16
	Residential Subscriber Login and Processes	17
	PPP Subscriber Login and Service Activation	18
	Web Login for PPP Subscribers	18
	PPP Login Interactions.....	19
	PPP Logout Interactions.....	21

	DHCP Subscriber Login and Service Activation	22
	Interface Startup	22
	Initial Login	23
	Initial DHCP Login Interactions.....	23
	DHCP Login to Subscriber Account Interactions	25
	Persistent DHCP Subscriber Login Interactions	26
	DHCP Subscriber Logout Interactions	28
	Static IP Subscribers	29
	Single PC, IP Address Known	29
	Subscriber IP Address Not Known	30
	Enterprise Subscriber Login Process	32
	Interface Startup	32
	Subscriptions and Activations	33
	Subscription Activation Interactions	34
	Subscription Deactivation Interactions	36
	Automatic Activation at Login	38
	Enterprise-Specific Remote Session Activation	38
Chapter 4	Configuring Subscriber-Related Properties on the SAE with the SRC CLI	41
	Configuring the Length of Time MAC Addresses Remain in SAE Cache.....	41
	Identifying a Profile for Unauthenticated Subscribers	43
	Configuring Interim Accounting for Services and Subscribers	43
	Avoiding Overcharges for Sessions That Time Out.....	44
	Allowing Multiple Logins from the Same IP Address	45
	Authenticating Registered Username/Password Pairs	46
	Configuring Timers for Session Reactivation	46
Chapter 5	Configuring Subscriber-Related Properties on the SAE on a Solaris Platform	49
	Overview	50
	Configuring the Length of Time MAC Addresses Remain in SAE Cache.....	50
	Max Cache Expiration Time Field	50
	Identifying a Profile for Unauthenticated Subscribers	51
	Unauthenticated User DN Field.....	51
	Configuring Interim Accounting for Services and Subscribers	52
	Interim Accounting Fields.....	52
	Avoiding Overcharges for Sessions That Time Out.....	53
	Idle Timeout Field.....	54
	Allowing Multiple Logins from the Same IP Address	54
	Allow Same IP Login Field	54
	Authenticating Registered Username/Password Pairs	55
	Login Registration Field	55
	Configuring Timers for Session Reactivation	56
	Background Service Activation Fields	56
	Modifying the SAE Property File.....	57
	Editing Properties with SDX Admin	57
	Editing Properties with a Text Editor	58
	Loading Subscriptions Based on RADIUS Authorization	58
	Accepting Login Names with Different Formats	60
	Default Login Parser Properties	61

Chapter 6	Classifying Interfaces and Subscribers with the SRC CLI	63
Overview of Classification Scripts	63	
How Classification Scripts Work	64	
Interface Classification Scripts	64	
Subscriber Classification Scripts	65	
DHCP Classification Scripts.....	65	
Overview of Configuring Classification Scripts	66	
Subscriber Classifiers	66	
DHCP Classifiers	66	
Interface Classifiers	66	
Classification Targets	67	
Target Expressions.....	67	
Classification Conditions.....	68	
Glob Matching.....	68	
Regular Expression Matching	69	
Classifying Interfaces	70	
Interface Classification Conditions.....	72	
Example: Managing Interfaces for Premium and Basic		
PPP and DHCP Subscribers	74	
Example: Managing Specific Interfaces.....	75	
Classifying Subscribers	76	
Subscriber Classification Conditions	79	
Sending DHCP Options to the JUNOS Router	82	
Subscriber Classification Targets.....	83	
Example: Subscriber Classification Scripts for Static IP Subscriber	83	
Example: Subscriber Classification Scripts Using a Subscriber Group	84	
Example: Subscriber Classification Scripts for Enterprise Subscribers.....	84	
Matching on the Interface Name	84	
Matching on the Interface Alias.....	85	
Example: Creating Router Interface Subscriber Session	85	
Example: Activating Services for a Group of Subscriber Sessions.....	85	
Classifying DHCP Subscribers	86	
DHCP Classification Conditions	87	
DHCP Classification Targets.....	89	
Selecting DHCP Parameters	89	
Setting DHCP Parameters with DHCP Options.....	90	
Creating DHCP Profiles	92	
 Chapter 7	 Classifying Interfaces and Subscribers on a Solaris Platform	 95
Overview of Classification Scripts	95	
How Classification Scripts Work	96	
Interface Classification Scripts	96	
Subscriber Classification Scripts	97	
DHCP Classification Scripts.....	97	
Configuring Classification Scripts	98	
Classification Targets	98	
Target Expressions.....	98	
Classification Criteria	99	
Glob Matching.....	99	
Regular Expression Matching	100	
Configuring Targets in Structured View	101	
Configuring Criteria in Structured View	102	
Configuring Targets and Criteria in Raw View	102	

Testing Subscriber and Interface Classification Scripts	103
Classifying Interfaces	104
Selecting Interface Classification Criteria	104
Configuring Interface Classification Targets	106
Example: Managing Interfaces for Premium and Basic PPP and DHCP Subscribers	107
Example: Managing Specific Interfaces	107
Example: Managing Interfaces by Using the Interface Description	108
Classifying Subscribers	108
Selecting Subscriber Classification Criteria	109
Sending DHCP Options to the JUNOS Router	112
Configuring Subscriber Classification Targets	114
Example: Subscriber Classification Scripts for Static IP Subscriber	114
Example: Subscriber Classification Scripts Using a Subscriber Group	115
Example: Subscriber Classification Scripts for Enterprise Subscribers	115
Matching on the Interface Name	115
Matching on the Interface Alias	115
Example: Subscriber Classification Scripts For a Wholesaler/Retailer Scenario	116
Example: Creating Router Interface Subscriber Session	116
Example: Activating Services for a Group of Subscriber Sessions	116
Classifying DHCP Subscribers	117
Selecting DHCP Classification Criteria	118
Configuring DHCP Classification Targets	119
Selecting DHCP Parameters	120
Setting DHCP Parameters with DHCP Options	120
Creating DHCP Profiles	123
Chapter 8 Overview of Plug-Ins Included with the SAE	129
How Internal Plug-Ins Work	129
Plug-In Pool	129
Event Publishers	130
Types of Internal Plug-Ins	130
Authorization Plug-Ins	130
Tracking Plug-Ins	131
Customizing RADIUS Packets with Plug-Ins	132
Assigning DHCP Addresses to Subscribers	132
Creating and Tracking Subscriber Sessions	134
Activating and Tracking Service Sessions	135
Chapter 9 Configuring Internal, External, and Synchronization Plug-Ins with the SRC CLI	137
Configuring Internal Plug-Ins	137
Configuring the SAE for External Plug-Ins	138
Configuring the State Synchronization Plug-In Interface	139
Chapter 10 Overview of Configuring Plug-Ins for Solaris Platforms	141
Configuring Plug-Ins with SDX Configuration Editor	141
Accessing the Plug-In Configuration	141
Creating Plug-In Instances	143
Configuring Internal Plug-Ins	143
Configuring the SAE for External Plug-Ins	144
Configuring the State Synchronization Plug-In Interface	146

Configuring Plug-Ins with SDX Admin	148
Configuring External Plug-Ins	148
Configuring Internal and Hosted Plug-Ins	148
Defining RADIUS Packets	149
Setting Up the Plug-In Instance to Use a Template	149
Configuring Event Publishers	149
Example: LDAP Authentication Plug-In	150
Example: Basic RADIUS Accounting Plug-In	150
Chapter 11 Configuring Authorization and Accounting Plug-Ins with SDX Configuration Editor	151
Configuring Tracking Plug-Ins	152
Configuring Flat File Accounting Plug-Ins.....	153
Configuring Headers for Flat File Accounting Plug-Ins	156
Configuring Basic RADIUS Accounting Plug-Ins	158
Configuring Flexible RADIUS Accounting Plug-Ins	158
Configuring Custom RADIUS Accounting-Plug-Ins.....	159
Configuring Authorization Plug-Ins.....	160
Limiting Subscribers on Router Interfaces	161
Configuring Basic RADIUS Authentication Plug-Ins	162
Configuring Flexible RADIUS Authentication Plug-Ins	163
Configuring Custom RADIUS Authentication Plug-Ins	164
Configuring LDAP Authentication Plug-Ins	166
Using RADIUS Plug-In Fields	170
Configuring UDP Ports for RADIUS Plug-Ins	174
Configuring Global UDP Ports	174
Global RADIUS UDP Port Field.....	174
Creating RADIUS Peers	175
Defining RADIUS Packets for Flexible RADIUS Plug-Ins with SDX Configuration Editor.....	176
Creating and Using RADIUS Templates.....	176
Configuring RADIUS Attributes	177
More About Using Flexible RADIUS Packet Definitions	182
Setting Values in Authentication Response Packets.....	183
Selecting IP Address Pools Using DHCP Response Packets.....	184
Configuring Event Publishers	184
Configuring Global and Default Retailer Event Publishers	185
Configuring Service-Specific Event Publishers.....	187
Configuring Retailer-Specific Event Publishers.....	188
Configuring Virtual Router-Specific Event Publishers	188
Chapter 12 Configuring Accounting and Authentication Plug-Ins with the SRC CLI	189
Creating RADIUS Peers	190
Related Information	191
Configuring Tracking Plug-Ins	192
Configuring Flat File Accounting Plug-Ins.....	193
Related Information	194
Configuring Headers for Flat File Accounting Plug-Ins	194
Configuring Basic RADIUS Accounting Plug-Ins	196
Related Information	198

Configuring Flexible RADIUS Accounting Plug-Ins	198
Related Information	200
Configuring Custom RADIUS Accounting-Plug-Ins.....	200
Related Information	203
Configuring Authentication Plug-Ins	203
Limiting Subscribers on Router Interfaces	204
Configuring Basic RADIUS Authentication Plug-Ins	205
Related Information	206
Configuring Flexible RADIUS Authentication Plug-Ins	207
Related Information	209
Configuring Custom RADIUS Authentication Plug-Ins	209
Related Information	212
Configuring LDAP Authentication Plug-Ins	212
Related Information	214
Configuring UDP Ports for RADIUS Plug-Ins	215
Configuring Global UDP Ports	215
Defining RADIUS Packets for Flexible RADIUS Plug-Ins with the SRC CLI ...	215
Using Default RADIUS Templates	216
Naming RADIUS Attribute Instances.....	216
Defining RADIUS Attributes	217
Standard RADIUS Attributes.....	217
Juniper Networks VSAs.....	217
Defining the Values of RADIUS Attributes.....	218
Configuring a RADIUS Packet Template.....	220
More About Using Flexible RADIUS Packet Definitions	222
Setting Values in Authentication Response Packets.....	223
Selecting IP Address Pools Using DHCP Response Packets.....	224
Configuring Event Publishers	224
Configuring Global and Default Retailer Event Publishers	225
Related Information	226
Configuring Service-Specific Event Publishers.....	227
Configuring Retailer-Specific Event Publishers.....	227
Configuring Virtual Router-Specific Event Publishers	227
 Chapter 13 Configuring Subscribers and Subscriptions with SDX Admin	 229
Overview of Configuring Subscribers and Subscriptions.....	229
LDAP Model for Subscribers	229
Subscriptions	230
Specifying the Activation Order for Subscriptions	231
LDAP Model for Subscriptions	231
Operators	232
Read Privileges.....	232
Management Privileges	233
Operators That Control All Retailers	234
LDAP Model for Operators	234
Tools for Adding Subscribers and Subscriptions	235
Inheritance of Properties and Subscriptions	235
Encryption Methods for Passwords.....	235
Adding Subscribers	236
Adding Retailers	236
Retailer Fields	238
Assigning Service Scopes	240
Adding Subscriber Folders.....	240
Subscriber Folder Fields	241

Adding Residential Subscribers	242
Residential Subscriber Fields.....	244
Adding Enterprises	246
Enterprise Fields	248
Adding Sites	249
Site Fields	250
Adding Routers as Subscribers.....	251
Router Subscriber Fields	252
Adding Operators	253
Operator Fields.....	254
Configuring Subscriptions	255
Configuring Subscriptions to Value-Added Services	255
Value-Added Subscription Fields	257
Allowing Multiple Subscriptions per Subscriber	258
Configuring Subscriptions to Outsourced Services	258
Outsource Service Subscription Fields.....	259
Configuring Access Subscriptions	261
Access Subscription Fields	262
Configuring RADIUS Subscriptions	264
RADIUS Subscription Fields.....	266
Configuring Substitutions for Subscriptions.....	269
Adding Substitutions.....	269
Substitutions to a Transmission Rate for a Scheduled Action	269
Modifying Substitutions	270
Validating Substitutions	270
Deleting Substitutions.....	271
Modifying and Deleting Subscribers and Subscriptions	271
Chapter 14	Configuring Subscribers and Subscriptions with the SRC CLI
	273
Overview of Configuring Subscribers and Subscriptions.....	274
Specifying the Activation Order for Subscriptions	274
Inheritance of Properties and Subscriptions	274
Enabling the Subscriber and Subscription Configuration on the SRC CLI.....	274
Adding Subscribers	275
Adding Retailers	276
Configuring Administrative Information for Retailers	277
Adding Subscriber Folders	278
Adding Residential Subscribers	279
Configuring Administrative Information for Residential Subscribers.....	281
Adding Enterprises.....	283
Configuring Administrative Information for Enterprise Subscribers.....	284
Adding Sites	285
Adding Devices as Subscribers.....	286
Adding Managers	287
Configuring Subscriptions	290
Allowing Multiple Subscriptions per Subscriber	292
Configuring Accesses	292

Part 2**Managing Access Portals for Residential Subscribers**

Chapter 15	Overview of the Residential Portal	299
	How Subscribers Use a Residential Portal	299
	Overview of a Residential Portal	300
	Subscriptions to Services	300
	Service Schedules in a Residential Portal	301
	Equipment Registration for DHCP Login	301
	Overview of the Sample Residential Portal	301
	Web Application Architecture	301
	Model Components	302
	View Components	302
	Control Components	302
	Behaviors for the Sample Residential Portal	302
Chapter 16	Installing and Configuring the Sample Residential Portal	303
	Before You Install and Configure the Sample Residential Portal	303
	Configuring Equipment Registration Behavior	304
	Configuring ISP Service Behavior	304
	Configuring Cable Behavior	305
	Authenticating Subscribers Through RADIUS	305
	Customizing How the Sample Residential Portal Handles	
	Unrecognized IP Subscribers	306
	Overview of Configuration Files for the Sample Residential Portal	306
	WEB-INF/portalBehavior.properties	307
	WEB-INF/struts-config.xml	309
	WEB-INF/tiles-defs.xml	311
	Installing the Sample Residential Portal	312
	Preparing the Application for Customization	313
	Configuring the Sample Residential Portal	313
	Deploying the Updated WAR File	314
	Testing a Portal Application	314
	Removing Access to the Sample Residential Portal	314
Chapter 17	How Subscribers Use the Sample Residential Portal	315
	Overview of the Sample Residential Portal	315
	Before You Use the Sample Residential Portal	315
	Logging In to the Sample Residential Portal Using a Simulated User Profile	316
	Logging In to the Sample Residential Portal	316
	Managing Services from the Sample Residential Portal	318
	Starting and Stopping Services	319
	Getting Usage Information	321
	Setting Up the Type of Service Activation	322
	Setting Up Service Schedules	323
	Specifying Values for Times	324
	Setting Times	325
	Setting Actions	326
	Subscribing to Services	327
	Registering Equipment for DHCP Login	328
	Disabling Equipment Registration	330
	Logging Out of the Sample Residential Portal	332
	Using the Sample Residential Portal from PDAs	333

Chapter 18	Developing a Residential Portal	335
	Before You Develop a Residential Portal	335
	Development Tools to Create a Residential Portal.....	336
	Virtual IP Address for Policies	337
	Configuring a Virtual Portal Address with SDX Configuration Editor	337
	Virtual Portal Address Field	337
	Redirecting Traffic to a Captive Portal Web Page	338
	Sequence for Redirecting Traffic.....	338
	Configuring the SRC Software in a Multihop Environment.....	339
	Managing Security for Public Wireless LAN Applications	339
	Developing a Portal Based on the Sample Residential Portal	340
	Preparing to Develop a Portal Based on the Sample Residential Portal ..	340
	Creating a Portal Project	341
	Building the Portal	341
	Deploying the Portal	341
	Testing a Portal Application	342

Part 3

Redirecting Subscriber Traffic Through Redirect Server

Chapter 19	Redirecting Subscriber Traffic	345
	Overview of Traffic Redirection	345
	Proxy Request Management	345
	HTTP Proxy and DNS	347
	Redirect Server Redundancy	347
	Before You Configure Redundancy for the Redirect Server	348
	Protection Against Denial-of-Service Attacks	348
Chapter 20	Configuring Traffic Redirection with the SRC CLI	349
	Configuration Statements for the Redirect Server	350
	Before You Configure the Redirect Server on a C-Series System.....	351
	Configuring the Redirect Server	351
	Configuring General Properties for the Redirect Server	352
	Configuring a Connection Between the Redirect Server and the Directory ...	353
	Defining Traffic to Transmit to the Redirect Server	354
	Changing The Number of Requests That the Redirect Server Accepts	355
	Specifying Extensions for Files that the Redirect Server Accepts.....	356
	Verifying Configuration for the Redirect Server.....	357
	Configuring the DNS Server for the Redirect Server	357
	Configuring the Redirect Server to Support HTTP Proxies	358
	Configuring a Redundant Redirect Server	359
	Configuring Logging for the Redirect Server	360
	Changing the Configuration for the Redirect Server	361
	Assessing Load for Redirect Server	361
Chapter 21	Configuring Traffic Redirection on a Solaris Platform	363
	Installing the Redirect Server	363
	Configuration Overview for Redirect Server	364

Configuring IP Filter	364
Example: Creating a Rule to Redirect Traffic to a Different Port Number	365
Example: Creating a Rule to Redirect Unauthorized Traffic	366
Configuring Redirect Server from the redir.properties File	366
Configuration Properties for the Redirect Server	367
Configuring Logging for Redirect Server	372
Changing the Configuration for Redirect Server	372

Part 4

Designing Services for Enterprise Manager Portal

Chapter 22	Reviewing and Configuring Policies and Services for Enterprise Manager Portal	375
Overview of Services for Enterprise Manager Portal	375	
Directory Structure	376	
Priorities for Subscriptions	376	
Before You Configure Services for Enterprise Manager Portal	377	
Configuring Firewall Policies and Services for Enterprise Manager Portal	377	
Overview of Basic Firewall Services and Policies	378	
Tasks to Configure Firewall Policies and Services	379	
Configuring Basic Firewall Policies	379	
Configuring Basic Firewall Services	380	
Reviewing the fwrule Policy Group for Exceptions to Stateful Firewalls	380	
Reviewing the FirewallRule Service for Exceptions to Stateful Firewalls	380	
Reviewing Services for Exceptions to Stateless Firewalls	381	
Parameter Values Used by Services for Exceptions to Stateless Firewalls	382	
Planning Services for Custom Firewall Exceptions	382	
Configuring Policies for Custom Firewall Exceptions	383	
Configuring Services for Custom Firewall Exceptions	384	
Configuring Priorities for Stateless or Stateful Firewall Services	384	
Configuring Priorities to Have Enterprise Services Work Together ..	384	
Configuring Global Priority Ranges from Policy Editor	385	
Configuring Global Priority Ranges from SDX Admin	385	
Configuring Priorities for Individual Scopes by Defining Them in Services	385	
Using Stateless Firewall and BoD Applications Together	386	
Configuring NAT Policies and Services for Enterprise Manager Portal	386	
Configuring the dynsrcnat Policy Group	387	
Reviewing the DynSrcNat Service	387	
Configuring the staticdstnat Policy Group	387	
Configuring the StaticDstNat Service	387	
Configuring the staticsrcnat Policy Group	388	
Configuring the StaticSrcNat Service	388	
Configuring Bandwidth Policies and Services for Enterprise Manager Portal	388	
Parameter Values Used by BoD Services	389	
Bandwidth Policies for Different Routing Platforms	389	
Configuring Basic BoD Policies	390	

Configuring Basic BoD Services	390
Configuring BoD Policies	391
Configuring BoD Services	392
Using BoD Services to Assign Traffic to Bandwidth Categories	393
Using BoD and Basic BoD Services Together	
to Supply Class of Service.....	393
Setting Up Forwarding Preferences—Example 1	394
Setting Up Forwarding Preferences—Example 2	395
Enabling Schedules for Subscriptions for Enterprise Manager Portal	396
Configuring VPNs for Enterprise Manager Portal.....	396
Before You Configure VPN Policies and Services	396
Configuring Policies for BoD Traffic Destined for VPNs	397
Configuring Services for BoD Traffic Destined for VPNs	397
Billing Subscribers Through SCU/DCU for JUNOS Routing Platforms	398

Chapter 23 Adding VPNs from JUNOS Routing Platforms with the SRC CLI 399

Before You Add a JUNOS VPN to the SRC Configuration	399
Configuring VPNs to Integrate into an SRC Network	400
Configuration Statements for Adding VPNs and Extranet Clients	400
Adding VPNs for Retailers and Enterprises.....	401
Verifying and Updating Configuration of Extranets for VPNs.....	402

Chapter 24 Adding VPNs from JUNOS Routing Platforms 405

Overview of VPNs in the SRC Network.....	405
Implementing a Routing Scheme for VPNs	406
Configuring VPNs to Integrate into an SRC Network	406
Adding VPNs with a Data Integrator	406
Adding VPNs with SDX Admin	407
VPN Fields	408
Modifying VPNs	408
Adding Extranet Clients to VPNs	409
Removing Extranet Clients.....	411
Locating and Removing Inactive Subscriptions to a VPN.....	411
Deleting VPNs from the Directory	412

Part 5 Managing Access Portals for Enterprise Subscribers

Chapter 25 Overview of Enterprise Service Portals 415

Function of Enterprise Service Portals.....	415
Consistency of Data in the Directory	416
Privileges of IT Managers.....	416
Developing and Customizing Enterprise Service Portals	416
Identifying the SAE	417
Enterprise Service Portals Provided with the SRC Software.....	417
Sample Enterprise Service Portal.....	417
Enterprise Manager Portal	418
NAT Address Management Portal	418
Enterprise Service Portal Audit Plug-In	419
Network Information Collector with Enterprise Service Portals	419
Service Parameters	420

	Substitutions and the Parameter Acquisition Path.....	420
	Power of Substitutions.....	421
	Substituting Values for Policy Parameters.....	422
	Managing Subscriptions to Aggregate Services.....	423
	Configuring Your Web Browser to Use an Enterprise Service Portal.....	423
	Accessing Enterprise Service Portals.....	423
Chapter 26	Planning Deployment for Enterprise Service Portals	425
	Architecture of Enterprise Service Portals.....	425
	Elements for an Enterprise Service Portal.....	426
	Communication Protocols.....	426
	Deployment Scenario for an Enterprise Service Portal.....	427
	Deciding Which Enterprise Service Portal to Use.....	428
	Planning Number of Instances of an Enterprise Service Portal.....	428
	Planning Namespace Hierarchy for an Enterprise Service Portal.....	428
Chapter 27	Installing and Configuring Enterprise Service Portals	431
	Before You Install an Enterprise Service Portal.....	431
	Installing Enterprise Service Portals.....	432
	Preparing the Web Applications for Customization.....	433
	Configuring Connections to the Directory.....	433
	Initialization Properties for Enterprise Service Portals.....	433
	Configuring Deployment Settings for Enterprise Manager Portal.....	435
	Deployment Properties for Enterprise Manager Portal.....	435
	Deploying the Enterprise Service Portals.....	441
	Configuring the URL for an Enterprise Service Portal.....	441
	Writing an Application to Allow a Machine to Provide	
	Public IP Addresses for NAT.....	441
	Configuring an Enterprise Service Portal.....	442
	Accessing the Configuration Files.....	442
	Configuring Connections to the Subscriber Directory.....	443
	Configuring Connections to the Service Directory	
	on Solaris Platforms.....	446
	Configuring Search Bases for Each Directory.....	449
	Configuring the Logging Properties.....	450
	Configuring a NIC Proxy.....	451
	Configuring Directory Eventing for SAE Identification.....	451
	Exporting the Configuration to the Directory.....	452
	Configuring an Enterprise Service Portal Audit Plug-In.....	452
	Overview of Configuration for an Enterprise Service	
	Portal Audit Plug-In.....	454
	Configuring the Sample Enterprise Service Portal Audit Plug-In.....	454
	Configuring a Customized Enterprise Service Portal Audit Plug-In.....	456
Chapter 28	Managing Enterprise Service Portals	459
	Displaying Information About Your Control in the Enterprise.....	459
	Updating Data That the Enterprise Service Portal Displays.....	460
	Managing Operators.....	460
	Creating Managers.....	461
	Managers Fields.....	461
	Modifying Managers.....	463
	Deleting Managers.....	463

Chapter 29	Managing Services with Enterprise Manager Portal	465
	Overview of Enterprise Manager Portal	465
	Getting Help on Enterprise Manager Portal	466
	Setting the Configuration Level for Enterprise Manager Portal	466
	Managing Schedules.....	467
	Creating a Schedule	468
	Applying a Schedule to a Service	472
	Disabling a Schedule for a Service	473
	Changing Schedules.....	474
	Managing Subscriptions to Bandwidth-on-Demand Services	474
	Planning Subscriptions to BoD Services	475
	Creating a Subscription to BoD Services	475
	Setting a Bandwidth Level	475
	Adding Subscriptions to BoD Services	477
	Modifying Rules for a Subscription to a BoD Service.....	485
	Modifying the Bandwidth Level	486
	Moving the Bandwidth Level.....	486
	Deleting a Subscription for a BoD Service.....	486
	Deleting the Bandwidth Level	486
	Monitoring Use of Subscriptions to BoD Services	487
	Integrating VPNs into an SRC Network.....	487
	Modifying Subscriber VPN Configuration	487
	Creating Extranets	489
	Deleting Extranets	489
	Sending Traffic to a VPN.....	490
	Modifying the VPN to Which the Router Sends Traffic	490
	Stopping the Router from Sending Traffic to VPNs	491
	Classifying Traffic for Stateful Firewall Exceptions and NAT Rules	491
	Classifying Traffic	492
	Modifying Values for Traffic Classifications.....	496
	Deleting Traffic Classifications	496
	Subscribing to Firewall Services	496
	Before You Configure Firewall Exception Rules	497
	Creating Subscriptions to Firewall Services.....	497
	Creating Firewall Exceptions for Stateless Firewalls.....	498
	Creating Firewall Exceptions for Stateful Firewalls.....	508
	Adding a Schedule to a Firewall Exception	511
	Modifying Firewall Exceptions	511
	Deleting Firewall Exceptions.....	511
	Deleting Basic Firewalls	512
	Monitoring the Use of Subscriptions to Firewall Services	513
	Working with IP Addressing and NAT Services	513
	Requesting Public IP Addresses for NAT Services	513
	Canceling Requests for Public IP Addresses.....	515
	Returning Public IP Addresses to Service Providers	515
	Applying NAT Rules to Traffic.....	516
	Configuring Public IP Addresses for Outgoing Traffic.....	517
	Configuring Public IP Addresses for Incoming Traffic	518
	Configuring Fixed Public Addresses for Outgoing Traffic	520
	Modifying NAT Rules	520
	Deleting NAT Rules.....	520
	Monitoring the Status of Subscriptions	520
	Troubleshooting Subscriptions That Are Not Functioning Correctly	522
	Troubleshooting Subscriptions of Unknown Status	523

Chapter 30	Using NAT Address Management Portal	525
	Overview of NAT Address Management Portal.....	525
	Assigning IP Addresses	526
	Acknowledging the Release of IP Addresses.....	527
Chapter 31	Using the Sample Enterprise Service Portal	529
	Overview of the Sample Enterprise Service Portal.....	529
	Starting the Sample Enterprise Service Portal	530
	Subscribing to Services	531
	Activating Subscriptions.....	532
	Deactivating Subscriptions	533
	Suspending Subscriptions	533
	Canceling Suspensions of Subscriptions.....	533
	Monitoring Use of Subscriptions.....	533
	Specifying Values for Service Parameters in Subscriptions.....	534
	Restoring Default Values for Service Parameters In Subscriptions.....	534
	Deleting Subscriptions	535
	Monitoring Service Sessions for a Subscription	535
	Defining Networks for Departments in an Enterprise.....	536
	Modifying Network Definitions for Departments in an Enterprise.....	537
	Deleting Network Definitions for Departments in an Enterprise.....	537
Chapter 32	Developing an Enterprise Service Portal	539
	Developing a Portal Based on the Sample Enterprise Service Portal.....	539
	Preparing to Develop a Sample-Based Enterprise Service Portal	540
	Creating a Portal Project for a Sample-Based Enterprise Service Portal	540
	Building a Sample-Based Enterprise Service Portal.....	541
	Deploying a Sample-Based Enterprise Service Portal.....	541
	Testing a Sample-Based Enterprise Service Portal	541
	Using a Virtual Address for the Portal.....	542
	Index	543

About This Guide

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

- Objectives on page xix
- Audience on page xix
- Documentation Conventions on page xx
- Related Juniper Networks Documentation on page xxi
- Obtaining Documentation on page xxiii
- Documentation Feedback on page xxiii
- Requesting Support on page xxiv

Objectives

This guide describes how to manage and configure subscribers and subscriptions, including subscriber logins and logouts, classifying subscribers and subscriber interfaces, using plug-ins for authorization and authentication and to collect accounting data. It also describes how to develop and use residential and enterprise portals.



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

Audience

This guide is intended for experienced system and network specialists working with 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 Session and Resource Control (SRC) networks. For users who deploy the SRC software on a Solaris platform, we also assume that readers are familiar with the Lightweight Directory Access Protocol (LDAP) and the UNIX operating system.

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

Documentation Conventions

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

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

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

Table 1: Notice Icons




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

Table 2: Text Conventions

Convention	Description	Examples
Bold typeface	<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 sans serif typeface	Represents text that the user must type.	<code>user@host# set cache-entry-age cache-entry-age</code>
Monospace sans serif typeface	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>

Table 2: Text Conventions (continued)

Convention	Description	Examples
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/sdx/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.
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 chapter, appendix, and 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>Chapter 2, Services</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.	<code>Plugin.radiusAcct-1.class = \net.juniper.smgmt.sae.plugin\RadiusTrackingPluginEvent</code>
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.)	<code>diagnostic line</code>

Related Juniper Networks Documentation

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

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

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

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

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

Document	Description
Core Documentation Set	
<i>C-series Hardware Guide</i>	Describes the hardware platforms and how to install, maintain, replace, and troubleshoot them. The guide also includes specifications.
<i>SRC-PE Getting Started Guide</i>	Describes the SRC software and explains how to set up an initial configuration and manage a C-series platform. The guide describes how to set up and start the SRC CLI and C-Web, as well as other SRC configurations. It provides information about setting up an initial SRC configuration on a Solaris platform. The guide also describes how to upgrade the SRC software and how to use the SRC configuration tools. It includes reference material for the SRC documentation.
<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.
<i>SRC-PE Network Guide: SAE, Juniper Networks Routers, and NIC</i>	Describes how to use and configure the SAE and the NIC. This guide also provides detailed information for using JUNOS routers and JUNOS routing platforms in the SRC network.
<i>SRC-PE Integration Guide: Network Devices, Directories, and RADIUS Servers</i>	Describes how to integrate external components—network devices, directories, and RADIUS servers—into the SRC network. The guide provides detailed information about integrating specific models of the external components.
<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 sample residential portals and 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 JUNOS routers; managing subscribers in a wireless roaming environment; providing voice over IP (VoIP) services; integrating the SRC software in a PCMM environment, including the use of the Juniper Policy Server (JPS); mirroring subscriber traffic on JUNOS routers; demonstrating network resource management features in a sample IP television (IPTV) application; and demonstrating the integration of prepaid services in a sample application.
<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 Comprehensive Index</i>	Provides a complete index of the SRC guides, excluding the <i>C-series Hardware Guide</i> and the <i>SRC CLI Command Reference</i> .
<i>J-Web User Interface Guide</i>	Provides general information about the J-Web interface.

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

Document	Description
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, applications to integrate the Juniper Networks Intrusion Detection and Protection (IDP) software into an SRC-managed environment, an application to provide endpoint security by integrating Juniper Networks Instant Virtual Extranet (IVE) Host Checker, a traffic-mirroring Web application, an application to integrate IP address managers with the SAE, an application to provide tracking and QoS control at the application level by integrating the SRC software with the Ellacoya deep packet inspection (DPI) platform, an application to control volume usage, and the SRC-ACP (Admission Control Plug-In) application.
Release Notes	
<i>SRC-PE Release Notes</i> <i>SRC Application Library 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> . Release notes are included in the corresponding software distribution and are available on the Web.

Obtaining Documentation

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

<http://www.juniper.net/>

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

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation to better meet your needs. Send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at

<http://www.juniper.net/techpubs/docbug/docbugreport.html>

If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version

Requesting Support

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

Part 1

Managing Subscribers and Subscriptions

Chapter 1

Overview of Subscribers and Subscriptions on a C-series Platform

This chapter provides an overview of subscribers, subscriptions, and managers on a C-series platform. Topics include:

- Overview of Subscribers on page 3
- Overview of Subscriptions on page 4
- Enterprise Subscriber and Subscription Hierarchy on page 4
- Overview of Managers on page 6

Overview of Subscribers

A subscriber is an object in the directory for which you can configure subscriptions to services. The SRC software distinguishes between types of subscribers, as described in Table 4.

Table 4: Types of Subscribers

Subscriber	Description
Retailers	Internet service providers who either manage their own subscribers or outsource the management of subscribers to a service provider who deploys the SRC software. The SRC software uses retailer objects to group subscribers who belong to an administrative domain.
Residential	Individual subscribers or households—multiple subscribers who use one or more computers and share the same connection. In a household, subscribers can share the same service subscription or can have their own individualized service profiles.
Enterprise	An organization, such as a corporation. An enterprise subscriber can contain site subscribers that represent physical locations or groups within the organization. Enterprises and sites contain access subscribers; an access represents a layer 2 connection between a device at a customer's physical location and a router that gives the enterprise subscribers access to the Internet and, in some cases, a virtual private network (VPN).
Sites	One or more locations—physical or virtual—within an enterprise that share service subscriptions and physical access to services and that are each managed as a unique entity. For example, the XYM Corporation might have a site in Boston and a site in Toronto. Each of these sites can have its own set of subscribed services.

Table 4: Types of Subscribers (continued)

Subscriber	Description
Device	An SRC-managed device that is used to activate services on nonsubscriber interfaces. It is used primarily to provide integration with applications that use traffic mirroring on JUNOS routing platforms.
Subscriber folders	Objects that group subscribers.

Overview of Subscriptions

A subscription is an object that represents an enrollment to a service. Each subscription provides access to a particular service for that subscriber. A subscriber can have multiple subscriptions to a service.

If the service provider uses the SRC directory to hold all their subscriber data, residential subscribers must subscribe to primary services—such as Broadband Remote Access Server (B-RAS) through Point-to-Point protocol (PPP) or B-RAS through Dynamic Host Configuration Protocol (DHCP)—before subscribing to a service.

Enterprise subscribers must subscribe to an access (that is, a leased line), either directly or in a site or subscriber folder that is subordinate to the enterprise. Without an access subscription, a service session cannot run in the network.

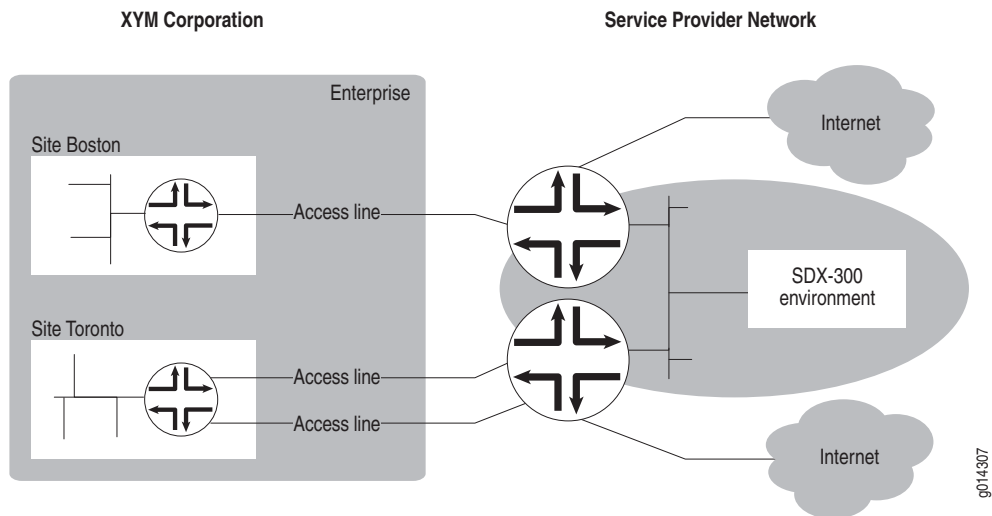
Enterprise Subscriber and Subscription Hierarchy

In the enterprise model, a subscriber is an individual physical access line managed through the enterprise service portal over which services are delivered by the service provider. In the enterprise, the SRC software supports the organization of the enterprise in the following hierarchy (Figure 1):

- Enterprise—The business itself as a customer of the service provider; for example, the XYM Corporation. An enterprise can have its own set of subscriptions over a physical access line.
- Site—One or more locations, physical or virtual, within the enterprise that share service subscriptions and physical access to services and that are each managed as a unique entity. For example, the XYM Corporation might have a site in Boston and a site in Toronto. Each of these sites can have its own set of subscribed services.
- Access line—A physical access line (usually within a site) from the customer to the service provider's router; the router is configured to access the SRC environment and the Internet and/or the customer's network-based VPN. An access line can have its own set of subscribed services.

Enterprise IT managers can use the enterprise service portal to manage interfaces connecting enterprise sites to the network. These interfaces can be leased-line connections or authenticated PPP and DHCP connections.

Figure 1 shows an enterprise hierarchy.

Figure 1: Enterprise Hierarchy

Sites and access lines are subordinate to an enterprise; the enterprise sometimes contains sites and access lines. Access lines are subordinate to a site; the site contains access lines.

In Figure 1, the XYM Corporation enterprise contains two subordinate sites, Boston and Toronto. The Boston site contains a single subordinate access line, whereas the Toronto site contains two subordinate access lines. All three access lines connect to a router in the service provider network. An individual access line, for example, might be a T1 line running PPP or a T3 line running Frame Relay.

Enterprise Subscription Hierarchy

The organizational levels of the enterprise receive subscribed services in a hierarchical manner. The availability of a subscription to a higher level affects its availability to a lower level.

- Enterprise—Subscriptions apply to all sites and all access lines across the enterprise.
- Site—Subscriptions apply to all access lines grouped within a site.
- Access line—Subscriptions apply to a given access line that connects the enterprise to the service provider's network.

Overview of Managers

In relation to subscribers and subscriptions, a manager is an object that represents an IT manager in an organization. Retailers, subscriber folders, enterprises, sites, and accesses can support one or more managers.

Read Privileges

Managers have privileges to read:

- The objects they control
- Parent subscribers, up to the retailer
- Subscriptions of parent subscribers, up to the retailer
- All objects that represent services, service scopes, policies, and global variables that are defined for the subscriber to which the manager is added

Management Privileges

You can specify one or more management privileges for managers. If you do not specify privileges for a manager, the manager has only read privileges. Table 5 shows the privilege levels and the privileges associated with the levels.

Table 5: Privilege Levels and Associated Tasks

Privilege Level	Tasks That Managers with This Privilege Can Perform
Administrator	<ul style="list-style-type: none"> ■ Add, delete and modify managers ■ Add, delete, and modify subscriptions ■ Modify subscribers, including the ability to add, delete, and modify substitutions for subscribers ■ Manually activate and deactivate subscription sessions
Subscription	<ul style="list-style-type: none"> ■ Add, delete, and modify subscriptions ■ Manually activate and deactivate subscription sessions
Substitution	Add, delete, and modify substitutions in subscribers and subscriptions
Activation	<ul style="list-style-type: none"> ■ Configure automatic activation of services ■ Manually activate and deactivate subscription sessions
VPNs	Modify, export, and cancel the export of VPNs

A manager has management privileges for its associated subscriber and for that subscriber's subordinate objects:

- Managers in an enterprise have control over the enterprise and all sites and accesses in the enterprise.
- Managers in a site have control over the site and all accesses it contains. In addition they have read access to the enterprise, subscriber folder, and retailer that are configured above the site.
- Managers in an access have control over only that access.

Managers That Control All Retailers

You can add managers that have control over all retailers and their subordinate enterprises. To do so, configure the manager at the [edit subscribers retailer name manager] hierarchy.

Chapter 2

Overview of Subscribers and Subscriptions on a Solaris Platform

This chapter provides an overview of subscribers, subscriptions, and operators in the Solaris version of the SRC software. Topics include:

- Overview of Subscribers on page 9
- Overview of Subscriptions on page 10
- Enterprise Subscriber and Subscription Hierarchy on page 11
- Overview of Operators on page 12

Overview of Subscribers

A subscriber is an object in the directory for which you can configure subscriptions to services. The SRC software distinguishes between types of subscribers, as described in Table 6.

Table 6: Types of Subscribers

Subscriber	Description
Retailers	Internet service providers who either manage their own subscribers or outsource the management of subscribers to a service provider who deploys the SRC software. The SRC software uses retailer objects to group subscribers who belong to an administrative domain.
Residential	Individual subscribers or households—multiple subscribers who use one or more computers and share the same connection. In a household, subscribers can share the same service subscription or can have their own individualized service profiles.
Enterprise	An organization, such as a corporation. An enterprise subscriber can contain site subscribers that represent physical locations or groups within the organization. Enterprises and sites contain access subscribers; an access represents a layer 2 connection between a device at a customer's physical location and a router that gives the enterprise subscribers access to the Internet and, in some cases, a virtual private network (VPN).
Sites	One or more locations—physical or virtual—within an enterprise that share service subscriptions and physical access to services and that are each managed as a unique entity. For example, the XYM Corporation might have a site in Boston and a site in Toronto. Each of these sites can have its own set of subscribed services.

Table 6: Types of Subscribers (continued)

Subscriber	Description
Access	A physical access (usually within a site) from the customer to the service provider's router; the router is configured to access the SRC environment and the Internet and/or the customer's network-based VPN. An access line can have its own set of subscribed services.
Router	An SRC-managed router that is used to activate services on nonsubscriber interfaces. It is used primarily to provide integration with applications that use traffic mirroring on JUNOS routing platforms. For information about traffic mirroring, see <i>SDX Application Library Guide</i> .
Subscriber folders	Objects that group subscribers. The object immediately subordinate to a retailer must be a subscriber folder. Subscriber folders can also be subordinate to enterprises, accesses, and sites.

Overview of Subscriptions

A subscription is an object in the directory that represents an enrollment to a service. Each subscription provides access to a particular service for that subscriber. A subscriber can have multiple subscriptions to a service. Table 7 shows the type of subscriptions you can configure for each type of subscriber.

Table 7: Allowable Service Subscriptions for Different Types of Subscribers

Type of Subscriber	Service Subscriptions You Can Configure
Retailer	Outsourced service subscription Value-added subscription
Subscriber folder	Value-added subscription
Enterprise	Access subscription Value-added subscription
Site	Access subscription Value-added subscription
Access	RADIUS subscription Value-added subscription
Residential subscriber	RADIUS subscription Value-added subscription

If the service provider uses the SRC directory to hold all their subscriber data, residential subscribers must subscribe to primary services—such as Broadband Remote Access Server (B-RAS) through Point-to-Point protocol (PPP) or B-RAS through Dynamic Host Configuration Protocol (DHCP)—before subscribing to a value-added service.

Enterprise subscribers must subscribe to an access service (that is, a leased line), either directly or in a site or subscriber folder that is subordinate to the enterprise. Without an access subscription, a service session cannot run in the network.

Retailers can subscribe to outsourced services if a service provider sources the access out through tunneling (Layer 2 Tunneling Protocol [L2TP] or PPP Terminated Aggregation [PTA]).

Enterprise Subscriber and Subscription Hierarchy

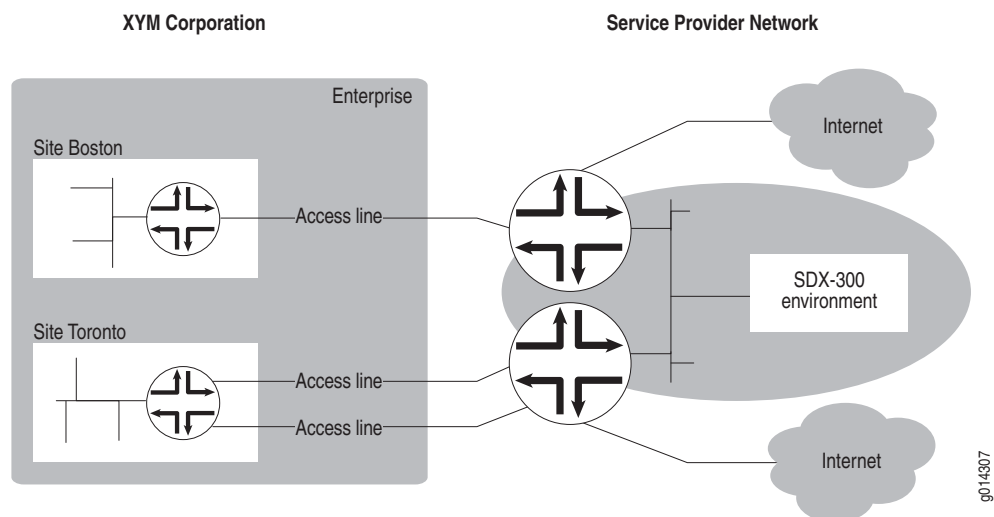
In the enterprise model, a subscriber is an individual physical access line managed through the enterprise service portal over which services are delivered by the service provider. In the enterprise, the SRC software supports the organization of the enterprise in the following hierarchy (Figure 2):

- Enterprise—The business itself as a customer of the service provider; for example, the XYM Corporation. An enterprise can have its own set of subscriptions over a physical access line.
- Site—One or more locations, physical or virtual, within the enterprise that share service subscriptions and physical access to services and that are each managed as a unique entity. For example, the XYM Corporation might have a site in Boston and a site in Toronto. Each of these sites can have its own set of subscribed services.
- Access line—A physical access line (usually within a site) from the customer to the service provider's router; the router is configured to access the SRC environment and the Internet and/or the customer's network-based VPN. An access line can have its own set of subscribed services.

Enterprise IT managers can use the enterprise service portal to manage interfaces connecting enterprise sites to the network. These interfaces can be leased-line connections or authenticated PPP and DHCP connections.

Figure 2 shows an enterprise hierarchy.

Figure 2: Enterprise Hierarchy



Sites and access lines are subordinate to an enterprise; the enterprise is sometimes said to contain sites and access lines. Access lines are subordinate to a site; the site contains access lines.

In Figure 2, The XYM Corporation enterprise contains two subordinate sites, Boston and Toronto. The Boston site contains a single subordinate access line, whereas the Toronto site contains two subordinate access lines. All three access lines connect to a router in the service provider network. An individual access line, for example, might be a T1 line running PPP or a T3 line running Frame Relay.

Enterprise Subscription Hierarchy

The different organizational levels of the enterprise receive subscribed services in a hierarchical manner. The availability of a subscription to a higher level affects its availability to a lower level.

- Enterprise—Subscriptions apply to all sites and all access lines across the enterprise.
- Site—Subscriptions apply to all access lines grouped within a site.
- Access line—Subscriptions apply to a given access line that connects the enterprise to the service provider's network.

Overview of Operators

This section describes operators for subscribers and subscriptions. You can also configure operators for various SRC components. For information about setting up a multilayered access control scheme for operators, see *SRC-PE Integration Guide, Chapter 10, Access Control Scheme*.

In relation to subscribers and subscriptions, an operator is an object in the directory that represents an IT manager in an organization or a manager who works for a wholesaler and has control over all retailers. Retailers, subscriber folders, enterprises, sites, and accesses can support one or more operators.

When you add an enterprise with SDX Admin, the software creates a default operator for that enterprise. You can add additional operators for enterprises and create operators for retailers, subscriber folders, sites, and accesses.

You can also add an operator that has control over all retailers. See *Operators That Control All Retailers* on page 234.

Operator Read Privileges

Operators have privileges to read:

- The objects they control
- Parent subscribers, up to the retailer
- Subscriptions of parent subscribers, up to the retailer
- All objects that represent services, service scopes, policies, and global variables that are defined for the subscriber to which the operator is added

Operator Management Privileges

You can specify one or more management privileges for operators. If you do not specify privileges for an operator, the operator has only read privileges. The default operator that SDX Admin adds to an enterprise has the highest privilege level, called administrator. Table 8 shows the privilege levels and the privileges associated with the levels.

Table 8: Privilege Levels and Associated Tasks

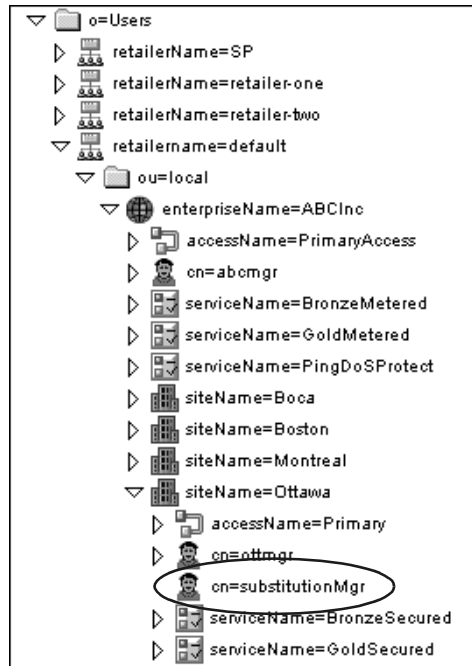
Privilege Level	Tasks That Operators with This Privilege Can Perform
Administrator	<ul style="list-style-type: none"> ■ Add, delete and modify operators ■ Add, delete, and modify subscriptions ■ Modify subscribers, including the ability to add, delete, and modify substitutions for subscribers ■ Manually activate and deactivate subscription sessions
Subscription	<ul style="list-style-type: none"> ■ Add, delete, and modify subscriptions ■ Manually activate and deactivate subscription sessions
Substitution	Add, delete, and modify substitutions in subscribers and subscriptions
Activation	<ul style="list-style-type: none"> ■ Configure automatic activation of services ■ Manually activate and deactivate subscription sessions
VPNs	Modify, export, and cancel the export of VPNs

An operator has management privileges for its associated subscriber and for that subscriber's subordinate objects. For example, operators in an enterprise have control over the enterprise and all sites and accesses in the enterprise. Similarly, operators in a site have control over the site and all accesses it contains. Operators in an access have control over only that access.

For example, in the directory shown in Figure 3, the operator substitutionMgr:

- Can manage substitutions of the site called Ottawa and its subordinate objects.
- Has read access to all services, service scopes, policies, and global variables that are defined for the site called Ottawa.
- Has read access to the site called Ottawa and its subordinate objects.
- Has read access to the parent subscribers: the enterprise ABCInc, the subscriber folder local, and the retailer default.
- Has read access to the subscriptions of the parent subscribers.

Figure 3: Sample Operator Access Privileges



Chapter 3

Subscriber Logins and Service Activation

This chapter gives an overview of how different types of subscribers log in to the network and how services and subscribers are activated. Topics include:

- Overview of Login Events and Processes on page 15
- Residential Subscriber Login and Processes on page 17
- PPP Subscriber Login and Service Activation on page 18
- DHCP Subscriber Login and Service Activation on page 22
- Static IP Subscribers on page 29
- Enterprise Subscriber Login Process on page 32
- Subscriptions and Activations on page 33
- Automatic Activation at Login on page 38

Overview of Login Events and Processes

Because of the different ways that residential and enterprise subscribers connect, the login interactions between the components differ according to the type of subscriber. Because residential customers can connect by PPP, DHCP, or static IP addresses, the interactions between the SRC components differ according to the method of connection that a residential subscriber uses. However, there is only one type of login interaction—the subscriber interface login interaction—for enterprise subscribers.

Logins to plug-ins can occur during the login to the SAE or during the activation of subscriptions. For these processes, many of the interactions between the SRC components are the same regardless of the type of subscriber and the type of connection.

Login Events

Each login process begins with a login event, as described in Table 9.

Table 9: Login Events

Login Event	Event Is Triggered When	SAE Response
AUTHINTF	An interface responds to authentication, such as authentication for a PPP session. (Supported on JUNOSe routers.)	Invokes subscriber classification script, creates subscriber session.
INTF	An interface comes up and the interface classifier script determines that the SAE should manage the interface, unless the interface comes up as a result of an authenticated PPP session. (Supported on JUNOS routing platform and JUNOSe routers.)	Invokes subscriber classification script, creates subscriber session.
ADDR	A subscriber obtains an unauthenticated IP address from the router through DHCP. (Supported on JUNOSe routers.)	Invokes subscriber classification script, creates subscriber session.
AUTHADDR	A subscriber obtains an authenticated IP address from the router through DHCP. (Supported on JUNOSe routers.)	Invokes subscriber classification script, creates subscriber session.
PORTAL	The portal API is invoked by a JSP Web page to log in a subscriber. (Supported on JUNOS routing platform and JUNOSe routers.)	Authenticate subscriber, invokes subscriber classification script, creates subscriber session.
ASSIGNEDIP	An application accesses a subscriber object for an assigned IP subscriber that is not currently loaded into memory.	Invoke subscriber classification script, creates subscriber session.

Summary of the Login Process

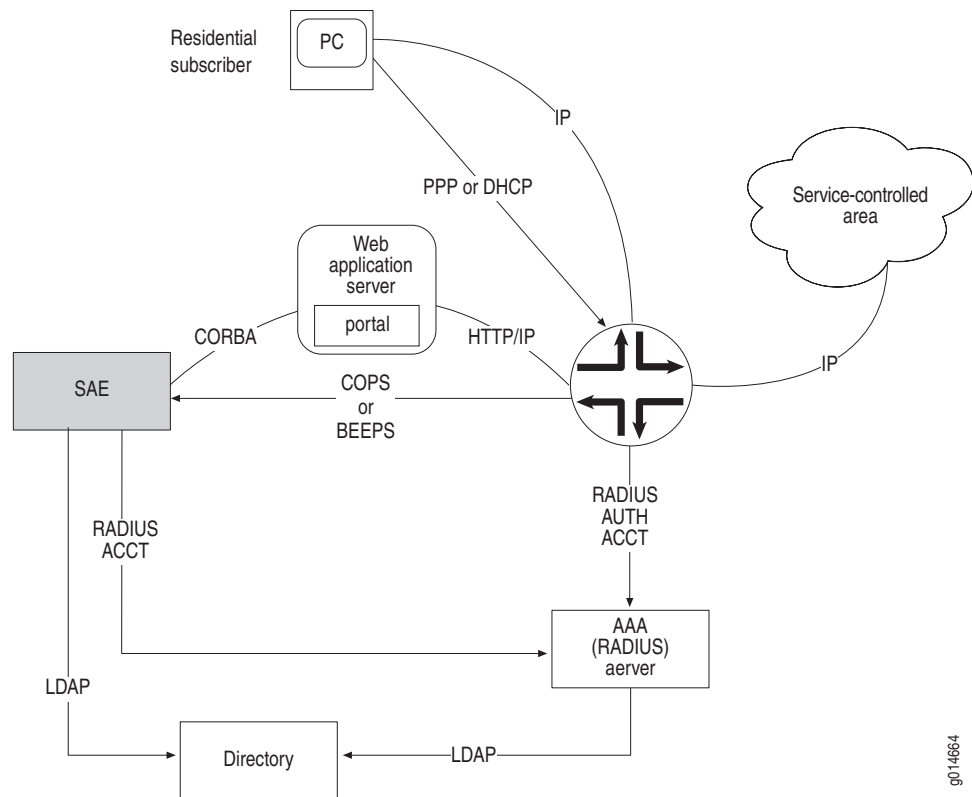
The SAE login process is summarized in the steps below. If any of the steps fail, the login process stops, and no subscriber session is created.

1. A login event occurs (see Table 9) and triggers the login process.
2. In case of a portal login, the SAE invokes the authentication plug-ins to authenticate the request.
3. The SAE invokes the subscriber classification script and provides to the script details about the login event (for example, interface name, subscriber IP address if available, login name if available, and login event type).
4. The script sends an LDAP query that uniquely identifies a subscriber entry in the directory to the SAE.
5. The SAE loads the subscriber entry from the directory and uses the entry to create a subscriber session in memory.
6. The SAE queries all configured authorization plug-ins about whether it should allow the login.
7. The SAE completes the login process by activating the subscriber's activate-on-login subscriptions.

Residential Subscriber Login and Processes

This section focuses on residential subscriber configurations involving authenticated PPP, DHCP, and static IP. The PPP, DHCP, and static IP cases are distinguished by the type and configuration of the networking software on the network device used to access the router. Figure 4 shows how residential subscribers connect to SRC components.

Figure 4: Components Involved in Subscription Activation



The residential subscriber's network device (such as a computer, cellular telephone, or set-top box) connects through a layer 2 connection to the router. The network device is configured for network access with PPP or DHCP.

The router and the SAE use a RADIUS server for authentication, accounting, and optionally IP address allocation. The router can also locally manage the allocation of IP addresses to residential subscribers' PCs. A directory supporting LDAP holds the database of subscriber, service, and subscription information. Both the SAE and the RADIUS server use the directory.

Once connected to the network, the subscriber's network device exchanges IP data packets with resources in a service-controlled area. From the service provider's perspective, the resource to which access is controlled may be the network itself or content servers in the network.

The SAE manages the subscriber's IP interface on the router to control the level of access that the subscriber gets to the service-controlled area. The level of access can be anything from viewing a portal page that allows the subscriber to select a service to varying the network access speed. The subscriber can actively and instantly request access to the service-controlled area by selecting items on Web pages generated by the SAE. Selecting these items triggers the SAE to instantly reconfigure the subscriber's IP interface on the router.

The SAE communicates with JUNOSe routers through COPS messages.

The SAE communicates with JUNOS routing platforms through BEEP messages.

PPP Subscriber Login and Service Activation

PPP subscribers access the network by using either special PPP or PPP over Ethernet software on their network access device. PPP access provides a means to configure the subscriber's network access device with several network parameters, including an IP address and a channel for transporting IP packets between the subscriber's network device and the router.

For subscribers with PPP access, logging in to the network consists of starting the PPP client, and logging out consists of stopping it. On PPP login, the router authenticates the subscriber as normal with a message to a RADIUS server. The router then notifies the SAE that there is a new IP interface on the router. The message to the SAE includes information such as the subscriber's IP address (if assigned by the router or RADIUS server), PPP login ID, and router interface ID. Using this information, the SAE retrieves the information to construct the default policies. The SAE then activates subscription policies, which are downloaded to the router and applied to the subscriber's network interface.

Subscribers can log in to the system with different accounts to different retail Internet service providers (ISPs). Subscribers use a different login ID for each account.

PPP requires special software on a network access device. The PPP software must be installed and maintained by the subscriber. The software can interfere with other applications.

Web Login for PPP Subscribers

In a PPP session, an IP address and a subscriber profile are authenticated at the same time. However, for some applications a split of subscriber profile and PPP session is useful; for example:

- Generic PPP account—An ISP could offer generic PPP login names and passwords for everybody and use Web-based login to identify subscribers.
- Device-based PPP—A PPP login may be used between a digital subscriber line (DSL) access device and a router. In this case a PPP login does not correspond to a subscriber session.
- Subaccounts with different services.

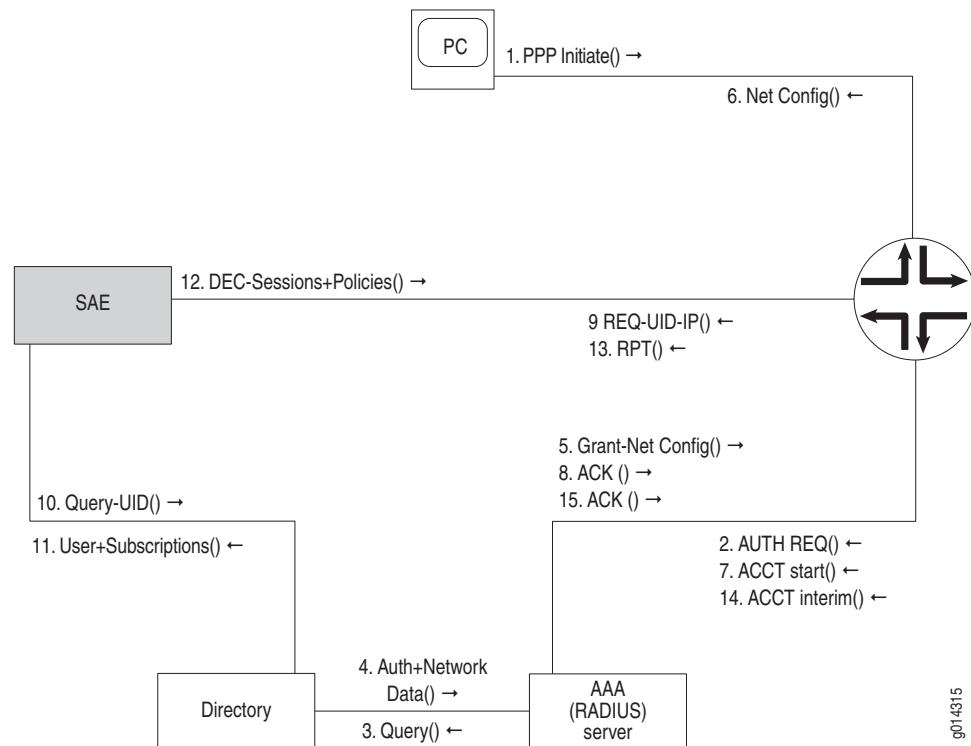
As a consequence, the Service Selection Portal (SSP) API allows creation of a Web application that:

- Allows PPP subscribers to log out—When the PPP subscriber logs out, the current subscriber session is closed, all active services are deactivated, and accounting records are generated. The unauthenticated subscriber entry is then associated with the IP address of the subscriber. This process is similar to a DHCP logout.
- Forces an unauthenticated PPP subscriber (that is, a PPP subscriber account that is bound to the unauthenticated subscriber entry or to an anonymous subscriber entry) to log in—The subscriber provides a username, realm (domain), and password. Authentication is processed in the same way as a DHCP login.

PPP Login Interactions

Figure 5 shows the interactions that take place during a PPP login.

Figure 5: PPP Login Interactions



The login sequence is as follows:

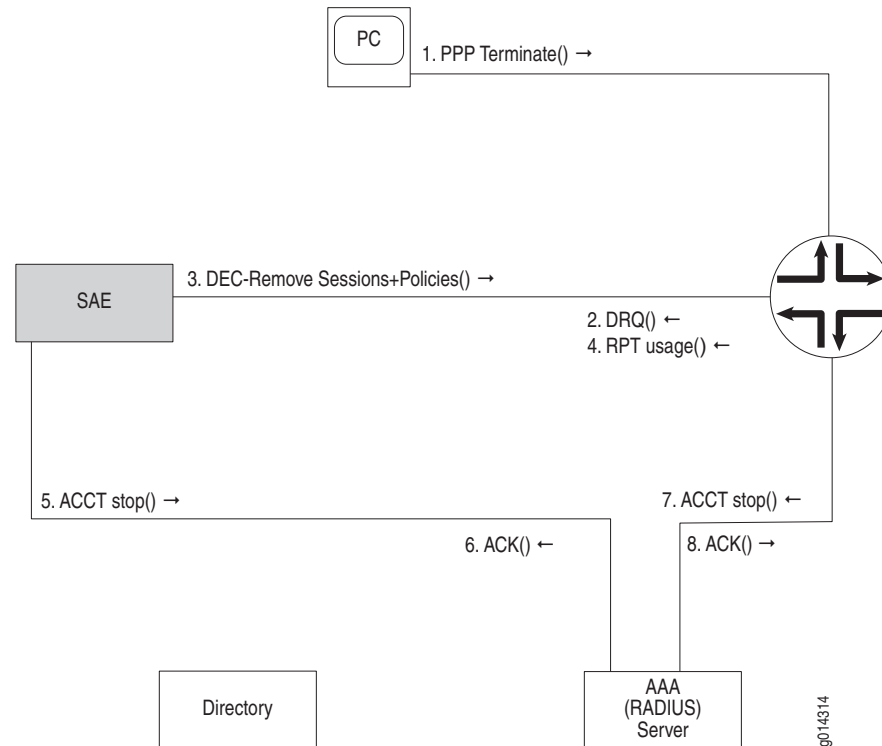
1. The subscriber initiates a PPP login by starting a PPP client on his or her network device.
2. The router sends an authentication request to the RADIUS server.
3. The RADIUS server sends a user ID query to the directory.

4. The directory responds with the data (IP address for the subscriber's network device) needed to authenticate the login, and then completes the configurations of the interface on the router and on the subscriber's network device.
5. If the authentication succeeds, the RADIUS server responds to the router with a grant message, including the network configuration parameters.
6. The configurations of the PPP and IP interfaces on the router and subscriber's network device are completed.
7. The router sends an accounting start message to the RADIUS server, indicating that a subscriber session has started.
8. The RADIUS server acknowledges the accounting start message.
9. The router sends a COPS or BEEP request message to the SAE. The message includes the user ID and the IP address assigned to the IP interface on the subscriber's network device. The SAE associates the subscriber's IP address with the subscriber session so that it can associate later requests from the subscriber with this session by looking at the source IP address of the request.
10. The SAE uses the subscriber ID to look up the subscriber's data in the directory.
11. The directory responds with data about the subscriber and the associated subscriptions. This data specifies which subscriptions should be automatically activated.
12. The SAE sends a series of decision (DEC) messages to the router. These messages tell the router to attach default policies and policies for automatically activated subscriptions to the subscriber's interface. They also tell the router to store subscriber and service sessions so that if the SAE fails, the subscriber can continue using his or her active subscriptions. If the SAE fails, the router connects to a backup SAE that synchronizes all session information and then takes over management of active subscribers on the router. During the synchronization process, active sessions are not affected.
13. The router acknowledges the decision messages with a report (RPT) message.
14. If interim accounting is enabled, the router periodically sends an accounting request to the RADIUS server to store an interim accounting record.
15. The RADIUS server sends an acknowledge message to the router, acknowledging the receipt of the interim accounting record.

PPP Logout Interactions

Figure 6 shows the interactions that take place when a subscriber logs out of a PPP session.

Figure 6: PPP Logout



The logout sequence is as follows:

1. The subscriber triggers his or her PPP software to close the PPP session with the router.
2. The router sends a COPS or BEEP delete request (DRQ) message, informing the SAE that the subscriber's IP interface is being shut down.
3. The SAE responds with decision (DEC) messages, requesting the router to remove the default and active subscription policies and sessions for the subscriber.
4. The router responds with a report (RPT) message that includes the usage data for the subscriptions that were just deactivated.
5. The SAE sends an accounting stop message to the RADIUS server, indicating that a service session has stopped. The stop message includes the usage data. (For information about service sessions, see *Subscriptions and Activations* on page 33.)
6. The RADIUS server acknowledges the accounting stop request.

7. The router sends an accounting stop message to the RADIUS server, indicating that a subscriber session has stopped.
8. The RADIUS server acknowledges the accounting stop request.

DHCP Subscriber Login and Service Activation

The DHCP system uses Ethernet to send data between a network device and the router. The DHCP client is built into the operating system. DHCP subscribers log in to the SAE to identify themselves, get personalized services, and select the retail ISP they want to use. Anonymous subscribers can log in to the SAE to view their account and subscription information.

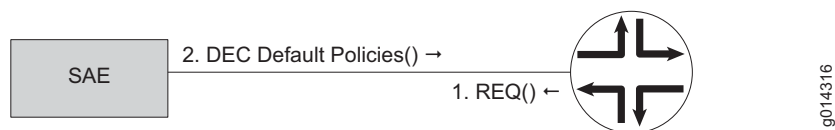
Like a subscriber with PPP access, a subscriber with DHCP access can have several accounts. The subscriber logs in to the different accounts at different times. This setup allows subscribers access to different sets of subscriptions. It supports a household in which different members share the same computer but subscribe to different services. Members of the household can get different bills for the services they use.

Subscribers can create a persistent login. In this case, the SAE stores the MAC address of the network device, along with the subscriber ID and password. This way, the network device is logged in to the subscriber account every time the device is started. Using the SAE core API, one can provide a check box on the portal page that allows the subscriber to create a persistent login. See *Persistent DHCP Subscriber Login Interactions* on page 26.

Interface Startup

An IP interface for DHCP subscribers can come up on the router without subscribers explicitly triggering its creation by logging in. When an interface comes up, the SAE runs an interface classifier script to determine whether it should manage the interface and, if so, which default policies to apply to the interface. Thus, for DHCP subscribers, default policies are applied as soon as the IP interface on the router comes up independently of any subscriber login. Figure 7 shows this interaction.

Figure 7: DHCP Interface Startup



The startup sequence is as follows:

1. When the IP interface on the router comes up, the router sends a COPS request (REQ) to the SAE to let it know that the new interface exists.
2. The SAE runs an interface classification script to determine whether it should manage the new interface. If the SAE manages the interface, then the SAE downloads the default policies for the interface on the router.

Initial Login

When a DHCP subscriber starts a network device for the first time, the SAE has no information about who the subscriber is and what subscriptions the subscriber has. The SAE assigns default policies and an unauthenticated subscriber profile to the subscriber. The unauthenticated subscriber profile gives the subscriber access to services that are available without authentication.

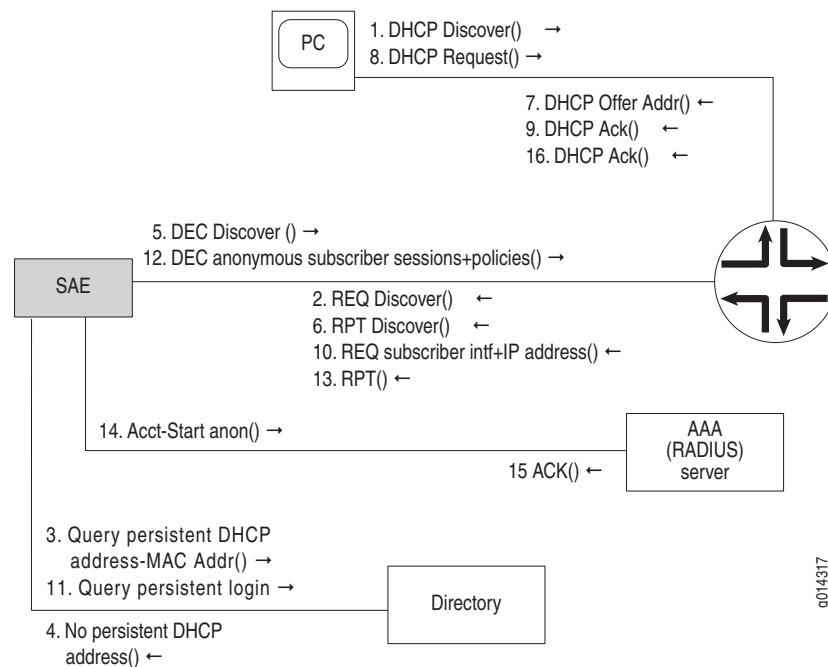
The first time a subscriber's network device starts, the router assigns an IP address to it. This address allows the subscriber access only to the SAE. The router provides this IP address for a short period of time called the lease time. After the lease time is over, the router provides a permanent IP address.

The system builds SAE applications to allow subscribers to register with the network if they are first-time subscribers of the network.

Initial DHCP Login Interactions

Figure 8 shows the interactions that take place when a DHCP subscriber starts a network device.

Figure 8: DHCP Subscriber Initial Login



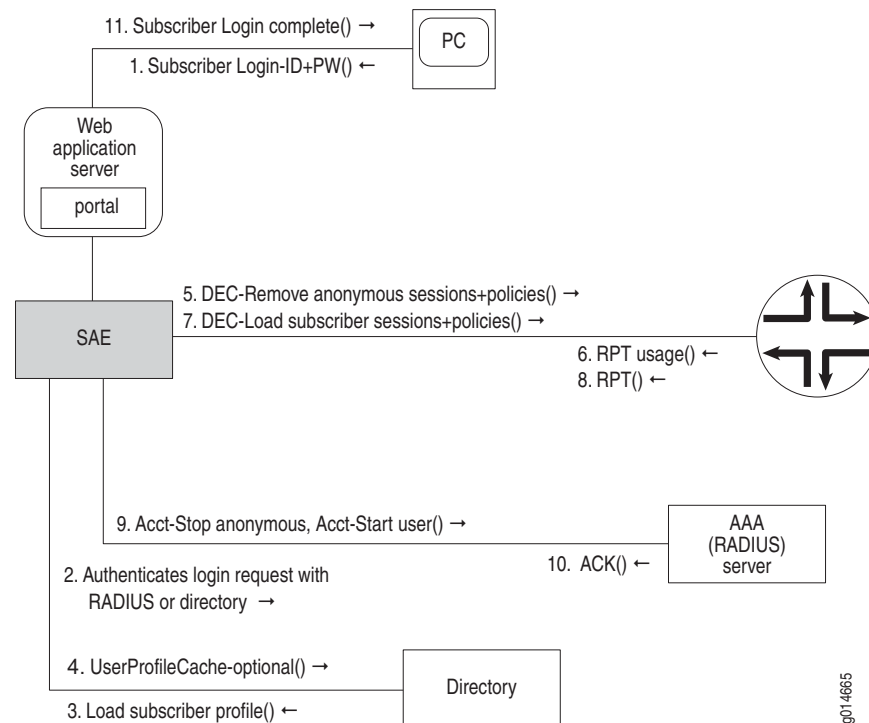
For this example, we assume that the directory responses show that there are no persistent subscriber logins. The startup sequence is as follows:

1. The DHCP client in the subscriber's network device broadcasts a discover message to the router.
2. The router acts on the discover message by sending a COPS request (REQ) message to the SAE, indicating that an IP address is about to be assigned by the local DHCP server on the local router. This request includes the MAC address of the subscriber's network device and the DHCP options sent by the client.
3. The SAE queries the directory to detect any persistent DHCP address assignments associated with the subscriber's network device. Persistent DHCP address assignments are indexed by the MAC address of the device from which they originate.
4. The directory responds with an indication that there are no persistent DHCP address assignments associated with the subscriber's network device.
5. The SAE responds to the router with a COPS decision (DEC) message, requesting the router to assign an unauthenticated address to the subscriber device.
6. The router acknowledges the address assignment decision message with a COPS report (RPT) message.
7. The router allocates and offers an IP address to the subscriber's network device.
8. The network device sends a request for the address that the router offered.
9. The router acknowledges the address request.
10. The router sends a COPS request message that includes the subscriber's interface and the assigned IP address.
11. The SAE looks up persistent logins or runs the subscriber classification script and creates a subscriber session based on the loaded subscriber profile.
12. The SAE downloads sessions for the newly logged in unauthenticated subscriber and the policies for the subscriptions that this subscriber account has configured for automatic activation. (Identification of which unauthenticated subscriber account to use is configurable in the SAE and is a function of attributes found in the original COPS request message of Step 2.)
13. The router stores the sessions, applies the policies to the subscriber's IP interface, and then acknowledges the decision with a COPS report.
14. If accounting is configured for the subscriptions, the SAE sends an accounting start message to the RADIUS server.
15. The RADIUS server acknowledges the accounting message.
16. The DHCP server on the router acknowledges the DHCP renew request.

DHCP Login to Subscriber Account Interactions

Figure 9 shows the interactions that take place when a DHCP subscriber logs in to a subscriber account. The account changes from an anonymous subscriber to an authenticated subscriber with personalized subscriptions.

Figure 9: DHCP Subscriber Login



The sequence is as follows:

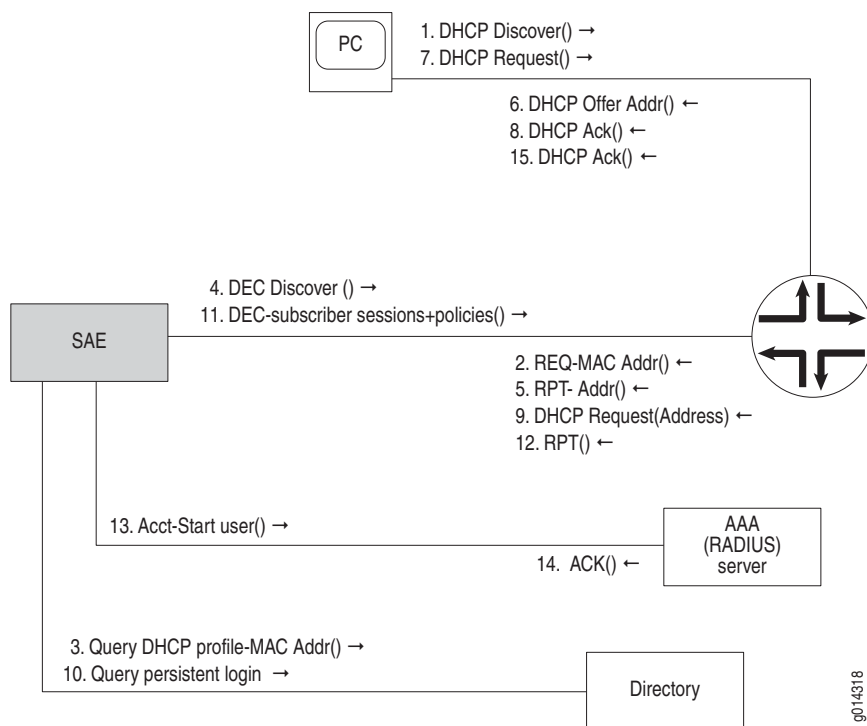
1. The subscriber's network device sends a request to the SAE to log in to the subscriber account with the subscriber ID and password (PW).
2. The SAE authenticates the request using the configured authentication plug-in.
3. If authentication is successful, SAE loads a subscriber profile from the directory.
4. If this is a persistent login, the SAE creates an entry in the directory in the userProfileCache object. The entry is keyed to the network device's MAC address and associates the MAC address with the subscriber ID and password. The next time the subscriber starts the device, the system automatically logs in the subscriber's account.
5. The SAE sends a COPS decision (DEC) message, instructing the router to deactivate the policies and sessions associated with the active subscriptions.
6. The router acknowledges the COPS decision message with a COPS report (RPT) message that includes usage information for the active subscriptions.
7. The SAE sends a COPS decision message to load sessions and policies for the automatically activated subscriptions for the new subscriber account.

8. The router acknowledges these decisions with COPS report messages.
9. The SAE sends the RADIUS server accounting stop messages for the subscriptions that were deactivated, and accounting start messages for the subscriptions that were activated.
10. The RADIUS server acknowledges the accounting messages.
11. The SAE responds to the subscriber's original request with a login successful message. A typical application would return a Web page that gives the subscriber the ability to activate and deactivate subscriptions.

Persistent DHCP Subscriber Login Interactions

Figure 10 shows the interactions that take place when a DHCP subscriber starts a device on the network after having previously been logged in as a persistent subscriber.

Figure 10: Persistent DHCP Subscriber Login



g014318

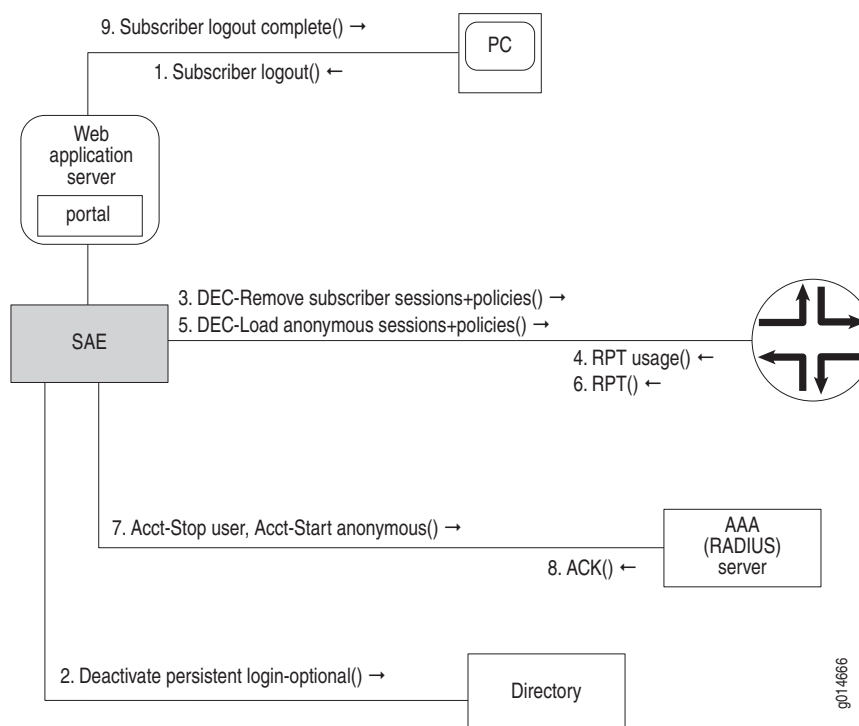
The login sequence is as follows:

1. The DHCP client in the subscriber's network device sends a discover message to the router.
2. The router sends a COPS request (REQ) message to the SAE, informing the SAE that the router has received a DHCP discover request. The message includes the MAC address of the subscriber's network device and the DHCP options sent with the discover request.
3. The SAE queries the directory for a DHCP profile associated with the MAC address of the subscriber's network device.
4. The SAE sends the router a COPS decision (DEC) message, instructing the router to assign an IP address to the subscriber's network access device based on the information stored in the DHCP profile.
5. The router acknowledges the address assignment decision message with a COPS report (RPT) message.
6. The router allocates and offers an IP address to the subscriber's network access device.
7. The subscriber's network access device sends a request message to the router, requesting the address that was offered.
8. The router acknowledges the address request.
9. The router sends a COPS request message to the SAE that includes the subscriber's interface and the assigned IP address.
10. The SAE queries the directory for persistent logins, and the directory responds with the subscriber account information for the persistent login, including the subscriptions that are to be automatically activated.
11. The SAE starts the subscriber session and downloads session data for the subscriber account and the policies for the subscriptions that this subscriber account has configured for automatic activation.
12. The router stores the session data and applies the policies to the subscriber's IP interface. The router then acknowledges the decision message with a COPS report message.
13. If accounting is configured for the automatically activated subscriptions, then the SAE sends an accounting start message to the RADIUS server.
14. The RADIUS server acknowledges the accounting start message.
15. The router acknowledges the DHCP request messages with a DHCP acknowledge message.

DHCP Subscriber Logout Interactions

Figure 11 shows the interactions that take place when a DHCP subscriber logs out of a subscriber account. The account changes from an authenticated subscriber to an anonymous subscriber with generic subscriptions and limited access.

Figure 11: DHCP Subscriber Logout



The logout sequence is as follows:

1. The subscriber's network device sends a request to the SAE to log out of its current subscriber session.
2. The subscriber may request to deactivate persistent login. If the subscriber deactivates persistent login, the SAE deletes the entry in the directory. If the subscriber does not deactivate the persistent login, then the account is automatically logged in the next time the same network device is started.
3. The SAE sends a COPS decision (DEC) message to the router, instructing the router to remove the sessions and policies associated with the active subscriptions.
4. The router responds with a COPS report (RPT) message that includes the usage information for the deactivated subscriptions.
5. The SAE sends a COPS decision message to add sessions and policies for the automatically activated subscriptions for the anonymous account to which the subscriber has switched.
6. The router acknowledges the COPS decision message by sending a COPS report message to the SAE.

7. The SAE sends the RADIUS server accounting stop messages for the subscriptions that were deactivated, and accounting start messages for the subscriptions that were activated.
8. The RADIUS server acknowledges these accounting messages.
9. The SAE responds to the subscriber's logout request, showing that the logout is complete.

Static IP Subscribers

The SAE supports residential subscribers who use statically assigned IP addresses. Statically assigned means that the network does not create events that contain information about the IP address of the subscriber. The SAE can handle the case in which a router interface is dedicated to one subscriber. This subscriber can be a single PC or multiple PCs that are managed by the same household.

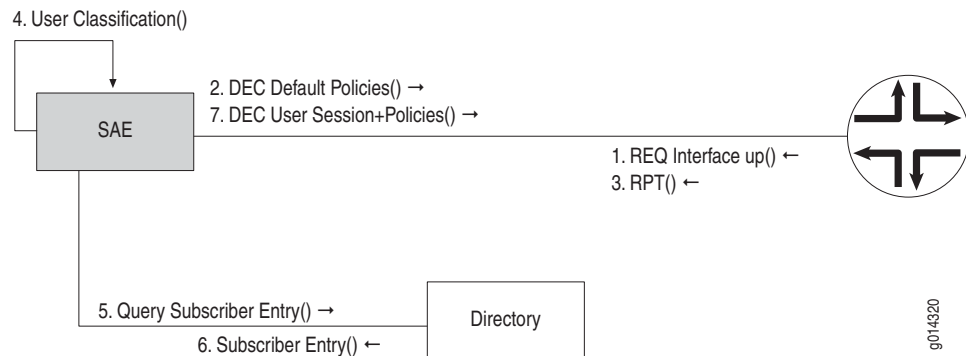
Single PC, IP Address Known

See Figure 12.

1. When the interface dedicated to the subscriber comes up, the router sends a COPS or BEEP request (REQ) message to the SAE. The SAE calls the interface classification script to determine whether the interface is being managed and which default policies are applied.
2. The SAE sends a decision (DEC) message to the router, requesting that the router attach the selected default policies.
3. The router acknowledges the decision message with a report message.
4. The SAE calls the subscriber classification script to determine whether a subscriber session needs to be started. The subscriber classification script responds with an LDAP query.
5. The SAE uses the LDAP query to look up a subscriber entry in the directory.
6. The directory responds with data about the subscriber and the associated subscriptions. The IP address assigned to the subscriber can be part of the data returned from the directory. If the IP address cannot be stored in the directory, it is also possible to integrate the SAE with an external data source (for example, a database maintained by an existing provisioning system), to look up the IP address of the subscriber.

As in the PPP case, the SAE associates the subscriber session with the IP address so it can handle later requests by looking up the source IP address of the HTTP request.

7. The SAE sends decision messages that install policies for automatically activated subscriptions.

Figure 12: Static IP Subscriber Login**Subscriber IP Address Not Known**

See Figure 13.

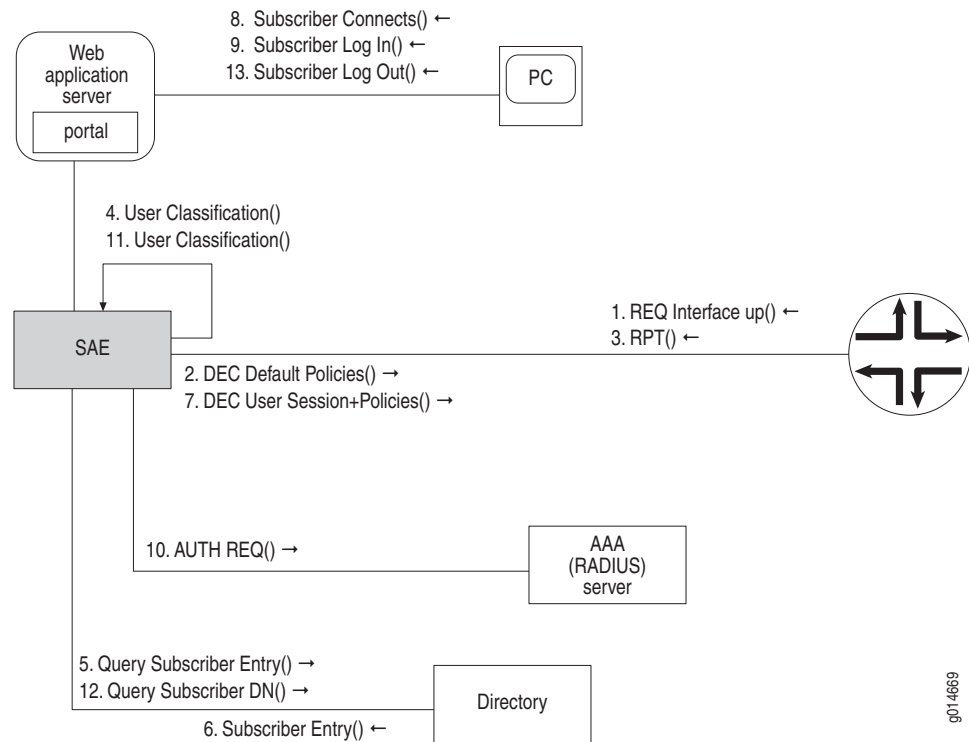
1. When the interface dedicated to the subscriber comes up, the router sends a BEEP or COPS request (REQ) message to the SAE. The SAE calls the interface classification script to determine whether the interface is being managed and which default policies are applied.
2. The SAE sends a decision (DEC) message to the router, requesting that the router attach the selected default policies.
3. The router acknowledges the decision message with a report (RPT) message.
4. The SAE invokes the subscriber classification script to determine whether a subscriber session needs to be started. The subscriber classification script responds with an LDAP query.
5. The SAE uses the LDAP query to look up a subscriber entry in the directory.
6. The directory responds with data about the subscriber and the associated subscriptions.

The SAE associates the subscriber session with the DN of the subscriber entry so that later requests can be handled. One consequence of associating the subscriber entry with the DN is that it is not possible to have more than one subscriber session for a single DN active at the same time.

7. The SAE sends decision messages that install policies for automatically activated subscriptions.
8. The subscriber connects to the portal. Because the IP address of the subscriber is not associated with a subscriber session, a login page is displayed instead.
9. The subscriber provides a username and password.
10. The SAE authenticates the request (for example, by using the RADIUS authentication plug-in) and calls the subscriber classification script.

11. The subscriber classification script returns an LDAP query. The SAE uses the query to look up the DN of the subscriber entry in the directory.
12. The SAE uses the DN returned from the directory to find a subscriber session and associates it with the IP address of the HTTP request. The SAE handles subsequent accesses to the portal by looking up the IP address of the HTTP request.
13. The subscriber logs out from the SAE. The SAE does not change the subscriber session associated with the DN of the subscriber, but removes the association of the subscriber IP address with the subscriber session.

Figure 13: Subscriber IP Address Not Known



g014669

Enterprise Subscriber Login Process

Enterprise subscribers may connect through any access method. Any of the events described in Table 9 on page 16 can initiate an enterprise login.

Interface Startup

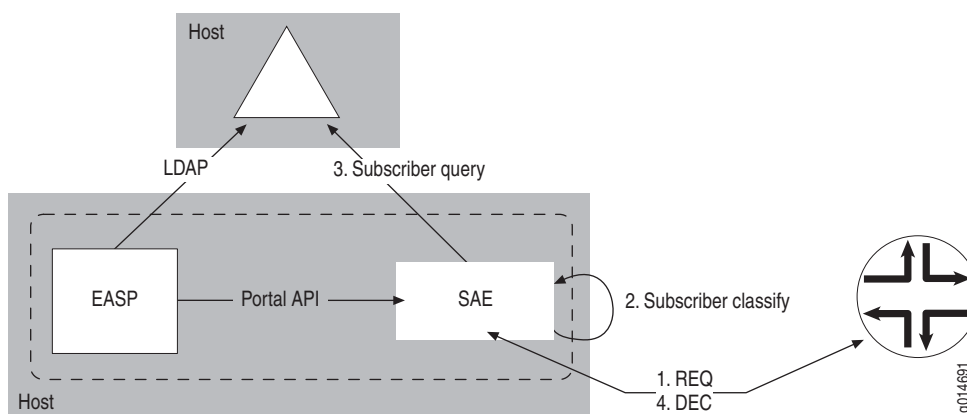
When a router interface comes up, the router sends a message to the SAE with information about that interface.

The SAE classifies the subscriber to determine the default interface policies. An SAE subscriber classification rule matches the attributes of the interface and describes how to formulate an LDAP query that retrieves the access entry in the directory that corresponds to the router interface.

Based on the response from the directory, the SAE creates a subscriber session and associates it with the DN of the access entry in the directory. The SAE then sends the router a message to install all the policies for subscriptions for the access line that are set to administratively active.

Figure 14 shows the stages involved in activating an enterprise subscriber session.

Figure 14: Enterprise Subscriber Session Activation



Subscriptions and Activations

Each subscriber purchases a set of services; this purchase is known as a subscription. Information about the subscriptions is stored in the directory and is used by a residential service selection portal application to generate controls that enable the subscriber to:

- Activate and deactivate subscriptions.
- Subscribe to services.
- Configure subscriptions to be automatically activated.

The service selection application can be either a Web application or an API. When the service selection application is a Web application, the controls are Web pages with buttons and links to click on (see Figure 15 and Figure 16). However, the service selection application provides an open API that makes it possible to build applications that are controlled by mechanisms other than Web pages. For instance, customers can build service selection applications that are controlled by applications running in the system tray area of the Windows task bar. This deployment consolidates the control of subscribers' active network services and the speed of their Internet connection, along with their control of other aspects of their PC, such as the clock settings and audio volumes.

Figure 15: Service Activation Page

Service Selection Portal

- Services
- Usage
- Account
- Schedules
- Subscribe
- Register
- Unregister

Search

Services

You can start or stop a service by clicking on the circle in the "Status" column. A green circle (●) means the service is currently on. A red circle (●) means the service is currently off.

You can persistently activate a service by clicking on the check box in the "Persistent" column. Persistently activated services are automatically activated when you login to the portal.

Internet

Service Description	Status	Password required	Persistent	Price
Example for rate limited internet (requires matching default policies)	●		<input type="checkbox"/>	N/A

Copyright © 1999-2003 Juniper Networks

Figure 16: Subscription Activation Page

virneo
The network that keeps you surfing

Hello Jane User

Home Logout Contact us

Service Selection Portal

- Services
- Usage
- Account
- Schedules
- Subscribe**
- Register
- Unregister

Search

Subscribe

All available services are listed below.

It may take a minute for your new subscriptions to take effect.

Internet Overwrite Security Video Quality of Service Audio News Denial of Service

Service Name	Service description	Subscribed	Unsubscribed
Internet-Bronze	Example for rate limited internet (requires matching default policies)	<input checked="" type="radio"/>	<input type="radio"/>
Internet-Gold	Example for rate limited internet (requires matching default policies)	<input type="radio"/>	<input checked="" type="radio"/>
Internet-Silver	Example for rate limited internet (requires matching default policies)	<input type="radio"/>	<input checked="" type="radio"/>

OK Cancel

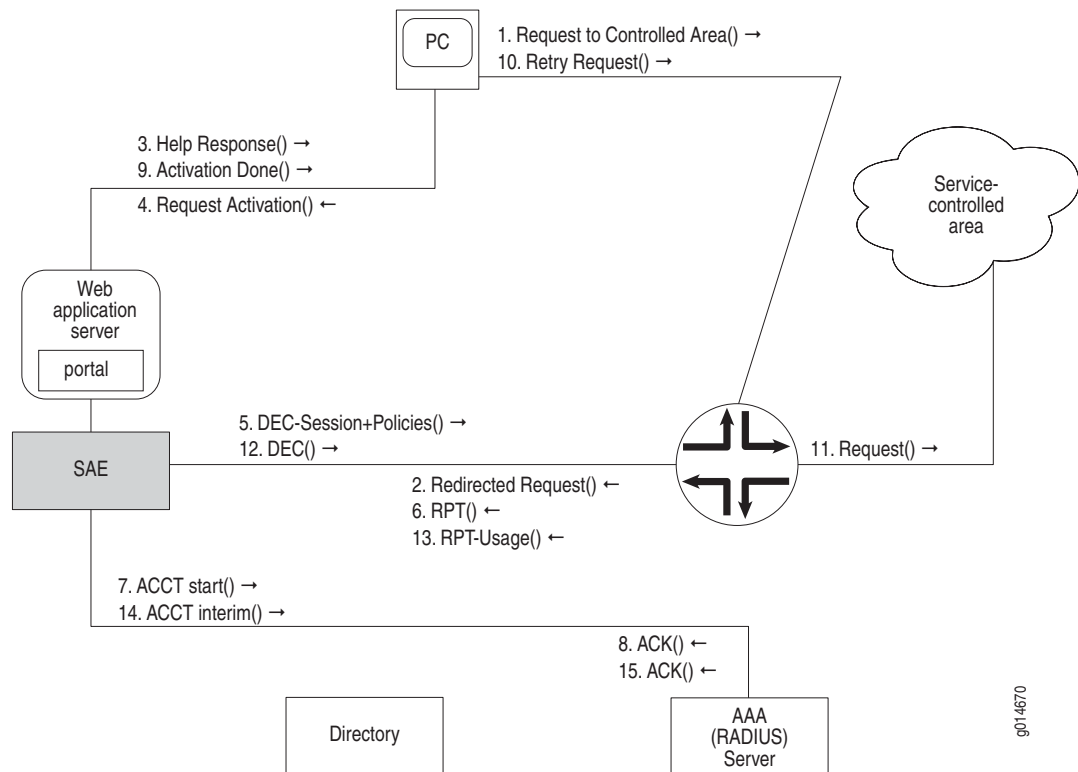
virneo

Copyright © 1999-2003 Juniper Networks

Many of the activation and deactivation interactions work in the same way, whether the subscriber is a residential subscriber or an enterprise subscriber. However, some interactions apply only to enterprise subscribers (see *Enterprise-Specific Remote Session Activation* on page 38).

Subscription Activation Interactions

Clicking a button on the Web page to activate a service session causes the SAE to download the policies associated with the service to the subscriber's IP interface on the router. Figure 17 shows the interactions among the components shown in Figure 4 on page 17 during the activation process. This scenario assumes that the subscriber has already logged in.

Figure 17: Subscription Activation

The activation sequence is as follows:

1. Before the subscription is activated, the subscriber makes a request to the corresponding subscription resource in the service-controlled area.
2. A default policy that matches the request on the router causes the router to redirect the request to the SAE.
3. The SAE responds to the request with a help desk Web page, requesting that the subscriber activate the subscription before trying to access the resource.
4. The subscriber clicks a button on the service selection portal Web page, requesting the activation of the subscription.

5. The SAE sends a COPS or BEEP decision (DEC) message to the router, requesting the installation of policies for the subscription on the subscriber's IP interface on the router, as well as service session information.

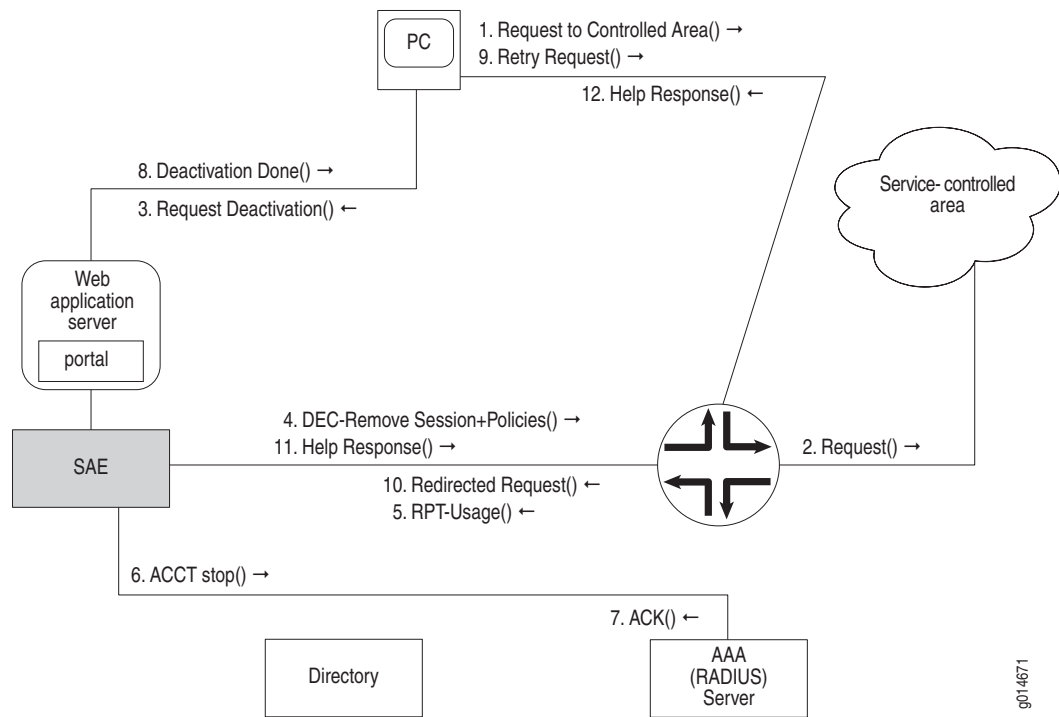
At start time, the SAE loads all services and policy templates from the directory. At activation time, the policy templates for the service are instantiated with values that are determined at activation, such as the subscriber's IP address. The router stores session information so that if the SAE fails, the subscriber can continue using his or her active subscriptions. If the SAE fails, the router connects to a backup SAE. The backup SAE synchronizes all session information and then takes over management of all active subscribers on the router.

6. The router responds with a report (RPT) message acknowledging the decision message.
7. The SAE sends an accounting start message to the RADIUS server.
8. The RADIUS server acknowledges the accounting start message.
9. The SAE responds to the subscriber's activation request, indicating that the subscription is active.
10. The subscriber may now retry the request for access to the controlled resource.
11. This time, the request to the controlled resource matches the policy from the newly activated subscription, so the router allows the request to be routed normally. Depending on the policy, the router may also apply QoS processing.
12. If interim accounting is enabled, the SAE periodically sends a decision message requesting usage data.
13. The router responds with a report message that contains usage data for the subscription. The usage data consists of the number of bytes and packets that the policies processed for the subscription.
14. The SAE stores the usage data in interim accounting records in the RADIUS server.
15. The RADIUS server acknowledges the interim accounting record.

Subscription Deactivation Interactions

Clicking a button on the Web page to deactivate a service causes the SAE to request that the router remove the policies for the service from the subscriber's IP interface on the router.

Figure 18 shows the interactions among the components shown in Figure 4 on page 17 during the subscription deactivation process. This scenario assumes that the subscriber has already logged in.

Figure 18: Subscription Deactivation

The deactivation sequence is as follows:

1. The subscriber sends a request to deactivate a subscription to a resource in the service-controlled area.
2. The request matches a policy that allows the request to be forwarded to the resource in the service-controlled area.
3. The subscriber clicks on a field on a Web page to request that the SAE deactivate the subscription.
4. As a result, the SAE sends a COPS or BEEP decision (DEC) message to the router to remove policies for the subscription from the subscriber interface and the service session from memory.
5. The router acknowledges the decision message with a report (RPT) message that contains service usage. The usage is the number of bytes and packets that the policies processed for the subscription.
6. An accounting stop record that includes the subscription usage information is written in the RADIUS server.
7. The RADIUS server acknowledges the accounting message.
8. The SAE sends a message to the subscriber, informing the subscriber that the subscription has been deactivated.

9. Because the policy for the subscription was removed from the subscriber interface on the router, any request for access is directed to the SAE.
10. The subscriber may now retry to request access to the controlled resource.
11. As was the case before the subscription was activated, the SAE generates a help desk Web page response that is relayed to the subscriber.

Automatic Activation at Login

An activate-on-login subscription is a subscription that is configured to start every time the subscriber logs in.

A manual subscription is a subscription that is configured to start only by an action from the subscriber.

For example, residential subscriber Elizabeth has designated her high-speed subscription to automatically activate every time she logs in. On the other hand, her video subscription is not activated unless she activates it by clicking a button on a portal page. It is possible to integrate the SAE with a video-on-demand server so that the video service is automatically activated when Elizabeth logs in. This type of configuration ensures access to the server and to QoS for the video stream. When the video stream is finished, the video-on-demand server triggers the SAE to stop the video service.

Residential subscriber Robert is interested in streaming audio. He sets his subscriptions so that regular-speed service, along with his subscription to an audio service, is automatically activated every time he logs in.

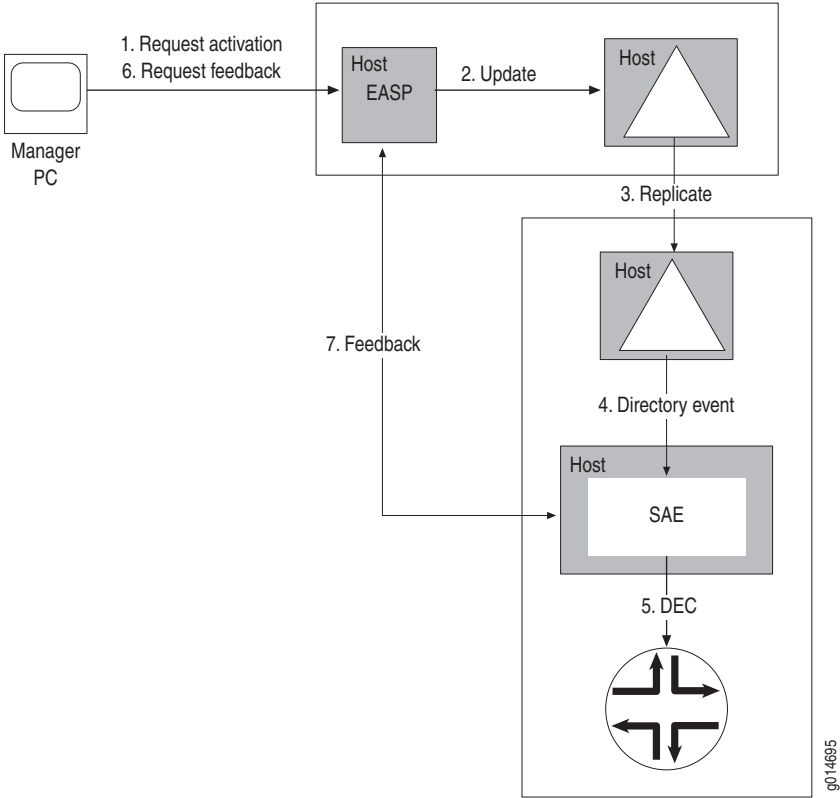
Enterprise-Specific Remote Session Activation

When a subscription is set for automatic activation through the Web interface, a service session request message is sent from the manager's PC to the Enterprise Manager Portal. The Enterprise Manager Portal writes this request to the directory, and the directory eventing system (DES) notifies the SAE affected by this request of the directory event. The SAE then sends a COPS or BEEP decision message to the router to download the policies for the activated subscription.

The enterprise manager must explicitly request feedback to see whether the session succeeded and what the operational values for the service parameters actually are. To do this, the enterprise manager sends a feedback request to the Enterprise Manager Portal. To process this request, the Enterprise Manager Portal sends a feedback request to the remote SAE managing the access through CORBA and returns the response to the enterprise manager's browser.

Figure 19 shows the sequence of messaging events that occur between the manager PC, the Enterprise Manager Portal, the master and shadow directories, the remote SAE, and the router.

Figure 19: Remote Session Activation Sequence



Chapter 4

Configuring Subscriber-Related Properties on the SAE with the SRC CLI

This chapter describes how to use the SRC CLI to configure subscriber-related properties on the SAE. You can use the SRC CLI to configure the SAE on a C-series platform or on a Solaris platform.

You can also use SDX Configuration Editor, SDX Admin, or a text editor to configure the SAE on Solaris platforms. See *Chapter 5, Configuring Subscriber-Related Properties on the SAE on a Solaris Platform*.

Topics in this chapter include:

- Configuring the Length of Time MAC Addresses Remain in SAE Cache on page 41
- Identifying a Profile for Unauthenticated Subscribers on page 43
- Configuring Interim Accounting for Services and Subscribers on page 43
- Avoiding Overcharges for Sessions That Time Out on page 44
- Allowing Multiple Logins from the Same IP Address on page 45
- Authenticating Registered Username/Password Pairs on page 46
- Configuring Timers for Session Reactivation on page 46

Configuring the Length of Time MAC Addresses Remain in SAE Cache

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.

Use the following configuration statement to configure the length of time that a subscriber profile remains in the SAE's in-memory cache:

```
shared sae configuration driver {
    mac-cache-expiration mac-cache-expiration;
}
```

To configure the amount of time that subscriber profiles remain in the SAE's in-memory cache:

1. From configuration mode, access the SAE driver configuration statement.

```
user@host# edit shared sae configuration driver
```

2. Specify the amount of time that subscriber profiles remain in the SAE's cache.

```
[edit shared sae configuration driver]
user@host# set mac-cache-expiration mac-cache-expiration
```

3. (Optional) Verify your configuration.

```
[edit shared sae configuration driver]
user@host# show mac-cache-expiration
mac-cache-expiration 1800;
```

Identifying a Profile for Unauthenticated Subscribers

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.

Use the following configuration statement to specify an unauthenticated subscriber profile.

```
shared sae configuration driver {
    unauthenticated-subscriber-dn unauthenticated-subscriber-dn
}
```

To specify an unauthenticated subscriber profile:

1. From configuration mode, access the SAE driver configuration statement.

```
user@host# edit shared sae configuration driver
```

2. Specify a subscriber profile for unauthenticated access to the portal.

```
[edit shared sae configuration driver]
user@host# set unauthenticated-subscriber-dn unauthenticated-subscriber-dn
```

3. (Optional) Verify your configuration.

```
[edit shared sae configuration driver]
user@host# show unauthenticated-subscriber-dn
unauthenticated-subscriber-dn
uniqueID=unauthentication,ou=local,RetailerName=default,o=Users,<base>;
```

Configuring Interim Accounting for Services and Subscribers

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.

Use the following configuration statements to configure interim accounting.

```
shared sae configuration interim-accounting {
    service-interim-accounting;
    service-interim-interval service-interim-interval;
    subscriber-interim-accounting;
    subscriber-interim-interval subscriber-interim-interval;
}
```

To set up interim accounting:

1. From configuration mode, access the configuration statement for interim accounting.

```
user@host# edit shared sae configuration interim-accounting
```

2. (Optional) Enable service interim accounting.

```
[edit shared sae configuration interim-accounting]
user@host# set service-interim-accounting
```

3. Specify the interval between service interim accounting messages.

```
[edit shared sae configuration interim-accounting]
user@host# set service-interim-interval service-interim-interval
```

4. (Optional) Enable interim accounting for subscribers.

```
[edit shared sae configuration interim-accounting]
user@host# set subscriber-interim-accounting
```

5. Specify the interval between subscriber interim accounting messages.

```
[edit shared sae configuration interim-accounting]
user@host# set subscriber-interim-interval subscriber-interim-interval
```

6. Verify your configuration.

```
[edit shared sae configuration interim-accounting]
user@host# show
service-interim-accounting;
service-interim-interval 900;
subscriber-interim-accounting;
subscriber-interim-interval 900;
```

Avoiding Overcharges for Sessions That Time Out

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 to avoid overcharges for the session.

Use the following configuration statement to configure the length of time that a subscriber profile remains in the SAE's in-memory cache:

```
shared sae configuration idle-timeout {
    adjust-session-time;
}
```

To adjust the session time:

1. From configuration mode, access the SAE idle timeout configuration statement.

```
user@host# edit shared sae configuration idle-timeout
```

2. Enable when an idle timeout terminates a session, the session time reported in the accounting stop message is reduced by the idle time.

```
[edit shared sae configuration idle-timeout]
user@host# set adjust-session-time
```

3. (Optional) Verify your configuration.

```
[edit shared sae configuration idle-timeout]
user@host# show
adjust-session-time;
```

Allowing Multiple Logins from the Same IP Address

You can specify whether the SAE allows a login from the same IP address without requiring that the previous session logs 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.

Use the following configuration statement to specify whether or not the SAE allows multiple logins from the same IP address:

```
shared sae configuration subscriber-sessions {
  allow-same-ip-login;
}
```

To specify whether the SAE allows a login from the same IP address without requiring that the previous session logs out first:

1. From configuration mode, access the subscriber sessions statement.

```
user@host# edit shared sae configuration subscriber-sessions
```

2. Enable or disable whether the SAE allows a login from the same IP address without requiring that the previous session logs out first.

```
[edit shared sae configuration subscriber-sessions]
user@host# set allow-same-ip-login
```

3. (Optional) Verify your configuration.

```
[edit shared sae configuration subscriber-sessions]
user@host# show
adjust-session-time;
```

Authenticating Registered Username/Password Pairs

You can specify whether the application programming interface (API) method `registerLoginCredentials` authenticates the registered username/password or creates the registration without authentication. You should enable this setting if your authentication server does not allow authentication while a session for the authenticated username is active.

Use the following configuration statement to specify whether or not registered username/password pairs are authenticated:

```
shared sae configuration login-registration {
    registration-authentication;
}
```

To specify whether or not registered username/password pairs are authenticated:

1. From configuration mode, access the subscriber sessions statement.

```
user@host# edit shared sae configuration login-registration
```

2. Enable or disable whether registered username/password pairs are authenticated.

```
[edit shared sae configuration login-registration]
user@host# set registration-authentication
```

3. (Optional) Verify your configuration.

```
[edit shared sae configuration login-registration]
user@host# show
registration-authentication;
```

Configuring Timers for Session Reactivation

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.

Use the following configuration statements to configure background session reactivation behavior

```
shared sae configuration service-activation {
    retry-time retry-time;
    retry-limit retry-limit;
}
```

To configure session reactivation behavior:

1. From configuration mode, access the service activation statements.

```
user@host# edit shared sae configuration service-activation
```

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.

```
[edit shared sae configuration service-activation]  
user@host# set retry-limit retry-limit
```

3. Configure the time between attempts to activate a service session if activation fails or to deactivate a service session if deactivation fails.

```
[edit shared sae configuration service-activation]  
user@host# set retry-time retry-time
```

4. (Optional) Verify your configuration.

```
[edit shared sae configuration service-activation]  
user@host# show  
retry-time 60;  
retry-limit -1;
```


Chapter 5

Configuring Subscriber-Related Properties on the SAE on a Solaris Platform

This chapter describes how to configure subscriber-related properties on the SAE with SDX Configuration Editor or by modifying a property file. You can use SDX Configuration Editor and property files on a Solaris platform.

You can also use the SRC CLI to configure an SAE on the C-series platform or on a Solaris platform. See *Chapter 4, Configuring Subscriber-Related Properties on the SAE with the SRC CLI*.

Topics in this chapter include:

- Overview on page 50
- Configuring the Length of Time MAC Addresses Remain in SAE Cache on page 50
- Identifying a Profile for Unauthenticated Subscribers on page 51
- Configuring Interim Accounting for Services and Subscribers on page 52
- Avoiding Overcharges for Sessions That Time Out on page 53
- Allowing Multiple Logins from the Same IP Address on page 54
- Authenticating Registered Username/Password Pairs on page 55
- Configuring Timers for Session Reactivation on page 56
- Modifying the SAE Property File on page 57
- Loading Subscriptions Based on RADIUS Authorization on page 58
- Accepting Login Names with Different Formats on page 60

Overview

The SAE property file contains SAE configuration data that is stored in the directory.

You can modify the SAE property file with SDX Configuration Editor, SDX Admin, or a standard text editor. The following sections show how to configure SAE properties with SDX Configuration Editor. Each field description includes a property name, which is used if you modify the properties with SDX Admin or a text editor.

Configuring the Length of Time MAC Addresses Remain in SAE Cache

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. To configure this time period in SDX Configuration Editor:

1. In the navigation pane, select a directory configuration object for the SAE that you want to configure.
2. Select the **Router** tab.

MAC Cache Expiration Time	1800
---------------------------	------

3. Fill in the field as described in *Max Cache Expiration Time Field* on page 50.

Max Cache Expiration Time Field

Use this field to configure the length of time that a subscriber profile remains in the SAE's in-memory cache.

MAC Cache Expiration Time

- Amount of time that a subscriber profile remains in the SAE's in-memory cache.
- Value—Number of seconds in the range 0–2147483647

- Guidelines—Configure this parameter to be greater than the time required for a DHCP subscriber to transition from an unauthenticated IP address to an authenticated IP address or vice versa. The time required for a DHCP subscriber to transition from one IP address to another depends on the lease times configured on the JUNOS router and the instructions given to the subscriber on the Web portal, such as reboot your PC now.
- Default—1800
- Property name—maxMacCacheEntryAge

Identifying a Profile for Unauthenticated Subscribers

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 with SDX Configuration Editor:

1. In the navigation pane, select a directory configuration object for the SAE that you want to configure.
2. Select the **Router** tab.



Unauthenticated User DN

3. Fill in the field as described in *Unauthenticated User DN Field* on page 51.

Unauthenticated User DN Field

Use the field in this section to specify the unauthenticated user DN.

Unauthenticated User DN

- Identifies a subscriber profile for unauthenticated access to the portal.
- Value— < DN >
- Default—
`uniqueID = unauthenticated, ou = local, retailerName = default, o = Users, < base >`
- Property name—Router.unauthUserDn

Configuring Interim Accounting for Services and Subscribers

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. You can override these settings for specific services by configuring an accounting interim interval in the value-added service configuration.

To configure interim accounting with SDX Configuration Editor:

1. In the navigation pane, select a directory configuration object for the SAE that you want to configure.
2. Select the **Miscellaneous** tab, and expand the **Interim Accounting** section.

Interim Accounting	
Service Interim Accounting	Yes
Service Interim Interval [s]	900
User Interim Accounting	Yes
User Interim Interval [s]	900

3. Fill in the fields as described in *Interim Accounting Fields* on page 52.

Interim Accounting Fields

Use the fields in this section to configure interim accounting.

Service Interim Accounting

- Enables or disables service interim accounting. If enabled, the SAE continually generates Interim-Update accounting requests for all active services at the interval specified in the Service Interim Interval field.
- Value—Yes or No
- Default—Yes
- Property name—AccountingMgr.interim.accounting.running

Service Interim Interval [s]

- Interval between service interim accounting messages. A short interval causes the SAE to send many messages to the router and to the RADIUS servers. A long interval can result in a large loss of accounting information in the event of a system failure.
- Value—Number of seconds in the range 900–86400
- Default—900
- Property name—AccountingMgr.interim.accounting.polling.interval

User Interim Accounting

- Enables or disables interim accounting for subscribers. If enabled, the SAE continually generates Interim-Update accounting requests for all active subscribers at the interval specified in the User Interim Interval field.
- Value—Yes or No
- Default—Yes
- Property name—AccountingMgr.user.interim.accounting.running

User Interim Interval [s]

- Interval between subscriber interim accounting messages. A short interval causes the SAE to send many messages to any configured accounting servers. A long interval can result in a large loss of accounting information in the event of a system failure.
- Value—Number of seconds in the range 900–86400
- Default—900
- Property name—AccountingMgr.user.interim.accounting.polling.interval

Avoiding Overcharges for Sessions That Time Out

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 to avoid overcharges for the session. To adjust the session time with SDX Configuration Editor:

1. In the navigation pane, select a directory configuration object for the SAE that you want to configure.
2. Select the **Miscellaneous** tab, and expand the **Idle Timeout** section.



The screenshot shows a configuration window with a tab labeled 'Idle Timeout'. Below the tab, there is a row with the label 'Adjust Session Time' and a dropdown menu currently showing 'Yes'. To the right of the dropdown is a small icon of a document with a pencil.

3. Fill in the field as described in *Idle Timeout Field* on page 54.

Idle Timeout Field

Use the field in this section to specify whether or not the session time reported in accounting stop messages are adjusted.

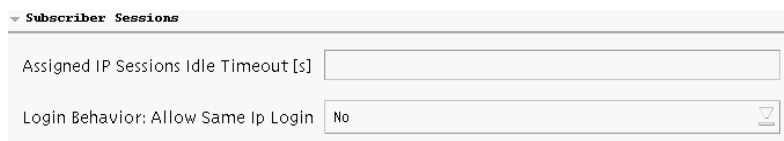
Adjust Session Time

- Specifies whether, when an idle timeout terminates a session, the session time reported in the accounting stop message is reduced by the idle time. This way the session time is accurately reported to avoid overcharges for the session.
- Value
 - True—Reduces the session time by the amount of time specified by the idle timeout
 - False—Does not reduce the session time by the amount of time specified by the idle timeout
- Default—True
- Property name—AccountingMgr.adjustSessionTime

Allowing Multiple Logins from the Same IP Address

You can specify whether or not the SAE allows multiple logins from the same IP address. To do so with SDX Configuration Editor:

1. In the navigation pane, select a directory configuration object for the SAE that you want to configure.
2. Select the **Miscellaneous** tab, and expand the **Subscriber Sessions** section.



▼ **Subscriber Sessions**

Assigned IP Sessions Idle Timeout [s]

Login Behavior: Allow Same Ip Login No

3. Fill in the Login Behavior: Allow Same IP Login field as described in *Allow Same IP Login Field* on page 54.

Allow Same IP Login Field

Use the field in this section to specify whether or not the SAE allows multiple logins from the same IP address.

Login Behavior: Allow Same IP Login

- Specifies whether the SAE allows a login from the same IP address without requiring that the previous session logs out first.
- Value
 - Yes—SAE logs in the new subscriber session and automatically logs out the previous session.
 - No —SAE denies login requests if a subscriber session for an IP address is active.
- Property name—UserManager.sameIpLogin

Authenticating Registered Username/Password Pairs

You can specify whether or not registered username/password pairs are authenticated. To do so with SDX Configuration Editor:

1. In the navigation pane, select a directory configuration object for the SAE that you want to configure.
2. Select the **Miscellaneous** tab, and expand the **Login Registration** section.



The screenshot shows a configuration window with a tab labeled 'Login Registration'. Below the tab, there is a field labeled 'Registration authentication' with a dropdown menu currently showing 'Yes'. A small icon is visible to the right of the dropdown.

3. Fill in the field as described in *Login Registration Field* on page 55.

Login Registration Field

Use the field in this section to specify whether or not registered username/password pairs are authenticated.

Registration authentication

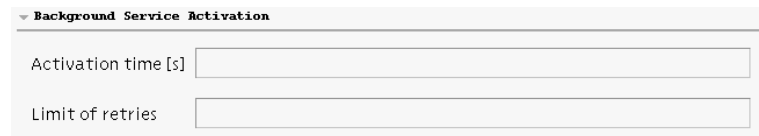
- Specifies whether the application programming interface (API) method registerLoginCredentials authenticates the registered username/password or creates the registration without authentication.
- Value—Yes or No
- Guidelines—Set to Yes if your authentication server does not allow authentication while a session for the authenticated username is active.
- Property name—RegisterLoginCredentials.authenticateRegistration

Configuring Timers for Session Reactivation

If a service session fails unexpectedly, the SAE tries to start the session again in the background. You can change how many times the SAE tries to activate the session and the interval between these attempts. In most instances, the default values do not need to be changed.

To configure session reactivation behavior with SDX Configuration Editor:

1. In the navigation pane, select a directory configuration object for the SAE that you want to configure.
2. Select the **Miscellaneous** tab, and expand the **Background Service Activation** section.



The screenshot shows a configuration window with a tab labeled 'Background Service Activation'. Below the tab, there are two input fields. The first field is labeled 'Activation time [s]' and the second field is labeled 'Limit of retries'.

3. Fill in the fields as described in *Background Service Activation Fields* on page 56.

Background Service Activation Fields

Use the fields in this section to configure service reactivation behavior for the SAE.

Activation time [s]

- Time between attempts to activate a service session if activation fails or to deactivate a service session if deactivation fails. This process takes place in the background.
- Value—Number of seconds in the range -1–9223372036854775807
-1 indicates no limit
- Default—60
- Property name—Service.background.retry_time

Limit of retries

- Number of times the SAE tries to activate a service session if activation fails or to deactivate a service session if deactivation fails. This process takes place in the background.
- Value—Integer in the range -1–21 474 836 47
-1 indicates no limit
- Default— -1
- Property name—Service.background.retry_limit

Modifying the SAE Property File

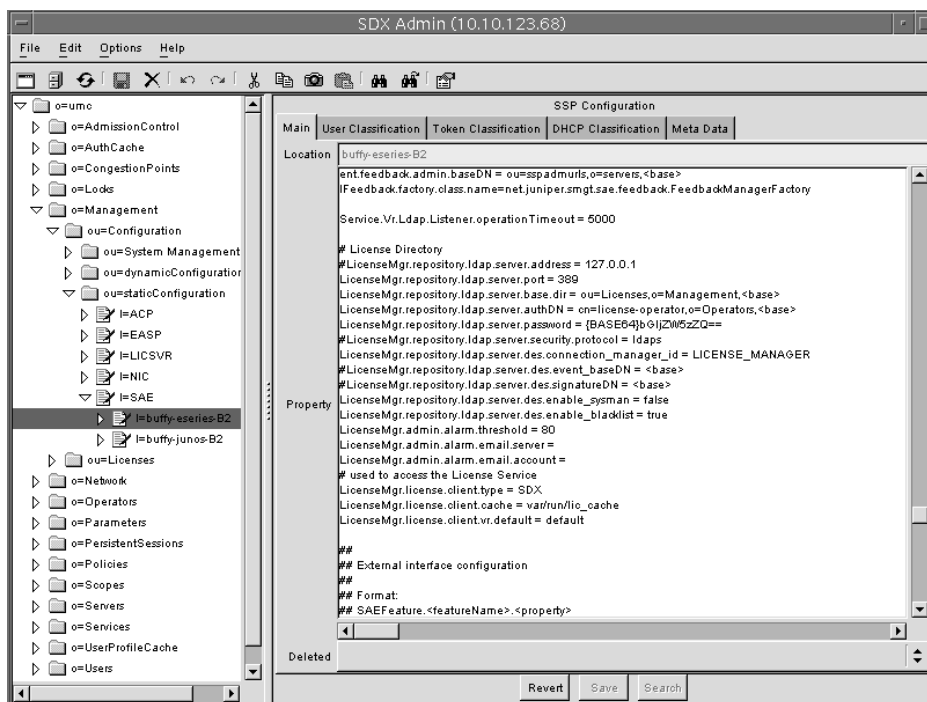
This section shows how to edit the property file with SDX Admin or a standard text editor. Use the property names that are included in field descriptions for properties in SDX Configuration Editor.

Editing Properties with SDX Admin

To edit the properties with SDX Admin:

1. In the SDX Admin navigation pane, access the object *I = SAE*, *ou = staticConfiguration*, *ou = configuration*, *o = management*, *o = umc*.
2. In this folder, click on the *I = POP-ID* object associated with this SAE.

The SAE configuration appears in the Main tab in the SSP Configuration pane.



3. Scroll to the text you want to edit, or click **Search** to find an item in the configuration file.
4. Add or modify the relevant information, and click **Save**.

Editing Properties with a Text Editor

To edit the properties with a text editor:

1. Open a shell in the directory in which you installed the SAE.

The default installation directory for SAE is */opt/UMC/sae*.

2. Download the properties to a file with the SAE configuration utility.

etc/config -g <filename>

A file called *<filename>* , which contains the SAE properties, appears in the *sae* subdirectory.

3. Edit the file with a text editor, such as VI or EMACS.
4. Update the object's file properties with the SAE configuration utility.

etc/config -p <filename>

Loading Subscriptions Based on RADIUS Authorization

You can set up the SAE to load subscriptions based on values that it receives in RADIUS authorization response packets. For this method of loading subscriptions to work, the subscriber must be subscribed to the service.

To use this feature, you set up the RADIUS authorization plug-in to return the *setLoadServices* attribute, and you specify a regular expression in the SAE property file. When the plug-in returns the *setLoadServices* attribute, the SAE applies the regular expression to the string in the *setLoadServices* attribute.

There are two SAE properties that you can use to set the expression:

- **SubscriptionParser.regex**—Specifies the regular expression that is used to match a single service name.
- **SubscriptionParser.auto**—Specifies the number of a group of services that corresponds to activate-on-login services. That is, if a subscription is matched by this group, it is activated.

For example:

```
SubscriptionParser.regex = ([^;!]*);|([^;!]*)!
SubscriptionParser.auto = 2
```

A group match corresponds to a regular expression that is enclosed in (). In this example, the regular expression in the subscription parser contains two groups:

1. A string of characters other than “;” and “!”, followed by “;”
2. A string of characters other than “;” and “!”, followed by “!”

The value of 2 in the `SubscriptionParser.auto` property causes the second group of services—services followed by `!`—to be activated on login. For example, if the `setLoadServices` string is `video-gold;audio-gold!`, it is parsed to `video-gold` and `audio-gold`. The `audio-gold` subscription is activated provided that the subscriber is subscribed to `audio-gold` services.



NOTE: Persistent service sessions are not parsed. That is, if a subscriber has activated persistent service sessions, then these sessions are activated independent of the RADIUS authorization responses.

Another way to load subscriber services based on RADIUS authorization is to use the `serviceBundle` vendor-specific attribute (VSA) as input to the subscriber classification script and load different subscriber profiles based on the RADIUS response. Different subscriber profiles subscribe to different services. This approach gives wholesalers a basic tool to outsource service subscriptions to a retailer. The wholesaler and retailer must agree on a RADIUS attribute (for example, `serviceBundle`) that is provided by the retailer and interpreted by the SAE (that is, the wholesaler).

The subscription parser properties are located in `/opt/UMC/sae/etc/dir.template`. (See *Modifying the SAE Property File* on page 57.)

SubscriptionParser.regex

- Regular expression that is applied to the `setLoadServices` attribute in RADIUS authorization response packets. The regular expression matches a single service name and is applied repeatedly until no match is found.
- Value—Regular expression; you can group matches by enclosing them in parenthesis `()`.
- Default—"`([^\;!]*);|([^\;!]*)!`"
- Property name—`SubscriptionParser.regex`

SubscriptionParser.auto

- Expression that identifies the number of a group of services that are to be activated automatically. If a subscription is matched by this group, it is automatically activated.
- Value—Expression
- Default—2
- Example—The default regular expression corresponds to a string of service names that are separated by `,` or `!`. If a service name is followed by `!`, it is activated automatically.
- Property name—`SubscriptionParser.auto`

Accepting Login Names with Different Formats

You can configure the SAE to accept login names of different formats. For example, the format `subscriberName@domainName` is a common format for the login name of subscribers who connect through PPP; however, other subscribers may use other formats, such as `domainName/userName`.

To configure the SAE to accept these different formats, you specify a set of properties that parse the login name to obtain the `userName` and `domainName` objects for the subscriber. Each property contains a regular expression that includes one or two subexpressions—*independent expressions in the complete regular expression*—each of which is enclosed in parentheses.

The property for login name parsing has the form:

```
LoginName.parser.<number>.<userGroup>[.<domainGroup>] = \
<regular expression>
```

number

- Number that specifies the order in which the SAE should apply the property when it parses the `loginName`. The SAE applies the properties in the specified order from lowest to highest.

userGroup

- Number of the backreference that extracts the username.
- In the following example, the `userGroup` backreference is set to 1. This means that the first backreference in the expression `([^\@]*)` identifies the username:
`LoginName.parser.1.1.2 = ([^\@]*)@(.*)`

domainGroup

- Optional number of the backreference that extracts the domain name.
- In the following example, the `domainGroup` backreference is set to 1. Therefore, the first backreference in the expression `([^\@]*)` identifies the domain name:
`LoginName.parser.2.2.1 = ([^\@]*)/(.*)`

regular expression

- Regular expression that includes one or two subexpressions—*independent expressions in the complete regular expression*—each of which is enclosed in parentheses.
- When you define regular expressions for a domain name parser, you must include four backslashes (`\\`) to effect a single backslash. For example, suppose you define the following parser:

```
LoginName.parser.1.2.1 = (.*)[\\]\\(.*)
```

This example parses the login name `isp1\jane` as:

```
domain name: isp1
username: jane
```

- For more information about using regular expressions for this feature, see: <http://jakarta.apache.org/regexp/apidocs/org/apache/regexp/RE.html>

Default Login Parser Properties

Table 10 shows default properties that the SAE uses to parse login names. Table 11 shows some examples of subscriber and domain names obtained through the default parsing properties.

Table 10: Default SAE Properties That Parse Login Names

Property	Function	Values
LoginName.parser.1.1.2 = <code>([^\@]*)@(.*)</code>	Parses login names of the format <code>userName@domainName</code>	LoginName.parser.1.1.2—First parser applied by the SAE to login names; first backreference identifies the username, and second backreference identifies the domain name. <code>([^\@]*)</code> —First backreference: username is a string of characters other than the at-sign (<code>@</code>). <code>@</code> —An at-sign precedes the domain name. <code>(.*)</code> —Second backreference: domain name is a string of characters.
LoginName.parser.2.2.1 = <code>([^\/]*)/(.*)</code>	Parses login names of the format <code>domainName/userName</code>	LoginName.parser.2.2.1—Second parser applied by the SAE to login names; second backreference identifies the subscriber name, and first backreference identifies the domain name. <code>([^\/]*)</code> —First backreference: domain name is a string of characters other than the forward slash (<code>/</code>). <code>/</code> —A forward slash precedes the username. <code>(.*)</code> —Second backreference: username is a string of characters.
LoginName.parser.3.1 = <code>(.*)</code>	Parses login names that contain no domain name	LoginName.parser.3.1—Third parser applied by the SAE to login names; first backreference identifies the username, no domain name. <code>(.*)</code> —First backreference: username is a string of characters.

Table 11: Examples of Subscriber and Domain Names Obtained from Default Properties

Login Name	Output from Default Parsing Properties
joeUser@isp1.com	<ul style="list-style-type: none"> ■ The username is joeUser. ■ The domain name is isp1.com.
isp1/joe	<ul style="list-style-type: none"> ■ The username is joe. ■ The domain name is isp1.
isp1/joe@isp2	<ul style="list-style-type: none"> ■ The username is isp1/joe. ■ The domain name is isp2.

Chapter 6

Classifying Interfaces and Subscribers with the SRC CLI

This chapter provides information for configuring and using classification scripts with the SRC command line interface (CLI).

You can also use SDX Admin to configure classification scripts on Solaris platforms. See *Chapter 7, Classifying Interfaces and Subscribers on a Solaris Platform*.

Topics in this chapter include:

- Overview of Classification Scripts on page 63
- Overview of Configuring Classification Scripts on page 66
- Classifying Interfaces on page 70
- Classifying Subscribers on page 76
- Classifying DHCP Subscribers on page 86
- Selecting DHCP Parameters on page 89
- Creating DHCP Profiles on page 92

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* on page 16 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* on page 132 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 `start` 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

Use the following configuration statements to define interface classification scripts:

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

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

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 define interface classification scripts:

1. From configuration mode, enter the interface classifier configuration for a device.

```
user@host# edit shared network device erx-node1 interface-classifier
```

2. Create a rule for the subscriber classifier. You can create multiple rules for the classifier.

```
[edit shared network device erx-node1 interface-classifier]
user@host# edit rule rule-3
```

3. Configure either a target or a script for the rule.

```
[edit shared network device erx-node1 interface-classifier rule rule-3]
user@host# set script script
```

OR

```
[edit shared network device erx-node1 interface-classifier rule rule-3]
user@host# set target target
```

4. If you configured a target for the rule, you must configure a match condition for the rule. You can create multiple conditions for the rule. See *Interface Classification Conditions* on page 72.

```
[edit shared network device erx-node1 interface-classifier rule rule-3]
user@host# set condition name
```

5. (Optional) Change the order of rules.

```
[edit shared network device erx-node1 interface-classifier]
user@host# insert rule rule-5 before rule-4
```

6. (Optional) Rename a rule.

```
[edit shared network device erx-node1 interface-classifier]
user@host# rename rule rule-5 to DHCP
```

7. (Optional) Verify the classifier rule configuration.

```
[edit shared network device erx-node1 interface-classifier rule rule-3]
user@host# show
target /sample/junose/PPP-special;
condition {
  "pppLoginName=\"*@special.com\"";
}
```

8. (Optional) Verify the interface classifier configuration.

```
[edit shared network device erx-node1 interface-classifier]
user@host# show
rule rule-1 {
  script "
# Use the following syntax:
#
# descr-file ::= [script] section*
# section    ::= ('[' type ']' nl conditions) | ('[*]' nl script)
# type       ::= 'a-zA-Z0-9-_*'
# nl         ::= '\\n'
# conditions ::= ((('#'|';') comment) |
#                 (['&'|'|'] field-name ( '='|'=='|'!=') match) nl)*
# field-name ::= member of InterfaceObject
# match      ::= UNIX style filename matching
# script     ::= regular python script, defined functions need to be
#                 included in the list \"classify\"
#
# the section-names correspond to a PolicyList object below
# o=Policies, o=umc:
# [name] => DN: \"policyGroupName=name, o=Policies, o=umc\"
#
# Use one of the following \"field names\":
# pppLoginName      - set to \"user@realm\", if interface is PPP
# interfaceName     - name of the ERX Interface in CLI syntax
# virtualRouterName - name of the VR the interface is connected to

";
}
rule rule-2 {
  script "
# apply different default policies for PPP subscribers in realm
\"special.com\"
def log(obj):
    from net.juniper.smgmt.sae import Main
    icc = Main.theComponentRegistry.get(\"icc.component\")
    if icc is None:
        Main.theComponentRegistry.put(\"icc.component\", [])
    else:
        icc.append(obj)
classify.append(log)
";
}
rule rule-3 {
  target /sample/junose/PPP-special;
  condition {
    "pppLoginName=\"*@special.com\"";
  }
}
rule rule-4 {
  target /sample/junose/PPP;
  condition {
```

```

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

```

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”

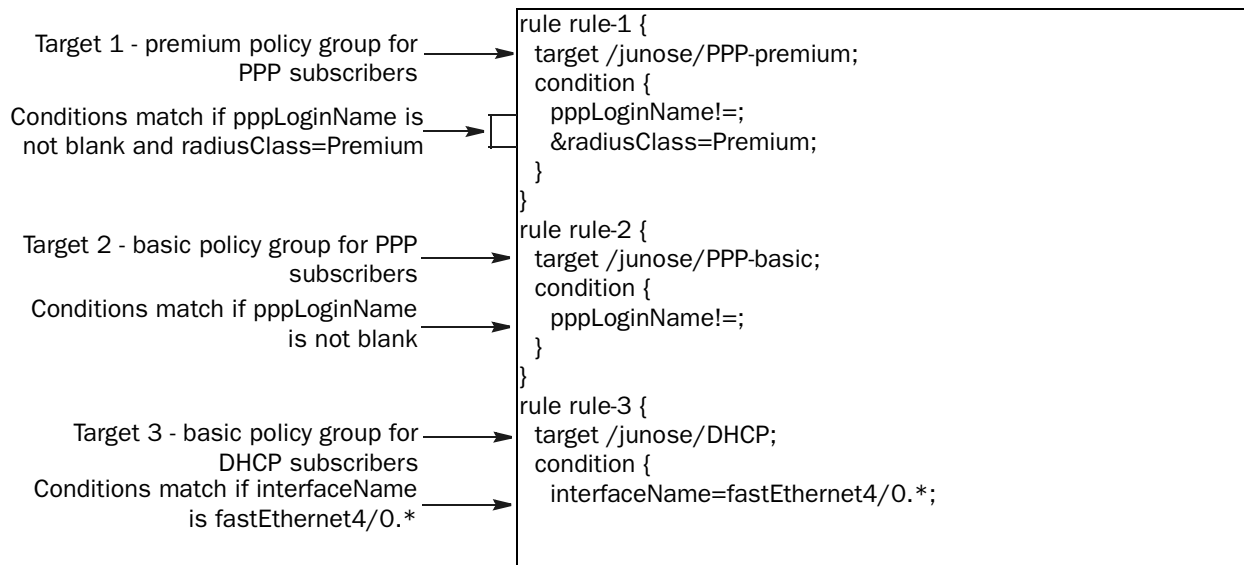
virtualRouterName

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

Example: Managing Interfaces for Premium and Basic PPP and DHCP Subscribers

In this scenario, the router manages two types of PPP interfaces—DHCP subscriber interfaces and static IP interfaces. The `fastEthernet4/0.1` to `fastEthernet4/0.999` interfaces are VLAN interfaces used to terminate DHCP subscribers.

The service provider has separated the PPP subscribers into a premium subscriber group and a basic subscriber group. These groups are distinguished by a different set of default policies applied to the PPP interface. The RADIUS class attribute in the RADIUS profile for premium subscribers is set to Premium. The rules in the interface classification script for this scenario are:



The script is processed as follows:

1. If `pppLoginName` is not blank and `radiusClass` is Premium, the PPP-premium policy group is sent to the SAE, and script processing stops.
2. If script processing proceeds and `pppLoginName` is not blank, the PPP-basic policy group is sent to the SAE, and script processing stops.
3. If script processing proceeds and `interfaceName` is `fastEthernet 4/0.0` through `fastEthernet 4/0.999`, the DHCP policy group is sent to the SAE, and script processing stops.

Example: Managing Specific Interfaces

This example causes the SAE to load the DHCP policy group on IP interfaces on Fast Ethernet modules in slot 3/port 1, slot 1/port 1, or any port on slot 2. The SAE then manages these interfaces.

```
[edit shared network device erx-node2 interface-classifier rule rule-1]
user@host# show
target /junose/DHCP;
condition {
    interfaceName=FastEthernet3/1;
    interfaceName=FastEthernet1/1;
    interfaceName=FastEthernet2/*;
}
```

Example: Managing Interfaces by Using the Interface Description

This example causes the SAE to load the DHCP policy group on any interface where the ifAlias starts with DHCP-subscribers.

```
[edit shared network device erx-node2 interface-classifier rule rule-2]
user@host# show
target /junose/DHCP;
condition {
    ifAlias=DHCP-subscribers*;
}
```

For this approach, you will need to use the `ip description` command to configure interface aliases that begin with DHCP-subscribers for all interfaces that support DHCP subscribers.

Classifying Subscribers

Changes that you make to subscriber classification scripts do not affect subscriber sessions that are already established. One effect of this behavior is that static IP subscriber sessions are not closed if the classification script is changed in a way that would no longer cause the SAE to load a profile for certain subscribers.

On JUNOS routers that use the COPS-PR or COPS XDR router drivers, you can create a subscriber session for the router interface to start services such as script services and aggregate services. The SAE creates the router interface, but does not install any policies on it. You can create a subscriber classification rule, but not an interface classification rule for this interface.

Use the following configuration statements to define subscriber classification scripts:

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

```
shared sae subscriber-classifier rule name condition name ...
```

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 define subscriber classification scripts:

1. From configuration mode, enter the subscriber classifier configuration. In this sample procedure, the subscriber classifier is configured in the west-region SAE group.

```
user@host# edit shared sae group west-region subscriber-classifier
```

2. Create a rule for the subscriber classifier. You can create multiple rules for the classifier.

```
[edit shared sae group west-region subscriber-classifier]
user@host# edit rule rule-2
```

3. Configure either a target or a script for the rule.

```
[edit shared sae group west-region subscriber-classifier rule rule-2]
user@host# set target target
```

OR

```
[edit shared sae group west-region subscriber-classifier rule rule-2]
user@host# set script script
```

If you configure a target, see *Subscriber Classification Targets* on page 83.

4. If you configured a target for the rule, configure a match condition for the rule. You can create multiple conditions for the rule. See *Subscriber Classification Conditions* on page 79.

```
[edit shared sae group west-region subscriber-classifier rule rule-2]
user@host# edit condition name
```

5. (Optional) Change the order of rules.

```
[edit shared sae group west-region subscriber-classifier]
user@host# insert rule rule-5 before rule-4
```

6. (Optional) Rename a rule.

```
[edit shared sae group west-region subscriber-classifier]
user@host# rename rule rule-5 to Retailer
```

7. (Optional) Verify the classifier rule configuration.

```
[edit shared sae group west-region subscriber-classifier rule rule-2]
user@host# show
target <-unauthenticatedUserDn->;
condition {
    "loginType == \"ADDR\"";
    "loginType == \"AUTHADDR\"";
}
```

8. (Optional) Verify the subscriber classifier configuration.

```
[edit shared sae group west-region subscriber-classifier]
user@host# show
rule rule-1 {
    script "# User Classification script
#
# The following attributes MAY be available for comparison.
# Attributes that are not available will have the value \"\" (empty
string).
#
# loginType: one of \"INTF\", \"AUTHINTF\", \"ADDR\", \"AUTHADDR\",
#             \"PORTAL\", \"ASSIGNEDIP\"
# userName: Everything before the \"@\" in the user's login name.
# domainName: Everything after the \"@\" in the user's login name.
# serviceBundle: A RADIUS VSA available if the login event involves
#                 authentication with a properly configured RADIUS server.
# radiusClass: The RADIUS class of user's ERX interface.
# virtualRouterName: The name of the user's virtual router.
# interfaceName: The name of the user's ERX interface (e.g.
#                 \"fastEthernet3/1.0\")
# ifAlias: The alias of the user's ERX interface, as configured on the
ERX.
# ifDesc: The description of the user's ERX interface, as configured on
#          the ERX.
# nasPortId: The user's ERX interface including Layer 2 access information
#             (e.g. \"fastEthernet 3/1.0:3\")
# macAddress: The MAC address of the user, if he is a DHCP user.
# retailerDn: Generated by SSP for backwards compatibility; see below.
#
# The loginType value available to this user classifier script will be
# one of the following:
#
# \"INTF\":
# An INTF login is triggered every time an interface comes up and the
# interface classifier script determines that SAE should manage that
# interface, and the interface has not been authenticated by the router.
#
```

```

# \"AUTHINTF\":
# An AUTHINTF login is triggered every time an authenticated
# interface comes up, for example as a result of an authenticated PPP
# session.
#
# \"ADDR\":
# An ADDR login is triggered every time an 'unauthenticated' IP
# address is handed out by the DHCP server in the ERX.
#
# \"AUTHADDR\":
# An AUTHADDR login is triggered every time an 'authenticated' IP
# address is handed out by the DHCP server in the ERX.
#
# \"PORTAL\":
# A PORTAL login is triggered every time the portal API is invoked to
# login a user.
#
# See the customer documentation for a description of the values
# for each login type available in the script.
#
# One of the values available during some types of logins is the
# 'retailerDn'. This is a generated value available for backwards
# compatibility with previous versions of SAE. SAE generates this
# value as follows:
#
# The retailerDn value is generated by, first, determining an
# effective user domain name, and second, locating the retailer
# entry in LDAP that contains that effective domain name. If no
# such retailer exists, the retailerDn value will be \"\".
#
# The effective user domain name is the first of the following that yields
# a result:
#
# 1. For PPP, PORTAL, and PUBLIC logins where a non-empty domainName
#    is supplied, that non-empty domain name is used as the effective
#    domain name.
#
# 2. For INTF logins, and for PPP, PORTAL, and PUBLIC logins where a
#    non-empty domain name is not supplied, the effective domain name
#    is the name of the user's virtual router, unless that effective
#    domain does not exist in some retailer in LDAP.
#
# 3. If neither step 1 nor step 2 yields an effective domain name,
#    \"default\" is used as the effective domain name.
#
";
}
rule rule-2 {
  target <-unauthenticatedUserDn->;
  condition {
    "loginType == \"ADDR\"";
    "loginType == \"AUTHADDR\"";
  }
}
rule rule-3 {
  target <-retailerDn->??sub?(uniqueID=<-userName->);
  condition {
    "retailerDn != \"\"";
    "& userName != \"\"";
  }
}
}

```

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 JUNOS Router* on page 82.

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 JUNOS routers, it is the description configured with the **interface description** command
- Example—ifAlias = “dhcp-subscriber1 2”

ifDesc

- Alternate name for the interface that is used by SNMP. This name is a system-generated name.
- Value
 - On a JUNOS 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 JUNOS router instance
- Example—For JUNOS 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 JUNOS 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
- <Login name>
- 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.
- 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 JUNOS 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 JUNOS 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 JUNOS routers.)
 - ADDR—For unauthenticated address login requests. Triggered when the DHCP server in the JUNOS router provides an unauthenticated IP address. (Supported on JUNOS routers.)
 - AUTHADDR—For authenticated address login requests. Triggered when the DHCP server in the JUNOS router provides an authenticated IP address. (Supported on JUNOS routers.)
 - PORTAL—Triggered when the portal API is invoked to log in a subscriber. (Supported on JUNOS routing platforms and JUNOS 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 JUNOS 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 JUNOS Router

Subscriber classification scripts support DHCP options conveyed through COPS. When COPS reports an address, the JUNOS 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 12 are in the classification context of subscriber classification scripts.

Table 12: 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()	
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.
- 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.

Example: Subscriber Classification Scripts for Static IP Subscriber

In cases such as bridged 1483 DSL with a single subscriber, you can write the subscriber classification script so that it loads a specific subscriber profile. If the interface is matched to a subscriber profile, a subscriber session is immediately established. An SAE application (for example, a portal) can still force the subscriber with this subscriber profile to perform a Web login.

One way to achieve the mapping of subscriber interface to subscriber profile is to provision the assigned interface name in the associated subscriber profile in LDAP. In this case the subscriber classification script can include a rule like this:

```
[edit shared sae group west-region subscriber-classifier rule rule-1]
user@host# show
target retailerName=default,o=Users,o=umc??sub?(interfaceName=<-interfaceName->);
condition {
    "loginType=="INTF\ "";
    "&interfaceName=fastEthernet*";
}
```

Another way may include a special encoding of the interface alias (ifAlias) field of the subscriber interface. This encoding must then be provisioned when the interface for the subscriber is provisioned. In this example, the encoding SAE-username is chosen for ifAlias; for example, for subscriber juser the interface alias would be set to SAE-juser. The match is performed with a regular expression, which separates the user ID from the ifAlias prefix.

```
[edit shared sae group west-region subscriber-classifier rule rule-1]
user@host# show
target retailerName=default,o=Users,o=umc??sub?(uniqueID=<-userId>);
condition {
  "loginType=="INTF\"";
  "&ifAlias=~SAE-(?P<userId>.*)"
}
```

Example: Subscriber Classification Scripts Using a Subscriber Group

To support scenarios in which the SAE has no access to the subscriber database, the SAE can load anonymous profiles for groups of subscribers. The following example loads a particular subscriber profile when subscribers of domain another-isp.com log in

```
[edit shared sae group west-region subscriber-classifier rule rule-1]
user@host# show
target uniqueID=anon,ou=default,retailerName=another-isp,o=Users,o=umc;
condition {
  "domainName=another-isp.com"
}
```

Example: Subscriber Classification Scripts for Enterprise Subscribers

For enterprise subscribers, you can create one general subscriber classifier script that matches a unique subscriber profile to each managed router interface. The subscriber profile is the access subscription that represents an Internet access in an enterprise. The following examples show two approaches to creating the general classifier script. You can use one of these strategies or a combination of strategies.

Matching on the Interface Name

In this scenario, you configure the interface name field in the access subscription for the site to match an interface on the router. The format for the interface name could be: interfaceName@virtualRouterName@routerName. You then create a classification script that searches for subscriber profiles that match a specific interface. For example:

```
[edit shared sae group west-region subscriber-classifier rule rule-1]
user@host# show
target ou=Managed
CPE,retailerName=Retailer-Two,o=Users,o=UMC??sub?(interfaceName=<-interfaceName->@<-virtualRouterName->);
condition {
  "loginType=="INTF\"";
  "&interfaceName=="fe*\"";
}
```

Matching on the Interface Alias

For JUNOSe routers, you can configure the interface description on the router in a format that the classifier script can match to the interface alias in an access subscription. In a simple case, you can configure the interface description only for interfaces that terminate a managed CPE, and match them to the interface alias in the directory. The subscriber classifier could be configured as follows:

```
[edit shared sae group west-region subscriber-classifier rule rule-1]
user@host# show
target ou=Managed CPE,retailerName=Retailer-Two,o=Users,o=UMC??sub?(interfaceAlias=<-ifAlias->);
condition {
    ifAlias != \"\"
}
```

Example: Creating Router Interface Subscriber Session

Aggregate services or script services can be activated on a router instead of an interface or DHCP address. On JUNOSe routers that use the COPS-PR or COPS XDR router driver, the SAE automatically creates a router interface; and then a subscriber session as specified by the subscriber classification script.

For example, the following script searches for a router profile in the directory under ou = routers, retailerName = default, o = Users, o = umc, with a routerName attribute that matches the virtual router name (such as default@erx-node1).

```
[edit shared sae group west-region subscriber-classifier rule rule-1]
user@host# show
target ou=routers,retailname=default,o=Users,o=UMC??sub?(routerName=<-virtualRouterName->);
condition {
    "interfaceName=="Router\"";
}
```

Example: Activating Services for a Group of Subscriber Sessions

A subscriber classification script can assign a shared subscriber profile and a login name to a subscriber session for a group of interface subscriber sessions. The following example assigns the login name idp@idp to subscriber sessions for JUNOSe interfaces that have core specified as the ifAlias (as configured on the JUNOSe router).

```
[edit shared sae group IDP subscriber-classifier rule rule-3]
root@buffy# show
target routerName=idp,ou=interfaces,retailname=SP-IDP,o=Users,o=UMC?loginName=idp@idp;
condition {
    "ifAlias=="core\"";
}
```

You can use this type of subscriber classification to activate a service for a group of interface subscriber sessions that are to be treated the same. For example, in the configuration for an aggregate service, a fragment service could be created for all subscriber interface sessions on interfaces identified by the ifAlias core on a virtual router. The subscriber reference expression in the configuration for the fragment service would reference the virtual router name and the login name, such as vr = "<- virtualRouterName ->", login_name = "idp@idp."

You can also use the SAE CORBA remote API to get lists of the subscriber sessions that share the same login name.

Classifying DHCP Subscribers

Use the following configuration statements to configure DHCP classification scripts:

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

```
shared sae dhcp-classifier rule name condition name ...
```

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. From configuration mode, enter the DHCP classifier configuration. In this sample procedure, the classifier is configured in the west-region SAE group.

```
user@host# edit shared sae group west-region dhcp-classifier
```

2. Create a rule for the subscriber classifier. You can create multiple rules for the classifier.

```
[edit shared sae group west-region dhcp-classifier]
user@host# edit rule rule-1
```

3. Configure either a target or a script for the rule.
4. (Optional) Configure the target for the rule.

```
[edit shared sae group east-region dhcp-classifier rule rule-1]
user@host# set target target
```

OR

```
[edit shared sae group east-region dhcp-classifier rule rule-1]
user@host# set script script
```

If you configure a target, see *DHCP Classification Targets* on page 89.

5. If you configured a target for the rule, configure a match condition for the rule. You can create multiple conditions for the rule. See *DHCP Classification Conditions* on page 87.

```
[edit shared sae group east-region dhcp-classifier rule rule-1]
user@host# edit condition name
```

6. (Optional) Change the order of rules.

```
[edit shared sae group east-region dhcp-classifier]
user@host# insert rule rule-5 before rule-4
```

7. (Optional) Rename a rule.

```
[edit shared sae group east-region dhcp-classifier]
user@host# rename rule rule-2 to dhcp
```

8. (Optional) Verify the classifier rule configuration.

```
[edit shared sae group east-region dhcp-classifier rule rule-1]
user@host# show
target cn=default,<-dhcpProfileDN->;
condition {
  1;
}
```

9. (Optional) Verify the DHCP classifier configuration.

```
[edit shared sae group west-region dhcp-classifier]
user@host# show
rule rule-1 {
  script "# DHCP classification script
#
# The DHCP classification script can use the following fields:
#
# interfaceName      - interface where DHCP DISCOVER was received.
# ifAlias             - \"ip description\" of interface
# ifDesc              - SNMP standard name of interface
# nasPortId           -
# virtualRouterName   - VR where DHCP DISCOVER was received
# macAddress          - MAC address of DHCP client
# dhcp                - DHCP options
# poolName            - DHCP Pool name set by authorization plug-in
# authVirtualRouterName - VR name set by authorization plug-in
# dhcpProfileDN        - search base for DHCP Profiles

";
}
rule rule-2 {
  target cn=default,<-dhcpProfileDN->;
  condition {
    1;
  }
}
```

DHCP Classification Conditions

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

authVirtualRouterName

- Name of JUNOS virtual router that is set by an authorization plug-in through the authorization response.
- Value—Name of the virtual router in the format `vrname@hostname`

dhcp

- DHCP options. See *Setting DHCP Parameters with DHCP Options* on page 90.

dhcpProfileDN

- Search base for DHCP profiles. The DN can be used in target expressions.
- Value—DN of DHCP profile

interfaceName

- Name of the interface where the DHCP discover message was received.
- Value—Name of the interface in your router CLI syntax
- Example—interfaceName = fastEthernet6/0

ifAlias

- Description of the interface where the DHCP discover request was received.
- 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-subscriber1 2”

ifDesc

- Alternate name for the interface where the DHCP discover request was received. This is a system-generated name that is used by SNMP.
- 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.

macAddress

- MAC address of the DHCP client that appears in DHCP request.
- 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.)

poolName

- IP address pool name that is set by an authorization plug-in through the authorization response.
- Value—Name of an address pool configured on the JUNOSe router

virtualRouterName

- Name of the virtual router.
- Value—Name of the virtual router in the format `vrname@hostname`

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* on page 87.

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 JUNOS 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.

For more information about how the SAE handles DHCP subscribers, see:

- Assigning DHCP Addresses to Subscribers on page 132
- DHCP Subscriber Login and Service Activation on page 22

Setting DHCP Parameters with DHCP Options



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

DHCP servers use DHCP options to configure DHCP clients. The DHCP local server in the JUNOS 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 13 on page 90 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.

Table 13: 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
cookie-servers	8	ip-address
lpr-servers	9	ip-address
impress-servers	10	ip-address

Table 13: DHCP Options Supported on the SAE (continued)

Option Name	Option Number	Option Type
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
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

Table 13: DHCP Options Supported on the SAE (continued)

Option Name	Option Number	Option Type
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
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
nnntp-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

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.

You can also create DHCP profiles manually with SDX Admin or by adding DHCP profile entries to the directory. 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.

For more information about how the SAE handles DHCP subscribers, see:

- Assigning DHCP Addresses to Subscribers on page 132
- DHCP Subscriber Login and Service Activation on page 22

Use the following configuration statements to create a DHCP profile:

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

To create a DHCP profile:

1. From configuration mode, enter the DHCP cached authentication profile configuration.

```
user@host# edit shared auth-cache cached-dhcp-profile default
```

2. (Optional) Configure a description for the profile.

```
[edit shared auth-cache cached-dhcp-profile default]
user@host# set description description
```

3. (Optional) Configure the name of the IP address pool on the JUNOS router from which a DHCP address is selected.

```
[edit shared auth-cache cached-dhcp-profile default]
user@host# set pool-name pool-name
```

4. (Optional) Configure the fixed IP address that is offered to the DHCP client if the client is part of a network in the configured DHCP pool.

```
[edit shared auth-cache cached-dhcp-profile default]
user@host# set ip-address ip-address
```

5. (Optional) Configure the DHCP options that are used to configure DHCP clients.

```
[edit shared auth-cache cached-dhcp-profile default]
user@host# set dhcp-options dhcp-options
```

6. (Optional) Configure the name of the server used to boot the DHCP client.

```
[edit shared auth-cache cached-dhcp-profile default]
user@host# set boot-server-name boot-server-name
```

7. (Optional) Configure the name of a boot file used to boot the DHCP client.

```
[edit shared auth-cache cached-dhcp-profile default]
user@host# set boot-file-name boot-file-name
```

8. (Optional) Configure the name of the JUNOS virtual router that holds the IP address pool.

```
[edit shared auth-cache cached-dhcp-profile default]
user@host# set virtual-router virtual-router
```

9. (Optional) Configure the name of the JUNOS interface that is used to check the validity of system-created DHCP profiles.

```
[edit shared auth-cache cached-dhcp-profile default]
user@host# set local-interface local-interface
```

10. (Optional) Configure the length of time the supplied IP address is valid.

```
[edit shared auth-cache cached-dhcp-profile default]
user@host# set lease-time lease-time
```

11. (Optional) Configure the name of DHCP user without the domain name.

```
[edit shared auth-cache cached-dhcp-profile default]
user@host# set user-name user-name
```

12. (Optional) Configure the vendor-specific RADIUS attribute that specifies the SRC service bundle to use.

```
[edit shared auth-cache cached-dhcp-profile default]
user@host# set service-bundle service-bundle
```

13. (Optional) Configure the RADIUS attribute class.

```
[edit shared auth-cache cached-dhcp-profile default]
user@host# set radius-class radius-class
```

14. (Optional) Verify your configuration.

```
[edit shared auth-cache cached-dhcp-profile default]
user@host# show
description "This DHCP profile is used to select addresses from the
\"default\"
pool.";
virtual-router *;
local-interface *;
```

Chapter 7

Classifying Interfaces and Subscribers on a Solaris Platform

This chapter provides information for configuring and using classification scripts with SDX Admin.

You can also use the SRC CLI to configure classification scripts on the C-series platform or on a Solaris platform. See *Chapter 9, Configuring Internal, External, and Synchronization Plug-Ins with the SRC CLI*.

Topics in this chapter include:

- Overview of Classification Scripts on page 95
- Configuring Classification Scripts on page 98
- Testing Subscriber and Interface Classification Scripts on page 103
- Classifying Interfaces on page 104
- Classifying Subscribers on page 108
- Classifying DHCP Subscribers on page 117
- Selecting DHCP Parameters on page 120
- Creating DHCP Profiles on page 123

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 session 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 *criteria*.

- 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 in the directory. The result of interface classification scripts is a policy group in the directory.
- Criteria are match criteria. The script attempts to match criteria in the script to information sent from the router. For example, match criteria for a subscriber classification script might be login type or domain name. Match criteria 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 criteria. When an object needs classification, the script processes the targets in turn. Within each target, the script processes criteria sequentially. When it finds that the classification criteria 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 criteria sequentially as the criteria appear in the script, you should put more specific criteria at the beginning of the script and less specific criteria 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 criteria in the interface classification script. The script examines each criterion in sequential order to find a match.

- If it finds a match, the script processing stops, and the target for that criterion is returned to the SAE. The target is the distinguished name (DN) of a policy group in the directory. 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 command-line interface (CLI) remain in effect. The SAE does not install policies, and the JUNOS router does not send reports for this interface anymore.

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* on page 16 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 when the subscriber attempted to log in (for example, interface name, 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 criteria in the subscriber classification script. The script examines each criterion in sequential order to find a match.

- If it finds a match, the script processing stops, and the target for the matching criterion is returned to the SAE. The target is an LDAP query that uniquely identifies a subscriber entry in the directory. The SAE loads the subscriber entry from the directory 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 on the interface.

DHCP Classification Scripts

DHCP classification scripts choose DHCP profiles. See *Assigning DHCP Addresses to Subscribers* on page 132 for information about how DHCP classification scripts are used.

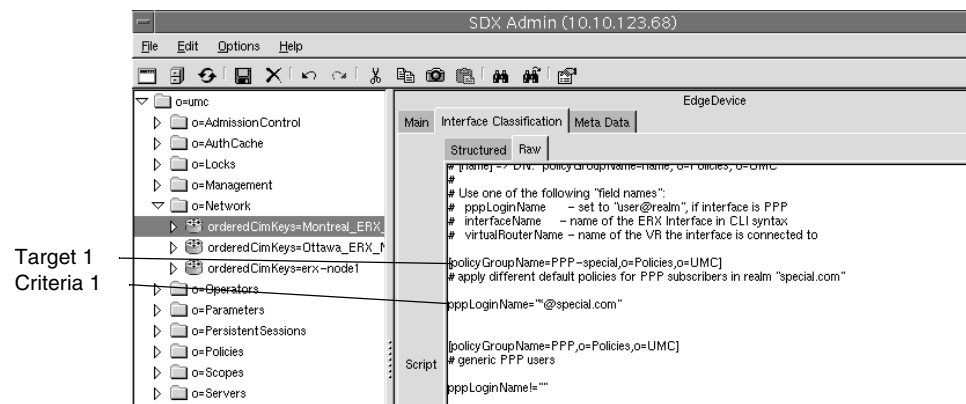
Configuring Classification Scripts

Classification scripts are organized into sections. Each section has a target and one or more classification criteria. The general layout of a classification script is that targets are enclosed in square brackets ([]) and precede their criteria:

```
[target-1] (see Figure 20)
  criteria-1 (see Figure 20)
  criteria-2
```

```
[target-2]
  criteria-1
  criteria-2
```

Figure 20: Target and Criteria Structure



Classification Targets

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

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

Target Expressions

A target can contain expressions. These expressions can refer to an object in the SAE's memory or configuration, to specific matching criteria, 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]` return the element index of a sequence. The first element is at index 0.
- Slicing—`var[start : end]` create a substring of the variable `var` starting at index `start` to, but not including, index `end`; for example, `var = Hello`, `var[2:4] = ll`

Classification Criteria

You organize classification criteria by putting one criterion per line, and joining a criterion with the previous criterion by:

- OR if the line does not contain a prefix or if it is prefixed with a `|` (pipe) character. A criterion joined by OR is examined only if the previous conditions have not produced a positive match. If any of the criteria joined by OR matches, the target is selected.
- AND if the line is prefixed with an `&` (ampersand) character. A criterion joined by AND is examined only if the previous condition matches.

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

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` # match the string “fastEthernet3/0” directly
- `interfaceName = fast*3/1` # match any string that starts with “fast” and ends with “3/1”
- `interfaceName = fast*3/1.*` # start with “fast”, contains “3/1.” arbitrary ending
- `interfaceName = fast*3/[2-57]` # start 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]"

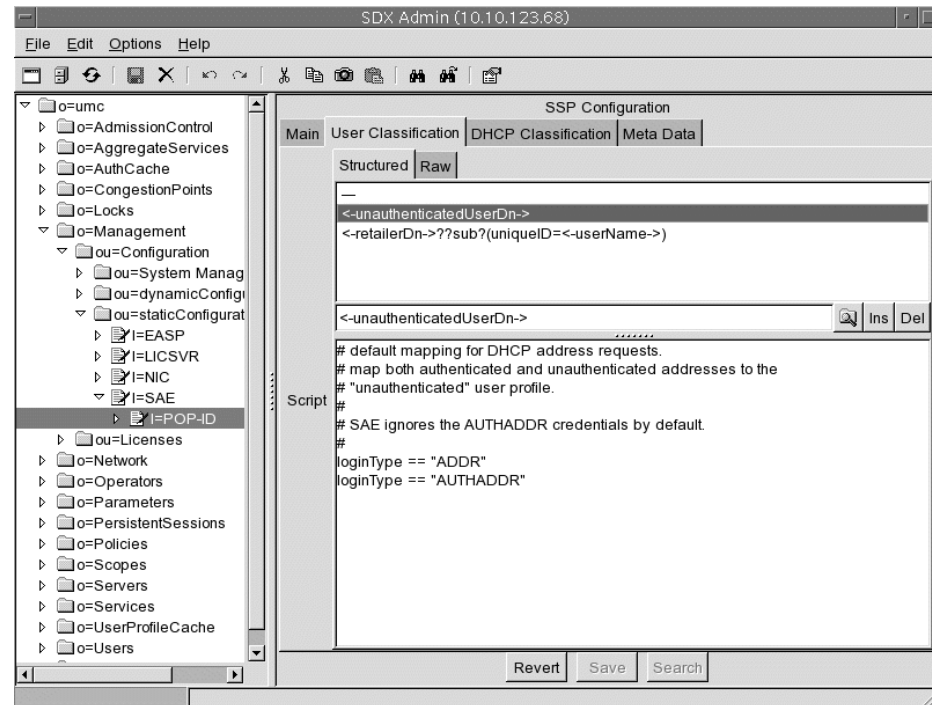
ifAlias =~ (?P<dn>name=(?P<name>[^,]*).*)
# match a string starting with "name=". The whole match is
# stored in the variable "dn". A submatch which does not
# contain any ","-characters and starts after "name="
# is stored in variable "name"
```

Configuring Targets in Structured View

You can create and modify classification scripts with SDX Admin. SDX Admin provides two views of classification scripts—structured and raw. You can switch between the two views at any time and make changes in either view.

Figure 21 shows the structured view of a subscriber classification script.

Figure 21: Classification Script—Structured View



The targets are displayed in the first field. The first entry in the target list (---) corresponds to the (unnamed) header section of the classification script. It always exists as the first entry; you cannot delete the target or insert a target in front of it.

To reorder targets, drag a target inside the target list. To edit a target, select the target, which copies the target into an edit field and shows the classification criteria in the Script field. You can then edit the target, or you can use the three buttons to the right of the target editing field to do the following:


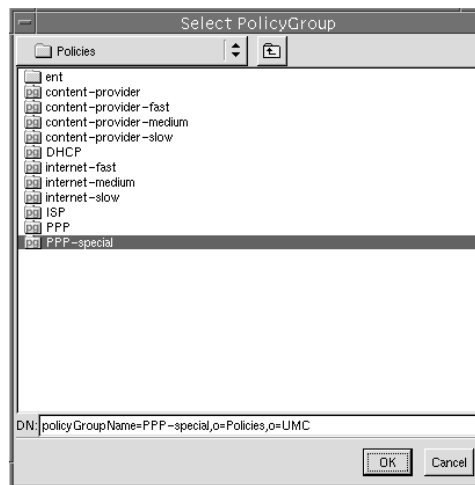
-  —Opens a dialog box that you can use to select the distinguished name (DN) of an object in the directory. Figure 22 shows the dialog box for interface classification scripts; it contains the DNs of existing policy groups. Subscriber classification scripts display the DNs of objects in the *o = Users* directory. Dynamic Host Configuration Protocol (DHCP) classification scripts display the DNs of cached DHCP profiles.

Figure 22: Select PolicyGroup Dialog Box

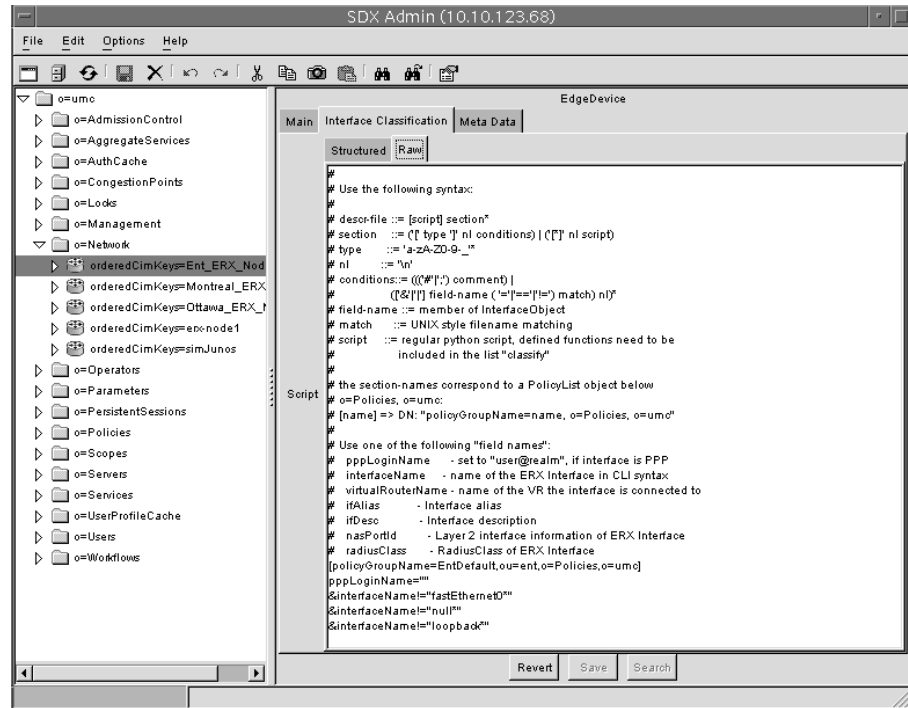
- Ins—Inserts a new target after the highlighted target (or at the end if no target is selected)
- Del—Deletes the highlighted target

Configuring Criteria in Structured View

Select the target for which you want to configure criteria. SDX Admin displays the classification criteria for the target in the Script field. You can edit the criteria directly in the Script field.

Configuring Targets and Criteria in Raw View

Figure 23 shows the raw view of a classification script. When you are in the raw view, you can copy and paste the contents of a classification script to another object in the directory.

Figure 23: Classification Script—Raw View

Testing Subscriber and Interface Classification Scripts

SAE Web Admin provides a classifier tester that you can use to test subscriber and interface classification scripts. It contains a form that holds the classification script and a form for defining the fields of a subscriber classification context or an interface object.

The test first compiles the classification script. Then it creates a classification context object based on user input, and it invokes the classification script on this context. For subscriber classification scripts, the returned LDAP query is executed.

The output of the test page contains:

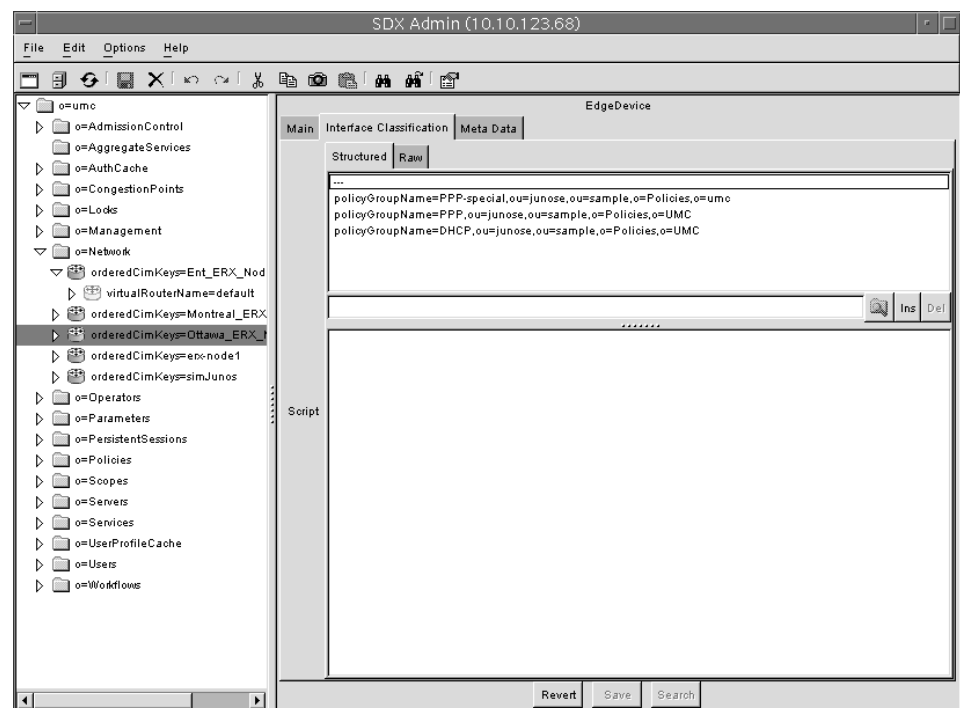
- Any compilation or classification errors
- The return value of the classification script; that is, the DN of a policy list or an LDAP query for loading a subscriber profile
- The object returned by the LDAP query (or an error message if the query did not return a unique object)

Classifying Interfaces

To define interface classification scripts with SDX Admin:

1. In the SDX Admin navigation pane, access a router object in *o = network*, *o = umc*.
2. Click the **Interface Classification** tab.

The following pane appears.



3. Use the information in *Selecting Interface Classification Criteria* on page 104 and *Configuring Interface Classification Targets* on page 106 to configure an interface classification script.

Selecting Interface Classification Criteria

Interface classification criteria define match criteria that are used to find a policy group. Use the fields in this section to define classification criteria.

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 JUNOS 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 JUNOS 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 JUNOS 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”

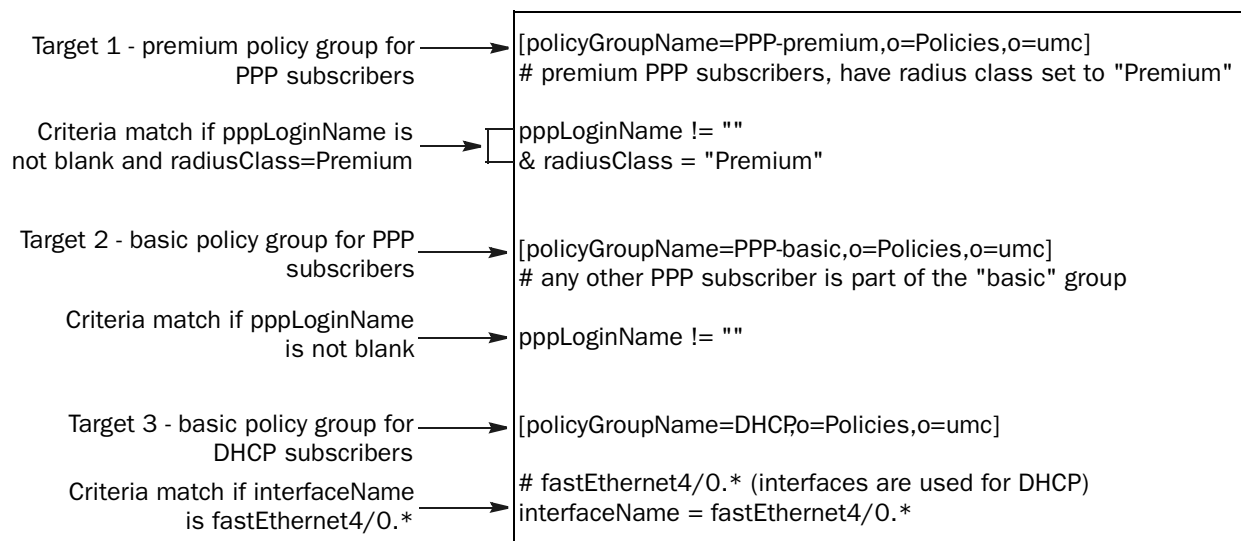
Configuring Interface Classification Targets

The targets of the interface classification scripts are DNs of policy group objects defined in the directory. For example, policyGroupName = DHCP, o = Policies, o = umc

Example: Managing Interfaces for Premium and Basic PPP and DHCP Subscribers

In this scenario, the router manages two types of PPP interfaces—DHCP subscriber interfaces and static IP interfaces. The fastEthernet4/0.1 to fastEthernet4/0.999 interfaces are VLAN interfaces used to terminate DHCP subscribers.

The service provider has separated the PPP subscribers into a premium subscriber group and a basic subscriber group. These groups are distinguished by a different set of default policies applied to the PPP interface. The RADIUS class attribute in the RADIUS profile for premium subscribers is set to Premium. The interface classification script for this scenario is:



The script is processed as follows:

1. If pppLoginName is not blank and radiusClass is Premium, the PPP-premium policy group is sent to the SAE, and script processing stops.
2. If script processing proceeds and pppLoginName is not blank, the PPP-basic policy group is sent to the SAE, and script processing stops.
3. If script processing proceeds and interfaceName is fastEthernet 4/0.0 through fastEthernet 4/0.999, the DHCP policy group is sent to the SAE, and script processing stops.

Example: Managing Specific Interfaces

This example causes the SAE to load the DHCP policy group on IP interfaces on Fast Ethernet modules in slot 3/port 1, slot 1/port 1, or any port on slot 2. The SAE then manages these interfaces.

```
[policyGroupName=DHCP,o=Policies,o=umc]
interfaceName=FastEthernet3/1
interfaceName=FastEthernet1/1
interfaceName=FastEthernet2/*
```

Example: Managing Interfaces by Using the Interface Description

This example causes the SAE to load the DHCP policy group on any interface where the ifAlias starts with DHCP-subscribers.

```
[policyGroupName=DHCPo=Policies,o=umc]
ifAlias="DHCP-subscribers*"
```

For this approach, you will need to use the **ip description** command to configure interface aliases that begin with DHCP-subscribers for all interfaces that support DHCP subscribers.

Classifying Subscribers

Changes that you make to subscriber classification scripts do not affect subscriber sessions that are already established. One effect of this behavior is that static IP subscriber sessions are not closed if the classification script is changed in a way that would no longer cause the SAE to load a profile for certain subscribers.

On JUNOSe routers that use the COPS-PR or COPS XDR router drivers, you can create a subscriber session for the router interface to start services such as script services and aggregate services. The SAE creates the router interface, but does not install any policies on it. You can create a subscriber classification rule, but not an interface classification rule for this interface.

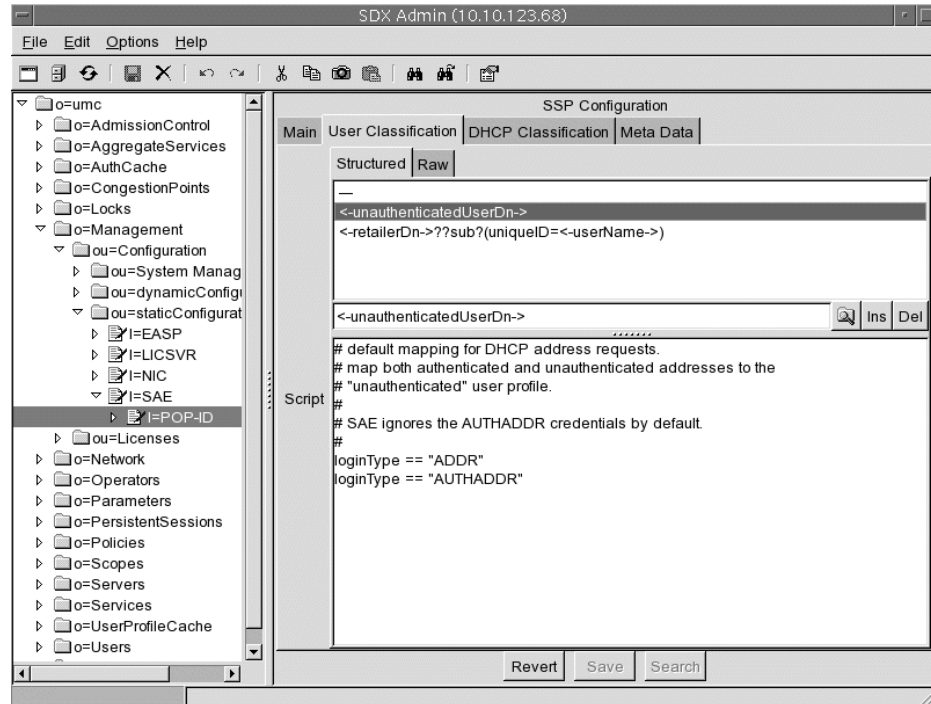
To define subscriber classification scripts with SDX Admin:

1. In the SDX Admin navigation pane, access the SAE object *I = SAE*, *ou = staticConfiguration*, *ou = configuration*, *o = management*, *o = umc*.
2. In this folder, click on the *I = POP-ID* object associated with this SAE.

The SSP Configuration pane appears.

3. Click the **User Classification** tab.

The following screen appears.



Use the information in *Selecting Subscriber Classification Criteria* on page 109 and *Configuring Subscriber Classification Targets* on page 114 to configure the subscriber classification script for an SAE object.

Selecting Subscriber Classification Criteria

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

dhcp

- DHCP options. See *Sending DHCP Options to the JUNOS Router* on page 112.

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)
- 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
- <Login name >
- 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.
- 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 JUNOS 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 JUNOS Router

Subscriber classification scripts support DHCP options conveyed through COPS. When COPS reports an address, the JUNOS 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 14 are in the user classification context of subscriber classification scripts.

Table 14: 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()	
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 for 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).

Configuring 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.
- **scope**—Scope of search in the directory
 - **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.

Example: Subscriber Classification Scripts for Static IP Subscriber

In cases such as bridged 1483 DSL with a single subscriber, you can write the subscriber classification script so that it loads a specific subscriber profile. If the interface is matched to a subscriber profile, a subscriber session is immediately established. An SAE application (for example, a portal) can still force the subscriber with this subscriber profile to perform a Web login.

One way to achieve the mapping of subscriber interface to subscriber profile is to provision the assigned interface name in the associated subscriber profile in LDAP. In this case the subscriber classification script can include a rule like this:

```
[retailerName=default,o=Users,o=umc??sub?(interfaceName=<-interfaceName->)]
# all fastEthernet interfaces are connected to static IP subscriber
loginType = INTF
& interfaceName = fastEthernet*
```

Another way may include a special encoding of the interface alias (ifAlias) field of the subscriber interface. This encoding must then be provisioned when the interface for the subscriber is provisioned. In this example, the encoding SSP-username is chosen for ifAlias; for example, for subscriber juser the interface alias would be set to SSP-juser. The match is performed with a regular expression, which separates the user ID from the ifAlias prefix.

```
[retailerName=default,o=Users,o=umc??sub?(uniqueID=<-userId->)]
loginType = INTF
& ifAlias =~ SSP-(?P<userId>.*)
```

Example: Subscriber Classification Scripts Using a Subscriber Group

To support scenarios where SAE has no access to the subscriber database, SAE can load anonymous profiles for groups of subscribers. The following example loads a particular subscriber profile when subscribers of domain another-isp.com log in.

```
[uniqueID=anon,ou=default,retailerName=another-isp,o=Users,o=umc]
domainName = another-isp.com
```

Example: Subscriber Classification Scripts for Enterprise Subscribers

For enterprise subscribers, you can create one general subscriber classifier script that matches a unique subscriber profile to each managed router interface. The subscriber profile is the access subscription that represents an Internet access in an enterprise. The following examples show two approaches to creating the general classifier script. You can use one of these strategies or a combination of strategies.

Matching on the Interface Name

In this scenario, you configure the interface name field in the access subscription for the site to match an interface on the router. The format for the interface name could be: interfaceName@virtualRouterName@routerName. You then create a classification script that searches for subscriber profiles that match a specific interface. For example:

```
[ou=Managed CPE,retailerName=Retailer-Two,o=Users,o=UMC??sub?\
(interfaceName=<-interfaceName->@<-virtualRouterName->)]
loginType = INTF
& interfaceName = "fe*"
```

Matching on the Interface Alias

For JUNOS routers, you can configure the interface description on the router in a format that the classifier script can match to the interface alias in an access subscription. In a simple case, you can configure the interface description only for interfaces that terminate a managed CPE, and match them to the interface alias in the directory. The subscriber classifier could be configured as follows:

```
[ou=Managed CPE,retailerName=Retailer-Two,o=Users,o=UMC??sub?\
(interfaceAlias=<-ifAlias->)]
ifAlias != ""
```

Example: Subscriber Classification Scripts For a Wholesaler/Retailer Scenario

In a wholesaler/retailer scenario, where the wholesaler owns the SAE but the retailer authenticates subscribers using RADIUS, it is possible to use a RADIUS vendor-specific attribute (VSA) (serviceBundle = Juniper(4874) #31) to send information from the RADIUS profile to the SAE. The subscriber classification script is then used to load a different subscriber profile with different subscriptions based on information stored in the RADIUS database of the retailers; for example:

```
[uniqueId=<-serviceBundle->,ou=default,retailerName=another-isp,o=Users,o=umc]
domainName = another-isp.com
& serviceBundle != ""
```

Alternatively, the target can be written as an LDAP search, taking advantage of the domain name-to-retailer object mapping of the SAE; for example,

```
[<-retailerDn->??sub?(uniqueId=<-serviceBundle->]
serviceBundle != ""
```

Example: Creating Router Interface Subscriber Session

Aggregate services or script services can be activated on a router instead of an interface or DHCP address. On JUNOSe routers that use the COPS-PR or COPS XDR router driver, the SAE automatically creates a router interface; and then a subscriber session as specified by the subscriber classification script.

For example, the following script searches for a router profile in the directory under ou = routers, retailerName = default, o = Users, o = umc, with a routerName that matches the virtual router name (such as default@erx-node1).

```
[ou=routers,retailerName=default,o=Users,o=UMC??one?(routerName=<-virtualRouter
Name->)]
interfaceName = Router
```

Example: Activating Services for a Group of Subscriber Sessions

A subscriber classification script can assign a shared subscriber profile and a login name to a subscriber session for a group of interface subscriber sessions. The following example assigns the login name idp@idp to subscriber sessions for JUNOSe interfaces that have core specified as the ifAlias (as configured on the JUNOSe router).

```
[routerName=idp,ou=interfaces,retailername=SP-IDP,o=Users,o=UMC?loginName=idp
@idp]
# core facing interfaces on JUNOSe routers in JUNOSe POPs
ifAlias=="core"
```

You can use this type of subscriber classification to activate a service for a group of interface subscriber sessions that are to be treated the same. For example in the configuration for an aggregate service, a fragment service could be created for all subscriber interface sessions on interfaces identified by the ifAlias core on a virtual router. The subscriber reference expression in the configuration for the fragment service would reference the virtual router name and the login name, such as vr = "<- virtualRouterName ->", login_name = "idp@idp."

You can also use the SAE CORBA remote API to get lists of the subscriber sessions that share the same login name.

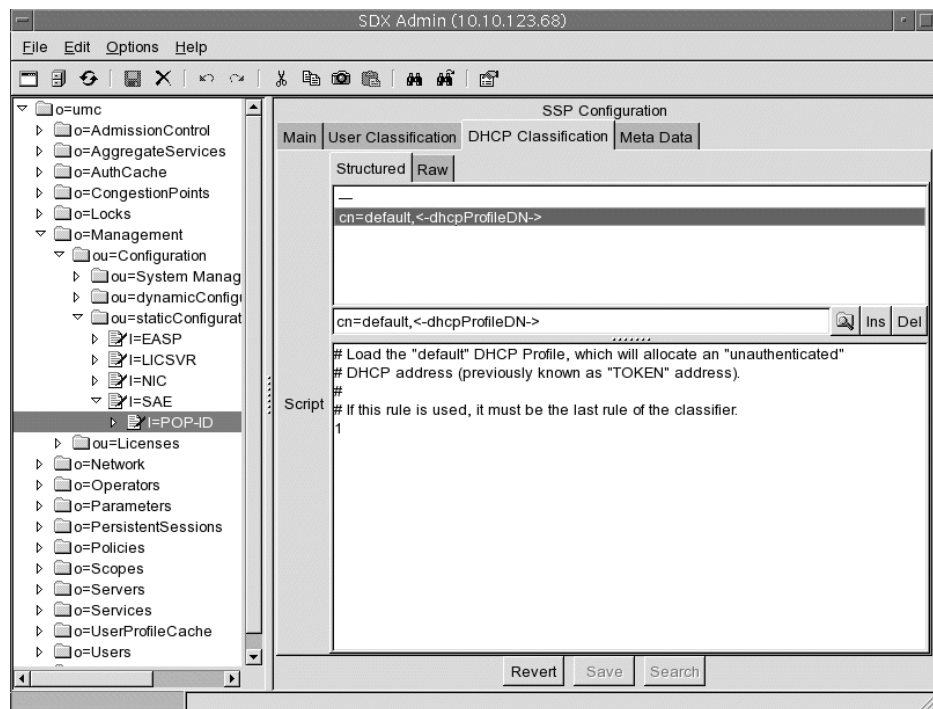
Classifying DHCP Subscribers

DHCP classification scripts are stored in the directory in the `dhcpProfileClassification` attribute of the `umcConfiguration` object class. They contain fields set by the address request and authorization response.

To configure DHCP classification scripts with SDX Admin:

1. In the SDX Admin navigation pane, access the object *I = SAE*, *ou = staticConfiguration*, *ou = configuration*, *o = management*, *o = umc*.
2. In this folder, click on the *I = POP-ID* object associated with this SAE.
3. Select the **DHCP Classification** tab.

The structured view of the DHCP classification configuration appears.



Use the information in *Selecting DHCP Classification Criteria* on page 118 and *Configuring DHCP Classification Targets* on page 119 to configure the DHCP classification script for an SAE object.

Selecting DHCP Classification Criteria

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

authVirtualRouterName

- Name of JUNOS virtual router that is set by an authorization plug-in through the authorization response.
- Value—Name of the virtual router in the format `vrname@hostname`

dhcp

- DHCP options. See *Setting DHCP Parameters with DHCP Options* on page 120.

dhcpProfileDN

- Search base for DHCP profiles. The DN can be used in target expressions.
- Value—DN of DHCP profile

interfaceName

- Name of the interface where the DHCP discover message was received.
- Value—Name of the interface in your router CLI syntax
- Example—`interfaceName = fastEthernet6/0`

ifAlias

- Description of the interface where the DHCP discover request was received.
- Value—Interface description that is configured on the router. For JUNOS routers, it is the description configured with the **interface description** command
- Example—`ifAlias = "dhcp-subscriber12"`

ifDesc

- Alternate name for the interface where the DHCP discover request was received. This is a system-generated name that is used by SNMP.
- Value
 - On a JUNOS router, the format of the description is:
`ip<slot>/<port>.<subinterface>`
 - On the JUNOS routing platform, `ifDesc` is the same as `interfaceName`.

macAddress

- MAC address of the DHCP client that appears in DHCP request.
- 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.)

poolName

- IP address pool name that is set by an authorization plug-in through the authorization response.
- Value—Name of an address pool configured on the JUNOSe router

virtualRouterName

- Name of the virtual router.
- Value—Name of the virtual router in the format vrname@hostname

Configuring 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 *Selecting DHCP Classification Criteria* on page 118.

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 JUNOS 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 in the directory. Parameters in the DHCP profile override authorization parameters.

For more information about how the SAE handles DHCP subscribers, see:

- Assigning DHCP Addresses to Subscribers on page 132
- DHCP Subscriber Login and Service Activation on page 22

Setting DHCP Parameters with DHCP Options



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

DHCP servers use DHCP options to configure DHCP clients. The DHCP local server in the JUNOS 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 15 on page 121 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.

Table 15: 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
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
arp-cache-timeout	35	int32
ieee802-3-encapsulation	36	int8
default-tcp-ttl	37	int8
tcp-keepalive-interval	38	int32

Table 15: DHCP Options Supported on the SAE (continued)

Option Name	Option Number	Option Type
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
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
nnntp-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

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.

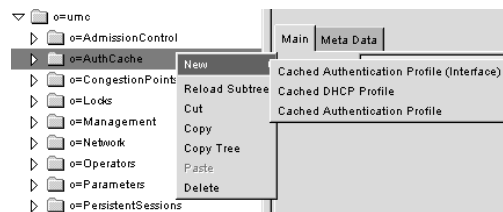
You can also create DHCP profiles manually with SDX Admin or by adding DHCP profile entries to the directory. DHCP profiles are stored in the *o = AuthCache* directory in the `dhcpProfile` object class. The `dhcpProfile` object class is subordinate to the `cachedAuthenticationProfil`s object class. Manually created profiles are keyed by the `cn` (common name) attribute.

For more information about how the SAE handles DHCP subscribers, see:

- Assigning DHCP Addresses to Subscribers on page 132
- DHCP Subscriber Login and Service Activation on page 22

To create a DHCP profile with SDX Admin:

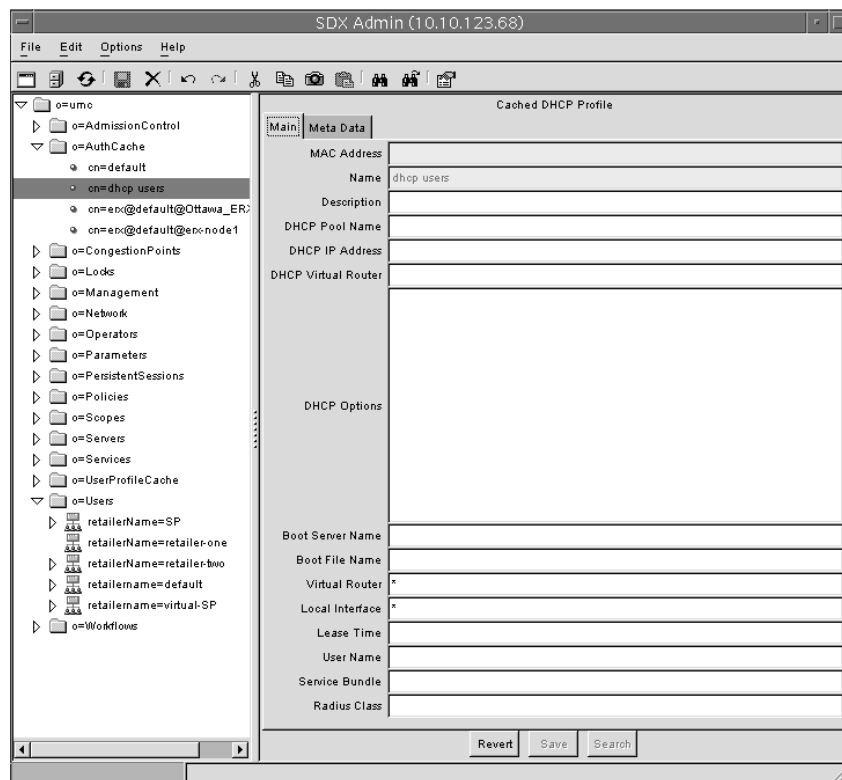
1. Highlight **AuthCache**, and right-click.
2. Select **New > Cached DHCP Profile**.



The New Cached DHCP Profile dialog box appears.

3. Assign a name to the profile.
4. Click **OK**.

The Cached DHCP Profile pane appears.



5. Fill in the fields as described in this section.

MAC Address

- Naming attribute for system-created DHCP profiles. When a DHCP subscriber first logs in to the SAE, the subscriber's equipment is registered, and the SAE caches the MAC address in the *o=AuthCache* directory. System-created profiles are keyed by MAC address.
- Value—SAE fills in the MAC address
- Default—No value
- Attribute name—macAddress

Name

- Naming attribute for manually created DHCP profiles. Manually created profiles are keyed by MAC address.
- Value—String
- Default—No value
- Attribute name—cn

Description

- Text description of the profile.
- Value—String
- Default—No value
- Attribute name—Description

DHCP Pool Name

- Name of the IP address pool on the JUNOS router from which a DHCP address is selected.
- Value—String, optional
- Default—No value
- Attribute name—radiusFramedPool

DHCP IP Address

- Fixed IP address that is offered to the DHCP client if the client is part of a network in the configured DHCP pool.
- Value—String, optional
- Default—No value
- Attribute name—radiusFramedIPAddress

DHCP Virtual Router

- Name of the JUNOS virtual router that holds the IP address pool.
- Value—String, optional
- Default—No value
- Attribute name—virtualRouterName

DHCP Options

- Defines DHCP options that are used to configure DHCP clients. See *Setting DHCP Parameters with DHCP Options* on page 120 for more information.
- Value—You define DHCP options in the format:

option = value [, value...]

where option is the option name or number (see Table 15 on page 121) and values are entered based on the type of option:

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

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

- Default—No value
- Attribute name—dhcpOptions

Boot Server Name

- Name of the server used to boot the DHCP client.
- Value—String, length < 64
- Default—No value
- Attribute name—dhcpServer

Boot File Name

- Name of a boot file used to boot the DHCP client.
- Value—String, length < 128
- Default—No value
- Attribute name—bootFileName

Virtual Router

- Name of the JUNOS virtual router that is used to check the validity of system-created DHCP profiles.
- Value—Name of the virtual router in the format *vrname@hostname*. An * (asterisk) means that the values for the virtual router are ignored when the cached profile is used. Use an * if you do not know the virtual router to which the subscriber will connect.
- Default—* (asterisk)
- Attribute name—checkVrName

Local Interface

- Name of the JUNOS interface that is used to check the validity of system-created DHCP profiles.
- Value—Name of interface in JUNOS CLI syntax (for example, *fastethernet6/0*). An * (asterisk) means that the values for the local interface are ignored when the cached profile is used. Use an * if you do not know the interface to which the subscriber will connect, or you want to allow the subscriber to connect through multiple interfaces. You can also enter expressions of the form *@expr = value*.
- Default—* (asterisk)
- Attribute name—localInterface

Lease Time

- Length of time the supplied IP address is valid.



NOTE: This parameter is not currently implemented on the JUNOSe router. The DHCP lease time that the SAE sends to the JUNOSe router is ignored.

- Value—Number of seconds
- Default—No value
- Attribute name—leaseTime

User Name

- Name of DHCP user without the domain name.
- Value—String that specifies the information to the left of the @ character in <userName> @ <domainName> .
- Default—No value
- Attribute name—userName

Service Bundle

- Vendor-specific RADIUS attribute that specifies the SDX service bundle to use.
- Value—String
- Default—No value
- Attribute name—serviceBundle

Radius Class

- RADIUS attribute class.
- Value—String that maps to a RADIUS attribute class
- Default—No value
- Attribute name—radiusClass

Chapter 8

Overview of Plug-Ins Included with the SAE

This chapter gives an overview of the features of the SAE. Topics include:

- How Internal Plug-Ins Work on page 129
- Types of Internal Plug-Ins on page 130
- Assigning DHCP Addresses to Subscribers on page 132
- Creating and Tracking Subscriber Sessions on page 134
- Activating and Tracking Service Sessions on page 135

How Internal Plug-Ins Work

Plug-ins work with the SAE through events. Events such as subscriber logins and logouts, as well as service activation and deactivation, trigger the SAE to create event objects and send them to plug-in instances that are configured to receive the events. When a plug-in receives an event, it processes the event. For example, when a subscriber logs in, the SAE sends the username and password to an authentication plug-in that compares the username and password with data stored in a directory.

The plug-in configuration is made up of a plug-in pool and event publishers.

Plug-In Pool

The plug-in pool consists of plug-in instances. A plug-in instance describes a particular plug-in that can handle events that it receives from the SAE. An authorization plug-in instance might be set up to perform RADIUS authentication when it receives a subscriber login event. A tracking plug-in instance might be set up to write accounting information to a file when it receives service session events.

For each type of plug-in you can create multiple instances that contain different configurations of the plug-in.

If you have multiple retailers, you might use different authentication methods and servers to authenticate each retailer's subscribers. In this case you could set up an authentication plug-in instance for each retailer.

You could also set up a tracking plug-in instance to write certain accounting information to a file whenever it receives an event. Then you could set up another instance that writes different accounting information to a different file. You could then use one instance to track subscriber sessions and another to track service sessions. Or you could set up plug-in instances to track different types of services.

Event Publishers

Event publishers tell the SAE which events to send to which plug-in instances. There are four types of event publishers. Each type determines the scope of events that are sent to plug-in instances.

- Service-specific publishers—Authenticate subscribers of a particular service, authorize sessions for the service, and track subscriber activity related to the service
- Retailer-specific publishers—Authenticate and track subscribers and authorize DHCP address allocations for subscribers who log in to the domain(s) of a particular retailer
- Virtual router-specific publishers—Authenticate and track managed interfaces on a particular virtual router
- Global publishers—Authorize all subscriber sessions, track all subscriber and service sessions, authorize DHCP address allocations for all DHCP subscribers, and authorize all subscribers to change their subscriptions; authenticate subscribers and authorize DHCP address allocations for subscribers who log in to a retailer domain for which no retailer-specific authentication plug-ins are specified; and track all router interfaces that the SAE manages

Each publisher can notify a number of plug-in instances when an event occurs, and each plug-in instance can be registered with a number of publishers.

Types of Internal Plug-Ins

There are two main types of plug-ins: authorization plug-ins and tracking plug-ins.

Authorization Plug-Ins

Authorization plug-ins can perform both authentication (that is, verify the originator of a request) and authorization. Authorization can include the setting of service session parameters such as session timeout or authorizing services based on the current load of the router.

You can set up authorization plug-ins to:

- Globally authorize all subscriber sessions.
- Authenticate subscribers who belong to a particular retailer's domain.
- Globally authenticate and/or authorize all service sessions.
- Authenticate and/or authorize sessions for a particular service.

- Globally authorize DHCP address allocations.
- Authorize DHCP address allocation for subscribers who log in to a particular retailer's domain.
- Globally authorize subscribers to change their subscriptions.
- Authenticate administrators so that they can access SDX Web Admin.



NOTE: Event publishers send events to all configured plug-in instances. For authentication to succeed, all authentication plug-ins that receive the authentication request must grant authentication.

Tracking Plug-Ins

Tracking plug-ins track activity or log accounting information. You can set up tracking plug-ins to:

- Globally track all subscribers.
- Track subscribers who belong to a particular retailer's domain.
- Globally track all service sessions.
- Track service sessions for individual services.
- Track QoS service sessions for individual services and attach the required QoS profile to the JUNOS subscriber interface.

Tracking plug-ins keep the state of active sessions and provide usage and accounting data. For each subscriber and service session, plug-ins can track when the session is activated and deactivated and can keep interim updates. For example, when the SAE activates a service, it sends a Service Session Start event to tracking plug-in instances that are registered to receive events for that service. When the service is stopped, the SAE sends a Service Session Stop event to all tracking plug-ins that received the Service Session Start event. If interim accounting is configured, service session interim update events are sent at regular intervals to all tracking plug-ins that are registered to receive the event.

One application of tracking plug-ins is to keep usage records, such as session time and volume counters. Service-tracking plug-ins can set a timeout for a service session in response to start and interim updates that the plug-in receives for the session. When a service session is active longer than the defined timeout, the SAE stops the session and sends service session stop events to the tracking plug-ins.

Another application is to track QoS services and attach the required QoS profile to the subscriber interface. See *SRC-PE Solutions Guide, Chapter 1, Managing Tiered and Premium Services with QoS on JUNOS Routers*.

Customizing RADIUS Packets with Plug-Ins

RADIUS internal plug-ins include flexible RADIUS plug-ins and custom RADIUS plug-ins that let you customize RADIUS authentication and accounting packets that the SAE sends to RADIUS servers. You can specify which fields are included in various types of RADIUS packets and what information is contained in the fields.

For example, you can specify values in authentication response packets that will set session and idle timeouts, set the RADIUS class, and set the session volume quota. For accounting packets, you can specify which fields to include in accounting records.

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 or select a fixed address for each subscriber.

The main difference between flexible RADIUS plug-ins and custom RADIUS plug-ins is that custom plug-ins are designed to deliver better system performance than the flexible RADIUS plug-ins. 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.

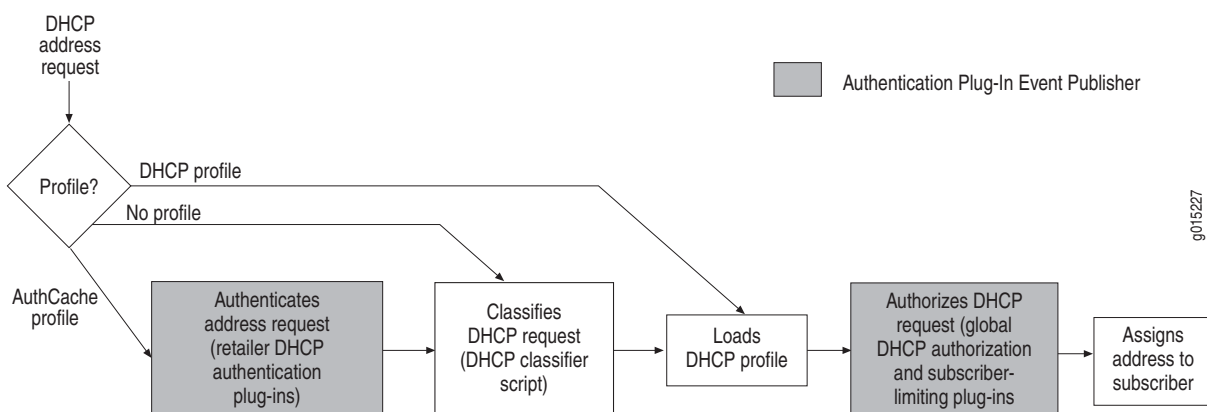
To customize RADIUS packets with a flexible RADIUS plug-in, see one of the following:

- *Defining RADIUS Packets for Flexible RADIUS Plug-Ins with SDX Configuration Editor* on page 176.
- *Defining RADIUS Packets for Flexible RADIUS Plug-Ins with the SRC CLI* on page 215.

Assigning DHCP Addresses to Subscribers

Figure 24 shows the process that the SAE uses to assign addresses to DHCP subscribers.

Figure 24: DHCP Address Assignment



To create and track a subscriber session for DHCP subscribers, the SAE:

1. Uses the client's media access control (MAC) address to look up a profile in cache or in the directory.
 - a. If the SAE finds an authCache profile, it continues with Step 2.
(The residential portal can register subscriber equipment and store the registration in an authCache profile. See *Equipment Registration for DHCP Login* on page 301.
 - b. If the SAE does not find a profile, it skips to Step 3.
 - c. If the SAE finds a DHCP profile, it skips to Step 4.

2. Authenticates the address request.

The SAE authenticates the request by using the configured DHCP authentication plug-ins. The DHCP authentication plug-ins are configured in the Retailer object in the directory. The SAE selects the retailer based on the domain name of the login request. If the Retailer object does not specify a DHCP authentication plug-in, the default retailer authentication plug-in is used for authentication.

If authentication fails, the SAE sends a discover decision with accept = false to the router.

3. Classifies the DHCP request.

The SAE runs a DHCP classification script to select the DHCP profile to load. If it does not find a profile, the SAE sends a discover decision with accept = false to the router.

4. Loads a DHCP profile.

The SAE loads the selected DHCP profile from the directory.

5. Authorizes the DHCP request.

The SAE authorizes the request by using the globally configured DHCP authorization plug-ins, which can include a subscriber-limiting plug-in.

Note that if the DHCP profile contains configuration parameters and the DHCP authorization plug-ins also return parameters, the plug-in parameters take precedence.

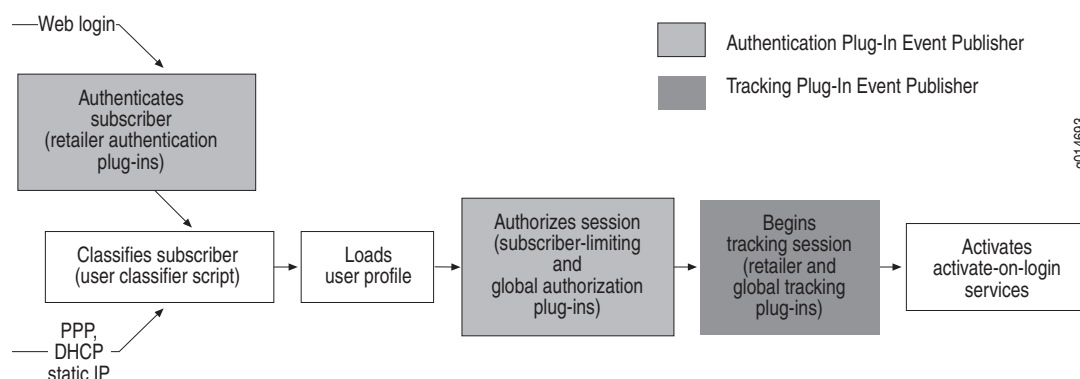
6. Assigns the address to the subscriber.

The SAE sends a DHCP discover decision to the router, which enables the router to assign an address to the subscriber. When the subscriber accepts the assigned address, the router sends an address request to the SAE, and the SAE starts processing a DHCP login request. See *Creating and Tracking Subscriber Sessions* on page 134.

Creating and Tracking Subscriber Sessions

Figure 25 shows the process that the SAE uses to create and begin tracking subscriber sessions.

Figure 25: Creating and Tracking Subscriber Sessions



To create and track a subscriber session, the SAE:

1. Authenticates the login request.
 - a. Web logins are authenticated by the SAE directly. The SAE maps the login request to a retailer object in the directory by matching the requested domain name. If the retailer object:
 - Has an authentication plug-in configured, the SAE asks the plug-in to authenticate the subscriber.
 - Does not have an authentication plug-in configured, the SAE sends the authentication request to the default retailer authentication plug-in.
 - b. PPP and static IP interface addresses are authenticated by the router using the RADIUS setup configured in the router. The SAE is notified only after the authentication is completed successfully.

2. Classifies the subscriber.

The SAE runs a subscriber classification script to select the subscriber profile to load.

3. Loads a subscriber profile.

The SAE loads the selected subscriber profile from the directory.

4. Authorizes the subscriber session.

The SAE authorizes the subscriber session before it starts the session:

- a. The SAE checks the number of concurrent logins of the subscriber profile and its parent and sibling profiles and sends an event to the subscriber-limiting plug-in. If the maximum number of allowed concurrent logins configured in the plug-in is exceeded, the subscriber session is not authorized.
- b. The SAE calls the global subscriber authorization plug-in instances, which can perform custom authorization.

If any of the previous steps fail, the SAE either keeps the currently active subscriber profile (in case of a Web login) or loads the unauthenticated subscriber profile. The reason for the failure is stored in the unauthenticated profile and can be displayed when the subscriber eventually connects to the portal.

5. Sends start subscriber tracking events.

The SAE sends subscriber session start events to tracking plug-ins configured for the associated retailer and to global subscriber tracking plug-in instances.

When a subscriber session is closed, the SAE sends subscriber session stop tracking events to the same plug-ins that received the subscriber session start events.

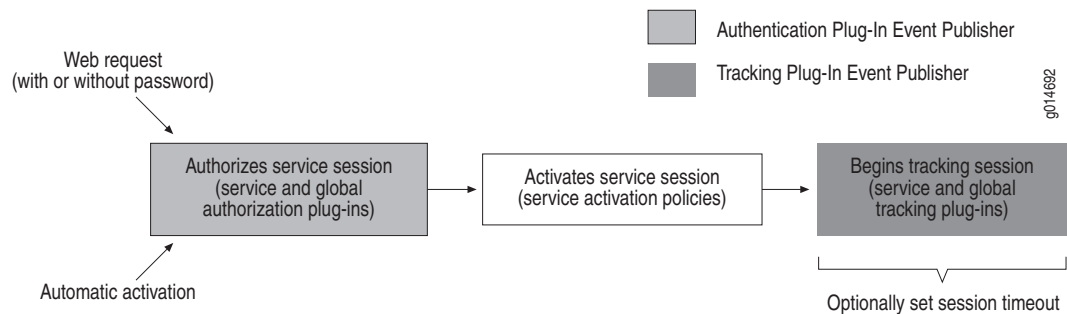
The SAE does not create subscriber session interim update events.

6. Activates services for the subscriber that are set up to activate on login.

Activating and Tracking Service Sessions

Figure 26 shows the process that the SAE uses to activate and then track services. The SAE can activate services in one of two ways:

- Automatically—After the SAE creates a subscriber session, it activates all activate-on-login service subscriptions.
- Manually—Through a call of the portal application programming interface (API) method `Subscription.setActive`. This method is typically provided in the form of a Web portal and allows interaction with the subscriber.

Figure 26: Activating and Tracking Service Sessions

To activate and begin tracking a service session, the SAE:

1. Authorizes the service session.

The SAE sends events to authorization plug-in instances configured for the service and to global service authorization plug-in instances.

Service authorization plug-ins may perform authentication as well as authorization. If you define a plug-in instance to perform authentication, the portal developer must set username and password values before subscribers try to activate the service. Because the subscriber must provide the username and password, it is not possible to automatically activate a service that requires authentication.

2. Activates the services by applying service activation policies.
3. Begins tracking the service.

Sends a service session start event to the tracking plug-in instances configured for the service and to the global service tracking plug-in instances. If interim accounting is configured, a service session interim update event is sent at regular intervals to all tracking plug-ins that are registered to receive the event.

When a service is stopped (either explicitly through a call to the portal API, or implicitly through the termination of the associated subscriber session or through a timeout), a service session stop event is sent to all tracking plug-ins that received the service session start event.

Service-tracking plug-ins can set the session timeout of a service session in response to Service Session Start and Service Session Interim Update events. When a service session is active longer than the defined timeout, the SAE closes the session and sends the appropriate Service Session Stop events.

Chapter 9

Configuring Internal, External, and Synchronization Plug-Ins with the SRC CLI

This chapter describes how to use the SRC CLI to configure internal, external, and state synchronization plug-ins.

You can also use SDX Configuration Editor or SDX Admin to configure plug-ins on Solaris platforms. See *Chapter 10, Overview of Configuring Plug-Ins for Solaris Platforms*.

Topics in this chapter include:

- Configuring Internal Plug-Ins on page 137
- Configuring the SAE for External Plug-Ins on page 138
- Configuring the State Synchronization Plug-In Interface on page 139

Configuring Internal Plug-Ins

Use the following configuration statements to configure internal plug-ins:

```
shared sae configuration plug-ins pool name internal {  
    plug-in-class plug-in-class;  
}  
  
shared sae configuration plug-ins pool name internal properties name {  
    value;  
}
```

To configure an internal plug-in:

1. From configuration mode, access the internal plug-in configuration.

user@host# **edit shared sae configuration plug-ins pool intnl internal**
2. Configure the Java class name of the plug-in.

```
[edit shared sae configuration plug-ins pool intnl internal]  
user@host# set plug-in-class plug-in-class
```

3. Access the internal plug-in property configuration.

```
[edit shared sae configuration plug-ins pool intnl internal]
user@host# edit properties prop
```

4. Configure properties that define the plug-in. Enter values in the format property name = expression.

```
[edit shared sae configuration plug-ins pool internalPlugin internal properties prop]
user@host# set value
```

Configuring the SAE for External Plug-Ins

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, Chapter 1, Overview of the SAE*.

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 do so with the SRC CLI, use the following configuration statements:

```
shared sae configuration plug-ins pool name external {
  corba-object-reference corba-object-reference;
  attr [(host | router-name | interface-name | interface-alias | interface-descr | port-id |
  user-ip-address | login-name | accounting-id | auth-user-id | if-radius-class |
  if-session-id | service-name | radius-class | event-time | session-id |
  terminate-cause | session-time | in-octets | out-octets | in-packets | out-packets |
  nas-ip | user-mac-address | service-session-name | service-session-tag | user-type |
  user-radius-class | user-session-id | primary-user-name | subscription-name |
  login-id | if-index | event-time-millisecond | nas-port | operational | user-inet-address
  | nas-inet-address | router-type | interface-speed | service-bundle | user-dn | uid |
  domain | retailer-dn | password | service-scope | session-timeout |
  downstream-bandwidth | upstream-bandwidth | dhcp-packet | aggr-session-id |
  aggr-login-name | aggr-user-dn | aggr-user-inet-address | aggr-accounting-id |
  aggr-auth-user-id)...];
}
```

To configure an external plug-in:

1. From configuration mode, access the external plug-in configuration.

```
user@host# edit shared sae configuration plug-ins pool NicAgent external
```

2. Configure the object reference of the external plug-in that is exported to the SAE.

```
[edit shared sae configuration plug-ins pool NicAgent external]
user@host# set corba-object-reference corba-object-reference
```

3. Configure the attributes that are sent to the external plug-in.

```
[edit shared sae configuration plug-ins pool NicAgent external]
user@host# set attr [(host | router-name | interface-name | interface-alias | ...)...]
```

4. (Optional) Verify your configuration.

```
[edit shared sae configuration plug-ins pool NicAgent external]
user@host# show

corba-object-reference corbaloc:boston:8801/nic;
attributes [ router-name router-type interface-descr interface-speed
service-bundle ];
```

Configuring the State Synchronization Plug-In 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.

Use the following configuration statements to configure the state synchronization plug-in:

```
shared sae configuration plug-ins state-synchronization {
    fail-queue-size fail-queue-size;
    fail-queue-age fail-queue-age;
    batch-time batch-time;
    keepalive-time keepalive-time;
}
```

```
shared sae configuration plug-ins manager {
    threads threads;
}
```

To configure the state synchronization plug-in interface:

1. From configuration mode, access the state synchronization plug-in configuration.

```
user@host# edit shared sae configuration plug-ins state-synchronization
```

2. Configure the maximum number of plug-in events that are stored while the communication with a state synchronization plug-in is interrupted.

```
[edit shared sae configuration plug-ins state-synchronization]
user@host# set fail-queue-size fail-queue-size
```

3. Configure the maximum time that plug-in events are stored while the communication with a state synchronization plug-in is interrupted.

```
[edit shared sae configuration plug-ins state-synchronization]
user@host# set fail-queue-age fail-queue-age
```

4. Configure the time that the SAE waits for other plug-ins to become ready before starting a synchronization sequence.

```
[edit shared sae configuration plug-ins state-synchronization]
user@host# set batch-time batch-time
```

5. Configure the time that the SAE waits after an event before sending a ping to the remote plug-in.

```
[edit shared sae configuration plug-ins state-synchronization]
user@host# set keepalive-time keepalive-time
```

6. Configure the number of threads that the SAE maintains for plug-in synchronization.

```
[edit shared sae configuration plug-ins state-synchronization]
user@host# up
user@host# [edit shared sae configuration plug-ins]
user@host# set manager threads 5
```

7. (Optional) Verify your configuration.

```
[edit shared sae configuration plug-ins state-synchronization]
user@host# show
fail-queue-size 5000;
fail-queue-age -1;
batch-time 60;
keepalive-time 60;

user@host# [edit shared sae configuration plug-ins]
user@host# show
threads 5;
```

Chapter 10

Overview of Configuring Plug-Ins for Solaris Platforms

This chapter describes how to use SDX Configuration Editor and SDX Admin to configure plug-ins. It also shows how to configure internal, external, and state synchronization plug-ins.

You can also use the SRC CLI to configure a plug-ins on the C-series platform or on a Solaris platform. See *Chapter 9, Configuring Internal, External, and Synchronization Plug-Ins with the SRC CLI*.

Topics in this chapter include:

- Configuring Plug-Ins with SDX Configuration Editor on page 141
- Configuring Internal Plug-Ins on page 143
- Configuring the SAE for External Plug-Ins on page 144
- Configuring the State Synchronization Plug-In Interface on page 146
- Configuring Plug-Ins with SDX Admin on page 148

Configuring Plug-Ins with SDX Configuration Editor

You can use SDX Configuration Editor to create a configuration object or modify an existing one. Before you can modify an existing object, you need to import the configuration objects from the directory into SDX Configuration Editor.

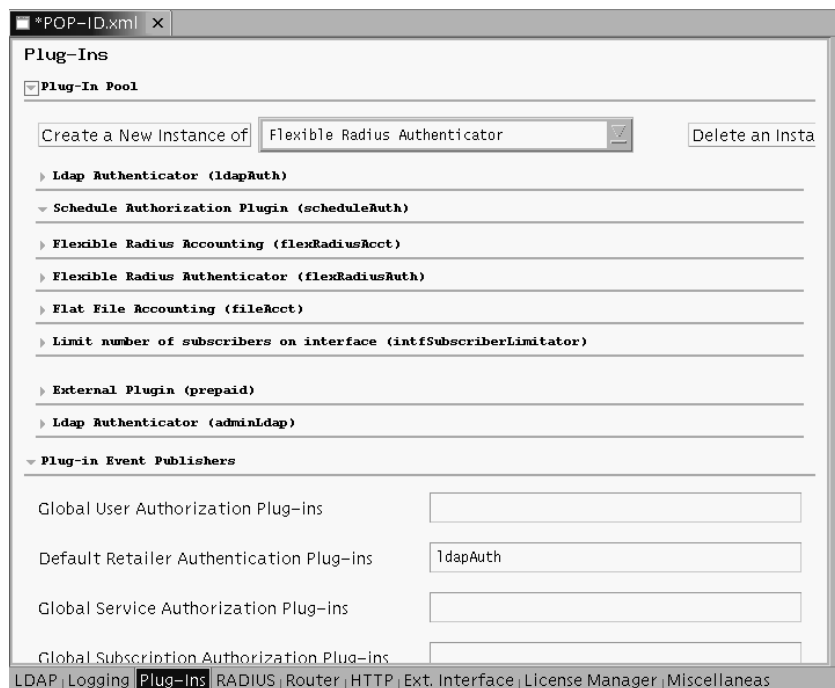
For information about how to use SDX Configuration Editor, see *SRC-PE Getting Started Guide, Chapter 39, Using SDX Configuration Editor*.

Accessing the Plug-In Configuration

To access the plug-in pool and event publisher configuration:

1. In the navigation pane, select the SAE object for which you want to configure plug-ins.
2. Select the **Plug-Ins** tab.

The Plug-Ins pane appears. This screen shows the Plug-In Pool area and the Plug-in Event Publishers area.



- To expand a configuration, click the triangle to the left of the configuration that you want to expand. When the configuration is expanded, the triangle points down.
- To collapse a configuration, click the triangle to the left of the configuration. When the configuration is collapsed, the triangle points to the right.

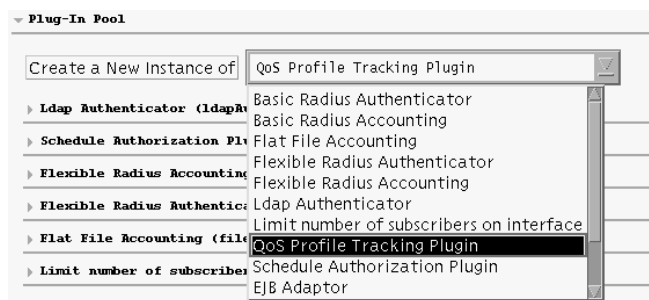
The Plug-In Pool area contains default plug-in instances that you can use as they are or modify. Instances are displayed by type of plug-in followed by the instance name in parentheses. For example, Ldap Authenticator (ldapAuth) is an LDAP authentication plug-in instance named ldapAuth.

The Plug-In Event Publishers area also contains several default plug-in instances.

Creating Plug-In Instances

To create a plug-in instance:

1. In the plug-in pool, select the type of plug-in instance from the drop-down list, and click **Create a New Instance of**.



The Create a New Instance dialog box appears.

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

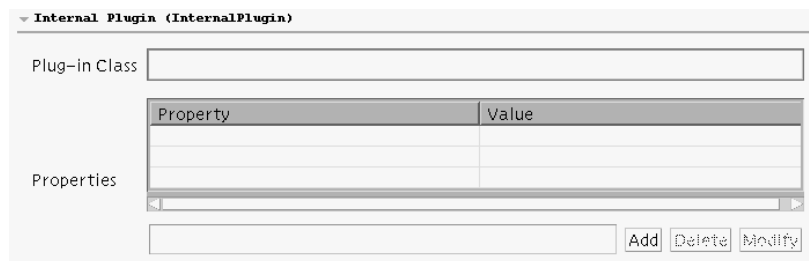
The instance appears in the plug-in pool.

Configuring Internal Plug-Ins

To configure an internal plug-in with SDX Configuration Editor:

1. In the Plug-In Pool area of the Plug-Ins pane, create an internal plug-in instance as described in *Creating Plug-In Instances* on page 143.

The instance appears in the Plug-In Pool area.



2. Fill in the fields for the plug-in instance as described below.

Plug-in Class

- Class name of the plug-in.
- Value—Java class name of the plug-in
- Default—No value
- Property name—Class

Properties

- Properties that define the plug-in. Enter properties in the format:
Plugin. < plug-in instance name > . < property name > = < expression >
- Configure the property table as follows:
 - To add a property, type the property definition in the field below the properties table, and click Add.
 - To modify a property, select the property, make your changes in the field below the property table, and click Modify.
 - To delete a property, select the property, and click Delete.
- Value—Property names and values that are available to the type of plug-in that you are configuring
- Default—No value

Configuring the SAE for External Plug-Ins

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, Chapter 1, Overview of the SAE*.

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 do so with SDX Configuration Editor:

1. In the Plug-In Pool area of the Plug-Ins pane, create an external plug-in instance as described in *Creating Plug-In Instances* on page 143.

The instance appears in the Plug-In Pool area.

2. Fill in the fields for the plug-in instance as described below.

CORBA Object reference

- Object reference of the external plug-in that is exported to the SAE. When the SAE sends the first event to a registered external plug-in, it resolves the object reference.
- Value—Supply the object reference in one of the following forms:
 - The absolute path to the interoperable object reference (IOR) file in the form `file:// <absolutePath>`
 - The corbaloc URL in the format `corbaloc:: <host> : <portNumber> / <path>`
 - `<host>` —Name or IP address of the host that supports the plug-in
 - `<portNumber>` —TCP/IP port number
 - `<path>` —Absolute path to plug-in
 - Common Object Services (COS) naming service in the form: `corbaname:: <host> [: <port>][/NameService]# <key>`
 - `<key>` —Provided by the publisher of the IOR to the COSnaming service.
 - The actual IOR in the form `IOR: <objectReference>`
- Default—No value
- Examples
 - Absolute path—`file:///var/acp/acp.ior`
 - corbaloc URL—`corbaloc:boston:8801/acp`
 - Actual IOR—`IOR:0000000000000002438444C3A736D67742E6A756E697...`
- Property name—`objectref`

Attributes

- Attributes that are sent to the external plug-in.



NOTE: Configure only the attributes required. If you do not specify attributes, all attributes are sent. Specifying fewer attributes improves the performance of the SRC network.

- Value—Comma-separated list of plug-in attributes. For a list of attributes and descriptions, see the documentation for the `sspPlugin.idl` file in the SRC software distribution at `/SDK/doc/idl/sspPlugin/html/index.html` or on the Juniper Networks Web site at <http://www.juniper.net/techpubs/software/management/sdx/api-index.html>
- Default—Comma-separated list of all possible attributes
- Property name—attr

Configuring the State Synchronization Plug-In 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 use SDX Configuration Editor to configure the state synchronization plug-in interface:

1. Access the plug-in configuration as described in *Accessing the Plug-In Configuration* on page 141.

The screenshot shows a configuration window titled "State Synchronization". It contains four input fields: "Size of Fail Queue" with value 5000, "Age of Fail Queue" with value -1, "Batch Time" with value 60, and "Keep Alive Time" with value 60. Below these fields is a section titled "Plug-in Manager" which is expanded, showing a checkbox and a field for "Number of Threads" with value 5.

2. Using the field descriptions below, fill in the fields in the State Synchronization and Plug-in Manager areas of the Plug-Ins pane.

Size of Fail Queue

- Maximum number of plug-in events that are stored while the communication with a state synchronization plug-in is interrupted.
- Value—Integer in the range 0-2147483647; -1 means unlimited
- Default—5000
- Property name—SyncPlugin.failQueue.maxSize

Age of Fail Queue

- Maximum time that plug-in events are stored while the communication with a state synchronization plug-in is interrupted.
- Value—Number of seconds in the range 0-2147483647; -1 means unlimited
- Default— -1
- Property name—SyncPlugin.failQueue.maxTime

Batch Time

- Time that the SAE waits for other plug-ins to become ready before starting a synchronization sequence.
- Value—Number of seconds in the range 0-2147483647
- Default—60
- Property name—SyncPlugin.batchTime

Keep Alive Time

- Time that the SAE waits after an event before sending a ping to the remote plug-in.
- Value—Number of seconds in the range 0-2147483647
- Default—60
- Property name—SyncPlugin.keepAliveTime

Number of Threads

- Number of threads that the SAE maintains for plug-in synchronization.
- Value—Integer in the range 0-2147483647
- Default—5
- Property name—PluginManager.threads

Configuring Plug-Ins with SDX Admin

This section provides guidelines for configuring plug-ins in the SAE property file with SDX Admin or a text editor. See *Modifying the SAE Property File* on page 57 for information about accessing the property file.

Configuring External Plug-Ins

There are two properties that you define for external plug-ins: `objectref` and `attr`. You must define both of these properties. Use the syntax:

```
Plugin.<plug-in instance name>.objectref = <object reference>
Plugin.<plug-in instance name>.attr = <attribute>
```

- `plug-in instance name`—Name that you choose to identify a particular plug-in instance.
- `object reference`—Specifies the object reference of the plug-in. You can define the object reference by specifying the absolute path to the IOR file, the corbaloc URL, the COS naming service, or the actual IOR.

The following example identifies the object reference by its absolute path to the IOR file:

```
Plugin.admissionControl.objectref = file:///var/acp/acp.ior
```

- `attribute`—Comma-separated list of attributes that the SAE sends to the plug-in. See *Fields* on page 154 for a list of attributes.



NOTE: Configure only the attributes required. Specifying fewer attributes improves the performance of the SRC network.

Configuring Internal and Hosted Plug-Ins

To define plug-in instances for internal and hosted plug-ins, use the syntax:

```
Plugin.<plug-in instance name>.<property name> = <expression>
```

- `plug-in instance name`—Name that you choose to identify a particular plug-in instance.
- `property name`—Each plug-in type has a list of properties that you can define. Use those names to configure properties in the file. Property names are case sensitive. For information about the properties that you can assign, see the section that describes the associated plug-in.
- `expression`—Sets a value for the property name. For information about the valid values that you can assign to each property, see the section that describes the associated plug-in.

For internal and hosted plug-ins, you must define the class property, which identifies the Java class name of the plug-in. The following example identifies the Java class name for plug-in instance `ldapAuth`:

```
Plugin.ldapAuth.class = net.juniper.smgmt.sae.plugin.LdapAuthenticator
```

For the Java class names of tracking plug-ins, see Table 16 on page 152. For the Java class names of authorization plug-ins, see Table 17 on page 161.

Defining RADIUS Packets

To create templates that define RADIUS packets in flexible RADIUS accounting and authentication plug-ins, use the syntax:

```
RadiusPacket.<template instance name>. <packet-type>.<id>[.type] =  
<expression>
```

- `template instance name`—Name that you choose to identify the template.
- `packet-type`—Assign one of the values described in Table 18 on page 177.
- `id[.type]`—Identifies a RADIUS attribute; use as described in *Property* on page 179.
- `expression`—Assigns a value to the RADIUS attribute; use in the same way as described in *Value* on page 180.

Setting Up the Plug-In Instance to Use a Template

To set up a RADIUS plug-in to use a template, define the template property as follows:

```
Plugin.<plug-in instance name>.template = RadiusPacket.<template instance  
name>
```

For example, to use the `stdAuth` template in the `flexRadiusAuth` plugin instance:

```
Plugin.flexRadiusAuth.template = RadiusPacket.stdAuth
```

Configuring Event Publishers

To configure global and default retailer event publishers, use the following syntax:

```
<event publisher>=<list of plug-in instances>
```

- `Event publisher`—Name of property that identifies the event publisher. See *Configuring Global and Default Retailer Event Publishers* on page 185 for the property names of global and default retailer publishers.
- `List of plug-in instances`—Comma-separated list of plug-in instances to which you want the publisher to send events.

The following is the default event publisher configuration. It sets the global subscriber tracking and global service tracking publishers to send events to the fileAcct plug-in instance, and sets the default retailer publisher to send events to ldapAuth.

```
#global plug-ins
User.auth.plugins =
User.tracking.plugins = fileAcct
Service.auth.plugins =
Service.tracking.plugins = fileAcct
Subscription.auth.plugins =
# default user authentication
Retailer.auth.plugins = ldapAuth
Interface.tracking.plugins =
# default dhcp authentication
Retailer.dhcpauth.plugins =
```

Example: LDAP Authentication Plug-In

The following LDAP authentication plug-in searches for objects of class inetOrgPerson, where the username is stored as the common name (cn):

```
Plugin.ldapAuthFoo.class = \ com.junipernetworks.ssc.plugin.LdapAuthenticator
Plugin.ldapAuthFoo.method = search
Plugin.ldapAuthFoo.host = 10.1.2.3
Plugin.ldapAuthFoo.bindDN = cn=admin
Plugin.ldapAuthFoo.bindPW = {BASE64}c3Nw
Plugin.ldapAuthFoo.filter = (objectclass=inetOrgPerson)
Plugin.ldapAuthFoo.nameAttr = cn
Plugin.ldapAuthFoo.pwdAttr = userPassword
```

Example: Basic RADIUS Accounting Plug-In

The following example configures the basic RADIUS accounting plug-in. The name of the plug-in instance is radiusAcct-1. It communicates with two peers: peer 0 over port 1813 at address 10.1.2.3 and peer 1 over port 1813 at 10.1.2.4. Load-balancing is set to failover. The RADIUS Calling-Station-Id is not sent to the plug-in.

```
Plugin.radiusAcct-1.class = net.juniper.smgmt.sae.plugin.\
RadiusTrackingPluginEventListener
Plugin.radiusAcct-1.loadBalancingMode = failover
Plugin.radiusAcct-1.local.timeout = 10000
Plugin.radiusAcct-1.CallingStationId = no
Plugin.radiusAcct-1.peer.0.remote.address = 10.1.2.3
Plugin.radiusAcct-1.peer.0.remote.port = 1813
Plugin.radiusAcct-1.peer.0.remote.password = secret
Plugin.radiusAcct-1.peer.1.remote.password = {BASE64}c2Vjc
Plugin.radiusAcct-1.peer.1.remote.address = 10.1.2.4
Plugin.radiusAcct-1.peer.1.remote.port = 1813
Plugin.radiusAcct-1.peer.1.remote.password = secret
```

Chapter 11

Configuring Authorization and Accounting Plug-Ins with SDX Configuration Editor

This chapter describes how to configure accounting and authorization plug-ins with SDX Configuration Editor. It also describes how to configure global and default retailer event publishers.

You can also configure plug-ins with the SRC CLI. See *Chapter 12, Configuring Accounting and Authentication Plug-Ins with the SRC CLI*.

Topics in this chapter include:

- Configuring Tracking Plug-Ins on page 152
- Configuring Authorization Plug-Ins on page 160
- Using RADIUS Plug-In Fields on page 170
- Configuring UDP Ports for RADIUS Plug-Ins on page 174
- Creating RADIUS Peers on page 175
- Defining RADIUS Packets for Flexible RADIUS Plug-Ins with SDX Configuration Editor on page 176
- Configuring Event Publishers on page 184

Configuring Tracking Plug-Ins

This section shows how to configure the tracking plug-ins described in Table 16.

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 router. 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 16: 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.smgt.sae.plugin.RadiusTrackingPluginEventListener
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—net.juniper.smgt.sae.plugin.CustomRadiusAccounting
Flat file accounting	Writes tracking information to a file in comma-separated format. Java class name—net.juniper.smgt.sae.plugin.FileTrackingPluginEventListener
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—net.juniper.smgt.sae.plugin.FlexibleRadiusTrackingPluginEventListener
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</i> in <i>SRC-PE Solutions Guide, Chapter 6, Configuring the SAE for a PCMM Environment with SDX Configuration Editor</i> . Java class name—net.juniper.smgt.sae.plugin.RksEventListener
QoS profile tracking	Ensures that as a subscriber activates and deactivates services, the correct QoS profile is attached to the subscriber interface. See <i>SRC-PE Solutions Guide, Chapter 1, Managing Tiered and Premium Services with QoS on JUNOS Routers</i> . Java class name—net.juniper.smgt.sae.plugin.qtp.QosProfileTrackingPluginEventListener

The overall steps to configure a tracking plug-in are:

1. Create and configure a plug-in instance in the plug-in pool. The following sections show how to create and configure an instance for each type of tracking plug-in.
2. Configure an event publisher to publish events to the plug-in instance.

See *Configuring Event Publishers* on page 184.

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*. You can modify the fileAcct instance, use it as is, or create a new instance.

Another item that you can configure for flat files is the names of the headers that appear in the file. See *Configuring Headers for Flat File Accounting Plug-Ins* on page 156.

To create flat-file accounting plug-in instances:

1. In the Plug-In Pool area of the Plug-Ins pane, create a flat file accounting instance as described in *Creating Plug-In Instances* on page 143.

The instance appears in the Plug-In Pool area.

2. Fill in the fields for the plug-in instance as described below.

Filename

- Name and location of the file to which the SAE writes accounting information. The SAE names accounting files by appending the timestamp for the start of the accounting period.
- Value—Path and name of file
- Default—*var/acct/log*
- Property name—File

Template

- Name of a template that defines header names for attributes listed in accounting files. See *Configuring Headers for Flat File Accounting Plug-Ins* on page 156.
- Value—Name of the template in the format FileAccounting. <template name>
- Default—FileAccounting.std
- Property name—Template

Interval [hour]

- Number of hours of information stored in each accounting file. When the interval expires, the SAE closes the file, renames it to the archive name, and creates a new file.
- Accounting files are aligned with midnight of the day the SAE process starts. If the interval is 24 hours, the SAE starts a new file at midnight every day beginning on the day that the SAE starts.
 - If the interval is a divisor of 24 hours (for example, 15 minutes, 30 minutes, 1 hour), there is a repeatable pattern of file starts. For example, if the interval is set to 6 hours, the SAE creates a new file at midnight, 6 am, 12 am, and 6 pm every day.
 - If the interval is not a divisor of 24, then the file-start times shift each day to different times of the day.
- If the SAE is restarted, the schedule for creating accounting files is reset to start at midnight.
- Value—Integer in the format <hour> [“:” <minute>]; there are no restrictions on interval length, but we recommend that you set a value that is a divisor of 24 hours
- Default—24
- Property name—Interval

Fields

- Attributes to be recorded as fields in the accounting file.
- Value—Comma-separated list of any of the following attributes:
 - NAS_ID—Identifier of the SAE (configurable)
 - PA_ACCOUNTING_ID—Accounting ID attribute from LDAP
 - PA_AGGR_ACCOUNTING_ID—Accounting ID of the subscriber who started the aggregate service session
 - PA_AGGR_AUTH_USER_ID—Subscriber ID that was used to authenticate the aggregate service session
 - PA_AGGR_LOGIN_NAME—Login name of subscriber who started the aggregate service session
 - PA_AGGR_SESSION_ID—Accounting session ID of the aggregate service session
 - PA_AGGR_USER_DN—Subscriber profile DN of the subscriber who started the aggregate service session
 - PA_AGGR_USER_IP—IP address of the subscriber who started the aggregate service session
 - PA_AUTH_USER_ID—Subscriber ID used for service authentication
 - PA_DOMAIN—Domain for secondary authentication
 - PA_DOWNSTREAM_BANDWIDTH—Downstream bandwidth for the service
 - PA_EVENT_TIME—Timestamp when the event was created

- PA_EVENT_TIME_MILLISECOND—Number of milliseconds since midnight 1970-01-01 UTC
- PA_IF_INDEX—SNMP index of the router interface
- PA_IF_RADIUS_CLASS—RADIUS class of the router interface
- PA_IF_SESSION_ID—Session ID assigned by the router
- PA_IN_OCTETS—Number of octets received from the subscriber (64 bit)
- PA_IN_PACKETS—Number of packets received from the subscriber (64 bit)
- PA_INTERFACE_ALIAS—Alias of router interface
- PA_INTERFACE_DESCR—Description of router interface
- PA_INTERFACE_NAME—Name of router interface
- PA_LOGIN_ID—Subscriber's login ID
- PA_LOGIN_NAME—Name of logged-in subscriber
- PA_NAS_IP—IP address that the router uses for accounting
- PA_NAS_INET_ADDRESS—IP address of the router that uses a byte array instead of an integer
- PA_NAS_PORT—Identifier that the router uses to identify the interface to RADIUS
- PA_OPERATIONAL—Flag that identifies whether an interface was operational at the time of the tracking event
- PA_OUT_OCTETS—Number of octets sent to the subscriber (64 bit)
- PA_OUT_PACKETS—Number of packets sent to the subscriber (64 bit)
- PA_PASSWORD—Password for secondary authentication
- PA_PORT_ID—Identifier of the physical interface (VirtualRouter@ERX interface slot/port.sub)
- PA_PRIMARY_USER_NAME—pppLoginName or public DhcpUserName
- PA_PROPERTY—Session property
- PA_RADIUS_CLASS—RADIUS class attribute
- PA_REPLY_MESSAGE—Message that a plug-in returns to the SAE during authorization
- PA_RETAILER_DN—Retailer DN associated with the domain
- PA_ROUTER_NAME—Name of the router
- PA_SERVICE_BUNDLE—RADIUS vendor-specific attribute (VSA) that a user authorization plug-in returns to the SAE
- PA_SERVICE_NAME—Name of SAE service
- PA_SERVICE_SCOPE—List of service scopes
- PA_SERVICE_SESSION_NAME—Name of dynamic service session
- PA_SERVICE_SESSION_TAG—Tag string assigned to dynamic service session
- PA_SESSION_ID—Session ID assigned by the SAE
- PA_SESSION_TIMEOUT—Number of seconds that the session is up

- PA_SESSION_VOLUME_QUOTA—Amount of data that a subscriber is allowed to upload or download
- PA_SSP_HOST—Hostname of the SAE server
- PA_SUBSCRIPTION_NAME—Name of the subscription
- PA_SUBSTITUTION—Parameter substitution set by a service or user authorization plug-in
- PA_TERMINATE_CAUSE—RADIUS termination cause (See RFC 2866—RADIUS Accounting (June 2000)—for possible values.)
- PA_TERMINATE_TIME—Time to end a subscriber session
- PA_UID—Subscriber ID used for secondary authentication
- PA_UPSTREAM_BANDWIDTH—Upstream bandwidth for the service
- PA_USER_DN—DN of the subscriber profile
- PA_USER_INET_ADDRESS—IP address of the subscriber that uses a byte array instead of an integer
- PA_USER_IP_ADDRESS—IP address of subscriber
- PA_USER_MAC_ADDRESS—MAC address of DHCP subscriber session
- PA_USER_SESSION_ID—RADIUS session ID for the subscriber session
- PA_USER_TYPE—Type of subscriber session: ASSIGNEDIP, AUTHINTF, INTF, ADDR, AUTHADDR, PORTAL
- PA_USER_RADIUS_CLASS—RADIUS class of the subscriber session that is associated with the service session
- STATUS—Accounting status: start, stop, and interim
- Default—STATUS,NAS_ID,PA_SSP_HOST,PA_ROUTER_NAME, PA_INTERFACE_NAME,PA_INTERFACE_ALIAS,PA_INTERFACE_DESCR, PA_PORT_ID,PA_USER_IP_ADDRESS,PA_LOGIN_NAME,PA_ACCOUNTING_ID, PA_AUTH_USER_ID,PA_IF_RADIUS_CLASS,PA_IF_SESSION_ID, PA_SERVICE_NAME,PA_RADIUS_CLASS,PA_EVENT_TIME,PA_SESSION_ID, PA_TERMINATE_CAUSE,PA_SESSION_TIME,PA_IN_OCTETS,PA_OUT_OCTETS, PA_IN_PACKETS,PA_OUT_PACKETS,PA_NAS_IP,PA_USER_MAC_ADDRESS, PA_SERVICE_SESSION_NAME,PA_SERVICE_SESSION_TAG,PA_USER_TYPE, PA_USER_RADIUS_CLASS,PA_USER_SESSION_ID
- Property name—Fields

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
```

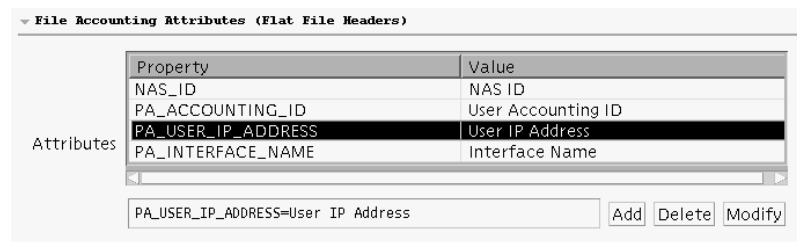
```
start,SSPuelmo,uemo,default@erx7_ssp57,FastEthernet1/1.1,,IP1/1.1,default@erx7
_ssp57 FastEthernet1/1:65535, 10.10.10.20,pebbles@virneo.net,,,,,erx fastEthernet
1/1:0001048619,Video-Gold,Video-Gold,Fri Jan 30 14:23:29 EDT 2004,
VideoGold:null:1064946209182, 0,0,0,0,0,0, 10.10.7.17,,,,PPP,
pebbles:1064946144841
```

You can assign your own names to the headers that appear in the file. To do so, you 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:

1. In the File-Acct Template tab, create a File Accounting Attributes instance as described in *Creating Plug-In Instances* on page 143.

The new instance appears.



2. Define header names in the attribute table in the format property = value, where property is the attribute name and value is the header name that you want to assign to the attribute. Configure the attribute table as follows:
 - To add an attribute, type the attribute definition in the format property = value in the field below the attribute table, and click **Add**.
 - To modify an attribute, select the attribute, make your changes in the field below the attribute table, and click **Modify**.
 - To delete an attribute, select the attribute, and click **Delete**.

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. In the Plug-In Pool area of the Plug-Ins pane, create a basic RADIUS accounting plug-in instance as described in *Creating Plug-In Instances* on page 143.

The instance appears in the Plug-In Pool area.

Basic Radius Accounting (BasicRadiusAcct)

Load Balancing Mode	Failover	
Failover fallback timer	-1	
NASIP		Disable
Retry Interval [ms]	1000	
Max Queue Length	10000	
Bind Address		Disable
UDP Port		Disable
Username	Login Name	
Calling Station Id	Do not use	
Default peer		
Peer Group		

2. Fill in the fields for the plug-in instance as described in *Using RADIUS Plug-In Fields* on page 170.
3. In the Peer Group area, create at least one RADIUS peer to use as the default peer. See *Creating RADIUS Peers* on page 175.

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.

You can also extend custom RADIUS plug-ins to perform the same functions as the flexible RADIUS plug-ins. These custom plug-ins are also internal plug-ins, but are designed to deliver better system performance. See *Configuring Custom RADIUS Accounting-Plug-Ins* on page 159.

To set up flexible RADIUS accounting plug-ins:

1. In the Plug-In Pool area of the Plug-Ins pane, create a flexible RADIUS accounting plug-in instance as described in *Creating Plug-In Instances* on page 143.

The instance appears in the Plug-In Pool area.

2. Fill in the fields for the plug-in instance as described in *Using RADIUS Plug-In Fields* on page 170.
3. In the Peer Group area, create at least one peer to use as the default peer. See *Creating RADIUS Peers* on page 175.
4. (Optional) Assign a RADIUS packet template to the instance, or create a packet definition for the instance. See *Defining RADIUS Packets for Flexible RADIUS Plug-Ins with SDX Configuration Editor* on page 176.

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 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 SRC software distribution in the folder `SDK/doc/sae/net/juniper/smgt/sae/radiuslib` or in the SAE Core API documentation on the Juniper Networks Web site at

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

For a sample implementation, see the following directory in the SRC software distribution:

SDK/plugin/java/src/net/juniper/smg/sample/radiuslib/RadiusPacketHandlerImpl.java.

To set up custom RADIUS accounting plug-ins:

1. In the Plug-In Pool area of the Plug-Ins pane, create a custom RADIUS accounting plug-in instance as described in *Creating Plug-In Instances* on page 143.

The instance appears in the Plug-In Pool area.

Custom Radius Accounting (customRADIUSaccounting-1)

Java Class of RADIUS Packet Handler	<input type="text"/>	
Class Path for RADIUS Packet Handler	<input type="text"/>	Disable
Append Acct-Status-Type Attribute	Yes	Disable
Require Mandatory Attributes	Yes	Disable
Load Balancing Mode	Failover	
Failover Failback Timer	-1	
Timeout [ms]	15000	
Retry Interval [ms]	3000	
Max Queue Length	10 000	
Bind Address	<input type="text"/>	Disable
UDP Port	<input type="text"/>	Disable
Default Peer	<input type="text"/>	
Peer Group		

2. Fill in the plug-in instance fields as described in *Using RADIUS Plug-In Fields* on page 170.
3. In the Peer Group area, create at least one peer to use as the default peer. See *Creating RADIUS Peers* on page 175.

Configuring Authorization Plug-Ins

This section shows how to configure the authorization plug-ins described in Table 17. 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 authorization 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.) Authorization succeeds if all plug-in calls succeed.

Table 17: Authorization Plug-Ins

Plug-In	Description
Basic RADIUS authentication	Sends authentication information to an external RADIUS authentication server or a group of redundant servers. Java class name— <code>net.juniper.smgt.sae.plugin.RadiusAuthPluginEventListener</code>
Custom RADIUS authentication	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. Java class name— <code>net.juniper.smgt.sae.plugin.CustomRadiusAuth</code>
Flexible RADIUS authentication	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. Java class name— <code>net.juniper.smgt.sae.plugin.FlexibleRadiusAuthPluginEventListener</code>
LDAP authentication	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. Java class name of the subscriber authentication plug-in— <code>net.juniper.smgt.sae.plugin.LdapAuthenticator</code> Java class name of the administrator authentication plug-in— <code>net.juniper.smgt.sae.plugin.adminLdap</code>
Limiting subscribers	Limits the number of authenticated subscribers who connect to an IP interface on the router. Java class name— <code>net.juniper.smgt.sae.plugin.LimitNumSubscriberPerIntfAuthPluginListener</code>

The overall steps to configure an authorization plug-in are:

1. Create and configure a plug-in instance in the plug-in pool. The following sections show how to create and configure an instance for each type of authorization plug-in.
2. Configure an event publisher to publish events to the plug-in instance.

See *Configuring Event Publishers* on page 184.

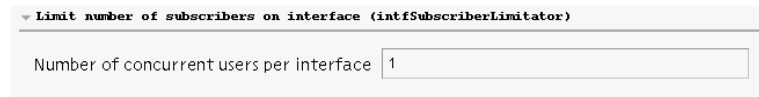
Limiting Subscribers on Router Interfaces

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 interfaces:

1. In the Plug-In Pool area of the Plug-Ins pane, create a Limit number of subscribers on interface plug-in instance as described in *Creating Plug-In Instances* on page 143.

The instance appears in the Plug-In Pool area.



▼ Limit number of subscribers on interface (intfSubscriberLimitator)

Number of concurrent users per interface

2. Fill in the number of authenticated subscribers that you want connected to an interface simultaneously.

Number of concurrent users per interface

- Number of authenticated subscribers who can connect to an IP interface on the router simultaneously.
- Value—Integer in the range 0–2147483647
- Default—1
- Property name—max_user

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. In the Plug-In Pool area of the Plug-Ins pane, create a basic RADIUS authentication plug-in instance as described in *Creating Plug-In Instances* on page 143.

The instance appears in the Plug-In Pool area.

Basic Radius Authenticator (BasicRadiusAuth)

Load Balancing Mode:

Fallover fallback timer:

NASIP:

Retry Interval [ms]:

Max Queue Length:

Bind Address:

UDP Port:

Default peer:

☒ **Peer Group**

Create a New Instance of:

Delete an Instance:

2. Fill in the fields for the plug-in instance as described in *Using RADIUS Plug-In Fields* on page 170.
3. In the Peer Group area, create at least one RADIUS peer to use as the default peer. See *Creating RADIUS Peers* on page 175.

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.

You can also extend custom RADIUS plug-ins to perform the same functions as the flexible RADIUS plug-ins. These custom plug-ins are also internal plug-ins, but are designed to deliver better system performance. See *Configuring Custom RADIUS Authentication Plug-Ins* on page 164.

To set up flexible RADIUS authentication plug-ins:

1. In the Plug-In Pool area of the Plug-Ins pane, create a flexible RADIUS authentication plug-in instance as described in *Creating Plug-In Instances* on page 143.

The instance appears in the Plug-In Pool area.

The screenshot shows the configuration window for the 'Flexible Radius Authenticator (flexRadiusAuth)'. The window has a title bar with a dropdown arrow and the text 'Flexible Radius Authenticator (flexRadiusAuth)'. Below the title bar, there are several configuration fields:

- Load Balancing Mode:** A dropdown menu set to 'Failover'.
- Failover fallback timer:** A text input field containing '-1'.
- Timeout [ms]:** A text input field containing '15000'.
- Retry Interval [ms]:** A text input field containing '3000'.
- Max Queue Length:** A text input field containing '10000'.
- Bind Address:** A text input field with a 'Disable' button to its right.
- UDP Port:** A text input field with a 'Disable' button to its right.
- Error handling:** A dropdown menu set to 'ignore'.
- Default peer:** A text input field containing '1'.
- Peer Group:** A section header with a right-pointing arrow.
- Template:** A text input field containing 'RadiusPacket.stdAuth'.
- Radius Packet Definition:** A section header with a right-pointing arrow.

2. Fill in the plug-in instance fields as described in *Using RADIUS Plug-In Fields* on page 170.
3. In the Peer Group area, create at least one peer to use as the default peer. See *Creating RADIUS Peers* on page 175.
4. (Optional) Assign a RADIUS packet template to the instance, or create a packet definition for the instance. See *Defining RADIUS Packets for Flexible RADIUS Plug-Ins with SDX Configuration Editor* on page 176.

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 which 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 SRC software distribution in the folder *SDK/doc/sae/net/juniper/smg/sae/radiuslib* or the SAE core API documentation on the Juniper Networks Web site at

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

For a sample implementation, see the following directory in the SRC software distribution:

SDK/plugin/java/src/net/juniper/smg/sample/radiuslib/RadiusPacketHandlerImpl.java.

To set up custom RADIUS authentication plug-ins:

1. In the Plug-In Pool area of the Plug-Ins pane, create a custom RADIUS authentication plug-in instance as described in *Creating Plug-In Instances* on page 143.

The instance appears in the Plug-In Pool area.

Custom Radius Authenticator (customRADIUSauth-1)

Java Class of RADIUS Packet Handler	<input type="text"/>
Class Path for RADIUS Packet Handler	<input type="text"/> <input type="button" value="Disable"/>
Require Mandatory Attributes	<input type="text" value="Yes"/> <input type="button" value="Disable"/>
Load Balancing Mode	<input type="text" value="Failover"/> <input type="button" value="Disable"/>
Failover Failback Timer	<input type="text" value="-1"/>
Timeout [ms]	<input type="text" value="15000"/>
Retry Interval [ms]	<input type="text" value="3000"/>
Max Queue Length	<input type="text" value="10 000"/>
Bind Address	<input type="text"/> <input type="button" value="Disable"/>
UDP Port	<input type="text"/> <input type="button" value="Disable"/>
Default Peer	<input type="text"/>
Peer Group <input type="button" value="➤"/>	



2. Fill in the plug-in instance fields as described in *Using RADIUS Plug-In Fields* on page 170.
3. In the Peer Group area, create at least one peer to use as the default peer. See *Creating RADIUS Peers* on page 175.

Configuring LDAP Authentication Plug-Ins

To create LDAP authentication plug-ins:

1. In the Plug-In Pool area of the Plug-Ins pane, create an Ldap authenticator plug-in instance as described in *Creating Plug-In Instances* on page 143.

The instance appears in the Plug-In Pool area.

▼ Ldap Authenticator (LdapAuthenticator)	
Method	<input type="text" value="Search"/> 
LDAP Server	<input type="text"/>
Bind DN	<input type="text"/>
Bind Password	<input type="password"/> <input type="button" value="Show"/>
Search Filter	<input type="text" value="(objectClass=umcSubscriber)"/> <input type="button" value="Disable"/>
Secured LDAP protocol	<input type="text"/>  <input type="button" value="Disable"/>
Search Base DN	<input type="text"/> <input type="button" value="Disable"/>
Name Attribute	<input type="text" value="uniqueId"/> <input type="button" value="Disable"/>
Password Attribute	<input type="text"/> <input type="button" value="Disable"/>
Service Bundle Attribute	<input type="text"/> <input type="button" value="Disable"/>
Session Volume Quota	<input type="text"/> <input type="button" value="Disable"/>
Timeout [ms]	<input type="text" value="5000"/> <input type="button" value="Disable"/>

2. Fill in the plug-in instance fields as described below.

Method

- LDAP authentication method that the SAE uses.
- Value
 - search—SAE searches the directory for the username that the subscriber enters, retrieves the found object, and compares the password stored in the object with the provided password.

You can store passwords in clear text or encrypted (hashed) format by using the crypt (UNIX /etc/passwd), SHA, or MD5 algorithms. The format for a hashed password is:

{crypt}hashed password, {sha}base64 SHA password, or {md5}base64 MD5 password.

- bind—SAE performs a directory search, retrieves the DN of the found object, and tries to bind this DN and the password that the subscriber provides.

If you specify the bind method, the plug-in uses the provided username and password to authenticate the directory (bind).

You can store passwords in clear text or encrypted (hashed) format by using the crypt (UNIX /etc/passwd), SHA, or MD5 algorithms. You must use an encryption method that the directory supports.

- Guidelines—Both search and bind have different implications for system security and performance. When you design the system, consider:
 - search—Because the SAE retrieves passwords from the directory, the directory must allow read access to the password. Allowing read access can be a security risk because an attacker may be able to read passwords in subscriber profiles. However, to lower the risk of password exposure, you can store passwords in encrypted (hashed) form.
 - bind—SAE sends the password to the directory for authentication. The advantage is that passwords never need to be read from the directory. However, passwords are sent in clear text, and an attacker could intercept them.

Bind is a relatively expensive operation that can affect system performance.

- Default—search
- Property name—method

LDAP Server

- Comma-separated list of IP addresses or hostnames of the LDAP authentication server.
- Value—IP address
- Default—127.0.0.1
- Property name—host

Bind DN

- DN used to authenticate access to the directory.
- Value—DN
- Default—*cn = ssp, ou = Components, o = Operators, < base >*
- Property name—bindDN

Bind Password

- Password that the SAE uses to authenticate its access to the directory to search for the subscriber profile. If you do not specify a bind DN or bind password, the SAE uses anonymous access.
- Value—Characters that make up the password; SDX Configuration Editor encodes the secret using base64
- Default—ssp
- Property name—bindPW

Search Filter

- Additional LDAP search filter that the SAE uses to search the directory for the subscriber profile. The initial search uses a search filter in the form *(&(nameAttribute = userName) filter)*. The search is successful when the username and the filter match.
- Value—Search filter syntax defined in RFC 2254—The String Representation of LDAP Search Filters (December 1997)
- Default—*(objectClass = umcSubscriber)*
- Property name—filter

Secured LDAP protocol

- Secure protocol used for LDAP connections with the directory. LDAPS, the only protocol supported, causes communication with the directory to be encrypted with Secure Sockets Layer (SSL).
- Value—LDAPS
- Default—LDAPS
- Property name—securityProtocol

Search Base DN

- Base DN for searching entries in the directory. If you do not specify a base DN, the SAE uses the DN of the associated retailer object.
- If you do not specify the base DN, the SAE takes a username in the form *subscriber@domain* and maps domain to a retailer object by comparing *domain* with the domain names stored in the retailer object. There are two special cases:
 - If domain is empty, first the virtual router name and then the name default are tried.
 - If a retailer defines * (asterisk) as a domain name, it is used to map all domains that cannot be mapped directly.

- Value—DN
- Default—No value
- Property name—baseDN

Name Attribute

- Name of the directory attribute that holds the username.
- Value—Attribute name
- Default—uniqueID
- Property name—nameAttr

Password Attribute

- Name of the directory attribute that stores the password.
- Value—Directory attribute name
- Default—userPassword
- Property name—pwdAttr

Service Bundle Attribute

- Name of the directory attribute that contains the name of the service bundle that is used for subscriber authentication. This value is made available to the subscriber classification process and can be used to select the subscriber profile to load.
- Value—Directory attribute name
- Default—No value
- Property name—serviceBundleAttr

Session Volume Quota

- Name of the LDAP attribute that contains the value of the session volume quota. The LDAP plug-in sets the session volume quota to this value.
- Value—Name of LDAP attribute.
- Default—No value
- Property name—sessionVolumeQuotaAttr

Timeout

- Maximum time the SAE waits for a response from a directory server. If the directory server does not respond to the request, the request fails and the SAE logs an error message.
- Value—Number of milliseconds in the range 0–2147483647
- Default—5000
- Property name—operationTimeout

Using RADIUS Plug-In Fields

This section describes the fields in RADIUS plug-ins.

Append Acct-Status-Type Attribute

- Specifies whether or not the plug-in includes the Acct-Status-Type attribute in a RADIUS accounting request packet.
- Values—Yes or No
- Default—Yes
- Property name —setAcctStatusType

Bind Address

- Source IP address that the plug-in uses to communicate with the RADIUS server.
- Value—IP address; if you do not specify an address, the global default address is used. The SAE automatically sets the global default address when you run the **etc/config** command during initial configuration of the SAE. The property for the global address is the AccountingMgr.local.address property in the */opt/UMC/sae/etc/default.properties* file.
- Default—No value
- Property name—local.address

Calling Station Id

- Specifies whether the SAE sends the MAC address of the subscriber in the Calling-Station-Id attribute.
- Value—Send Mac address or Do not use
- Default—Do not use
- Property name—CallingStationId

Class Path for RADIUS Packet Handler

- List of URLs that identify a location from which Java classes are loaded when the plug-in is initialized. Commas separate each URL in the list.
- Value— < class path >
- Guideline—If no value is specified, the SAE loads Java classes specified in the class path for the SAE, including the */opt/UMC/sae/lib* directory.
- Default—No value
- Property name —handler.classpath

Default peer

- Name of the RADIUS server to which the SAE sends accounting packets.
- Value—Name of the server as defined in the RADIUS peer configuration
- Default—No value
- Property name—defaultPeer

Error handling

- Configures the way the SAE handles errors.
- Value
 - ignore—Ignores incorrect definitions and logs them for debugging purposes
 - strict—Logs errors and discards the affected RADIUS packet
- Default—ignore
- Property name—attr_error

Failover fallback timer

- Controls if and when the SAE attempts to fail back to the default peer.
- Value—Integer
 - Number of seconds in the range 1–2147483647 after a failover that the SAE attempts to fail back
 - 0—SAE always attempts to fail back
 - –1—SAE never attempts to fail back
- Default— –1
- Property name—failbackTimer

Java Class of RADIUS Packet Handler

- Name of the Java class that implements the RadiusPacketHandler interface in the RADIUS Client Library.
- Value— < class name >
- Default—No value
- Example—net.juniper.smgmt.radius.RadiusPacketHandlerImpl
- Property name —handler.class

Load Balancing Mode

- Selects the mode for load-balancing RADIUS servers.
- Value—Failover, round-robin
 - Failover—SAE sends requests to the RADIUS server configured as the default peer. If the default peer fails, the SAE uses the next server configured in the peer group. The SAE cycles through the configured RADIUS servers as needed.
 - Round-robin—SAE alternates requests between all RADIUS servers configured in the peer group.
- Default—Failover
- Property name—loadBalancingMode

Max Queue Length

- Maximum number of unacknowledged RADIUS messages that the plug-in receives from the RADIUS server before it discards new messages.
- Value—Integer in the range 0–2147483647
- Default—10000
- Property name—local.maxWaitingQueueLength

NASIP

- Value of the NAS-Ip attribute.
- Value—SSP local IP, RADIUS client IP
 - SSP local IP—IP address of the SAE
 - RADIUS client IP—IP address of the virtual router
- Default—No value
- Property name—local.NASIP

Require Mandatory Attributes

- Specifies whether or not a RADIUS authentication or accounting request must contain all mandatory RADIUS attributes before sending the request packet.
- Values—Yes or No
- Default—Yes
- Property name—forceMandatoryAttr

Retry interval [ms]

- Time the SAE waits for a response from a RADIUS server before it resends the RADIUS packet. The SAE keeps sending RADIUS packets until either the server acknowledges the packet or the maximum timeout is reached.
- Value—Number of milliseconds in the range 0–2147483647
- Default—3000
- Property name—local.retryInterval

Template

- Name of a template that defines sets of RADIUS attributes included in accounting messages. You define templates in the RADIUS tab of SDX Configuration Editor. See *Defining RADIUS Packets for Flexible RADIUS Plug-Ins with SDX Configuration Editor* on page 176.
- Value—Name of the template in the format RadiusPacket. <template name> ; you can enter only one template name
- Default—RadiusPacket.sdtAcct
- Property name—RadiusPacket. <template name>

Timeout [ms]

- Maximum time the SAE waits for a response from a RADIUS server. If the RADIUS server does not respond to the request, the request fails and the SAE logs an error message.
- Value—Number of milliseconds in the range 0–9223372036854775807
- Default—10000
- Property name—local.timeout

UDP Port

- Source UDP port or a pool of ports that the plug-in uses to communicate with the RADIUS server.
- Value—You can enter a single port number, a pool of port numbers, or a list of port numbers and port ranges. If you do not specify a UDP port, the global default port is used (see *Configuring UDP Ports for RADIUS Plug-Ins* on page 174).
 - Port number in the range 1–65535
 - A range of ports in the format port-port; for example, 7000-7003
 - A comma-separated list of port numbers and port ranges
- Default—No value
- Example—7000-7003, 7006, 7007-7009
- Property name—local.port

Username

- Value of the User-Name attribute (RADIUS attribute [1]).
- Value—One of the following:
 - Login Name—Name used for login
 - Accounting ID—Value stored in the subscriber profile
 - Auth User Name—Name used to authenticate a service
 - Manager ID—Value of the manager ID in the service subscription; use this setting to identify subscribers to enterprise services. Manager ID is the value of modifiersName in the subscription; if modifiersName does not exist, manager ID is the value of creatorsName.
 - modifiersName—Contains DN of the administrator who last modified the entry in the directory
 - creatorsName—Contains DN of the administrator who created the entry in the directory
- Default—Login Name
- Property name—Username

Configuring UDP Ports for RADIUS Plug-Ins

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 with SDX Configuration Editor:

1. In the navigation pane, select a directory configuration object for the SAE that you want to configure.
2. Select the **Miscellaneous** tab, and expand the **Global RADIUS UDP Port** section.



The screenshot shows a configuration interface with a tab labeled 'Global RADIUS UDP Port'. Below the tab is a label 'UDP Port' followed by a rectangular text input field.

3. Fill in the field as described in *Global RADIUS UDP Port Field* on page 174.

Global RADIUS UDP Port Field

Use the field in this section to specify a global UDP port for RADIUS plug-ins.

UDP Port

- Source UDP port or a pool of ports that RADIUS plug-ins use to communicate with RADIUS servers.
- Value—You can enter a single port number, a pool of port numbers, or a list of port numbers and port ranges.
 - Port number in the range 1–65535
 - A range of ports in the format port-port; for example, 7000-7003
 - A comma-separated list of port numbers and port ranges

- Default—18130
- Example—7000-7003, 7006, 7007-7009
- Property name—AccountingMgr.local.port

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.



NOTE: If you configure more than one RADIUS peer in a plug-in instance that has the same properties, the SNMP counters for the plug-in will not update correctly. The reason is that the software does not know which RADIUS peer to send updates to.

RADIUS peers are configured in the peer group for each RADIUS plug-in instance. To create a RADIUS peer:

1. In the Peer Group area of a RADIUS plug-in instance, select **Radius Peer** and click **Create a New Instance of**.

The Create New Instance dialog box appears.

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

The new peer instance appears in the Peer Group area.

The screenshot shows the 'Peer Group' configuration area. At the top, there's a section titled 'Peer Group' with a dropdown menu currently set to 'Radius Peer'. To the left of the dropdown is a button labeled 'Create a New Instance of', and to the right is a button labeled 'Delete an Instance'. Below the dropdown, there's a section titled 'Radius Peer (1)'. This section contains three input fields: 'Server Address', 'Server Port', and 'Secret'. The 'Secret' field has a 'Show' button next to it.

3. Fill in the fields as described below.

Server Address

- IP address of the RADIUS server to which the SAE sends accounting data.
- Value—IP address
- Default—No value
- Property name—peer.#.remote.address

Server Port

- Port used for RADIUS accounting packets. RADIUS accounting servers typically use UDP port 1813 or 1646.
- Value—Valid UDP port
- Default—1813
- Property name—peer.#.remote.port

Secret

- Password that is shared with the RADIUS server. You must configure the same secret on the RADIUS server.
- Value—Shared secret; SDX Configuration Editor encodes the secret using BASE-64
- Default—No value
- Property name—peer.#.remote.password

Defining RADIUS Packets for Flexible RADIUS Plug-Ins with SDX Configuration Editor

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.

In SDX Configuration Editor, 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-in instances. You can apply the same template to multiple plug-in instances, but each plug-in instance can use only one template.
- Define attributes in the packet definition configuration of a flexible plug-in instance. These definitions override definitions in packet templates. You can use these packet definitions to exclude attributes that come from the template. To do so, you define the value of the attribute that you want to exclude as None.

Creating and Using RADIUS Templates

The SDX 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

You can use these templates as they are, modify them, or create new templates.

To create a template:

1. In the RADIUS tab, select **Template** from the drop-down list, and click **Create a New Instance of**.

The Create a New Instance dialog box appears.

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

The instance appears in the Radius Packet Template area.

The screenshot shows the 'RADIUS' configuration window. Under the 'Radius Packet Template' section, there are two buttons: 'Create a New Instance of' and 'Delete an Instance'. The 'Create a New Instance of' button has a dropdown menu currently showing 'Template'. Below these buttons are three expandable sections, each with a plus icon and a label: 'Template (stdAcct)', 'Template (stdAuth)', and 'Template (specialAuth)'.

3. Configure RADIUS attributes in the template as described in the next section.
4. Configure a plug-in instance to use the template by entering the name of the template in the format RadiusPacket. < template name > in the Template field of the plug-in instance configuration.

You can apply a template to multiple plug-in instances, but each plug-in instance can use only one template.

Configuring RADIUS Attributes

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 18 lists the available packet types.

Table 18: 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
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

Table 18: RADIUS Attribute Instance Names (continued)

Attribute Instance (Packet-Type)	Type of RADIUS Packet to Which Attribute Definition Is Applied
stop	Stop or Interim Update requests
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	User Session Start, Stop, or Interim requests
userresp	Any user authorization response
userstart	User Session Start requests
userstop	User Session Stop, or Interim requests

Use the steps below to configure attribute instances. You can follow them from within a RADIUS template or within a plug-in instance configuration.

You can configure attribute instances in a RADIUS template or within a plug-in instance configuration. To create and configure attribute instances for a:

- Template—Follow these steps in the Attributes configuration section of a template.
 - Plug-in instance—Follow these steps in the Radius Packet Definition of a plug-in instance.
1. Select **Radius Attributes** from the drop-down list, and click **Create a New Instance of**.

The Create a New Instance dialog box appears.

2. Assign a name that specifies the RADIUS packet type to which the attribute definition applies (see Table 18), and click **OK**.

A new attribute table of properties (RADIUS attributes) and values (the value assigned to an attribute) appears.

3. Configure the attribute table as follows:
 - To add an attribute, type the attribute definition in the format `property = value` in the field below the attribute table, and click **Add**.
 - To modify an attribute, select the attribute, make your changes in the field below the attribute table, and click **Modify**.
 - To delete an attribute, select the attribute, and click **Delete**.

Attributes

Create a New Instance of Delete an Instance

Radius Attributes (auth)

Property	Value
Chap-Challenge	"".join(chr(random.randrange(0
Chap-Password	password
NAS-IP-Address	localNasIp
NAS-Identifier	localNasId
NAS-Port	nasPort
User-Name	loginId
User-Password	password
vendor-specific.WISPr.Location-ID	interfaceAlias
vendor-specific.WISPr.Location-Name	hostName

Property

- RADIUS attribute.
- Value—Standard RADIUS attribute or JUNOS VSA specified as follows:
 - Standard RADIUS attribute 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
 - JUNOS VSA in 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

For example, 26.4874.50.text sets a value for Session-Volume-Quota VSA 26-50.
- Default—No value
- Property name— < id > [. < type >]

Value

- Defines the values of RADIUS attributes. Most values can be sent from the SAE to the plug-in. Some of the values can also be returned by the plug-in.
- Value—Standard values (see Table 19) or an expression
 - Expressions are evaluated with Python. For example: lowWord(inOctets) extracts the lower 32 bits of the 64-bit inOctets counter.
 - You can define multiple values for an expression in a comma-separated list.
- Default—No value
- Property name— < expression >

Table 19: Standard Values for RADIUS Attributes

Value	Type of Plug-In	Comments
accountingId	User and service tracking	
authUserId	Service tracking	
dhcp	User and service tracking	Provides access to DHCP packet. See Table 14 on page 113 for details.
domain	Authorization	
eventTime	User and service tracking	Seconds since 1970-01-01T00:00Z
ifRadiusClass	User and service tracking	
ifSessionId	User and service tracking	
inOctets	Service tracking	64-bit counter
inPackets	Service tracking	
interfaceAlias	User and service tracking	
interfaceDescr	User and service tracking	
interfaceName	User and service tracking	
localNasId	All	Configured NAS-ID
localNasIp	All	Configured NAS-IP
loginId	User and service authorization	ID provided by the subscriber; the loginId value is not separated into UID and domain name.
loginName	User and service tracking	Name that the subscriber uses to log in to portal
nasIp	User and service tracking	NAS IP address of the router
nasPort	User and service tracking	32-bit integer
outOctets	Service tracking	64-bit counter
outPackets	Service tracking	
password	User and service authorization	
portId	User and service tracking	ID of the port on the JUNOSe router; for example, FastEthernet 3/1:2001
primaryUserName	User and service tracking	Name that the subscriber uses for DHCP/PPP authentication
radiusClass	User tracking, user and service authorization	For service tracking, this value is taken from the RADIUS Access-Accept response. If the response does not contain a value, the RADIUS class defined in the service definition is used. This attribute can be set by an authorization response.

Table 19: Standard Values for RADIUS Attributes (continued)

Value	Type of Plug-In	Comments
replyMessage	User and service authorization	This attribute can only be set.
routerName	User and service tracking	
serviceBundle	User tracking and authorization	This attribute can be set by an authorization response.
serviceName	Service tracking	Sets an arbitrary attribute (for example, class) to the name of the service.
serviceSessionName	Service tracking	Named service session; empty for default session
serviceSessionTag	Service tracking	
sessionId	User and service tracking	
sessionTime	User and service tracking	
sessionTimeout	User tracking, user and service authorization	This attribute can be set by an authorization response.
sessionVolumeQuota	User authorization	<p>This attribute can only be set. It is sent for session tracking events and can be returned by service authorization events. It can be set and retrieved through the portal API and can also be defined through an LDAP attribute in the service definition.</p> <p>If the attribute is defined multiple times, the following precedence is observed:</p> <ol style="list-style-type: none"> 1. Service definition (lowest) 2. Authorization 3. API call (highest) <p>NOTE: The SAE does not enforce a volume quota directly; it only makes the attribute available to an external application that can control the volume quota.</p>
setAcctInterimTime	User authorization	Integer
setAuthVirtualRouterName	DHCP authorization	Text
setIdleTimeout(ATTR)	User authorization	
setLoadServices(ATTR)	User authorization	This attribute can only be set.
setPoolName	DHCP authorization	Text
setRadiusClass(ATTR)	User and service authorization	
setReplyMessage(ATTR)	User and service authorization	
setSessionTimeout(ATTR)	User and service authorization	
setServiceBundle(ATTR)	User authorization	
setSessionVolumeQuota(ATTR)	User authorization	
setSubstitution	User authorization	Text. Substitutions can be set only for service sessions.
setTerminateTime	User authorization	Text
setUserIpAddress	DHCP authorization	Integer
sspHost	User and service tracking	
terminateCause	User and service tracking	
uid	User and service authorization	
userDn	User and service tracking	

Table 19: Standard Values for RADIUS Attributes (continued)

Value	Type of Plug-In	Comments
userIpAddress	User and service tracking	
userMacAddress	User and service tracking	
userRadiusClass	Service tracking	RADIUS class of associated subscriber session
userSessionId	Service tracking	RADIUS session ID of associated subscriber session

More About Using Flexible RADIUS Packet Definitions

This section 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:

```
RadiusPacket.std.svcstop.Acct-Input-Octets = lowWord(inOctets)
RadiusPacket.std.svcstop.Acct-Output-Octets = lowWord(outOctets)
RadiusPacket.std.svcstop.Acct-Input-Packets = inPackets
RadiusPacket.std.svcstop.Acct-Output-Packets = outPackets
```

```
RadiusPacket.std.svcstop.Acct-Input-Gigawords = highWord(inOctets)
RadiusPacket.std.svcstop.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)

Table 19 on page 180 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

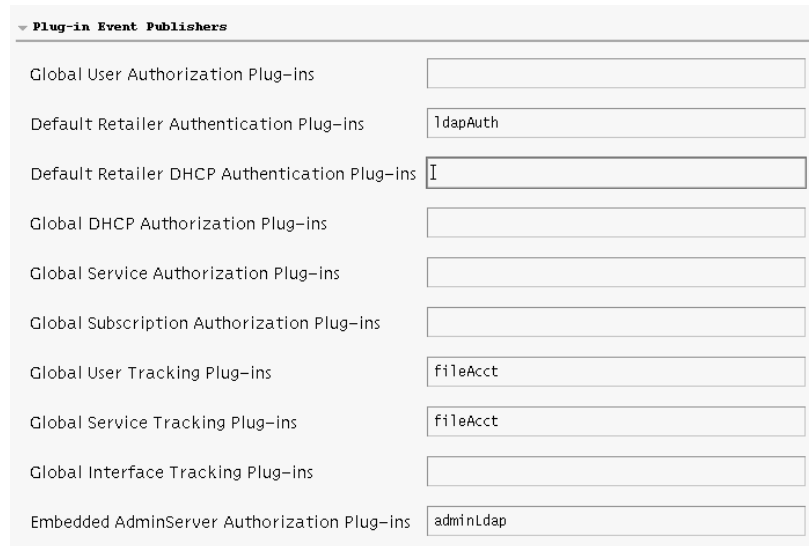
This section shows how to configure event publishers. It covers the following tasks:

- Configuring Global and Default Retailer Event Publishers on page 185
- Configuring Service-Specific Event Publishers on page 187
- Configuring Retailer-Specific Event Publishers on page 188
- Configuring Virtual Router-Specific Event Publishers on page 188

Configuring Global and Default Retailer Event Publishers

You can use SDX Configuration Editor to configure global and default retailer event publishers. To do so:

1. Access the plug-in configuration as described in *Accessing the Plug-In Configuration* on page 141.



Plug-in Event Publishers	
Global User Authorization Plug-ins	
Default Retailer Authentication Plug-ins	ldapAuth
Default Retailer DHCP Authentication Plug-ins	I
Global DHCP Authorization Plug-ins	
Global Service Authorization Plug-ins	
Global Subscription Authorization Plug-ins	
Global User Tracking Plug-ins	fileAcct
Global Service Tracking Plug-ins	fileAcct
Global Interface Tracking Plug-ins	
Embedded AdminServer Authorization Plug-ins	adminLdap

2. In the Plug-In Event Publishers area, enter a comma-separated list of plug-in instances in each event publisher field that you want to configure.

Global User Authorization Plug-ins

- Authorize all subscriber sessions. These plug-in instances are called after a subscriber profile is loaded but before a subscriber session is started. The SAE calls these plug-ins for each subscriber who logs in to a portal.
- These plug-in instances cannot perform authentication, because passwords are not available at this point in the login process. Therefore, if you specify plug-in instances that perform authentication, login requests will fail.
- Value—Comma-separated list of plug-in instances
- Default—No value
- Property name—User.auth.plugins

Default Retailer Authentication Plug-ins

- Authenticate subscribers who are assigned to retailer objects that do not specify an authentication plug-in. These plug-ins are called when a subscriber logs in to the domain. The authentication process for portal (Web) logins maps the supplied domain name to a retailer object.
- If you do not specify default retailer authentication plug-ins or retailer-specific plug-ins, subscribers are admitted without authentication.
- Value—Comma-separated list of plug-in instances

- Default—ldapAuth
- Property name—Retailer.auth.plugins

Default Retailer DHCP Authentication Plug-ins

- Authenticate DHCP address requests for subscribers who are assigned to retailer objects that do not specify a DHCP authorization plug-in. These plug-ins are called when the SAE receives a DHCP discover request from a client that has its username and password cached in the SAE. The username and password can either be cached persistently in the directory or temporarily in memory during a switch from an unauthenticated to an authenticated address.
- Value—Comma-separated list of plug-in instances
- Default—No value
- Property name—Retailer.dhcpauth.plugins

Global DHCP Authorization Plug-ins

- Authorize all DHCP address requests for all DHCP subscribers who log in to a portal. These plug-in instances are called for both authenticated and unauthenticated address requests.
- Value—Comma-separated list of plug-in instances
- Default—No value
- Property name—Dhcp.auth.plugins

Global Service Authorization Plug-ins

- Authorize all service sessions. These plug-ins are called before a service session is started, and are called for every service session started by any SAE subscriber.
- Value—Comma-separated list of plug-in instances
- Default—No value
- Property name—Service.auth.plugins

Global Subscription Authorization Plug-ins

- Authorize subscribers to change their subscriptions. These plug-ins are called when a subscriber tries to modify, subscribe to, or unsubscribe from a subscription.
- Value—Comma-separated list of plug-in instances
- Default—No value
- Property name—Subscription.auth.plugins

Global User Tracking Plug-ins

- Track all subscriber sessions. These plug-in instances are called for every subscriber session that is started and stopped. They are called after a subscriber session has started and when the session is stopped.
- Value—Comma-separated list of plug-in instances

- Default—fileAcct
- Property name—User.tracking.plugins

Global Service Tracking Plug-ins

- Track all service sessions. These plug-in instances are called for every service session that is started and stopped. They are called after a service session starts, when the service session stops, and during interim updates.
- Value—Comma-separated list of plug-in instances
- Default—fileAcct
- Property name—Service.tracking.plugins

Global Interface Tracking Plug-ins

- Track all interfaces that the SAE manages. You can set up the publisher to send interface tracking events to plug-in instances or to a network information collector (NIC) SAE plug-in agent. These plug-in instances and/or NIC SAE plug-in agents are called for every managed interface that is started and stopped. They are called after an interface comes up, when new policies are installed on the interface, and when the interface goes down.
- Value—Comma-separated list of plug-in instances or NIC SAE plug-in agents
- Default—No value
- Property name—Interface.tracking.plugins

Embedded AdminServer Authorization Plug-ins

- Authorize administrators to connect to the embedded Web server, which is used to access SAE Web Admin.
- Value—Comma-separated list of plug-in instances
- Default—adminLdap
- Property name—AdminServer.realm.auth.plugins

Configuring Service-Specific Event Publishers

In the value-added services definition in SDX Admin, you can configure two event publishers for a service:

- Authorization plug-ins—Authenticate subscribers of the service and/or authorize service sessions for this service. These plug-in instances are called before a subscription to this service is activated.
- Tracking plug-ins—Track service sessions of this service. These plug-in instances are called when a service session is started and stopped and during interim updates.

You configure these event publishers in the SSP Services window in SDX Admin. See *SRC-PE Services and Policies Guide, Chapter 2, Managing Services on a Solaris Platform*.

Configuring Retailer-Specific Event Publishers

In the retailer definition in SDX Admin, you can configure three event publishers for a retailer:

- Authentication plug-ins—Authenticate subscribers who log in to the domains of the retailer. These plug-in instances are called when a subscriber tries to log in to the SAE through the portal login.

If you do not specify retailer-specific authentication plug-ins, the default retailer authentication plug-ins are called. If you do not specify default retailer authentication plug-ins, subscribers are admitted without authentication.

- Tracking plug-ins—Track sessions of subscribers who log in to the domains of the retailer. These plug-in instances are called after a subscriber session has started and when the session is stopped.
- DHCP authorization plug-ins—Authenticate DHCP address requests for subscribers who log in to the domains of the retailer.

You configure these event publishers in the Retailer pane in SDX Admin. See *Adding Retailers* on page 236.

Configuring Virtual Router-Specific Event Publishers

In the virtual router definition in SDX Admin, you can configure an interface-tracking plug-in event publisher for a virtual router. These plug-in instances are called when a managed interface is started and stopped. They are called after an interface comes up, when new policies are installed on the interface, and when the interface goes down.

You configure this event publisher in the VirtualRouter pane in SDX Admin. For information about configuring virtual routers for JUNOSe routers, see *SRC-PE Network Guide, Chapter 6, Using JUNOSe Routers in the SRC Network with a Solaris Platform*. For information about configuring virtual routers for JUNOS routing platforms, see *SRC-PE Network Guide, Chapter 8, Using JUNOS Routing Platforms in the SRC Network with a Solaris Platform*.

Chapter 12

Configuring Accounting and Authentication Plug-Ins with the SRC CLI

This chapter describes how to configure authentication and accounting plug-ins, with the SRC CLI. It also describes how to configure global and default retailer event publishers.

You can also configure these plug-ins with SDX Configuration Editor. See *Chapter 11, Configuring Authorization and Accounting Plug-Ins with SDX Configuration Editor*.

Topics in this chapter include:

- Creating RADIUS Peers on page 190
- Configuring Tracking Plug-Ins on page 192
- Configuring Authentication Plug-Ins on page 203
- Configuring UDP Ports for RADIUS Plug-Ins on page 215
- Defining RADIUS Packets for Flexible RADIUS Plug-Ins with the SRC CLI on page 215
- Configuring Event Publishers on page 224

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. Use the following configuration statements to configure a RADIUS peer:

```
shared sae configuration plug-ins pool name radius-accounting peer-group name {
    server-address server-address;
    server-port server-port;
    secret secret;
}
```

```
shared sae configuration plug-ins pool name radius-authentication peer-group name {
    server-address server-address;
    server-port server-port;
    secret secret;
}
```

```
shared sae configuration plug-ins pool name custom-radius-accounting peer-group
name {
    server-address server-address;
    server-port server-port;
    secret secret;
}
```

```
shared sae configuration plug-ins pool name custom-radius-authentication peer-group
name {
    server-address server-address;
    server-port server-port;
    secret secret;
}
```

```
shared sae configuration plug-ins pool name flex-radius-accounting peer-group name {
    server-address server-address;
    server-port server-port;
    secret secret;
}
```

```
shared sae configuration plug-ins pool name flex-radius-authentication peer-group
name {
    server-address server-address;
    server-port server-port;
    secret secret;
}
```

To create a RADIUS peer:

1. From configuration mode, access the RADIUS peer configuration for the plug-in that you are configuring. In this sample procedure, the RADIUS peer is configured in the west-region SAE group.

```
user@host# edit shared sae group west-region configuration plug-ins pool  
basicRadius radius-accounting peer-group peer1
```

2. Configure the IP address of the RADIUS server to which the SAE sends accounting data.

```
[edit shared sae group west-region configuration plug-ins pool basicRadius  
radius-accounting peer-group peer1]  
user@host# set server-address server-address
```

3. Configure the port used for RADIUS packets.

```
[edit shared sae group west-region configuration plug-ins pool basicRadius  
radius-accounting peer-group peer1]  
user@host# set server-port server-port
```

4. Configure the password that is shared with the RADIUS server. You must configure the same password on the RADIUS server.

```
[edit shared sae group west-region configuration plug-ins pool basicRadius  
radius-accounting peer-group peer1]  
user@host# set secret secret
```

5. (Optional) Verify your configuration.

```
[edit shared sae group west-region configuration plug-ins pool basicRadius  
radius-accounting peer-group peer1]  
user@host# show  
server-address 10.10.1.1;  
server-port 1812;  
secret *****;
```

Related Information

For additional information, see the following source:

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

Configuring Tracking Plug-Ins

This section shows how to configure the tracking plug-ins described in Table 20.

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 router. 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 20: 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.smgt.sae.plugin.RadiusTrackingPluginEventListener
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—net.juniper.smgt.sae.plugin.CustomRadiusAccounting
Flat file accounting	Writes tracking information to a file in comma-separated format. Java class name—net.juniper.smgt.sae.plugin.FileTrackingPluginEventListener
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—net.juniper.smgt.sae.plugin.FlexibleRadiusTrackingPluginEventListener
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</i> in <i>SRC-PE Solutions Guide, Chapter 5, Configuring the SAE for a PCMM Environment with the SRC CLI</i> . Java class name—net.juniper.smgt.sae.plugin.RksEventListener
QoS profile tracking	Ensures that as a subscriber activates and deactivates services, the correct QoS profile is attached to the subscriber interface. See <i>SRC-PE Solutions Guide, Chapter 1, Managing Tiered and Premium Services with QoS on JUNOS Routers</i> . Java class name—net.juniper.smgt.sae.plugin.qtp.QosProfileTrackingPluginEventListener

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. See *Configuring Headers for Flat File Accounting Plug-Ins* on page 194.

Use the following configuration statements to create flat-file accounting plug-in instances:

```
shared sae configuration plug-ins pool name file-accounting {
    filename filename;
    template template;
    interval interval;
    fields [(status | nas-id | host | router-name | interface-name | interface-alias |
    interface-descr | port-id | user-ip-address | login-name | accounting-id | auth-user-id |
    if-radius-class | if-session-id | service-name | radius-class | event-time | session-id |
    terminate-cause | session-time | in-octets | out-octets | in-packets | out-packets |
    nas-ip | user-mac-address | service-session-name | service-session-tag | user-type |
    user-radius-class | user-session-id | primary-user-name | subscription-name |
    login-id | if-index | event-time-millisecond | nas-port | operational | user-inet-address
    | nas-inet-address | router-type | interface-speed)...];
}
```

To create flat-file accounting plug-ins:

1. From configuration mode, access the basic RADIUS accounting plug-in configuration. In this sample procedure, the plug-in called fileAcct is configured in the west-region SAE group.

```
user@host# edit shared sae group west-region configuration plug-ins pool  
fileAcct file-accounting
```

2. Configure the name and location of the file to which the SAE writes accounting information.

```
[edit shared sae group west-region configuration plug-ins pool fileAcct  
file-accounting]  
user@host# set filename filename
```

3. Configure the name of the template that defines header names for attributes listed in accounting files.

```
[edit shared sae group west-region configuration plug-ins pool fileAcct  
file-accounting]  
user@host# set template template
```

4. Configure the number of hours of information stored in each accounting file.

```
[edit shared sae group west-region configuration plug-ins pool fileAcct  
file-accounting]  
user@host# set interval interval
```

5. Configure the fields that you want to record in the accounting file.

```
[edit shared sae group west-region configuration plug-ins pool fileAcct
file-accounting]
user@host# set fields [(status | nas-id | host | router-name | interface-name |
interface-alias | interface-descr | port-id | user-ip-address | login-name |
accounting-id | auth-user-id | if-radius-class | if-session-id | service-name |
radius-class | event-time | session-id | terminate-cause | session-time | in-octets |
out-octets | in-packets | out-packets | nas-ip | user-mac-address |
service-session-name | service-session-tag | user-type | user-radius-class |
user-session-id | primary-user-name | subscription-name | login-id | if-index |
event-time-millisecond | nas-port | operational | user-inet-address |
nas-inet-address | router-type | interface-speed)...]
```

6. (Optional) Verify your configuration.

```
[edit shared sae group west-region configuration plug-ins pool fileAcct
file-accounting]
user@host# show
filename var/acct/log;
template FileAccounting.std;
interval 24;
fields [ status nas-id host router-name interface-name interface-alias
interface-descr port-id user-inet-address login-name accounting-id
auth-user-id if-session-id service-name event-time session-id
terminate-cause session-time in-octets out-octets in-packets out-packets
nas-inet-address user-mac-address service-session-name service-session-tag
user-type user-session-id ];
```

Related Information

For additional information, see the following source:

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

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,SSPuelmo,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.

Use the following configuration statements to create a file accounting template:

```
shared sae configuration file-accounting-template name ...
```

```
shared sae configuration file-accounting-template name attributes name {
    value;
}
```

To set up a file accounting template:

1. From configuration mode, access the file accounting template configuration. In this sample procedure, the template called `std` is configured in the `west-region` SAE group.

```
user@host# edit shared sae group west-region configuration
file-accounting-template std
```

2. Define header names in the format `attribute "header name"` where the attribute name is the name of a field in the file accounting plug-in.

```
[edit shared sae group west-region configuration file-accounting-template std]
user@host# set attributes value
```

For example:

```
[edit shared sae group west-region configuration file-accounting-template std]
user@host# set attributes terminate-cause "RADIUS Termination Cause"
```

3. (Optional) Verify your configuration.

```
[edit shared sae group west-region configuration file-accounting-template
std]
user@host# show
attributes {
    terminate-cause "RADIUS Termination Cause";
    service-session-name "Service Session Name";
}
```

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.

Use the following configuration statements to configure RADIUS accounting plug-ins:

```
shared sae configuration plug-ins pool name radius-accounting {
    load-balancing-mode (failover | roundRobin);
    failback-timer failback-timer;
    nas-ip (Ssplp | Erxlp);
    retry-interval retry-interval;
    maximum-queue-length maximum-queue-length;
    bind-address bind-address;
    udp-port udp-port;
    username (login-name | accounting-id | auth-user-name | manager-id);
    calling-station-id (mac | no);
    default-peer default-peer;
}
```

To set up basic RADIUS accounting plug-ins:

1. From configuration mode, access the basic RADIUS accounting plug-in configuration. In this sample procedure, the plug-in called basicRadius is configured in the west-region SAE group.

```
user@host# edit shared sae group west-region configuration plug-ins pool  
basicRadius radius-accounting
```

2. Configure the mode for load-balancing RADIUS servers.

```
[edit shared sae group west-region configuration plug-ins pool basicRadius  
radius-accounting]  
user@host# set load-balancing-mode (failover | roundRobin)
```

3. Specify if and when the SAE attempts to fail back to the default peer.

```
[edit shared sae group west-region configuration plug-ins pool basicRadius  
radius-accounting]  
user@host# set failback-timer failback-timer
```

4. (Optional) Configure the value of the NAS-IP attribute.

```
[edit shared sae group west-region configuration plug-ins pool basicRadius  
radius-accounting]  
user@host# set nas-ip (Ssplp | Erxlp)
```

5. Configure the time the SAE waits for a response from a RADIUS server before it resends the RADIUS packet.

```
[edit shared sae group west-region configuration plug-ins pool basicRadius  
radius-accounting]  
user@host# set retry-interval retry-interval
```

6. Configure the maximum number of unacknowledged RADIUS messages that the plug-in receives from the RADIUS server before it discards new messages.

```
[edit shared sae group west-region configuration plug-ins pool basicRadius
radius-accounting]
user@host# set maximum-queue-length maximum-queue-length
```

7. (Optional) Configure the source IP address that the plug-in uses to communicate with the RADIUS server. If you do not specify an address, the global default address is used.

```
[edit shared sae group west-region configuration plug-ins pool basicRadius
radius-accounting]
user@host# set bind-address bind-address
```

8. (Optional) Configure the source UDP port or a range of source UDP ports used for communication with the RADIUS server. If you do not specify a UDP port, the global UDP port is used.

```
[edit shared sae group west-region configuration plug-ins pool basicRadius
radius-accounting]
user@host# set udp-port udp-port
```

9. Configure the value of the User-Name attribute (RADIUS attribute [1]).

```
[edit shared sae group west-region configuration plug-ins pool basicRadius
radius-accounting]
user@host# set username (login-name | accounting-id | auth-user-name |
manager-id)
```

10. Specify whether the SAE sends the MAC address of the subscriber in the Calling-Station-Id attribute.

```
[edit shared sae group west-region configuration plug-ins pool basicRadius
radius-accounting]
user@host# set calling-station-id (mac | no)
```

11. Configure the default peer, which is the RADIUS server to which the SAE sends packets for this plug-in.

```
[edit shared sae group west-region configuration plug-ins pool basicRadius
radius-accounting]
user@host# set default-peer default-peer
```

12. (Optional) Verify your configuration.

```
[edit shared sae group west-region configuration plug-ins pool basicRadius
radius-accounting]
user@host# show
load-balancing-mode failover;
failback-timer -1;
retry-interval 3000;
maximum-queue-length 10000;
username login-name;
calling-station-id no;
default-peer peer1;
```

Related Information

For additional information, see the following sources:

- For information about setting up SAE groups, see *SRC-PE Getting Started Guide, Chapter 16, Setting Up an SAE with the SRC CLI*.
- For information about setting up default peers, see *Creating RADIUS Peers* on page 190.

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.

Use the following configuration statements to configure flexible RADIUS accounting plug-ins:

```
shared sae configuration plug-ins pool name flex-radius-accounting {
    load-balancing-mode (failover | roundRobin);
    fallback-timer fallback-timer;
    timeout timeout;
    retry-interval retry-interval;
    maximum-queue-length maximum-queue-length;
    bind-address bind-address;
    udp-port udp-port;
    error-handling (0 | 1);
    default-peer default-peer;
    template template;
}
```

To set up flexible RADIUS accounting plug-ins:

1. From configuration mode, access the flexible RADIUS accounting plug-in configuration. In this sample procedure, the plug-in called flexRadiusAct is configured in the west-region SAE group.

```
user@host# edit shared sae group west-region configuration plug-ins pool flexRadiusAct flex-radius-accounting
```

2. Configure the mode for load-balancing RADIUS servers.

```
[edit shared sae group west-region configuration plug-ins pool flexRadiusAct flex-radius-accounting]
user@host# set load-balancing-mode (failover | roundRobin)
```

3. Specify if and when the SAE attempts to fail back to the default peer.

```
[edit shared sae group west-region configuration plug-ins pool flexRadiusAct flex-radius-accounting]
user@host# set fallback-timer fallback-timer
```

4. (Optional) Configure the maximum time the SAE waits for a response from a RADIUS server.

```
[edit shared sae group west-region configuration plug-ins pool flexRadiusAct
flex-radius-accounting]
user@host# set timeout timeout
```

5. Configure the time the SAE waits for a response from a RADIUS server before it resends the RADIUS packet.

```
[edit shared sae group west-region configuration plug-ins pool flexRadiusAct
flex-radius-accounting]
user@host# set retry-interval retry-interval
```

6. Configure the maximum number of unacknowledged RADIUS messages that the plug-in receives from the RADIUS server before it discards new messages.

```
[edit shared sae group west-region configuration plug-ins pool flexRadiusAct
flex-radius-accounting]
user@host# set maximum-queue-length maximum-queue-length
```

7. (Optional) Configure the source IP address that the plug-in uses to communicate with the RADIUS server. If you do not specify an address, the global default address is used.

```
[edit shared sae group west-region configuration plug-ins pool flexRadiusAct
flex-radius-accounting]
user@host# set bind-address bind-address
```

8. (Optional) Configure the source UDP port or a range of source UDP ports used for communication with the RADIUS server. If you do not specify a UDP port, the global UDP port is used.

```
[edit shared sae group west-region configuration plug-ins pool flexRadiusAct
flex-radius-accounting]
user@host# set udp-port udp-port
```

9. Configure the way the SAE handles errors.

```
[edit shared sae group west-region configuration plug-ins pool flexRadiusAct
flex-radius-accounting]
user@host# set error-handling (0 | 1)
```

10. Configure the name of the RADIUS server to which the SAE sends packets for this plug-in.

```
[edit shared sae group west-region configuration plug-ins pool flexRadiusAct
flex-radius-accounting]
user@host# set default-peer default-peer
```

11. Configure the name of the RADIUS packet template that defines attributes for this plug-in.

```
[edit shared sae group west-region configuration plug-ins pool flexRadiusAct
flex-radius-accounting]
user@host# set template template
```

12. (Optional) Verify your configuration.

```
[edit shared sae group west-region configuration plug-ins pool flexRadiusAct
flex-radius-accounting]
user@host# show
load-balancing-mode failover;
failback-timer -1;
timeout 15000;
retry-interval 3000;
maximum-queue-length 10000;
error-handling 0;
default-peer peer2;
template stdAcct;
peer-group peer2 {
  server-address 10.10.1.1;
  server-port 1818;
  secret *****;
}
```

Related Information

For additional information, see the following sources:

- For information about setting up SAE groups, see *SRC-PE Getting Started Guide, Chapter 16, Setting Up an SAE with the SRC CLI*.
- For information about setting up default peers, see *Creating RADIUS Peers* on page 190.
- For information about defining RADIUS packet templates, see *Defining RADIUS Packets for Flexible RADIUS Plug-Ins with the SRC CLI* on page 215.

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 SRC software distribution in the folder *SDK/doc/sae/net/juniper/smgt/sae/radiuslib* or in the SAE core API documentation on the Juniper Networks Web site at

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

For a sample implementation, see the following directory in the SRC software distribution:

SDK/plugin/java/src/net/juniper/smgt/sample/radiuslib/RadiusPacketHandlerImpl.java.

Use the following configuration statements to set up custom RADIUS accounting plug-ins:


```
shared sae configuration plug-ins pool name custom-radius-accounting {
    java-class-radius-packet-handler java-class-radius-packet-handler;
    class-path-radius-packet-handler class-path-radius-packet-handler;
    append-acct-status-type-attribute;
    require-mandatory-attributes;
    load-balancing-mode (failover | roundRobin);
    fallback-timer fallback-timer;
    timeout timeout;
    retry-interval retry-interval;
    maximum-queue-length maximum-queue-length;
    bind-address bind-address;
    udp-port udp-port;
    default-peer default-peer;
}
```

To set up custom RADIUS accounting plug-ins:

1. From configuration mode, access the custom RADIUS accounting plug-in configuration. In this sample procedure, the plug-in called customRadiusAct is configured in the west-region SAE group.

```
user@host# edit shared sae group west-region configuration plug-ins pool  
customRadiusAct custom-radius-accounting
```

2. Configure the name of the Java class that implements the RadiusPacketHandler interface in the RADIUS client library.

```
[edit shared sae group west-region configuration plug-ins pool customRadiusAct  
custom-radius-accounting]  
user@host# set java-class-radius-packet-handler java-class-radius-packet-handler
```

3. Configure the URLs that identify a location from which Java classes are loaded when the plug-in is initialized.

```
[edit shared sae group west-region configuration plug-ins pool customRadiusAct  
custom-radius-accounting]  
user@host# set class-path-radius-packet-handler class-path-radius-packet-handler
```

4. (Optional) Enable the plug-in to include the Acct-Status-Type attribute in a RADIUS accounting request packet.

```
[edit shared sae group west-region configuration plug-ins pool customRadiusAct  
custom-radius-accounting]  
user@host# set append-acct-status-type-attribute
```

5. (Optional) Specify that a RADIUS authentication or accounting request must contain all mandatory RADIUS attributes before sending the request packet.

```
[edit shared sae group west-region configuration plug-ins pool customRadiusAct  
custom-radius-accounting]  
user@host# set require-mandatory-attributes
```

6. Configure the mode for load-balancing RADIUS servers.

```
[edit shared sae group west-region configuration plug-ins pool customRadiusAct
custom-radius-accounting]
user@host# set load-balancing-mode (failover | roundRobin)
```

7. Specify if and when the SAE attempts to fail back to the default peer.

```
[edit shared sae group west-region configuration plug-ins pool customRadiusAct
custom-radius-accounting]
user@host# set fallback-timer fallback-timer
```

8. (Optional) Configure the maximum time the SAE waits for a response from a RADIUS server.

```
[edit shared sae group west-region configuration plug-ins pool customRadiusAct
custom-radius-accounting]
user@host# set timeout timeout
```

9. Configure the time the SAE waits for a response from a RADIUS server before it resends the RADIUS packet.

```
[edit shared sae group west-region configuration plug-ins pool customRadiusAct
custom-radius-accounting]
user@host# set retry-interval retry-interval
```

10. Configure the maximum number of unacknowledged RADIUS messages that the plug-in receives from the RADIUS server before it discards new messages.

```
[edit shared sae group west-region configuration plug-ins pool customRadiusAct
custom-radius-accounting]
user@host# set maximum-queue-length maximum-queue-length
```

11. (Optional) Configure the source IP address that the plug-in uses to communicate with the RADIUS server. If you do not specify an address, the global default address is used.

```
[edit shared sae group west-region configuration plug-ins pool customRadiusAct
custom-radius-accounting]
user@host# set bind-address bind-address
```

12. (Optional) Configure the source UDP port or a range of source UDP ports used for communication with the RADIUS server. If you do not specify a UDP port, the global UDP port is used.

```
[edit shared sae group west-region configuration plug-ins pool customRadiusAct
custom-radius-accounting]
user@host# set udp-port udp-port
```

13. Configure the name of the RADIUS server to which the SAE sends packets for this plug-in.

```
[edit shared sae group west-region configuration plug-ins pool customRadiusAct
custom-radius-accounting]
user@host# set default-peer default-peer
```

14. (Optional) From operational mode, verify your configuration.

```
[edit shared sae group west-region configuration plug-ins pool
customRadiusAct custom-radius-accounting]
user@host# show
java-class-radius-packet-handler
net.juniper.smgt.radius.RadiusPacketHandlerImpl;
append-acct-status-type-attribute;
load-balancing-mode failover;
failback-timer -1;
timeout 15000;
retry-interval 3000;
maximum-queue-length 10000;
default-peer peer3;
```

Related Information

For additional information, see the following sources:

- For information about setting up SAE groups, see *SRC-PE Getting Started Guide, Chapter 16, Setting Up an SAE with the SRC CLI*.
- For information about setting up default peers, see *Creating RADIUS Peers* on page 190.

Configuring Authentication Plug-Ins

This section shows how to configure the authentication plug-ins described in Table 21. 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 21: Authentication Plug-Ins

Plug-In	Description
Basic RADIUS authentication	Sends authentication information to an external RADIUS authentication server or a group of redundant servers. Java class name—net.juniper.smgt.sae.plugin.RadiusAuthPluginEventListener
Custom RADIUS authentication	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. Java class name—net.juniper.smgt.sae.plugin.CustomRadiusAuth
Flexible RADIUS authentication	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. Java class name—net.juniper.smgt.sae.plugin.FlexibleRadiusAuthPluginEventListener

Table 21: Authentication Plug-Ins (continued)

Plug-In	Description
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.

Use the following configuration statement to set up a plug-in that limits the number of subscribers who connect to interfaces:

```
shared sae configuration plug-ins pool name interface-subscriber-limit {
    concurrent-subscribers concurrent-subscribers;
}
```

To set up a plug-in that limits the number of subscribers on interfaces:

1. From configuration mode, access the custom RADIUS accounting plug-in configuration. In this sample procedure, the plug-in called `subsLimit` is configured in the `west-region` SAE group.

```
user@host# edit shared sae group west-region configuration plug-ins pool
subsLimit interface-subscriber-limit
```

2. Configure the number of authenticated subscribers who can connect to an IP interface on the router simultaneously.

```
[edit shared sae group west-region configuration plug-ins pool subsLimit
interface-subscriber-limit]
user@host# set concurrent-subscribers concurrent-subscribers
```

3. (Optional) Verify your configuration.

```
[edit shared sae group west-region configuration plug-ins pool subsLimit
interface-subscriber-limit]
user@host# show
concurrent-subscribers 1;
```

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.

Use the following configuration statements to set up basic RADIUS authentication plug-ins:

```
shared sae configuration plug-ins pool name radius-authentication {
    load-balancing-mode (failover | roundRobin);
    failback-timer failback-timer;
    nas-ip (Ssplp | Erxlp);
    retry-interval retry-interval;
    maximum-queue-length maximum-queue-length;
    bind-address bind-address;
    udp-port udp-port;
    default-peer default-peer;
}
```

To set up basic RADIUS authentication plug-ins:

1. From configuration mode, access the basic RADIUS authentication plug-in configuration. In this sample procedure, the plug-in called RadiusAuth is configured in the west-region SAE group.

```
user@host# edit shared sae group west-region configuration plug-ins pool  
RadiusAuth radius-authentication
```

2. Configure the mode for load-balancing RADIUS servers.

```
[edit shared sae group west-region configuration plug-ins pool RadiusAuth  
radius-authentication]  
user@host# set load-balancing-mode (failover | roundRobin)
```

3. Specify if and when the SAE attempts to fail back to the default peer.

```
[edit shared sae group west-region configuration plug-ins pool RadiusAuth  
radius-authentication]  
user@host# set failback-timer failback-timer
```

4. (Optional) Configure the value of the NAS-Ip attribute.

```
[edit shared sae group west-region configuration plug-ins pool RadiusAuth  
radius-authentication]  
user@host# set nas-ip (Ssplp | Erxlp)
```

5. Configure the time the SAE waits for a response from a RADIUS server before it resends the RADIUS packet.

```
[edit shared sae group west-region configuration plug-ins pool RadiusAuth  
radius-authentication]  
user@host# set retry-interval retry-interval
```

6. Configure the maximum number of unacknowledged RADIUS messages that the plug-in receives from the RADIUS server before it discards new messages.

```
[edit shared sae group west-region configuration plug-ins pool RadiusAuth
radius-authentication]
user@host# set maximum-queue-length maximum-queue-length
```

7. (Optional) Configure the source IP address that the plug-in uses to communicate with the RADIUS server. If you do not specify an address, the global default address is used.

```
[edit shared sae group west-region configuration plug-ins pool RadiusAuth
radius-authentication]
user@host# set bind-address bind-address
```

8. (Optional) Configure the source UDP port or a range of source UDP ports used for communication with the RADIUS server. If you do not specify a UDP port, the global UDP port is used.

```
[edit shared sae group west-region configuration plug-ins pool RadiusAuth
radius-authentication]
user@host# set udp-port udp-port
```

9. Configure the name of the RADIUS server to which the SAE sends packets for this plug-in.

```
[edit shared sae group west-region configuration plug-ins pool RadiusAuth
radius-authentication]
user@host# set default-peer default-peer
```

10. (Optional) Verify your configuration.

```
[edit shared sae group west-region configuration plug-ins pool RadiusAuth
radius-authentication]
user@host# show
load-balancing-mode failover;
failback-timer -1;
retry-interval 3000;
maximum-queue-length 10000;
default-peer peer1;
```

Related Information

For additional information, see the following sources:

- For information about setting up SAE groups, see *SRC-PE Getting Started Guide, Chapter 16, Setting Up an SAE with the SRC CLI*.
- For information about setting up default peers, see *Creating RADIUS Peers* on page 190.

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.

Use the following configuration statements to set up flexible RADIUS authentication plug-ins:

```
shared sae configuration plug-ins pool name flex-radius-authentication {
    load-balancing-mode (failover | roundRobin);
    fallback-timer fallback-timer;
    timeout timeout;
    retry-interval retry-interval;
    maximum-queue-length maximum-queue-length;
    bind-address bind-address;
    udp-port udp-port;
    error-handling (0 | 1);
    default-peer default-peer;
    template template;
}
```

To set up flexible RADIUS authentication plug-ins:

1. From configuration mode, access the flexible RADIUS authentication plug-in configuration. In this sample procedure, the plug-in called flexRadiusAuth is configured in the west-region SAE group.

```
user@host# edit shared sae group west-region configuration plug-ins pool  
flexRadiusAuth flex-radius-authentication
```

2. Configure the mode for load-balancing RADIUS servers.

```
[edit shared sae group west-region configuration plug-ins pool flexRadiusAuth  
flex-radius-authentication]  
user@host# set load-balancing-mode (failover | roundRobin)
```

3. Specify if and when the SAE attempts to fail back to the default peer.

```
[edit shared sae group west-region configuration plug-ins pool flexRadiusAuth  
flex-radius-authentication]  
user@host# set fallback-timer fallback-timer
```

4. (Optional) Configure the maximum time the SAE waits for a response from a RADIUS server.

```
[edit shared sae group west-region configuration plug-ins pool flexRadiusAuth  
flex-radius-authentication]  
user@host# set timeout timeout
```

5. Configure the time the SAE waits for a response from a RADIUS server before it resends the RADIUS packet.

```
[edit shared sae group west-region configuration plug-ins pool flexRadiusAuth
flex-radius-authentication]
user@host# set retry-interval retry-interval
```

6. Configure the maximum number of unacknowledged RADIUS messages that the plug-in receives from the RADIUS server before it discards new messages.

```
[edit shared sae group west-region configuration plug-ins pool flexRadiusAuth
flex-radius-authentication]
user@host# set maximum-queue-length maximum-queue-length
```

7. (Optional) Configure the source IP address that the plug-in uses to communicate with the RADIUS server. If you do not specify an address, the global default address is used.

```
[edit shared sae group west-region configuration plug-ins pool flexRadiusAuth
flex-radius-authentication]
user@host# set bind-address bind-address
```

8. (Optional) Configure the source UDP port or a range of source UDP ports used for communication with the RADIUS server. If you do not specify a UDP port, the global UDP port is used.

```
[edit shared sae group west-region configuration plug-ins pool flexRadiusAuth
flex-radius-authentication]
user@host# set udp-port udp-port
```

9. Configure the way the SAE handles errors.

```
[edit shared sae group west-region configuration plug-ins pool flexRadiusAuth
flex-radius-authentication]
user@host# set error-handling (0 | 1)
```

10. Configure the name of the RADIUS server to which the SAE sends packets for this plug-in.

```
[edit shared sae group west-region configuration plug-ins pool flexRadiusAuth
flex-radius-authentication]
user@host# set default-peer default-peer
```

11. Configure the name of the RADIUS packet template that defines attributes for this plug-in.

```
[edit shared sae group west-region configuration plug-ins pool flexRadiusAct
flex-radius-accounting]
user@host# set template template
```


12. (Optional) Verify your configuration.

```
[edit shared sae group west-region configuration plug-ins pool
flexRadiusAuth flex-radius-authentication]
user@host# show
load-balancing-mode failover;
failback-timer -1;
timeout 15000;
retry-interval 3000;
maximum-queue-length 10000;
error-handling 0;
default-peer 1;
template stdAuth;
peer-group 1 {
  server-address ;
  server-port 1812;
  secret *****;
}
```

Related Information

For additional information, see the following sources:

- For information about setting up SAE groups, see *SRC-PE Getting Started Guide, Chapter 16, Setting Up an SAE with the SRC CLI*.
- For information about setting up default peers, see *Creating RADIUS Peers* on page 190.
- For information about defining RADIUS packet templates, see *Defining RADIUS Packets for Flexible RADIUS Plug-Ins with the SRC CLI* on page 215.

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 SRC software distribution in the folder `SDK/doc/sae/net/juniper/smgt/sae/radiuslib` or the SAE core API documentation on the Juniper Networks Web site at

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

For a sample implementation, see the following directory in the SRC software distribution:

`SDK/plugin/java/src/net/juniper/smgt/sample/radiuslib/RadiusPacketHandlerImpl.java`.

Use the following configuration statements to set up custom RADIUS authentication plug-ins:

```

shared sae configuration plug-ins pool name custom-radius-authentication {
  java-class-radius-packet-handler java-class-radius-packet-handler;
  class-path-radius-packet-handler class-path-radius-packet-handler;
  require-mandatory-attributes;
  load-balancing-mode (failover | roundRobin);
  fallback-timer fallback-timer;
  timeout timeout;
  retry-interval retry-interval;
  maximum-queue-length maximum-queue-length;
  bind-address bind-address;
  udp-port udp-port;
  default-peer default-peer;
}

```

To set up custom RADIUS authentication plug-ins:

1. From configuration mode, access the custom RADIUS authentication plug-in configuration. In this sample procedure, the plug-in called customRadiusAuth is configured in the west-region SAE group.

```

user@host# edit shared sae group west-region configuration plug-ins pool
customRadiusAuth custom-radius-authentication

```

2. Configure the name of the Java class that implements the RadiusPacketHandler interface in the RADIUS client library.

```

[edit shared sae group west-region configuration plug-ins pool customRadiusAuth
custom-radius-authentication]
user@host# set java-class-radius-packet-handler java-class-radius-packet-handler

```

3. Configure the URLs that identify a location from which Java classes are loaded when the plug-in is initialized.

```

[edit shared sae group west-region configuration plug-ins pool customRadiusAuth
custom-radius-authentication]
user@host# set class-path-radius-packet-handler class-path-radius-packet-handler

```

4. (Optional) Specify that a RADIUS authentication or accounting request must contain all mandatory RADIUS attributes before sending the request packet.

```

[edit shared sae group west-region configuration plug-ins pool customRadiusAuth
custom-radius-authentication]
user@host# set require-mandatory-attributes

```

5. Configure the mode for load-balancing RADIUS servers.

```

[edit shared sae group west-region configuration plug-ins pool customRadiusAuth
custom-radius-authentication]
user@host# set load-balancing-mode (failover | roundRobin)

```

6. Specify if and when the SAE attempts to fail back to the default peer.

```

[edit shared sae group west-region configuration plug-ins pool customRadiusAuth
custom-radius-authentication]
user@host# set fallback-timer fallback-timer

```

7. (Optional) Configure the maximum time the SAE waits for a response from a RADIUS server.

```
[edit shared sae group west-region configuration plug-ins pool customRadiusAuth
custom-radius-authentication]
user@host# set timeout timeout
```

8. Configure the time the SAE waits for a response from a RADIUS server before it resends the RADIUS packet.

```
[edit shared sae group west-region configuration plug-ins pool customRadiusAuth
custom-radius-authentication]
user@host# set retry-interval retry-interval
```

9. Configure the maximum number of unacknowledged RADIUS messages that the plug-in receives from the RADIUS server before it discards new messages.

```
[edit shared sae group west-region configuration plug-ins pool customRadiusAuth
custom-radius-authentication]
user@host# set maximum-queue-length maximum-queue-length
```

10. (Optional) Configure the source IP address that the plug-in uses to communicate with the RADIUS server. If you do not specify an address, the global default address is used.

```
[edit shared sae group west-region configuration plug-ins pool customRadiusAuth
custom-radius-authentication]
user@host# set bind-address bind-address
```

11. (Optional) Configure the source UDP port or a range of source UDP ports used for communication with the RADIUS server. If you do not specify a UDP port, the global UDP port is used.

```
[edit shared sae group west-region configuration plug-ins pool customRadiusAuth
custom-radius-authentication]
user@host# set udp-port udp-port
```

12. Configure the name of the RADIUS server to which the SAE sends packets for this plug-in.

```
[edit shared sae group west-region configuration plug-ins pool customRadiusAuth
custom-radius-authentication]
user@host# set default-peer default-peer
```

13. (Optional) From operational mode, verify your configuration.

```
[edit shared sae configuration plug-ins pool customRadiusAuth
custom-radius-authorization]
user@host# show
java-class-radius-packet-handler
net.juniper.smgd.radius.RadiusPacketHandlerImpl;
require-mandatory-attributes;
load-balancing-mode failover;
failback-timer -1;
timeout 15000;
retry-interval 3000;
maximum-queue-length 10000;
default-peer peer4;
```

Related Information

For additional information, see the following sources:

- For information about setting up SAE groups, see *SRC-PE Getting Started Guide, Chapter 16, Setting Up an SAE with the SRC CLI*.
- For information about setting up default peers, see *Creating RADIUS Peers* on page 190.

Configuring LDAP Authentication Plug-Ins

Use the following configuration statements to configure LDAP authentication plug-ins:

```
shared sae configuration plug-ins pool name ldap-authentication {
  method (search | bind);
  server server;
  bind-dn bind-dn;
  bind-password bind-password;
  search-filter search-filter;
  (ldaps);
  search-base-dn search-base-dn;
  name-attribute name-attribute;
  password-attribute password-attribute;
  service-bundle-attribute service-bundle-attribute;
  session-volume-quota session-volume-quota;
  timeout timeout;
}
```

To create LDAP authentication plug-ins:

1. From configuration mode, access the custom LDAP authentication plug-in configuration. In this sample procedure, the plug-in called `ldapAuth` is configured in the `west-region` SAE group.

```
user@host# edit shared sae group west-region configuration plug-ins pool
ldapAuth ldap-authentication
```

2. Configure the LDAP authentication method that the SAE uses.

```
[edit shared sae group west-region configuration plug-ins pool ldapAuth
ldap-authentication]
user@host# set method (search | bind)
```

3. (Optional) Configure a comma-separated list of IP addresses or hostnames of the LDAP authentication server.

```
[edit shared sae group west-region configuration plug-ins pool ldapAuth
ldap-authentication]
user@host# set server server
```

4. (Optional) Configure the DN used to authenticate access to the directory.

```
[edit shared sae group west-region configuration plug-ins pool ldapAuth
ldap-authentication]
user@host# set bind-dn bind-dn
```

5. (Optional) Configure the password that the SAE uses to authenticate its access to the directory to search for the subscriber profile. If you do not specify a bind DN or bind password, the SAE uses anonymous access.

```
[edit shared sae group west-region configuration plug-ins pool ldapAuth
ldap-authentication]
user@host# set bind-password bind-password
```

6. (Optional) Configure the additional LDAP search filter that the SAE uses to search the directory for the subscriber profile.

```
[edit shared sae group west-region configuration plug-ins pool ldapAuth
ldap-authentication]
user@host# set search-filter search-filter
```

7. (Optional) Enable the secure protocol used for LDAP connections with the directory. LDAPS, the only secure protocol supported, causes communication with the directory to be encrypted with Secure Sockets Layer (SSL).

```
[edit shared sae group west-region configuration plug-ins pool ldapAuth
ldap-authentication]
user@host# set ldaps
```

8. (Optional) Configure the base DN for searching entries in the directory.

```
[edit shared sae group west-region configuration plug-ins pool ldapAuth
ldap-authentication]
user@host# set search-base-dn search-base-dn
```

9. (Optional) Configure the name of the directory attribute that holds the username.

```
[edit shared sae group west-region configuration plug-ins pool ldapAuth
ldap-authentication]
user@host# set name-attribute name-attribute
```

10. (Optional) Configure the name of the directory attribute that stores the password.

```
[edit shared sae group west-region configuration plug-ins pool ldapAuth
ldap-authentication]
user@host# set password-attribute password-attribute
```

11. (Optional) Configure the name of the directory attribute that contains the name of the service bundle that is used for subscriber authentication. This value is made available to the subscriber classification process and can be used to select the subscriber profile to load.

```
[edit shared sae group west-region configuration plug-ins pool ldapAuth
ldap-authentication]
user@host# set service-bundle-attribute service-bundle-attribute
```

12. (Optional) Configure the name of the LDAP attribute that contains the value of the session volume quota. The LDAP plug-in sets the session volume quota to this value.

```
[edit shared sae group west-region configuration plug-ins pool ldapAuth
ldap-authentication]
user@host# set session-volume-quota session-volume-quota
```

13. (Optional) Configure the maximum time the SAE waits for a response from a directory server.

```
[edit shared sae group west-region configuration plug-ins pool ldapAuth
ldap-authentication]
user@host# set timeout timeout
```

14. (Optional) From operational mode, verify your configuration.

```
[edit shared sae group west-region configuration plug-ins pool ldapAuth
ldap-authentication]
user@host# show
method search;
search-filter (objectClass=umcSubscriber);
name-attribute uniqueId;
timeout 5000;
```

Related Information

For additional information, see the following source:

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

Configuring UDP Ports for RADIUS Plug-Ins

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

Use the following configuration statement to configure global configuration ports:

```
shared sae configuration global-radius-udp-port {
    udp-port;
}
```

To configure global UDP ports:

1. From configuration mode, access the global RADIUS UDP port configuration. In this sample procedure, the UDP port is configured in the west-region SAE group.

```
user@host# edit shared sae group west-region configuration  
global-radius-udp-port
```

2. Configure the source UDP port or a pool of ports that RADIUS plug-ins use to communicate with RADIUS servers.

```
[edit shared sae group west-region configuration global-radius-udp-port]  
user@host# set udp-port
```

Defining RADIUS Packets for Flexible RADIUS Plug-Ins with the SRC CLI

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 22 lists the available packet types.

Table 22: 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
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

Table 22: RADIUS Attribute Instance Names (continued)

Attribute Instance (Packet-Type)	Type of RADIUS Packet to Which Attribute Definition Is Applied
userresp	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 JUNOSE 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 dhcpresp {
    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);
    }
}

```

Defining the Values of RADIUS Attributes

The values of RADIUS attributes can be a standard value (see Table 23) or an expression. Expressions are evaluated with Python. For example: `lowWord(inOctets)` extracts the lower 32 bits of the 64-bit `inOctets` counter. You can define multiple values for an expression in a comma-separated list.

Table 23: Standard Values for RADIUS Attributes

Value	Type of Plug-In	Comments
accountingId	User and service tracking	
authUserId	Service tracking	
dhcp	User and service tracking	Provides access to DHCP packet. See Table 12 on page 82 for details.
domain	Authorization	
eventTime	User and service tracking	Seconds since 1970-01-01T00:00Z
ifRadiusClass	User and service tracking	
ifSessionId	User and service tracking	
inOctets	Service tracking	64-bit counter
inPackets	Service tracking	
interfaceAlias	User and service tracking	
interfaceDescr	User and service tracking	
interfaceName	User and service tracking	
localNasId	All	Configured NAS-ID
localNasIp	All	Configured NAS-IP
loginId	User and service authorization	ID provided by the subscriber; the loginId value is not separated into UID and domain name.
loginName	User and service tracking	Name that the subscriber uses to log in to portal
nasIp	User and service tracking	NAS IP address of the router
nasPort	User and service tracking	32-bit integer
outOctets	Service tracking	64-bit counter
outPackets	Service tracking	
password	User and service authorization	

Table 23: Standard Values for RADIUS Attributes (continued)

Value	Type of Plug-In	Comments
portId	User and service tracking	ID of the port on the JUNOSe router; for example, FastEthernet 3/1:2001
primaryUserName	User and service tracking	Name that the subscriber uses for DHCP/PPP authentication
radiusClass	User tracking, user and service authorization	For service tracking, this value is taken from the RADIUS Access-Accept response. If the response does not contain a value, the RADIUS class defined in the service definition is used. This attribute can be set by an authorization response.
replyMessage	User and service authorization	This attribute can only be set.
routerName	User and service tracking	
serviceBundle	User tracking and authorization	This attribute can be set by an authorization response.
serviceName	Service tracking	Sets an arbitrary attribute (for example, class) to the name of the service.
serviceSessionName	Service tracking	Named service session; empty for default session
serviceSessionTag	Service tracking	
sessionId	User and service tracking	
sessionTime	User and service tracking	
sessionTimeout	User tracking, user and service authorization	This attribute can be set by an authorization response.
sessionVolumeQuota	User authorization	This attribute can only be set. It is sent for session tracking events and can be returned by service authorization events. It can be set and retrieved through the portal API and can also be defined through an LDAP attribute in the service definition. If the attribute is defined multiple times, the following precedence is observed: 1. Service definition (lowest) 2. Authorization 3. API call (highest) NOTE: The SAE does not enforce a volume quota directly; it only makes the attribute available to an external application that can control the volume quota.
setAcctInterimTime	User authorization	Integer
setAuthVirtualRouterName	DHCP authorization	Text
setIdleTimeout(ATTR)	User authorization	
setLoadServices(ATTR)	User authorization	This attribute can only be set.
setPoolName	DHCP authorization	Text
setRadiusClass(ATTR)	User and service authorization	
setReplyMessage(ATTR)	User and service authorization	
setSessionTimeout(ATTR)	User and service authorization	
setServiceBundle(ATTR)	User authorization	
setSessionVolumeQuota(ATTR)	User authorization	
setSubstitution	User authorization	Text. Substitutions can be set only for service sessions.

Table 23: Standard Values for RADIUS Attributes (continued)

Value	Type of Plug-In	Comments
setTerminateTime	User authorization	Text
setUserIpAddress	DHCP authorization	Integer
sspHost	User and service tracking	
terminateCause	User and service tracking	
uid	User and service authorization	
userDn	User and service tracking	
userIpAddress	User and service tracking	
userMacAddress	User and service tracking	
userRadiusClass	Service tracking	RADIUS class of associated subscriber session
userSessionId	Service tracking	RADIUS session ID of associated subscriber session

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.

Use the following configuration statements to configure a RADIUS packet template:

```
shared sae configuration radius-packet-template name ...
```

```
shared sae configuration radius-packet-template name radius-attributes name ...
```

```
shared sae configuration radius-packet-template name radius-attributes name
attributes name {
    value;
}
```

```
shared sae configuration plug-ins pool name flex-radius-accounting
radius-packet-definition name ...
```

```
shared sae configuration plug-ins pool name flex-radius-accounting
radius-packet-definition name attributes name {
    value;
}
```

```
shared sae configuration plug-ins pool name flex-radius-authentication
radius-packet-definition name ...
```

```
shared sae configuration plug-ins pool name flex-radius-authentication
radius-packet-definition name attributes name {
    value;
}
```

To configure a template:

1. From configuration mode, access the RADIUS packet template configuration. In this sample procedure, the stdAcct template is configured in the west-region SAE group.

```
user@host# edit shared sae group west-region configuration  
radius-packet-template stdAcct
```

2. Create an attribute instance using the names in Table 22 on page 216, and enter the configuration for the RADIUS attribute instance.

```
[edit shared sae group west-region configuration radius-packet-template stdAcct]  
user@host# edit radius-attributes name
```

3. Add RADIUS attribute definitions to the attribute instance. Repeat this step for each attribute.

```
[edit shared sae group west-region configuration radius-packet-template stdAcct  
radius-attributes svcstop]  
user@host# set attributes name value
```

For example:

```
[edit shared sae group west-region configuration radius-packet-template stdAcct  
radius-attributes svcstop]  
user@host# set attributes Acct-Session-ID sessionId
```

4. (Optional) Verify the configuration of your attribute instance.

```
[edit shared sae group west-region configuration radius-packet-template  
stdAcct radius-attributes svcstop]  
user@host# show  
attributes {  
  Acct-Input-Octets lowWord(inOctets);  
  Acct-Output-Octets lowWord(outOctets);  
  Acct-Input-Packets lowWord(inPackets);  
  Acct-Output-Packets lowWord(outPackets);  
  Acct-Input-Gigawords highWord(inOctets);  
  Acct-Output-Gigawords highWord(outOctets);  
}
```

5. (Optional) Verify the configuration of the RADIUS packet template.

```
[edit shared sae group west-region configuration radius-packet-template  
stdAcct radius-attributes svcstop]  
user@host# up  
[edit shared sae group west-region configuration radius-packet-template  
stdAcct]  
user@host# show  
radius-attributes svcstop {  
  attributes {  
    Acct-Input-Octets lowWord(inOctets);  
    Acct-Output-Octets lowWord(outOctets);  
    Acct-Input-Packets lowWord(inPackets);  
    Acct-Output-Packets lowWord(outPackets);  
    Acct-Input-Gigawords highWord(inOctets);  
    Acct-Output-Gigawords highWord(outOctets);  
  }  
}
```

```

}
radius-attributes stop {
  attributes {
    Acct-Session-Time sessionTime;
    Acct-Terminate-Cause terminateCause;
  }
}
radius-attributes svcacct {
  attributes {
    Class radiusClass;
  }
}
radius-attributes acct {
  attributes {
    Acct-Session-Id sessionId;
    NAS-Identifier localNasId;
    NAS-IP-Address localNasIp;
    Event-Time eventTime;
  }
}
radius-attributes startstop {
  attributes {
    Acct-Multi-Session-Id ifSessionId;
    NAS-Port-Id "\"%s %s\""%(routerName, portId or interfaceName)";
    NAS-Port "nasPort or None";
  }
}

```

More About Using Flexible RADIUS Packet Definitions

This section 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)

Table 23 on page 218 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

This topic shows how to configure event publishers. It covers the following tasks:

- Configuring Global and Default Retailer Event Publishers on page 225
- Configuring Service-Specific Event Publishers on page 227
- Configuring Retailer-Specific Event Publishers on page 227
- Configuring Virtual Router-Specific Event Publishers on page 227

Configuring Global and Default Retailer Event Publishers

Use the following configuration statements to configure global and default retailer event publishers.

```
shared sae configuration plug-ins event-publishers {
    subscriber-authorization subscriber-authorization;
    default-retailer-authentication default-retailer-authentication;
    default-retailer-dhcp-authentication default-retailer-dhcp-authentication;
    dhcp-authorization dhcp-authorization;
    service-authorization service-authorization;
    subscription-authorization subscription-authorization;
    subscriber-tracking subscriber-tracking;
    service-tracking service-tracking;
    interface-tracking interface-tracking;
    embedded-admin-server-authorization embedded-admin-server-authorization;
}
```

To configure global and default retailer event publishers:

1. From configuration mode, access the event publisher configuration. In this sample procedure, the event publishers are configured in the west-region SAE group.

```
user@host# edit shared sae group west-region configuration plug-ins  
event-publishers
```

2. Configure plug-ins that authorize subscriber sessions.

```
[edit shared sae group west-region configuration plug-ins event-publishers]  
user@host# set subscriber-authorization subscriber-authorization
```

3. Configure plug-ins that authenticate subscribers who are assigned to retailer objects that do not specify an authentication plug-in.

```
[edit shared sae group west-region configuration plug-ins event-publishers]  
user@host# set default-retailer-authentication default-retailer-authentication
```

4. Configure plug-ins that authenticate DHCP address requests for subscribers who are assigned to retailer objects that do not specify a DHCP authorization plug-in.

```
[edit shared sae group west-region configuration plug-ins event-publishers]  
user@host# set default-retailer-dhcp-authentication  
default-retailer-dhcp-authentication
```

5. Configure plug-ins that authorize all DHCP address requests for all DHCP subscribers who log in to a portal.

```
[edit shared sae group west-region configuration plug-ins event-publishers]  
user@host# set dhcp-authorization dhcp-authorization
```

6. Configure plug-ins that authorize all service sessions.

```
[edit shared sae group west-region configuration plug-ins event-publishers]  
user@host# set service-authorization service-authorization
```

7. Configure plug-ins that authorize subscribers to change their subscriptions.

```
[edit shared sae group west-region configuration plug-ins event-publishers]
user@host# set subscription-authorization subscription-authorization
```

8. Configure plug-ins that collect accounting data for all subscriber sessions.

```
[edit shared sae group west-region configuration plug-ins event-publishers]
user@host# set subscriber-tracking subscriber-tracking
```

9. Configure plug-ins that collect accounting data for all service sessions.

```
[edit shared sae group west-region configuration plug-ins event-publishers]
user@host# set service-tracking service-tracking
```

10. Configure plug-ins, including network information collector (NIC) SAE plug-in agents, that collect accounting data for all interfaces that the SAE manages.

```
[edit shared sae group west-region configuration plug-ins event-publishers]
user@host# set interface-tracking interface-tracking
```

11. Configure plug-ins that authorize administrators to connect to the embedded Web server, which is used to access SAE Web Admin.

```
[edit shared sae group west-region configuration plug-ins event-publishers]
user@host# set embedded-admin-server-authorization
embedded-admin-server-authorization
```

12. (Optional) Verify your configuration.

```
[edit shared sae group west-region configuration plug-ins event-publishers]
user@host# show
subscriber-authorization ;
default-retailer-authentication ldapAuth;
default-retailer-dhcp-authentication ;
dhcp-authorization ;
service-authorization ;
subscription-authorization ;
subscriber-tracking fileAcct;
service-tracking fileAcct;
interface-tracking ;
embedded-admin-server-authorization adminLdap;
```

Related Information

For additional information, see the following source:

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

Configuring Service-Specific Event Publishers

In the value-added services definition, you can configure two event publishers for a service:

- Authorization plug-ins—Authenticate subscribers of the service and/or authorize service sessions for this service. These plug-in instances are called before a subscription to this service is activated.
- Tracking plug-ins—Track service sessions of this service. These plug-in instances are called when a service session is started and stopped and during interim updates.

See *SRC-PE Services and Policies Guide, Chapter 1, Managing Services with the SRC CLI*.

Configuring Retailer-Specific Event Publishers

In the retailer definition, you can configure three event publishers for a retailer:

- Authentication plug-ins—Authenticate subscribers who log in to the domains of the retailer. These plug-in instances are called when a subscriber tries to log in to the SAE through the portal login.

If you do not specify retailer-specific authentication plug-ins, the default retailer authentication plug-ins are called. If you do not specify default retailer authentication plug-ins, subscribers are admitted without authentication.

- Tracking plug-ins—Track sessions of subscribers who log in to the domains of the retailer. These plug-in instances are called after a subscriber session has started and when the session is stopped.
- DHCP authorization plug-ins—Authenticate DHCP address requests for subscribers who log in to the domains of the retailer.

See *Adding Retailers* on page 236.

Configuring Virtual Router-Specific Event Publishers

In the virtual router definition, you can configure an interface-tracking plug-in event publisher for a virtual router. These plug-in instances are called when a managed interface is started and stopped. They are called after an interface comes up, when new policies are installed on the interface, and when the interface goes down.

For information about configuring virtual routers for JUNOS routers, see *SRC-PE Network Guide, Chapter 5, Using JUNOS Routers in the SRC Network with the SRC CLI*.

For information about configuring virtual routers for JUNOS routing platforms, see *SRC-PE Network Guide, Chapter 7, Using JUNOS Routing Platforms in the SRC Network with the SRC CLI*.

Chapter 13

Configuring Subscribers and Subscriptions with SDX Admin

This chapter shows how to use SDX Admin to add subscribers and operators to the directory and to configure subscriptions to services. You can use SDX Admin on Solaris platforms.

You can also use the SRC CLI to configure subscribers and subscriptions on the C-series platform or on a Solaris platform. See *Chapter 14, Configuring Subscribers and Subscriptions with the SRC CLI*.

Topics in this chapter include:

- Overview of Configuring Subscribers and Subscriptions on page 229
- Adding Subscribers on page 236
- Adding Operators on page 253
- Configuring Subscriptions on page 255
- Configuring Substitutions for Subscriptions on page 269
- Modifying and Deleting Subscribers and Subscriptions on page 271

Overview of Configuring Subscribers and Subscriptions

This section gives an overview of configuring subscribers and subscriptions for the SRC software.

LDAP Model for Subscribers

The Subscriber model provides a set of relationships between subscribers and managed services. You can view subscriber objects in the directory at *o = Users, o = umc* (*o = Users, o = umc* is the location for a default installation of the SRC software). If you install the sample data, you can see examples of subscriber configurations with SDX Admin.

For detailed information about the SRC LDAP schema, see the documentation in the SRC software distribution in the folder */SDK/doc/ldap* or on the Juniper Networks Web site at

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

Subscriber objects have the following classes:

- Residential subscribers—A residential subscriber has the object class `umcUser`, a subclass of `inetOrgPerson`. The object class `netOrgPerson` is derived from the X.500 classes `organizationalPerson` and `person`.
- Enterprise subscribers—Enterprise subscribers have the object class `umcEnterprise`. An enterprise subscriber can contain site subscribers that have the object class `umcSite`. Enterprises and sites contain access subscribers. Accesses have the object class `umcAccessServiceProfile`.
- Router subscribers—Router subscribers have the object class `umcRouterSubscriber`.
- Subscriber folders—A subscriber folder has the object class `organizationalUnit`. The object immediately subordinate to a retailer must be a subscriber folder. Subscriber folders can also be subordinate to enterprises, accesses, and sites.
- Retailers—Retailer objects have the object class `umcRetailer`.
- Auxiliary classes—The SRC software attaches the auxiliary class `umcSubscriber` to residential and enterprise subscribers to identify these objects as subscribers. The auxiliary class is created when the subscriber is added to the directory; this class holds general information about the subscriber, such as contact and billing information.

Subscriptions

A subscription is an object in the directory that represents an enrollment to a service. Each subscription provides access to a particular service for that subscriber. A subscriber can have multiple subscriptions to a service. Table 24 shows the type of subscriptions you can configure for each type of subscriber.

Table 24: Allowable Service Subscriptions for Different Types of Subscribers

Type of Subscriber	Service Subscriptions You Can Configure
Retailer	Outsourced service subscription
	Value-added subscription
Subscriber folder	Value-added subscription
Enterprise	Access subscription
	Value-added subscription
Site	Access subscription
	Value-added subscription
Access	RADIUS subscription
	Value-added subscription
Residential subscriber	RADIUS subscription
	Value-added subscription

If the service provider uses the SRC directory to hold all their subscriber data, residential subscribers must subscribe to primary services—such as Broadband Remote Access Server (B-RAS) through Point-to-Point protocol (PPP) or B-RAS through Dynamic Host Configuration Protocol (DHCP)—before subscribing to a value-added service.

Enterprise subscribers must subscribe to an access service (that is, a leased line), either directly or in a site or subscriber folder that is subordinate to the enterprise. Without an access subscription, a service session cannot run in the network.

Retailers can subscribe to outsourced services if a service provider sources the access out through tunneling (Layer 2 Tunneling Protocol [L2TP] or PPP Terminated Aggregation [PTA]).

Specifying the Activation Order for Subscriptions

Service providers and customers can specify the order in which the SAE activates subscriptions that are set up to activate on login for a particular subscriber. To specify the order, you define a numerical precedence for the activation of each subscription. The SAE activates services in ascending order of precedence; if multiple services have the same precedence, the SAE activates them in an unspecified order.

You can configure the activation order with SDX Admin (see *Value-Added Subscription Fields* on page 257) or the Enterprise Manager Portal.

LDAP Model for Subscriptions

The subscriber and service models provide a set of relationships between the subscribers and the managed services, including subscriptions.

When a residential or enterprise subscriber subscribes to a service, which could be either a primary service or a value-added service, a general service profile with subscriber-specific service information is assigned to the subscriber.

For example, when a residential subscriber subscribes to a primary service such as B-RAS, a RADIUS profile (umcRadiusPerson) is created and assigned to the subscriber. Value-added service profiles (sspServiceProfile) are created in case the subscriber also subscribes to a value-added service.

You can create service profiles (umcRadiusPerson, umcAccessServiceProfile, sspServiceProfile, and umcOutsourceServiceProfile) with a directory client, such as SDX Admin.

An access subscription is the same object as an access subscriber. An access has two roles:

1. A subscription to an access service. (The subscription to an access service makes it possible to trigger workflows for the service.)
2. A subscriber to value-added services.

For detailed information about the SRC LDAP schema and graphics of the object models, see the documentation in the SRC software distribution in the folder */SDK/doc/ldap* or on the Juniper Networks Web site at

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

Operators

This section describes operators for subscribers and subscriptions. You can also configure operators for various SRC components. For information about setting up a multilayered access control scheme for operators, see *SRC-PE Integration Guide, Chapter 10, Access Control Scheme*.

In relation to subscribers and subscriptions, an operator is an object in the directory that represents an IT manager in an organization. Retailers, subscriber folders, enterprises, sites, and accesses can support one or more operators.

When you add an enterprise with SDX Admin, the software creates a default operator for that enterprise. You can add additional operators for enterprises and create operators for retailers, subscriber folders, sites, and accesses.

You can also add an operator that has control over all retailers. See *Operators That Control All Retailers* on page 234.

Read Privileges

Operators have privileges to read:

- The objects they control
- Parent subscribers, up to the retailer
- Subscriptions of parent subscribers, up to the retailer
- All objects that represent services, service scopes, policies, and global variables that are defined for the subscriber to which the operator is added

Management Privileges

You can specify one or more management privileges for operators. If you do not specify privileges for an operator, the operator has only read privileges. The default operator that SDX Admin adds to an enterprise has the highest privilege level, called administrator. Table 25 shows the privilege levels and the privileges associated with the levels.

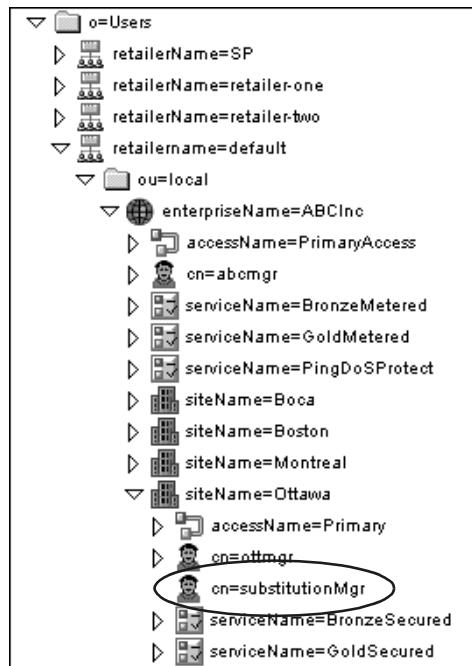
Table 25: Privilege Levels and Associated Tasks

Privilege Level	Tasks That Operators with This Privilege Can Perform
Administrator	<ul style="list-style-type: none"> ■ Add, delete and modify operators ■ Add, delete, and modify subscriptions ■ Modify subscribers, including the ability to add, delete, and modify substitutions for subscribers ■ Manually activate and deactivate subscription sessions
Subscription	<ul style="list-style-type: none"> ■ Add, delete, and modify subscriptions ■ Manually activate and deactivate subscription sessions
Substitution	Add, delete, and modify substitutions in subscribers and subscriptions
Activation	<ul style="list-style-type: none"> ■ Configure automatic activation of services ■ Manually activate and deactivate subscription sessions
VPNs	Modify, export, and cancel the export of VPNs

An operator has management privileges for its associated subscriber and for that subscriber's subordinate objects. For example, operators in an enterprise have control over the enterprise and all sites and accesses in the enterprise. Similarly, operators in a site have control over the site and all accesses it contains. Operators in an access have control over only that access.

For example, in the directory shown in Figure 27, the operator substitutionMgr:

- Can manage substitutions of the site called Ottawa and its subordinate objects.
- Has read access to all services, service scopes, policies, and global variables that are defined for the site called Ottawa.
- Has read access to the site called Ottawa and its subordinate objects.
- Has read access to the parent subscribers: the enterprise ABCInc, the subscriber folder local, and the retailer default.
- Has read access to the subscriptions of the parent subscribers.

Figure 27: Sample Operator Access Privileges

Operators That Control All Retailers

You can add operators that have control over all retailers and their subordinate enterprises. You add this type of operator in *o = Operators*, *o = umc*. The directory controls the operator's access to other objects in the directory.

LDAP Model for Operators

The Operator model provides a set of relationships between operators and the managed services and subscriptions. Operators have the object class *umcOperator*, a subclass of the object class *person*.

For detailed information about the SRC LDAP schema, see the documentation in the SRC software distribution in the folder */SDK/doc/ldap* or on the Juniper Networks Web site at

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

Tools for Adding Subscribers and Subscriptions

The way you add and manage subscribers depends on your SRC configuration. If you have a large base of subscribers, you will probably manage subscribers through your own database and map it to the SRC LDAP schema with a data integrator (see *SRC-PE Integration Guide, Chapter 9, Integrating Data with the LDAP Directory*) or another metadirectory technique. However, if you are working with a small number of subscribers, you can use SDX Admin to add subscribers to the SRC directory. In practice, you can use SDX Admin to configure subscriber bases when you are:

- Demonstrating or testing an SRC configuration with a small number of subscribers.
- Working with retailers to whom you supply Internet services, because the number of retailers will probably be fairly small, and the retailers will manage their own subscribers.
- Working with residential subscribers that you categorize by services purchased into a small number of groups. You add these groups of subscribers, rather than the individual subscribers, to the SRC directory.

Inheritance of Properties and Subscriptions

Subordinate subscribers inherit properties and value-added subscriptions from their parent subscribers, unless you specify a different value for the subordinate. Properties that a subscriber can inherit include the maximum number of concurrent logins and the session timeout. For example, if you configure a subscription to a video service for an enterprise and configure a different subscription to the same video service for a site within that enterprise, the site uses its own subscription rather than the inherited subscription. RADIUS and access subscriptions are not inherited.

Encryption Methods for Passwords

You can encrypt passwords for some types of subscribers and subscriptions. You must use an encryption method that your directory supports. Table 26 shows the encryption methods that different directories support.

Table 26: Encryption Methods Supported by Different Directories

Directory Type	Encryption Method			
	UNIX crypt	md5	sha	None
DirX	Yes	No	Yes	Yes
eTrust Directory	Yes	Yes	Yes	No
Oracle Internet Directory	Yes	Yes	Yes	Yes
Sun ONE	Yes	No	Yes	Yes
OpenLdap	Yes	Yes	Yes	Yes

Adding Subscribers

This section describes how to add and configure subscribers with SDX Admin. You can also add subscribers when they register through a portal. Data collected through portals is used to create profiles for the subscriber.

The tasks to configure subscribers are:

- Adding Retailers on page 236
- Adding Subscriber Folders on page 240

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.

- Adding Residential Subscribers on page 242
- Adding Enterprises on page 246
- Adding Sites on page 249
- Adding Routers as Subscribers on page 251

An access can be both a subscriber to a value-added service and a subscription to an access service. For information about configuring access subscriptions, see *Configuring Access Subscriptions* on page 261.

After you add subscribers, you can add operators and configure subscriptions. See *Adding Operators* on page 253 and *Configuring Subscriptions* on page 255.

Adding Retailers

If you customize the SRC software to cover 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 different retailer for each ISP.

To add a retailer:

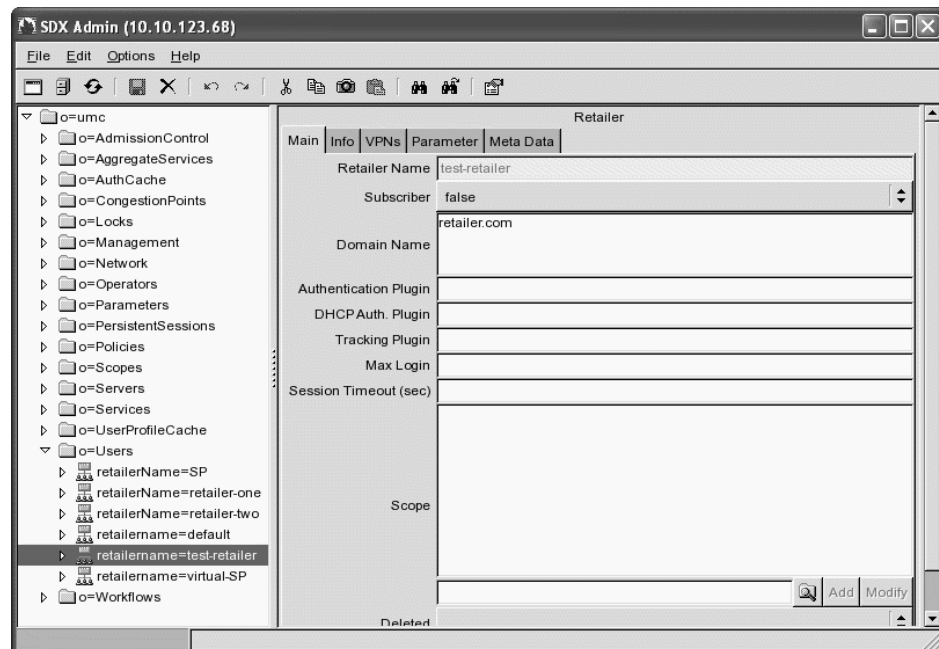
1. In the SDX Admin navigation pane, right-click **o = Users**, **o = umc**, and select **New > Retailer**.

The New Retailer dialog box appears.

2. Enter the Retailer Name and the Domain Name, and click **OK**.

- Retailer Name—Unique name of the retailer.
- Domain Name—ISP's domain name; for example, isp1.com.

An object for the new retailer appears in the navigation pane, and the Retailer pane appears.



3. Use the field descriptions in *Retailer Fields* on page 238 to configure the retailer, and then click Save.
4. Enter information in the other tabs:
 - Info tab—Enter the subscriber’s contact details and additional administrative information in this tab.
 - VPNs tab—Retailers can be extranet clients. Enter Imported Extranets in this tab. (See *Adding Extranet Clients to VPNs* on page 409.)
 - Parameter tab— Enter substitutions in this tab. (See *Configuring Substitutions for Subscriptions* on page 269.)

Retailer Fields

Use the fields in this section to configure retailers.

Subscriber

- Specifies whether or not a subscriber folder can subscribe to services. Subscriptions for the folder are inherited by all subscribers in the folder.
- Value
 - True—Subscriber folder is considered a subscriber.
 - False—Subscriber folder is not considered a subscriber.
- Default—False

Domain Name

- ISP's domain names.
- Value—Domain name in the format *domainName.domainExtension*
- Default—No value
- Example—isp1.com, isp1a.com

Authentication Plugin

- Name of the plug-in used to authenticate subscribers who log in to the domains specified for this retailer. If you do not specify a plug-in for the retailer, the SAE uses the default retailer authentication plug-in.
- Value—Name of the plug-in
- Default—No value

DHCP Authorization Plugin

- Name of the DHCP authorization plug-in used to authenticate DHCP address requests (DHCP discover requests) for subscribers who log in to the domains specified for this retailer. If you do not specify a plug-in for the retailer, the SAE uses the default retailer DHCP authentication plug-in.
- Value—Name of the plug-in
- Default—No value

Tracking Plugin

- Name of the plug-in used for accounting or tracking subscriber sessions. If you do not specify a plug-in for the retailer, the SAE uses the global user tracking plug-in.
- Value—Name of the plug-in
- Default—No value

Max Login

- Maximum number of concurrent logins for subscribers associated with this retailer.
- Value—Integer in the range 0–2147483647
- Guidelines—By default, all subordinate objects use this value. However, if you specify this value for a subordinate object, that object and its subordinate objects will use the subordinate’s value.
- Default—No value

Session Timeout (sec)

- Timeout for subscriber sessions.
- Value—Number of seconds in the range 0–2147483647
- Guidelines—By default, all subordinate objects use this value. However, if you specify this value for a subordinate object, that object and its subordinate objects will use the subordinate’s value.
- Default—No value

Scope

- Service scope assigned to this retailer.
- Value—See *Assigning Service Scopes* on page 240.
- Guidelines—By default, all subordinate objects use this value. However, if you specify this value for a subordinate object, that object and its subordinate objects will use the subordinate’s value.
- Default—No value


Deleted

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

Assigning Service Scopes

You can assign multiple service scopes to a subscriber, and you can assign a service scope to multiple subscribers. You must define the service scope before you can assign it to other objects. For information about service scopes, see *SRC-PE Services and Policies Guide, Chapter 2, Managing Services on a Solaris Platform*.

To assign a service scope:

1. In the Users folder of the SDX Admin navigation pane, click on the subscriber to which you want to assign the service scope.
2. Click the  icon below the Scope field in the Main tab of the associated pane.

The Select Object dialog box appears.

3. Select the service scopes.

To select multiple objects, shift-click or control-click service scopes.

4. Click **OK**, and then click **Add**.

The service scopes appear in the Scope field of the pane.

Adding Subscriber Folders

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.

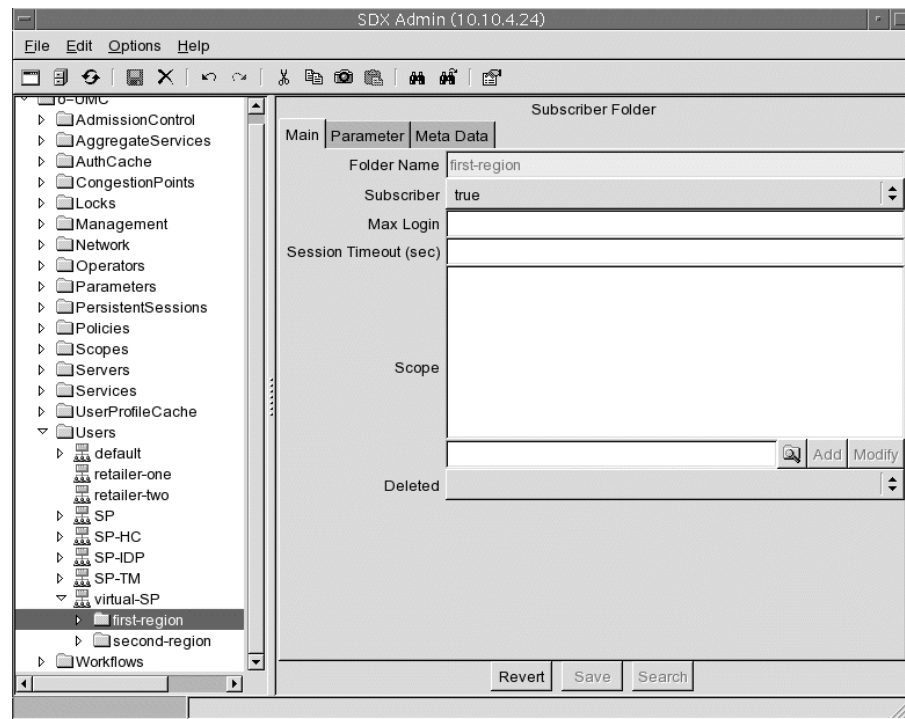
To create a subscriber folder:

1. In Users folder in the SDX Admin navigation pane, right-click the object in which you want to add the subscriber folder, and select **New > Subscriber Folder**.

The New Subscriber Folder dialog box appears.

2. Enter a name for the subscriber folder that is unique within the parent folder, and click **OK**.

An object for the new subscriber folder appears in the navigation pane, and the Subscriber Folder pane appears.



3. Use the field descriptions in *Subscriber Folder Fields* on page 241 to configure the subscriber folder, and then click Save.
4. Enter information in the other tabs:
 - Parameter tab— Enter substitutions in this tab. (See *Configuring Substitutions for Subscriptions* on page 269.)

Subscriber Folder Fields

Use the fields in this section to configure subscriber folders.

Max Login

- Maximum number of concurrent logins for subscribers associated with this subscriber folder.
- Integer in the range 0–2147483647
- Default—By default this value is inherited from parent objects. However, if you specify a value here, it overrides the default for this subscriber and all subordinate objects.

Session Timeout (sec)

- Timeout for subscriber sessions associated with this subscriber folder.
- Value—Number of seconds in the range 0–2147483647
- Default—By default, this value is inherited from parent objects. However, if you specify a value here, it overrides the default for this subscriber and all subordinate objects.

Scope

- Service scope assigned to subscribers associated with this subscriber folder.
- Value—See *Assigning Service Scopes* on page 240.
- Default—By default, this value is inherited from parent objects. However, if you specify a value here, it overrides the default for this subscriber and all subordinate objects.

Deleted

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

Adding Residential Subscribers

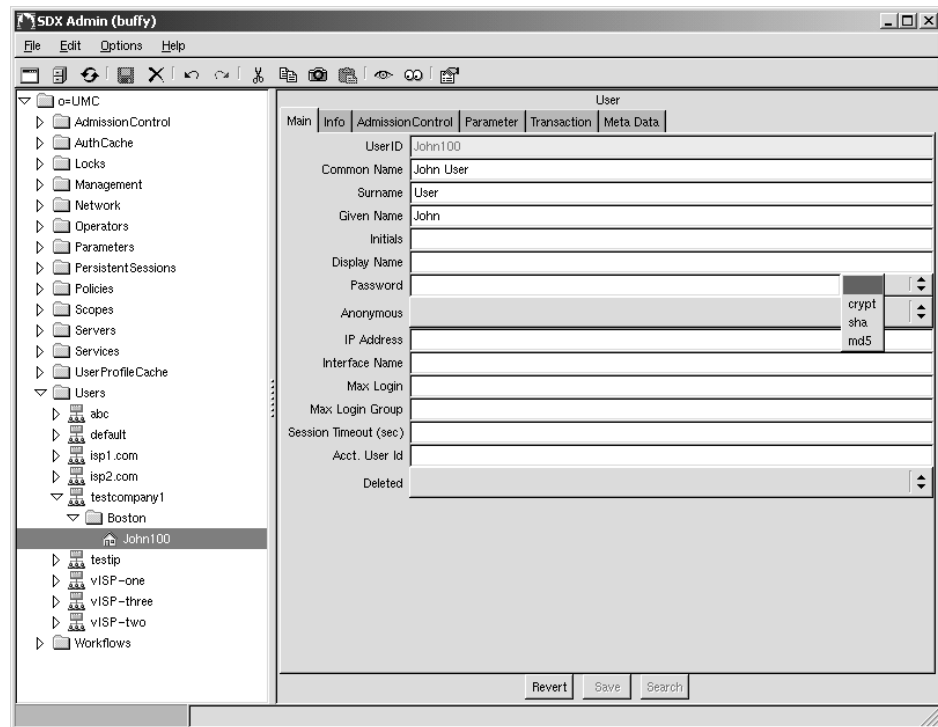
To add a residential subscriber:

1. In the navigation pane, right-click the subscriber folder to which you want to add the new subscriber, and select **New > User**.

The New User dialog box appears.

2. Enter the UserID and Common Name, and click **OK**.
 - UserID—Subscriber's unique login ID.
 - Common Name—Unique name that defines the subscriber in the directory and typically has the format firstName lastName or lastName firstName.

An object for the new subscriber appears in the navigation pane.



3. Use the field descriptions in *Residential Subscriber Fields* on page 244 to configure the subscriber, and then click Save.
4. Enter information in the other tabs:
 - Info tab—Enter the subscriber's contact details and additional administrative information in this tab.
 - AdmissionControl tab—If the Admission Control Plug-In (ACP) manages the subscriber, you must configure bandwidths for the subscriber in this tab. (See *SRC Application Library Guide*.)
 - Parameter tab— Enter substitutions in this tab. (See *Configuring Substitutions for Subscriptions* on page 269.)
 - Transaction tab—Enter information used by the Workflow application to manage transactions involving this subscriber profile. (See *SRC Application Library Guide*).

Residential Subscriber Fields

Use the fields in this section to configure residential subscriber objects.

Common Name

- Name that defines the subscriber in the directory.
- Value—Typically in the format firstName lastName or lastname firstName
- Default—No value

Surname

- Subscriber's last name.
- Value—Text
- Default—No value

Given Name

- Subscriber's first name.
- Value—Text
- Default—No value

Initials

- Subscriber's middle initial(s).
- Value—Text
- Default—No value

Display Name

- Subscriber's name as it appears in login screens.
- Value—Text
- Default—No value

Password

- Login password and type of encryption.
- Value—Enter a password, and select an encryption method that your directory supports (see Table 26 on page 235).
 - empty line—No encryption
 - crypt—Style is /etc/passwd
 - sha—Secure hash algorithm
 - md5—Message digest #5
- Default—No value

Anonymous

- Subscriber's permissions for making modifications to the subscriber's profile or service subscriptions.
- Value
 - True—Subscribers cannot modify their profiles or service subscriptions.
 - False—Subscribers can modify their profiles and service subscriptions.
- Default—No value

IP Address

- Static IP address on subscriber's system for subscribers who connect through PPP or a static IP address (not DHCP or RADIUS).
- Value—IP address
- Default—No value

Interface Name

- Type and specifier of the router interface and virtual router that manage this subscriber.
- Value
 - Name of the interface in your router CLI syntax
- Guidelines—Use this field when you want the subscriber classification script to identify the subscriber entry in the directory based on the interface name received from the router.
- Default—No value
- Example—For JUNOSe routers:
interfaceName = "fastethernet6/0.1 @vrName@routerName"

For JUNOS routing platforms:
interfaceName = "fe-0/1/0.0@vrName@routerName"

Max Login

- Maximum number of concurrent logins for this subscriber.
- Value—Integer in the range 0–2147483647
- Default—By default, this value is inherited from parent objects. However, if you specify a value here, it overrides the default for this subscriber and all subordinate objects.

Max Login Group

- Maximum number of concurrent logins for this subscriber and all objects below it in the navigation pane; typically the maximum number of concurrent logins for a household.
- Value—Integer in the range 0–2147483647
- Default—No value

Session Timeout (sec)

- Timeout for subscriber sessions.
- Value—Number of seconds in the range 0–2147483647
- Default—No session timeout

Acct. User id

- Value that identifies the profile in accounting records; for a household subscriber, all subordinate subscribers generally use the same ID.
- Value—Text
- Default—No value

Deleted

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

Adding Enterprises

When you add an enterprise, the SRC software creates a default operator within the enterprise (see *Operators* on page 232).

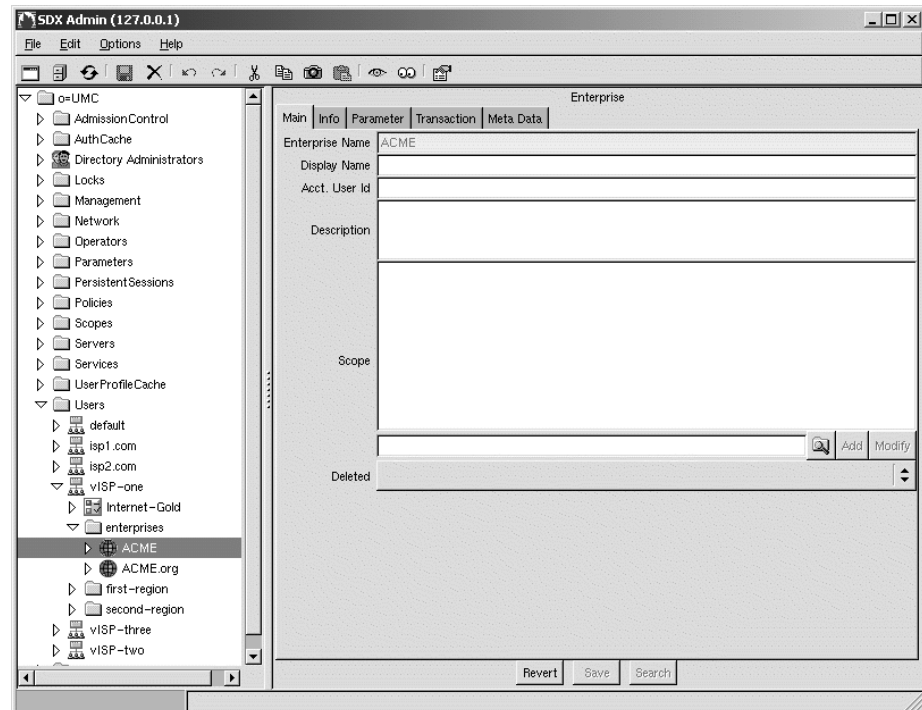
To add an enterprise subscriber:

1. In the navigation pane, right-click the subscriber folder to which you want to add the new subscriber, and select New > Enterprise.

The New Enterprise dialog box appears.

2. Enter a name for the enterprise that is unique for this retailer, and click OK.

The enterprise and a subordinate operator appear in the navigation pane. This default operator has the privilege level administrators.



3. Use the field descriptions in *Enterprise Fields* on page 248 to configure the enterprise, and then click Save.
4. Modify the password of the default operator that is subordinate to the enterprise; the default password is not valid.
5. Enter information in the other tabs:
 - Info tab—Enter the enterprise’s contact details and additional administrative information in this tab.
 - VPNs tab—Enterprises can be extranet clients. Enter imported extranets in this tab. (See *Adding Extranet Clients to VPNs* on page 409.)
 - Parameter tab—Enter substitutions in this tab. (See *Configuring Substitutions for Subscriptions* on page 269.)
 - Transaction tab—Enter information used by the Workflow application to manage transactions involving this subscriber profile. (See *SRC Application Library Guide*.)
6. Configure an access subscription for the enterprise. (See *Configuring Access Subscriptions* on page 261.)

Enterprise Fields

Use the fields in this section to configure enterprise subscribers.

Display Name

- Name that is displayed in enterprise management portals, if different from the enterprise name. An enterprise IT manager can change this name through the portal, whereas the enterprise name is fixed for the lifetime of the enterprise.
- Value—Text
- Default—No value

Acct User Id

- Name that identifies the enterprise in accounting records.
- Value—Text
- Default—No value

Description

- Information about the enterprise.
- Value—Text
- Default—No value

Scope

- Service scope assigned to subscribers associated with this enterprise. For information about service scopes, see *SRC-PE Services and Policies Guide, Chapter 2, Managing Services on a Solaris Platform*.
- Value—See *Assigning Service Scopes* on page 240.
- Default—By default, this value is inherited from parent objects. However, if you specify a value here, it overrides the default for this subscriber and all subordinate objects.

Deleted

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

Adding Sites

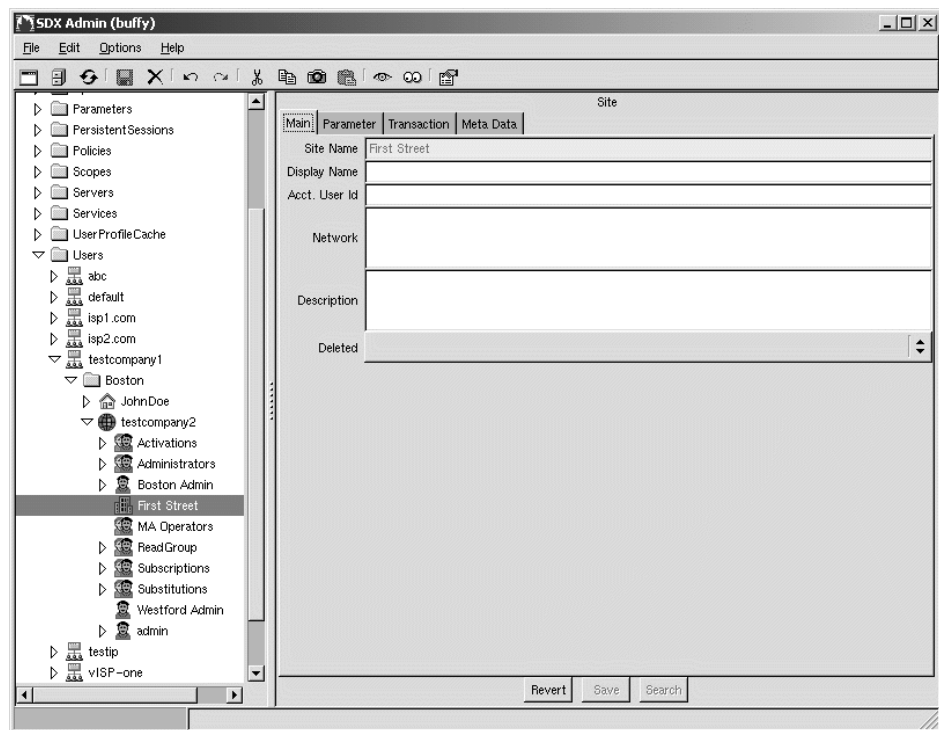
To add a site:

1. In the navigation pane, right-click the enterprise to which you want to add the new site, and select **New > Site**.

The New Enterprise dialog box appears.

2. Enter a name for the site that is unique for the enterprise, and click **OK**.

An object for the new site appears in the navigation pane, and the Site pane appears.



3. Use the field descriptions in *Site Fields* on page 250 to configure the site, and then click Save.
4. Enter information in the other tabs:
 - Parameter tab— Enter substitutions in this tab. (See *Configuring Substitutions for Subscriptions* on page 269.)
 - Transaction tab—Enter information used by the Workflow application to manage transactions involving this subscriber profile. (See *SRC Application Library Guide*.)
5. Configure an access subscription for the site. (See *Configuring Access Subscriptions* on page 261.)

Site Fields

Use the fields in this section to configure sites.

Display Name

- Name that is displayed in portals, if different from the site name. An IT manager can change this name through the portal.
- Value—Text
- Default—No value

Acct. User id

- Value that identifies the profile in accounting records.
- Value—Text
- Default—No value

Network

- Not currently used.
- Value—Text
- Default—No value

Description

- Information about the site.
- Value—Text
- Default—No value

Deleted

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

Adding Routers as Subscribers

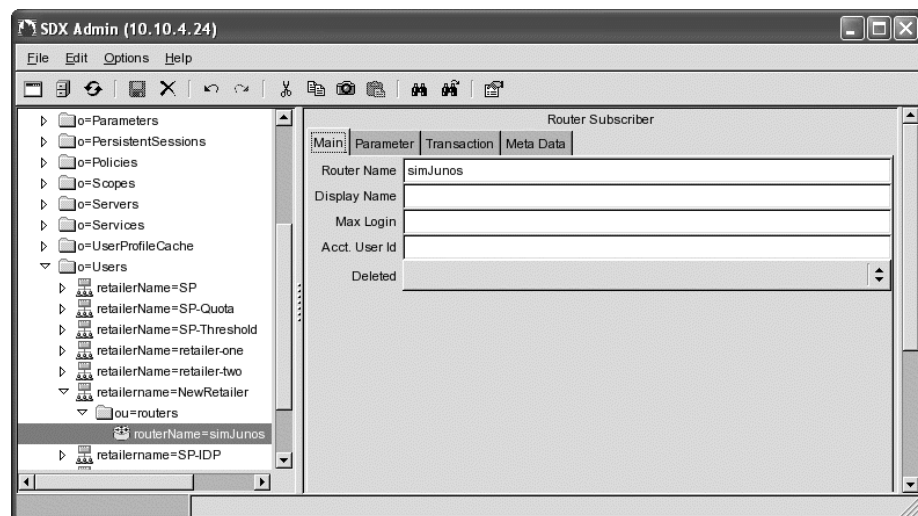
You can add routers as subscribers to enterprises and sites, as well as to subscriber folders. To add a router as a subscriber:

1. In the navigation pane, right-click the object to which you want to add the subscriber, and select **New > Router Subscriber**.

The New Router Subscriber dialog box appears.

2. Enter the name of a router that is configured in the directory.

An object for the new subscriber appears in the navigation pane, and the Router Subscriber pane appears.



3. Use the information in *Router Subscriber Fields* on page 252 to configure the Router Subscriber pane, and then click Save.
4. Enter information in the other tabs:
 - Parameter tab—Enter substitutions in this tab. (See *Configuring Substitutions for Subscriptions* on page 269.)
 - Transaction tab—Enter information used by the Workflow application to manage transactions involving this subscriber profile. (See *SRC Application Library Guide*.)

Router Subscriber Fields

Use the fields in this section to configure routers as subscribers.

Router Name

- Name assigned to the router in the directory.
- Value—Text
- Default—No value

Display Name

- Name of the router as it appears in login dialog boxes.
- Value—Text
- Default—No value

Max Login

- Maximum number of concurrent logins for subscribers associated with this retailer.
- Value—Integer in the range 0–2147483647
- Guidelines—By default, all subordinate objects use this value. However, if you specify this value for a subordinate object, that object and its subordinate objects will use the subordinate's value.
- Default—No value

Acct User Id

- Name that identifies the subscriber profile in accounting records.
- Value—Text
- Default—No value

Deleted

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

Adding Operators

You can add operators with SDX Admin, with an LDAP client, or through an enterprise service portal. If you add an enterprise with SDX Admin, the enterprise will have a default operator that represents the primary IT manager in the enterprise. If you add an enterprise with an LDAP client other than SDX Admin, you must also add to the enterprise an operator that represents the primary IT manager.

To add an operator with SDX Admin:

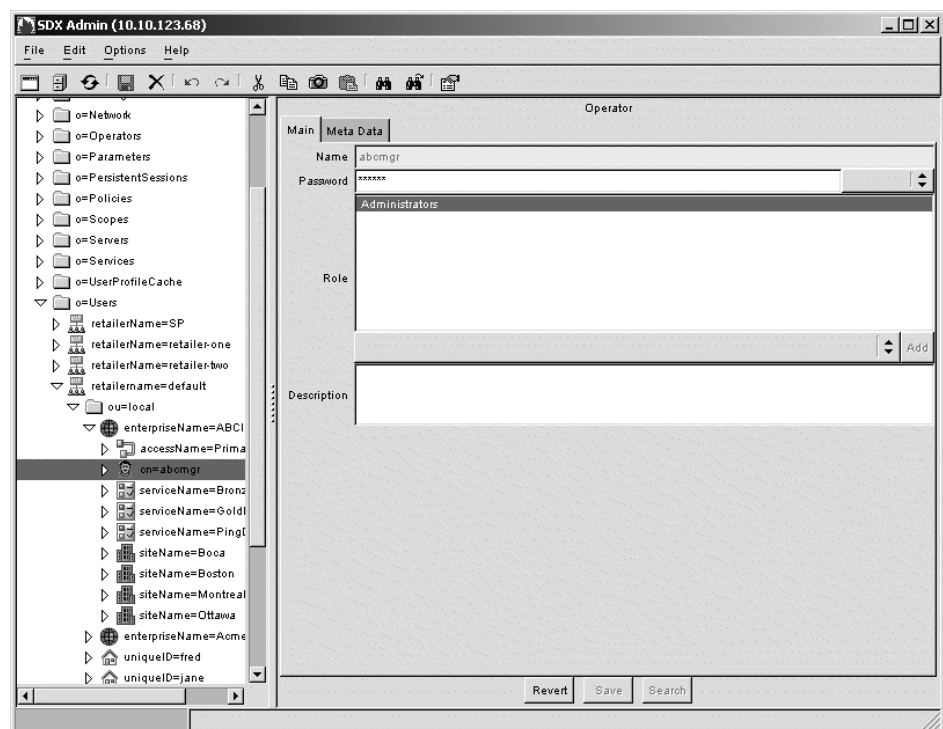
1. In the navigation pane, right-click the object to which you want to add an operator.
 - To add an operator to a subscriber, select the subscriber in *o = Users*, *o = umc*.
 - To add an operator that controls all retailers, select *o = Operators*, *o = umc*.

2. Select **New > Operator**.

The New Operator dialog box appears.

3. Enter a unique name for the operator, and click **OK**.

An object for the operator appears in the navigation pane, and the Operator pane appears.



4. Use the field descriptions in *Operator Fields* on page 254 to configure the operator, and then click **Save**.

Operator Fields

Use the fields in this section to configure operators.

Password

- Login password and type of encryption.
- Value—Enter a password, and select an encryption method that your directory supports (see Table 26 on page 235).
 - empty line—No encryption
 - crypt—Style is /etc/passwd
 - sha—Secure hash algorithm
 - md5—Message digest #5
- Default—No value for operators that you create. The default password for operators that SDX Admin creates when you add an enterprise is not valid. You must enter a new password.

Role

- Privilege level for the operator.
- Value—Select a privilege level in the menu (for a description of privilege levels, see Table 25 on page 233), and click Add. You can add multiple privilege levels.
If you do not specify a privilege level, the operator has read-only access to associated objects.
- Default—No value

Description

- Information about the operator.
- Value—Text
- Default—No value

Configuring Subscriptions

After you add subscribers, you configure service subscriptions for the subscribers. Residential or enterprise subscribers may also be able to configure subscriptions through the portal, and operators assigned to a subscriber object may be able to configure subscriptions for that object.

The following sections describe how to configure the different types of subscriptions:

- Configuring Subscriptions to Value-Added Services on page 255
- Configuring Subscriptions to Outsourced Services on page 258

- Configuring Access Subscriptions on page 261
- Configuring RADIUS Subscriptions on page 264

Configuring Subscriptions to Value-Added Services

You must add a value-added service to the directory before you can specify that service for subscribers. See *SRC-PE Services and Policies Guide, Chapter 2, Managing Services on a Solaris Platform*.

After you configure a subscription to a value-added 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 value-added services are available to subscribers. See *SRC-PE Services and Policies Guide, Chapter 5, Scheduling Services on a Solaris Platform*.

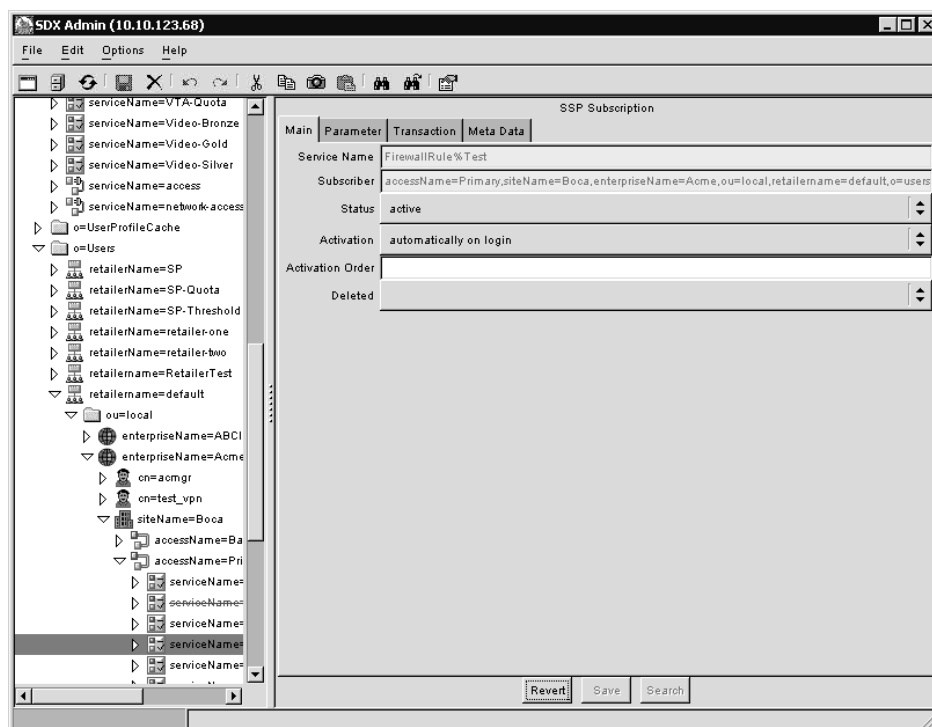
To configure a subscription to a value-added service:

1. In the SDX Admin navigation pane, right-click the subscriber to which you want to add a subscription, and select **New > SSP Subscription**.

The New SSP Subscription dialog box appears.

2. Complete the fields in the dialog box as follows:
 - a. Select a service from the Service Name menu.
 - b. To create multiple subscriptions to the same service, enter a subscription ID. (See *Allowing Multiple Subscriptions per Subscriber* on page 258.)
 - c. Click **OK**.

An object for the new subscription appears in the navigation pane, and the SSP Subscription pane appears.



3. Use the field descriptions in *Value-Added Subscription Fields* on page 257 to configure the subscription, and then click **Save**.
4. Enter information in the other tabs:
 - Parameter tab— Enter substitutions in this tab. (See *Configuring Substitutions for Subscriptions* on page 269.)
 - Transaction tab—Enter information used by the Workflow application to manage transactions involving this subscriber profile. (See *Application Library Guide*.)

Value-Added Subscription Fields

Use the fields in this section to configure value-added subscriptions.

Status

- Status of the service subscription.
- Value
 - active—Subscriber can activate this service.
 - suspended—Subscriber cannot activate this service, although it may be visible through a portal. If you change the value of this field to suspended while the subscription is active, the service is deactivated.
 - hidden—Service is not available through a portal and cannot be activated automatically when the subscriber logs in. If you change the value of this field to hidden while the subscription is active, the service is not deactivated.
- Default—Active

Activation

- Specifies how the service is activated.
- Value
 - manual—Subscriber must activate the service; the service is not activated automatically on login.
 - automatically on login—Service is activated automatically when the subscriber logs in.

The SRC software may modify this setting if the service appears in mutex groups. See *SRC-PE Services and Policies Guide, Chapter 2, Managing Services on a Solaris Platform*.

- Default value—Manual

Activation Order

- Specifies when the SAE should activate this subscription relative to the subscriber's other subscriptions that are configured to activate on login.
- Value—Integer in the range 0-2147483647
- Guidelines—Review all subscriptions that are configured to activate on login for this subscriber, and review the activation order for subscriptions of the parent subscribers. Assign the lowest number to the subscription that you want to activate first. Assign higher numbers to the other subscriptions in the order you want the SAE to activate them. If you assign the same value to multiple subscriptions, the SAE activates them in an unspecified order.
- Default—10000
- Example—200

Deleted

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

Allowing Multiple Subscriptions per Subscriber

To allow a subscriber to have a number of subscriptions to a service at the same time, 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 Subscriptions to Outsourced Services

Create an outsource subscription for retailers to specify that a retailer will use outsourced services from wholesalers. You must add an outsourced service to the directory before you specify that service for subscribers. See *SRC-PE Services and Policies Guide, Chapter 2, Managing Services on a Solaris Platform*.

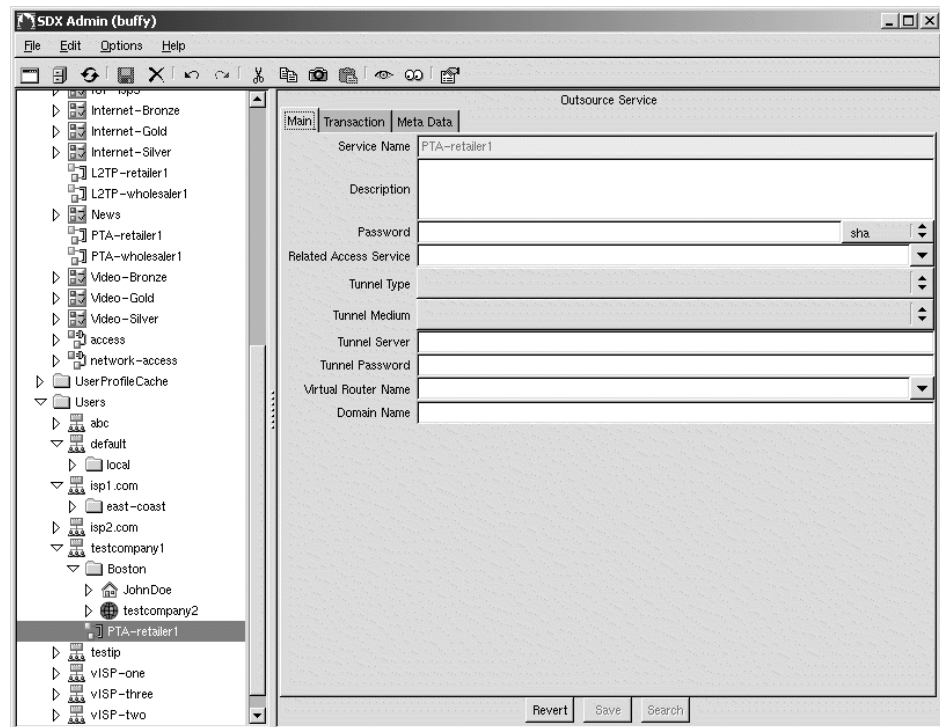
To configure a subscription to an outsourced service:

1. In the SDX Admin navigation pane, right-click the subscriber to which you want to add the subscription, and select **New > Outsource Service**.

The New Outsource Service dialog box appears.

2. Select a service from the Service Name menu, and click **OK**.

An object for the new outsource service subscription appears in the navigation pane, and the Outsource Service pane appears.



3. Use the field descriptions in *Outsource Service Subscription Fields* on page 259 to configure the outsource service subscription, and click **Save**.
4. Enter information in the other tabs:
 - Transaction tab—Enter information used by the Workflow application to manage transactions involving this subscriber profile. (See *SRC Application Library Guide*.)

Outsource Service Subscription Fields

Use the fields in this section to configure outsourced service subscriptions.

Description

- Information about this service.
- Value—Text
- Default—If a description exists for this outsourced service in the Services folder, the same description is visible in this pane.

Password

- Password for the outsourced service.
- Value—Enter a password, and select an encryption method that your directory supports (see Table 26 on page 235).
 - empty line—No encryption
 - crypt—Style is /etc/passwd
 - sha—Secure hash algorithm
 - md5—Message digest #5
- Default—No value

Related Access Service

- Access service that allows the retailer to use this tunnel and password.
- Value—Select an access service from the drop-down menu, or enter an access service
- Default—No value
- Example—*serviceName = BackupAccess, o = Services, o = umc*

Tunnel Type

- Encapsulation protocol used by this tunnel.
- Value
 - PPTP—Point-to-Point Tunneling Protocol
 - L2F—Layer 2 Forwarding Protocol
 - L2TP—Layer 2 Tunneling Protocol
- Default—No value

Tunnel Medium

- Address protocol used by this tunnel.
- Value
 - IPv4—Internet Protocol version 4
 - IPv6—Internet Protocol version 6
 - NSAP—Network Service Access Point
- Default—No value

Tunnel Server

- IP address of the tunnel server at the company that provides the outsourced service.
- Value—IP address
- Default—No value

Tunnel Password

- Password that this retailer uses to access the tunnel.
- Value—Password
- Default—No value

Virtual Router Name

- Name of the virtual router on the router that provides access to this tunnel
- Value—Virtual router name
- Default—No value

Domain Name

- Domain name of the company that provides the outsourced service.
- Value—Domain name
- Default—No value

Configuring Access Subscriptions

You must configure an access subscription for an enterprise or a site. An access subscription determines the way that the enterprise or site accesses Internet services, and specifies a set of value-added services that are available to the enterprise or site. You must add an access service to the directory before you create an access subscription. See *SRC-PE Services and Policies Guide, Chapter 2, Managing Services on a Solaris Platform*.

You can specify multiple access services; for example, you might want to specify primary and secondary services for Internet access.

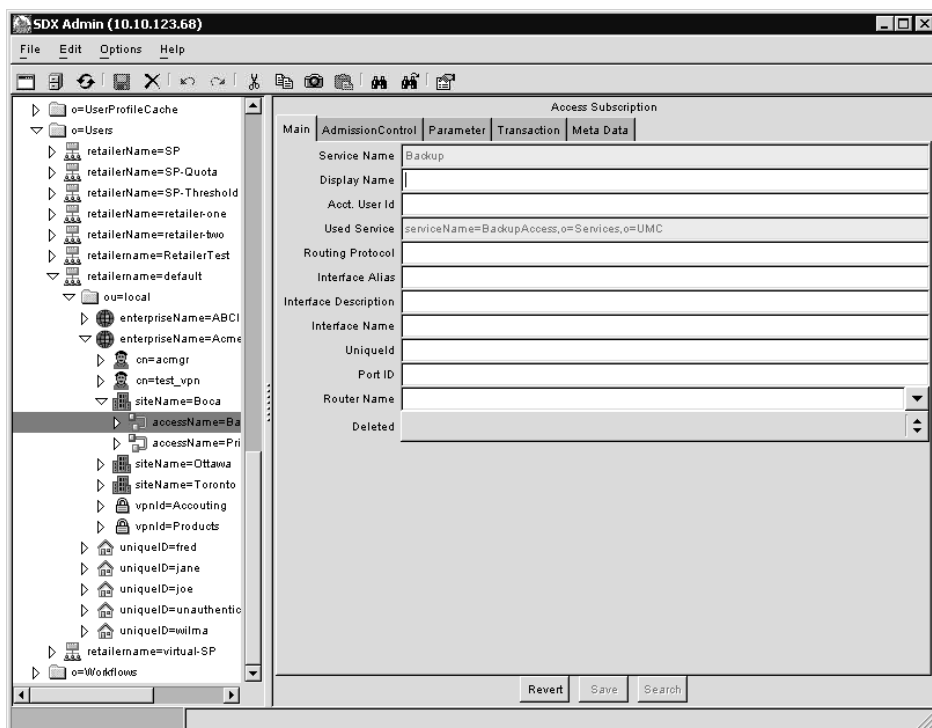
To configure a subscription to an access service:

1. In the SDX Admin navigation pane, right-click the enterprise or site for which you want to specify an access service, and select **New > Access Subscription**.

The New Access Subscription dialog box appears.

2. Enter a name for the subscription that is unique for the enterprise or site, select a service from the Used Service menu, and click **OK**.

An object for the new access subscription appears in the navigation pane, and the Access Subscription pane appears.



3. Use the field descriptions in *Access Subscription Fields* on page 262 to configure the access subscriptions, and click **Save**.
4. Enter information in the other tabs:
 - AdmissionControl tab—If the ACP manages the subscription, you must configure bandwidths for the subscription in this tab. (See *SRC Application Library Guide*.)
 - Parameter tab— Enter substitutions in this tab. (See *Configuring Substitutions for Subscriptions* on page 269.)
 - Transaction tab—Enter information used by the Workflow application to manage transactions involving this subscriber profile. (See *SRC Application Library Guide*.)

Access Subscription Fields

Use the fields in this section to configure access subscriptions. Subscriber classification scripts can use access subscription properties to match the interface in the network with an access in the directory.

Display Name

- Name that is displayed in enterprise management portals, if different from the service name. IT managers can change this name through the portal, whereas the service name is fixed for the lifetime of the access.
- Value—Text
- Default—No value

Acct. User id

- Value that identifies the service in accounting records.
- Value—Text
- Default—No value

Routing Protocol

- Not currently used.

Interface Alias

- Description of a router interface.
- Value—Interface description that is configured on the router
- Default—No value

Interface Description

- Alternate name of the interface that SNMP uses. This name is system-generated.
- 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.
- Default—No value
- Example—ifDesc = “IP3/1.1”

Interface Name

- Name of the interface.
- Value
 - Name of the interface in your router CLI syntax
 - FORWARDING_INTERFACE for routing instance (used by traffic mirroring)
- Default—No value
- Example—For JUNOSe routers: interfaceName = “fastethernet6/0.1”
For JUNOS routing platforms: interfaceName = “fe-0/1/0.0”
For forwarding interface: interfaceName = “FORWARDING_INTERFACE”

Uniqueid

- Router's unique ID.
- Value—Index of the router in the SNMP table for all interfaces.
- Default—No value

Port ID

- NAS port ID reported by the JUNOS router through COPS.
- Value—Includes interface name and additional layer 2 information
- Default—No value
- Example—nasPortId = "fastEthernet 3/1" (There is a space between fastEthernet and slot number 3/1 in the NAS port ID.)

Router Name

- Name of the router to which this access connects.
- Value—Select a name from the menu.
- Default—No value

Deleted

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

Configuring RADIUS Subscriptions

You must add a RADIUS service to the directory before you specify that service for subscribers. See *SRC-PE Services and Policies Guide, Chapter 2, Managing Services on a Solaris Platform*.

To configure a subscription to a RADIUS service:

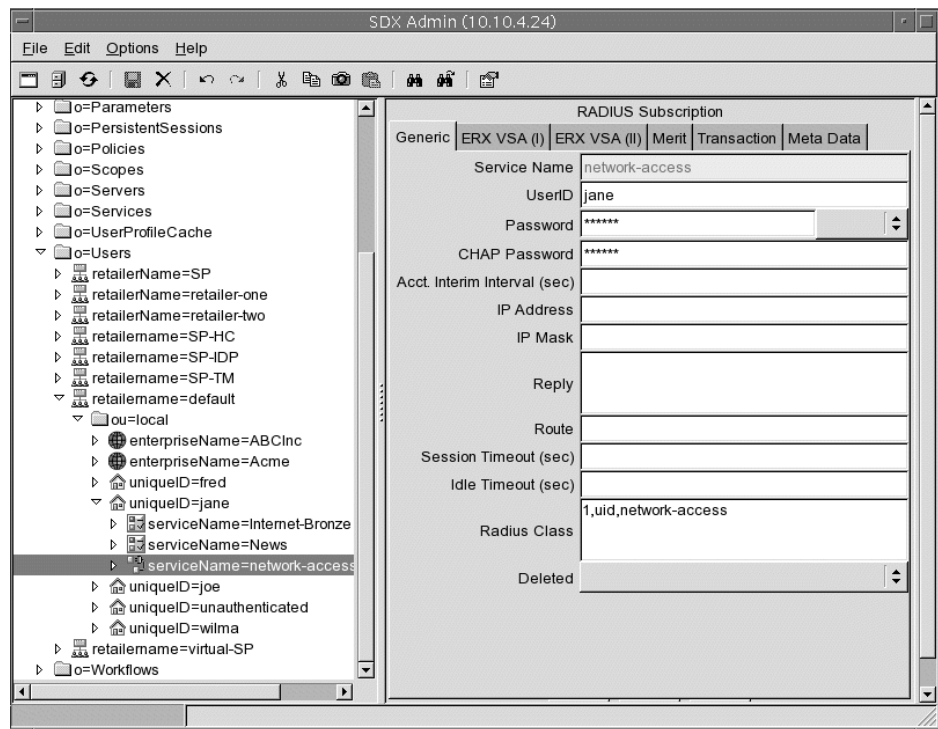
1. In the SDX Admin navigation pane, right-click the access subscription folder or residential subscription folder to which you want to add the new subscriber, and select **New > RADIUS Subscription**.

The New RADIUS Subscription dialog box appears.

2. Select a RADIUS service from the Service Name menu, and click **OK**.

An object for the new subscription appears in the navigation pane, and the RADIUS Subscription pane appears.

Some values for the RADIUS subscription are inherited from the RADIUS service. However, you can change these values to make them specific to the subscriber.



3. Use the field descriptions in *RADIUS Subscription Fields* on page 266 to configure the subscription, and click **OK**.

You can define RADIUS attributes in two formats:

- Generic schema, in which each RADIUS attribute corresponds to one LDAP attribute. These values are displayed in the Generic and ERX VSA tabs.
- Merit RADIUS schema, in which RADIUS attributes are entered as multiple values of a single LDAP attribute. These values are displayed in the Merit tab.

When you save the subscription object, values entered in one format are converted to the other format as well. This means that if you enter RADIUS attributes in the generic tab, the Merit RADIUS attributes are updated, and vice versa.

4. Enter information in the other tabs:

- ERX VSA tabs—For information about configuring in these tabs, see the information about configuring RADIUS services in *SRC-PE Services and Policies Guide, Chapter 2, Managing Services on a Solaris Platform*.
- Merit tab—If you are running an ordinary LDAP client, you must enter these attributes and click Save.

If you enter values in the Generic, ERX VSA(1), or ERX VSA(2) tabs and click Save, the values get populated in the Merit AAA Reply field. To set up AAA Check or AAA Deny policies, enter them in the appropriate Merit fields, and click Save.

See *SRC-PE Integration Guide, Chapter 12, Integrating Merit RADIUS* for more information.

- Transaction tab—Enter information used by the Workflow application to manage transactions involving this subscriber profile. (See *SRC Application Library Guide*.)

RADIUS Subscription Fields

Use the fields in this section to configure RADIUS subscriptions.

UserID

- Login ID that RADIUS uses to authenticate the subscriber.
- Value—Text
- Default—Inherited from the User ID attribute of the subscriber.

Password

- Password that the subscriber uses to access the RADIUS server.
- Value—Enter a password, and select an encryption method that your directory supports (see Table 26 on page 235).
 - empty line—No encryption
 - crypt—Style is /etc/passwd
 - sha—Secure hash algorithm
 - md5—Message digest #5
- Default—No value

CHAP Password

- Password that the subscriber uses for CHAP authentication on the RADIUS server.
- Value—CHAP password
- Default—No value

Acct. Interim Interval (sec)

- Interval between interim accounting messages for this service.
- Value—Number of seconds in the range 0-2147483648
 - No value—The globally configured accounting interim value is used.
 - 0—Interim accounting is disabled for this service.
- Default—No value; may be inherited from the RADIUS service

IP Address

- IP address for the subscriber's network.
- Value—IP address
- Default—No value

IP Mask

- Mask for the subscriber's subnet.
- Value—IP mask
- Default—No value

Reply

- Text to be displayed to the subscriber. This is the RADIUS Reply-Message attribute.
- Value—Text string
- Default—No value; may be inherited from the RADIUS service

Route

- Route from the subscriber to the RADIUS server
- Value—Route in the format compatible with *RFC 2865—Remote Authentication Dial In User Service (RADIUS) (June 2000)*: < ipAddress > / < ipLength > < gatewayAddress > < metric >
 - ipAddress—IP address of the subnet
 - ipLength—Optional value that specifies the number of high-order bits from the IP address of the subnet. Default values are:
 - 8 (for class A prefixes)
 - 16 (for class B prefixes)
 - 24 (for class C prefixes)

- gatewayAddress—IP address of the router that forwards traffic to the RADIUS server; a value of 0.0.0.0 indicates that the gateway address is the subscriber's IP address
- metric—Number in the range 1–254 that specifies a precedence for the route; a lower number indicates a higher precedence
- Default—No value
- Example:

```
192.168.1.0/24 192.168.1.1 1 2 -1 3 400
192.168.1.0 192.168.1.1 1
```

Session Timeout (sec)

- Timeout for RADIUS session.
- Value—Number of seconds in the range 0–2147483647
- Guidelines—If this timeout is lower than the timeout defined for the subscriber session, the SRC software uses the RADIUS timeout for subscriber sessions.
- Default—No value; may be inherited from the RADIUS service

Idle Timeout (sec)

- Time at which the RADIUS session ends if there is no activity between the subscriber and the RADIUS server.
- Value—Number of seconds in the range 0–2147483647
- Default—No value; may be inherited from the RADIUS service

RADIUS Class

- Arbitrary value that, if the RADIUS server supplies it, the network access server (NAS) includes in all accounting packets for the subscriber.
- Value—Text
- Default—No value; may be inherited from the RADIUS service

Deleted

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

Configuring Substitutions for Subscriptions

This section shows how to add, modify, validate, and delete substitutions in SDX Admin.

Adding Substitutions

To add a substitution:

1. In SDX Admin, select the **Parameter** tab for the subscriber to which you want to add a substitution.
2. In the unlabeled field below the Substitution field, enter the substitution in the correct syntax (see *Formatting Substitutions* on page 405). For example:

Substitution	Fixed	Name	Role	Value	Description
		dept	network		subnet of the department to apply the service to
	!	qos		interface_speed*0.5	gold qos is 50% of interface speed
	!	outside	network	dept	rename outside policy parameter to dept
!inside:network=any//always apply to any subnet inside the service provider					
					Validate Add Modify

3. Click **Add**.



NOTE: Substitutions for JUNOS routers may not be correctly displayed in the Substitution field for SDX Admin. To confirm the syntax of a JUNOS substitution, click on the substitution in the Substitution field, and observe the syntax in the entry field below the Substitution field.

Substitutions to a Transmission Rate for a Scheduled Action

When you use SDX Admin to assign substitutions to the Transmit Rate Unit for a Scheduler action, you can specify one of the following:

- “percent”
- “remainder”
- “bps”

Do not use the “rate_in_percent” value as it appears in Policy Editor for substitutions in SDX Admin. Do one or the other. For example in Policy Editor, specify a parameter called ‘x’ for the Transmit Rate Unit for a Scheduler Action and select rate_in_percent; or in SDX Admin, create a substitution as x = percent.

Modifying Substitutions

To modify a substitution:

1. In SDX Admin, select the **Parameter** tab for the subscription to which you want to add a substitution.
2. Select the substitution in the Substitutions field.
3. Modify the substitution in the unlabeled field below the Substitution field.
4. Click **Modify**.

Validating Substitutions

To validate a substitution:

1. In SDX Admin, select **Options > Configure**.

The Main Configuration window appears.

Main Configuration	
Encrypt userPassword	<input type="checkbox"/>
Show Objecttype	No
Delete Subtree	No
Subscriber Folder is Subscriber	No
Show Toolbar	Yes
Show Statusbar	Yes
LDAP timeout	20
UNDO levels	10
OSM Host	127.0.0.1
OSM Port	6001
OSM Transaction ID Prefix	SSCADMIN_
OSM Report Server Port	7001
Default Trap Receiver	127.0.0.1:162:public:1
DirX Server Address	
SAE Admin Web Application Server	
Tool Path	
<input type="button" value="Enable all Warnings"/>	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

2. In the SAE Admin Web Application Server field, enter the identifier of the host on which you installed SAE Web Admin, in the format: < host > : < port > .
 - < host > —Name or IP address of the host
 - < port > —Port number for SAE Web Admin
3. Click **OK**.
4. Select the substitution in the Substitution field.
5. Click **Validate**.

SDX Admin displays the result of the validation.

Deleting Substitutions

To delete a substitution, select it in the Substitutions field, right-click, and select **Delete**.

Modifying and Deleting Subscribers and Subscriptions

For information about modifying and deleting objects, see *SRC-PE Getting Started Guide, Chapter 38, Using SDX Admin*. For information about customizing fields when you modify an object, see the section that describes how to add that type of object.

Chapter 14

Configuring Subscribers and Subscriptions with the SRC CLI

This chapter shows how to use the SRC CLI to configure subscribers and managers and to configure subscriptions to services. You can use the SRC CLI on the C-series platform and on Solaris platforms.

You can also use SDX Admin to configure subscribers and subscriptions on a Solaris platform. See *Chapter 13, Configuring Subscribers and Subscriptions with SDX Admin*.

Topics in this chapter include:

- Overview of Configuring Subscribers and Subscriptions on page 274
- Enabling the Subscriber and Subscription Configuration on the SRC CLI on page 274
- Adding Subscribers on page 275
- Adding Retailers on page 276
- Adding Subscriber Folders on page 278
- Adding Residential Subscribers on page 279
- Adding Enterprises on page 283
- Adding Sites on page 285
- Adding Devices as Subscribers on page 286
- Adding Managers on page 287
- Configuring Subscriptions on page 290
- Configuring Accesses on page 292

Overview of Configuring Subscribers and Subscriptions

This section gives an overview of configuring subscribers and subscriptions for the SRC software.

Specifying the Activation Order for Subscriptions

You can specify the order in which the SAE activates subscriptions that are set up to activate on login for a particular subscriber. To specify the order, you define a precedence for the activation of each subscription. The SAE activates services in ascending order of precedence; if multiple services have the same precedence, the SAE activates them in an unspecified order.

You can configure the activation order by setting the **activation-order** option when you configure a subscription to a service with the SRC CLI. The enterprise manager portal automatically sets the activation order of some subscriptions to ensure they are activated before other subscriptions that depend on them.

Inheritance of Properties and Subscriptions

Subordinate subscribers inherit properties and SAE subscriptions from their parent subscribers, unless you specify a different value for the subordinate. Properties that a subscriber can inherit include the maximum number of concurrent logins and the session timeout. For example, if you configure a subscription to a video service for an enterprise and configure a different subscription to the same video service for a site within that enterprise, the site uses its own subscription rather than the inherited subscription.

Enabling the Subscriber and Subscription Configuration on the SRC CLI

Before you can configure subscribers and subscriptions with the SRC CLI, you must enable the policy, service, and subscriber editor on the SRC CLI. To do so:

- In operational mode, enter the following command:

```
user@host> enable component policy-service-subscriber
```

If you are using multiple C-series platforms, we recommend that you enable the policy, service, and subscriber editor on only one C-series platform on your network. 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

This section describes how to add and configure subscribers with the SRC CLI.

The tasks to configure subscribers are:

- Adding Retailers on page 276
- Adding Subscriber Folders on page 278

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.

- Adding Residential Subscribers on page 279
- Adding Enterprises on page 283
- Adding Sites on page 285
- Adding Devices as Subscribers on page 286

After you add subscribers, you can add managers and configure subscriptions. See *Adding Managers* on page 287 and *Configuring Subscriptions* on page 290.

Adding Retailers

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.

Use the following configuration statements to add a retailer:

```
subscribers retailer name {
    domain-name [domain-name...];
    authentication-plug-in [authentication-plug-in...];
    dhcp-authentication-plug-in [dhcp-authentication-plug-in...];
    tracking-plug-in [tracking-plug-in...];
    maximum-login maximum-login;
    session-timeout session-timeout;
    scope [scope...];
    substitution [substitution...];
}
```

To add a retailer:

1. From configuration mode, enter the retailer configuration. In this procedure, retailer-one is the name of the retailer.

```
user@host# edit subscribers retailer retailer-one
```

2. Configure the domain name(s) associated with the retailer.

```
[edit subscribers retailer retailer-one]
user@host# set domain-name [domain-name...]
```

3. (Optional) Configure the plug-in(s) used to authenticate subscribers who log in to the domains specified for this retailer.

```
[edit subscribers retailer retailer-one]
user@host# set authentication-plug-in [authentication-plug-in...]
```

4. (Optional) Configure the DHCP authorization plug-in(s) used to authenticate DHCP discover requests for subscribers who log in to the domains specified for this retailer.

```
[edit subscribers retailer retailer-one]
user@host# set dhcp-authentication-plug-in [dhcp-authentication-plug-in...]
```

5. (Optional) Configure the plug-in(s) used for accounting or tracking subscriber sessions.

```
[edit subscribers retailer retailer-one]
user@host# set tracking-plug-in [tracking-plug-in...]
```

6. (Optional) Configure the maximum number of concurrent logins for subscribers associated with this retailer.

```
[edit subscribers retailer retailer-one]
user@host# set maximum-login maximum-login
```

7. (Optional) Configure the timeout for subscriber sessions.

```
[edit subscribers retailer retailer-one]
user@host# set session-timeout session-timeout
```

8. (Optional) Assign service scopes to the retailer.

```
[edit subscribers retailer retailer-one]
user@host# set scope [scope...]
```

9. (Optional) Configure the actual values for parameters associated with this retailer.

```
[edit subscribers retailer retailer-one]
user@host# set substitution [substitution...]
```

10. (Optional) Verify your configuration.

```
[edit subscribers retailer retailer-one]
user@host# show
domain-name abc.com;
authentication-plug-in flexRadiusAuth;
tracking-plug-in fileAcct;
maximum-login 8;
session-timeout 6000;
```

Configuring Administrative Information for Retailers

Use the following configuration statements to configure administrative information about the retailer:

```
subscribers retailer name info {
    contact contact;
    e-mail e-mail;
    url url;
}
```

To add administrative information about retailers:

1. From configuration mode, enter the retailer subscriber info configuration. In this procedure, retailer-one is the name of the retailer.

```
user@host# edit subscribers retailer retailer-one info
```

2. (Optional) Configure a contact name for the retailer.

```
[edit subscribers retailer retailer-one info]
user@host# set contact contact
```

3. (Optional) Configure an e-mail address for the retailer.

```
[edit subscribers retailer retailer-one info]
user@host# set e-mail e-mail
```

4. (Optional) Configure a URL for the retailer.

```
[edit subscribers retailer retailer-one info]
user@host# set url url
```

5. (Optional) Verify your configuration.

```
[edit subscribers retailer retailer-one info]
user@host# show
contact "Mary Smith";
e-mail msmith@abc.com;
url www.abc.com;
```

Adding Subscriber Folders

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.

Use the following configuration statements to configure subscriber folders:

```
subscribers retailer name subscriber-folder folder-name {
    maximum-login maximum-login;
    session-timeout session-timeout;
    scope [scope...];
    substitution [substitution...];
}
```

To create a subscriber folder:

1. From configuration mode, enter the subscriber folder configuration. In this procedure, *retailer-one* is the name of the retailer and *local* is the name of the subscriber folder.

```
user@host# edit subscribers retailer retailer-one subscriber-folder local
```

2. (Optional) Configure the maximum number of concurrent logins for subscribers associated with this folder.

```
[edit subscribers retailer retailer-one subscriber-folder local]
user@host# set maximum-login maximum-login
```

3. (Optional) Configure the timeout for subscriber sessions associated with this folder.

```
[edit subscribers retailer retailer-one subscriber-folder local]
user@host# set session-timeout session-timeout
```

4. (Optional) Assign service scopes to the folder.

```
[edit subscribers retailer retailer-one subscriber-folder local]
user@host# set scope [scope...]
```

5. (Optional) Configure the actual values for parameters associated with this folder.

```
[edit subscribers retailer retailer-one subscriber-folder local]
user@host# set substitution [substitution...]
```

6. (Optional) Verify your configuration.

```
[edit subscribers retailer retailer-one subscriber-folder local]
user@host# show
session-timeout 9000;
scope POP-Boston;
```

Adding Residential Subscribers

Use the following configuration statements to configure residential subscribers:

```
subscribers retailer name subscriber-folder folder-name subscriber name {
  common-name common-name;
  surname surname;
  given-name given-name;
  initials initials;
  anonymous;
  ip-address ip-address;
  interface-name interface-name;
  maximum-login-group maximum-login-group;
  display-name display-name;
  encrypted-password encrypted-password;
  plain-text-password;
  maximum-login maximum-login;
  session-timeout session-timeout;
  accounting-user-id accounting-user-id;
  substitution [substitution...];
}
```

To add a residential subscriber:

1. From configuration mode, enter the residential subscriber configuration. In this procedure, peter is the name of the subscriber record.

```
user@host# edit subscribers retailer default subscriber-folder local subscriber
peter
```

2. Configure the name that defines the subscriber in the directory.

```
[edit subscribers retailer default subscriber-folder local subscriber peter]
user@host# set common-name common-name
```

3. Configure the subscriber's last name.

```
[edit subscribers retailer default subscriber-folder local subscriber peter]
user@host# set surname surname
```

4. (Optional) Configure the subscriber's first name.

```
[edit subscribers retailer default subscriber-folder local subscriber peter]
user@host# set given-name given-name
```

5. (Optional) Configure the subscriber's middle initial(s)

```
[edit subscribers retailer default subscriber-folder local subscriber peter]
user@host# set initials initials
```

6. (Optional) Specify whether the subscriber profile created with this subscriber definition is a shared profile. Subscribers cannot modify shared profiles.

```
[edit subscribers retailer default subscriber-folder local subscriber peter]
user@host# set anonymous
```

7. (Optional) Configure the IP address for subscribers who have fixed IP addresses, and for whom the SRC does not learn addresses through its management of routers or through calls to its notification API.

```
[edit subscribers retailer default subscriber-folder local subscriber peter]
user@host# set ip-address ip-address
```

8. (Optional) Configure the type and specifier of the router interface and virtual router that manage this subscriber.

```
[edit subscribers retailer default subscriber-folder local subscriber peter]
user@host# set interface-name interface-name
```

9. (Optional) Configure the maximum number of concurrent logins for this subscriber and all subordinate objects.

```
[edit subscribers retailer default subscriber-folder local subscriber peter]
user@host# set maximum-login-group maximum-login-group
```

10. (Optional) Configure the subscriber's name as it appears in login screens.

```
[edit subscribers retailer default subscriber-folder local subscriber peter]
user@host# set display-name display-name
```

11. (Optional) Configure the login password and type of encryption.

```
[edit subscribers retailer default subscriber-folder local subscriber peter]
user@host# set encrypted-password encrypted-password
```

12. (Optional) Configure the plain text password.

```
[edit subscribers retailer default subscriber-folder local subscriber peter]
user@host# set plain-text-password
```

13. (Optional) Configure the maximum number of concurrent logins for subscribers associated with this subscriber definition.

```
[edit subscribers retailer default subscriber-folder local subscriber peter]
user@host# set maximum-login maximum-login
```


14. (Optional) Configure the timeout for subscriber sessions associated with this subscriber.

```
[edit subscribers retailer default subscriber-folder local subscriber peter]
user@host# set session-timeout session-timeout
```

15. (Optional) Configure the value that identifies the subscriber in accounting records; for a household subscriber, all subordinate subscribers generally use the same ID.

```
[edit subscribers retailer default subscriber-folder local subscriber peter]
user@host# set accounting-user-id accounting-user-id
```

16. (Optional) Assign service scopes to the subscriber.

```
[edit subscribers retailer default subscriber-folder local subscriber peter]
user@host# set scope [scope...]
```

17. (Optional) Configure the actual values for parameters associated with this subscriber.

```
[edit subscribers retailer default subscriber-folder local subscriber peter]
user@host# set substitution [substitution...]
```

18. (Optional) Verify your configuration.

```
[edit subscribers retailer default subscriber-folder local subscriber peter]
user@host# show
common-name psmith;
surname smith;
initials A;
anonymous;
ip-address 10.10.62.3;
interface-name fastethernet6/0.1@vrName@routerName;
encrypted-password abcdefh;
session-timeout 9000;
```

Configuring Administrative Information for Residential Subscribers

Use the following configuration statements to configure administrative information about the subscriber:

```
subscribers retailer name subscriber-folder folder-name subscriber name info {
  home-phone home-phone;
  additional-phone additional-phone;
  fax fax;
  e-mail e-mail;
  city city;
  street street;
  postal-code postal-code;
  language language;
  job job;
  description description;
}
```

To add administrative information about residential subscribers:

1. From configuration mode, enter the residential subscriber info configuration. In this procedure, peter is the name of the subscriber.

```
user@host# edit subscribers retailer default subscriber-folder local subscriber peter info
```

2. (Optional) Configure a home phone number for the subscriber.

```
[edit subscribers retailer default subscriber-folder local subscriber peter info]
user@host# set home-phone home-phone
```

3. (Optional) Configure a second phone number for the subscriber.

```
[edit subscribers retailer default subscriber-folder local subscriber peter info]
user@host# set additional-phone additional-phone
```

4. (Optional) Configure a fax number for the subscriber.

```
[edit subscribers retailer default subscriber-folder local subscriber peter info]
user@host# set fax fax
```

5. (Optional) Configure an e-mail address for the subscriber.

```
[edit subscribers retailer default subscriber-folder local subscriber peter info]
user@host# set e-mail e-mail
```

6. (Optional) Configure the city for the subscriber.

```
[edit subscribers retailer default subscriber-folder local subscriber peter info]
user@host# set city city
```

7. (Optional) Configure the street address for the subscriber.

```
[edit subscribers retailer default subscriber-folder local subscriber peter info]
user@host# set street street
```

8. (Optional) Configure the postal code for the subscriber.

```
[edit subscribers retailer default subscriber-folder local subscriber peter info]
user@host# set postal-code postal-code
```

9. (Optional) Configure the language of the subscriber.

```
[edit subscribers retailer default subscriber-folder local subscriber peter info]
user@host# set language language
```

10. (Optional) Configure the job description of the subscriber.

```
[edit subscribers retailer default subscriber-folder local subscriber peter info]
user@host# set job job
```

11. (Optional) Configure a description for the subscriber.

```
[edit subscribers retailer default subscriber-folder local subscriber peter info]
user@host# set description description
```

Adding Enterprises

Use the following configuration statements to add an enterprise subscriber:

```
subscribers retailer name subscriber-folder folder-name enterprise name {
    display-name display-name;
    accounting-user-id accounting-user-id;
    description description;
    scope [scope...];
    substitution [substitution...];
}
```

To add an enterprise subscriber:

1. From configuration mode, enter the enterprise subscriber configuration. In this procedure, ABCInc is the name of the enterprise subscriber.

```
user@host# edit subscribers retailer default subscriber-folder local enterprise  
ABCInc
```

2. (Optional) Configure the name that is displayed in enterprise management portals, if different from the enterprise name.

```
[edit subscribers retailer default subscriber-folder local enterprise ABCInc]  
user@host# set display-name display-name
```

3. (Optional) Configure the name that identifies the enterprise in accounting records.

```
[edit subscribers retailer default subscriber-folder local enterprise ABCInc]  
user@host# set accounting-user-id accounting-user-id
```

4. (Optional) Enter a description of the enterprise.

```
[edit subscribers retailer default subscriber-folder local enterprise ABCInc]  
user@host# set description description
```

5. (Optional) Assign service scopes to the enterprise.

```
[edit subscribers retailer default subscriber-folder local enterprise ABCInc]  
user@host# set scope [scope...]
```

6. (Optional) Configure the actual values for parameters associated with this enterprise.

```
[edit subscribers retailer default subscriber-folder local enterprise ABCInc]  
user@host# set substitution [substitution...]
```

7. (Optional) Verify your configuration.

```
[edit subscribers retailer default subscriber-folder local enterprise  
ABCInc]  
user@host# show  
display-name ABCInc;  
description "This enterprise is sample data for use with JUNOS routers.  
The attached EntJunose scope contains enterprise services that are designed  
to work with JUNOSe."
```

```
scope [ EntJunose POP-Ottawa POP-Boca POP-Boston POP-Montreal ];
substitution [ "acct : network = 208.93.36.80 / 28" "eng : network =
208.93.36.64 / 28" ];
```

8. Configure an access subscription for the enterprise. (See *Configuring Accesses* on page 292.)

Configuring Administrative Information for Enterprise Subscribers

Use the following configuration statements to configure administrative information about the enterprise subscriber:

```
subscribers retailer name subscriber-folder folder-name enterprise name info {
    phone phone;
    fax fax;
    po-box po-box;
    city city;
    street street;
    state state;
    postal-code postal-code;
}
```

To add administrative information about enterprise subscribers:

1. From configuration mode, enter the enterprise subscriber info configuration. For example:

```
user@host# edit subscribers retailer default subscriber-folder local enterprise
ABCInc info
```

2. (Optional) Configure a phone number for the subscriber.

```
[edit subscribers retailer default subscriber-folder local enterprise ABCInc info]
user@host# set phone phone
```

3. (Optional) Configure a fax number for the subscriber.

```
[edit subscribers retailer default subscriber-folder local enterprise ABCInc info]
user@host# set fax fax
```

4. (Optional) Configure a post office box for the subscriber.

```
[edit subscribers retailer default subscriber-folder local enterprise ABCInc info]
user@host# set po-box po-box
```

5. (Optional) Configure the city for the subscriber.

```
[edit subscribers retailer default subscriber-folder local enterprise ABCInc info]
user@host# set city city
```

6. (Optional) Configure the street address for the subscriber.

```
[edit subscribers retailer default subscriber-folder local enterprise ABCInc info]
user@host# set street street
```

7. (Optional) Configure a state for the subscriber.

```
[edit subscribers retailer default subscriber-folder local enterprise ABCInc info]
user@host# set state state
```

8. (Optional) Configure the postal code for the subscriber.

```
[edit subscribers retailer default subscriber-folder local enterprise ABCInc info]
user@host# set postal-code postal-code
```

Adding Sites

Use the following configuration statements to add a site:

```
subscribers retailer name subscriber-folder folder-name enterprise name site name {
  network [network...];
  display-name display-name;
  accounting-user-id accounting-user-id;
  description description;
}
```

To add a site:

1. From configuration mode, enter the site configuration. In this procedure, ABCInc is the name of the enterprise, and Montreal is the name of the site.

```
user@host# edit subscribers retailer default subscriber-folder local enterprise
ABCInc site Montreal
```

2. (Optional) Record networks used at the site. If you build a custom enterprise manager application, you can access this information through the enterprise portal APIs.

```
[edit subscribers retailer default subscriber-folder local enterprise ABCInc site
Montreal]
user@host# set network [network...]
```

3. (Optional) Configure the name that is displayed in enterprise management portals, if different from the site name.

```
[edit subscribers retailer default subscriber-folder local enterprise ABCInc site
Montreal]
user@host# set display-name display-name
```

4. (Optional) Configure the name that identifies the site in accounting records.

```
[edit subscribers retailer default subscriber-folder local enterprise ABCInc site
Montreal]
user@host# set accounting-user-id accounting-user-id
```

5. (Optional) Enter a description of the site.

```
[edit subscribers retailer default subscriber-folder local enterprise ABCInc site
Montreal]
user@host# set description description
```

6. (Optional) Verify your configuration.

```
[edit subscribers retailer default subscriber-folder local enterprise ABCInc
site Montreal]
user@host# show
display-name "Montreal Office of ABC, Inc.";
accounting-user-id abcInc;
description "This enterprise is sample data for use with JUNOS routers.";
```

7. Configure an access for the site. (See *Configuring Accesses* on page 292.)

Adding Devices as Subscribers

Configure a device subscriber for subscriber sessions that manage the forwarding interface on JUNOS routing platforms and the router pseudo-subscriber on JUNOS routers.

You can add devices as subscribers to subscriber folders, enterprises, and sites. Use the following configuration statements to add a device as a subscriber:

```
subscribers retailer name subscriber-folder folder-name device device-name {
  display-name display-name;
  maximum-login maximum-login;
  accounting-user-id accounting-user-id;
  substitution [substitution...];
}
```

```
subscribers retailer name subscriber-folder folder-name enterprise name device
device-name {
  display-name display-name;
  maximum-login maximum-login;
  accounting-user-id accounting-user-id;
  substitution [substitution...];
}
```

```
subscribers retailer name subscriber-folder folder-name enterprise name site name
device device-name {
  display-name display-name;
  maximum-login maximum-login;
  accounting-user-id accounting-user-id;
  substitution [substitution...];
}
```

To add a device as a subscriber:

1. From configuration mode, enter the device subscriber configuration. In this procedure, default@TMJunosA is the name of the device.

```
user@host# edit subscribers retailer SP-TM subscriber-folder devices device
default@TMJunosA
```

2. (Optional) Configure the name of the device as you want it to appear in SRC applications, such as portals.

```
[edit subscribers retailer SP-TM subscriber-folder devices device
default@TMJunosA]
user@host# set display-name display-name
```

3. (Optional) Configure the maximum number of concurrent logins for subscribers associated with this device.

```
[edit subscribers retailer SP-TM subscriber-folder devices device
default@TMJunosA]
user@host# set maximum-login maximum-login
```

4. (Optional) Configure the name that identifies the device in accounting records.

```
[edit subscribers retailer SP-TM subscriber-folder devices device
default@TMJunosA]
user@host# set accounting-user-id accounting-user-id
```

5. (Optional) Configure the actual values for parameters associated with this device.

```
[edit subscribers retailer SP-TM subscriber-folder devices device
default@TMJunosA]
user@host# set substitution [substitution...]
```

6. (Optional) Verify your configuration.

```
[edit subscribers retailer SP-TM subscriber-folder devices device
default@TMJunosA]
user@host# show
display-name "Profile for JUNOS router";
accounting-user-id JunosRouter
```

Adding Managers

Use the following configuration statements to configure a manager:

```
subscribers retailer name manager name {
  role [(administrator | subscription | substitution | activation | vpn)...];
  encrypted-password encrypted-password;
  plain-text-password;
  description description;
}
```

```
subscribers retailer name subscriber-folder folder-name manager name {
  role [(administrator | subscription | substitution | activation | vpn)...];
  encrypted-password encrypted-password;
  plain-text-password;
  description description;
}
```

```
subscribers retailer name subscriber-folder folder-name enterprise name manager
name {
```

```

        role [(administrator | subscription | substitution | activation | vpn)...];
        encrypted-password encrypted-password;
        plain-text-password;
        description description;
    }

subscribers retailer name subscriber-folder folder-name enterprise name site name
manager name {
    role [(administrator | subscription | substitution | activation | vpn)...];
    encrypted-password encrypted-password;
    plain-text-password;
    description description;
}

subscribers retailer name subscriber-folder folder-name enterprise name access name
manager name {
    role [(administrator | subscription | substitution | activation | vpn)...];
    encrypted-password encrypted-password;
    plain-text-password;
    description description;
}

subscribers retailer name subscriber-folder folder-name enterprise name site name
access name manager name {
    role [(administrator | subscription | substitution | activation | vpn)...];
    encrypted-password encrypted-password;
    plain-text-password;
    description description;
}

subscribers retailer name subscriber-folder folder-name device device-name manager
name {
    role [(administrator | subscription | substitution | activation | vpn)...];
    encrypted-password encrypted-password;
    plain-text-password;
    description description;
}

subscribers retailer name subscriber-folder folder-name enterprise name device
device-name manager name {
    role [(administrator | subscription | substitution | activation | vpn)...];
    encrypted-password encrypted-password;
    plain-text-password;
    description description;
}

subscribers retailer name subscriber-folder folder-name enterprise name site name
device device-name manager name {
    role [(administrator | subscription | substitution | activation | vpn)...];
    encrypted-password encrypted-password;
    plain-text-password;
    description description;
}

```


To add a manager:

1. From configuration mode, enter the manager configuration. In this procedure, we are creating a manager called abcmgr in the ABCInc enterprise.

```
user@host# edit subscribers retailer default subscriber-folder local enterprise  
ABCInc manager abcmgr
```

2. (Optional) Configure the privilege level (role) for the manager.

```
[edit subscribers retailer default subscriber-folder local enterprise ABCInc manager  
abcmgr]  
user@host# set role [(administrator | subscription | substitution | activation |  
vpn)...
```

3. (Optional) Configure an encrypted password for the manager:

```
[edit subscribers retailer default subscriber-folder local enterprise ABCInc manager  
abcmgr]  
user@host# set encrypted-password encrypted-password
```

4. (Optional) Configure a plain text password for the manager.

```
[edit subscribers retailer default subscriber-folder local enterprise ABCInc manager  
abcmgr]  
user@host# set plain-text-password plain-text-password
```

5. (Optional) Enter a description for the manager.

```
[edit subscribers retailer default subscriber-folder local enterprise ABCInc manager  
abcmgr]  
user@host# set description description
```

6. (Optional) Verify your configuration.

```
[edit subscribers retailer default subscriber-folder local enterprise ABCInc  
manager abcmgr]  
user@host# show  
role administrator;  
encrypted-password secret;
```

Configuring Subscriptions

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. See *SRC-PE Services and Policies Guide, Chapter 1, Managing Services with the SRC CLI*.

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. See *SRC-PE Services and Policies Guide, Chapter 4, Scheduling Services with the SRC CLI*.

```
subscribers retailer name subscription subscription-name {
    status (active | suspended | hidden);
    activation (manual | automatically-on-login);
    activation-order activation-order;
    substitution [substitution...];
}
```

```
subscribers retailer name subscriber-folder folder-name subscription subscription-name
{
    status (active | suspended | hidden);
    activation (manual | automatically-on-login);
    activation-order activation-order;
    substitution [substitution...];
}
```

```
subscribers retailer name subscriber-folder folder-name subscriber name subscription
subscription-name {
    status (active | suspended | hidden);
    activation (manual | automatically-on-login);
    activation-order activation-order;
    substitution [substitution...];
}
```

```
subscribers retailer name subscriber-folder folder-name enterprise name subscription
subscription-name {
    status (active | suspended | hidden);
    activation (manual | automatically-on-login);
    activation-order activation-order;
    substitution [substitution...];
}
```

```
subscribers retailer name subscriber-folder folder-name enterprise name site name
subscription subscription-name {
    status (active | suspended | hidden);
    activation (manual | automatically-on-login);
    activation-order activation-order;
    substitution [substitution...];
}
```

```

subscribers retailer name subscriber-folder folder-name enterprise name access name
subscription subscription-name {
    status (active | suspended | hidden);
    activation (manual | automatically-on-login);
    activation-order activation-order;
    substitution [substitution...];
}

```

```

subscribers retailer name subscriber-folder folder-name device device-name
subscription subscription-name {
    status (active | suspended | hidden);
    activation (manual | automatically-on-login);
    activation-order activation-order;
    substitution [substitution...];
}

```

```

subscribers retailer name subscriber-folder folder-name enterprise name device
device-name subscription subscription-name {
    status (active | suspended | hidden);
    activation (manual | automatically-on-login);
    activation-order activation-order;
    substitution [substitution...];
}

```

```

subscribers retailer name subscriber-folder folder-name enterprise name site name
device device-name subscription subscription-name {
    status (active | suspended | hidden);
    activation (manual | automatically-on-login);
    activation-order activation-order;
    substitution [substitution...];
}

```

To configure a subscription to a service:

1. From configuration mode, enter the subscription configuration. In this procedure, peter is the name of the subscriber and Video-Gold is the name of the subscription.

```

user@host# edit subscribers retailer default subscriber-folder local subscriber
peter subscription Video-Gold

```

2. (Optional) Configure the status of the service subscription.

```

[edit subscribers retailer default subscriber-folder local subscriber peter
subscription Video-Gold]
user@host# set status (active | suspended | hidden)

```

3. (Optional) Specify how the service is activated.

```

[edit subscribers retailer default subscriber-folder local subscriber peter
subscription Video-Gold]
user@host# set activation (manual | automatically-on-login)

```

4. (Optional) Specify when the SAE should activate this subscription relative to the subscriber's other subscriptions that are configured to activate on login.

```
[edit subscribers retailer default subscriber-folder local subscriber peter
subscription Video-Gold]
user@host# set activation-order activation-order
```

5. (Optional) Configure the actual values for parameters associated with this subscription.

```
[edit subscribers retailer default subscriber-folder local subscriber peter
subscription Video-Gold]
user@host# set substitution [substitution...]
```

6. (Optional) Verify your configuration.

```
[edit subscribers retailer default subscriber-folder local subscriber peter
subscription Video-Gold]
user@host# show
status active;
activation manual;
```

Allowing Multiple Subscriptions per Subscriber

To allow a subscriber to have a number of subscriptions to a service at the same time, 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

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 secondary services for Internet access.

```
subscribers retailer name subscriber-folder folder-name enterprise name access name
{
    routing-protocol routing-protocol;
    interface-alias interface-alias;
    interface-description interface-description;
    interface-name interface-name;
    unique-id unique-id;
    port-id port-id;
    device-name device-name;
    display-name display-name;
    accounting-user-id accounting-user-id;
    substitution [substitution...];
}
```

```
subscribers retailer name subscriber-folder folder-name enterprise name site name
access name {
    routing-protocol routing-protocol;
    interface-alias interface-alias;
    interface-description interface-description;
    interface-name interface-name;
    unique-id unique-id;
    port-id port-id;
    device-name device-name;
    display-name display-name;
    accounting-user-id accounting-user-id;
    substitution [substitution...];
}
```

To configure a subscription to an access service:

1. From configuration mode, enter the subscription configuration. In this procedure, Acme is the name of the enterprise and AcmeAccess is the name of the access.

```
user@host# edit subscribers retailer SP-TM subscriber-folder subscribers  
enterprise Acme access AcmeAccess
```

2. (Optional) Record routing protocols used at the enterprise or site. If you build a custom enterprise manager application, you can access this information through the enterprise portal APIs.

```
[edit subscribers retailer SP-TM subscriber-folder subscribers enterprise Acme  
access AcmeAccess]  
user@host# set routing-protocol routing-protocol
```

3. (Optional) Configure the description of a router interface.

```
[edit subscribers retailer SP-TM subscriber-folder subscribers enterprise Acme  
access AcmeAccess]  
user@host# set interface-alias interface-alias
```

4. (Optional) Configure the alternate name of the interface that SNMP uses.

```
[edit subscribers retailer SP-TM subscriber-folder subscribers enterprise Acme
access AcmeAccess]
user@host# set interface-description interface-description
```

5. (Optional) Configure the name of the interface using your router CLI syntax

```
[edit subscribers retailer SP-TM subscriber-folder subscribers enterprise Acme
access AcmeAccess]
user@host# set interface-name interface-name
```

6. (Optional) Configure the router's unique ID, which is the index of the router in the SNMP table for all interfaces.

```
[edit subscribers retailer SP-TM subscriber-folder subscribers enterprise Acme
access AcmeAccess]
user@host# set unique-id unique-id
```

7. (Optional) Configure the network access server (NAS) port ID reported by the JUNOS router through the Common Open Policy Service (COPS).

```
[edit subscribers retailer SP-TM subscriber-folder subscribers enterprise Acme
access AcmeAccess]
user@host# set port-id port-id
```

8. (Optional) Configure the name of the router to which this access connects.

```
[edit subscribers retailer SP-TM subscriber-folder subscribers enterprise Acme
access AcmeAccess]
user@host# set router-name router-name
```

9. (Optional) Configure the name that is displayed in enterprise management portals, if different from the service name.

```
[edit subscribers retailer SP-TM subscriber-folder subscribers enterprise Acme
access AcmeAccess]
user@host# set display-name display-name
```

10. (Optional) Configure the value that identifies the service in accounting records.

```
[edit subscribers retailer SP-TM subscriber-folder subscribers enterprise Acme
access AcmeAccess]
user@host# set accounting-user-id accounting-user-id
```

11. (Optional) Configure the actual values for parameters associated with this subscription.

```
[edit subscribers retailer SP-TM subscriber-folder subscribers enterprise Acme
access AcmeAccess]
user@host# set substitution [substitution...]
```

12. (Optional) Verify your configuration.

```
[edit subscribers retailer SP-TM subscriber-folder subscribers enterprise
Acme access AcmeAccess]
user@host# show
interface-alias cust123-456;
interface-name fastethernet6/0.1;
```


Part 2

**Managing Access Portals for Residential
Subscribers**

Chapter 15

Overview of the Residential Portal

This chapter provides an overview of the SRC residential portal. The chapter contains the following sections:

- How Subscribers Use a Residential Portal on page 299
- Overview of a Residential Portal on page 300
- Subscriptions to Services on page 300
- Service Schedules in a Residential Portal on page 301
- Equipment Registration for DHCP Login on page 301
- Overview of the Sample Residential Portal on page 301

How Subscribers Use a Residential Portal

A residential portal is a Web application designed for use by individual subscribers who use their own computer to connect to the network, or households composed of multiple subscribers who use one or more computers and share the same network connection. The portal can be the single access point for subscribers to log in to the Internet. In addition to Internet access, a residential portal lets users manage subscriptions to services that supplement their basic Internet access package.

Residential portals can be used in wire-line, wireless, and roaming wireless environments:

- Fixed access environment—Subscribers can connect to a wholesaler or retailer using PPP, static IP, or DHCP through media such as cable, DSL, or telephone wire-line connections.

For DHCP connections that do not use equipment registration, PPP connections, or static IP connections, subscribers establish connections to a specific provider. If they want to connect to a different provider, subscribers log out of the current connection, and then log in to another one.

- Local wireless environment—Subscribers registered with the local wireless operator can connect to the location, typically by using DHCP.
- Roaming wireless environment—Subscribers can log in at a variety of wireless locations owned by service providers that participate in a roaming network agreement. Typically the connections use DHCP.

In each of these scenarios, the subscriber's experience is similar:

1. The subscriber connects to and logs in to an access point.
2. Based on the login, the subscriber's user profile is retrieved, and services are started on the router.
3. The subscriber's Web browser is redirected to a home or start page for the residential portal.
4. After logging in to the portal, subscribers can manage the services available from the provider.

Overview of a Residential Portal

Typically a residential portal is composed of dynamic Web pages that reference classes and methods from the Java packages and the Common Object Request Broker (CORBA) remote application programming interface (API) to:

- Authenticate subscribers, and log subscribers in to and out of the portal.
- Specify which services are to be available to subscribers.
 - Specify whether scheduling is available to subscribers and, if so, which scheduling features are available.
 - Specify whether the services start automatically at portal login or whether these services are to be started manually by the subscriber.
- Show subscribers accounting statistics for services that are active.
- Allow the subscribers to register their client devices to automatically obtain an authenticated IP address when they log in to the portal.

To use the SRC software to handle unauthorized requests to Web services and Web content sites, you install and configure the captive portal system. See *Redirecting Traffic to a Captive Portal Web Page* on page 338.

Subscriptions to Services

A residential portal lets subscribers manage subscriptions to additional services that a service provider makes available to subscribers. These services could provide additional bandwidth, access to specified content providers, or other services configured in the SAE.

Using a residential portal simplifies how service providers deliver services and how subscribers gain access to these services. The service provider can make services available to subscribers without directly contacting them, and subscribers can start and stop available services without contacting the service provider. Service providers can also charge for any service that a subscriber uses, based on the type of service and how long the subscriber uses the service. Through a residential portal, the service provider can provide information to subscribers about the cost and use of these services.

Service Schedules in a Residential Portal

A residential portal can allow users to subscribe to a service at scheduled times. For example, if a subscriber regularly views video every morning, the subscriber can set up a schedule to turn on a video-on-demand gold service (that is available from the service provider) every weekday morning at 9 a.m., and turn it off on the same day at 10:30 a.m. This way the subscriber has access to additional bandwidth only for the interval needed and pays for this service accordingly.

Equipment Registration for DHCP Login

The residential portal provides support for equipment registration for DHCP connections. Registration lets a subscriber automatically obtain an authenticated IP address when logging in to the portal. The equipment can be a device other than a PC, such as an IP phone or a set-top box. If a subscriber uses equipment registration and enables persistent login, the subscriber's authentication remains valid until the subscriber logs out of the system.

Overview of the Sample Residential Portal

The sample residential portal is a demonstration portal that shows how to use some of the features available in the Common Object Request Broker Architecture (CORBA) remote application programming interface (API) to create a Web application. You can customize the sample residential portal for your environment, or create a new Web application using the SAE CORBA remote API.

Web Application Architecture

The sample residential portal uses the Jakarta Struts Web application framework. Although Struts provides an easy and extensible framework for building Web applications, it is not required for building portals that use the CORBA remote API.

Jakarta Struts supports the model-view-control design paradigm, which separates an application into three sets of components:

- Model—Contains the data and business logic.
- View—Contains the presentation to the subscriber.
- Control—Contains the interface procedures.

The strict separation of the three layers promotes reuse of the components and allows easy adaptation of the application to different requirements.

Model Components

The model provides an abstraction layer of the CORBA remote API and contains the business logic, which determines how the sample portal behaves. The sample residential portal includes several implementations of the model (which we call behaviors) to demonstrate some typical usage scenarios. See *Behaviors for the Sample Residential Portal* on page 302 for more information.

View Components

The view components of the Web application provide the HTML code sent to the subscriber's browser. The view is implemented by means of JavaServer Pages (JSP) and several tag libraries provided as part of Jakarta Struts.

The tiles tag library provides a template mechanism to build Web pages based on reusable partial pages. The general layout of all pages of the portal application is defined in a single JSP page.

Control Components

The control components provide the interactions between the subscriber and the mode through the Action and ActionForm classes.

Action classes implement the functionality for a single operation, such as “list the subscriptions of a particular service category,” or “activate a service.”

ActionForm classes encapsulate data provided by the subscriber on an input form. The Struts framework initializes these classes with data entered in an HTML form and passes them to the appropriate action. The ActionForms are then passed to a view component that uses the data to initialize the content of fields in an input form.

Behaviors for the Sample Residential Portal

The sample residential portal provides two user behaviors (scenarios) that integrate with the Merit RADIUS server:

- Equipment registration

Used by subscribers who use Dynamic Host Configuration Protocol (DHCP) connections to register their devices to receive an authenticated IP address.

- Internet Service Provider (ISP) service

Used by subscribers who use Point-to-Point Protocol (PPP), static IP, or unauthenticated DHCP connections to log in to the portal and receive an unauthenticated IP address.

- Cable

Used by subscribers who have assigned IP addresses in a PacketCable Multimedia (PCMM) environment.

Chapter 16

Installing and Configuring the Sample Residential Portal

This chapter provides an overview of the sample residential portal, explains how to install and configure it, and describes how to create a portal based on the sample. The chapter contains the following sections:

- Before You Install and Configure the Sample Residential Portal on page 303
- Overview of Configuration Files for the Sample Residential Portal on page 306
- Installing the Sample Residential Portal on page 312
- Removing Access to the Sample Residential Portal on page 314

Before You Install and Configure the Sample Residential Portal

Before you install and configure the sample residential portal:

- Decide which behavior model the portal will use:
 - Equipment registration behavior—The equipment registration example demonstrates an application that provides an association between a subscriber and the equipment being used to make the DHCP connection. This type of association is used in many cable environments.
 - ISP service behavior—The ISP service example demonstrates an application that provides a means for subscribers to directly log in to a subscriber session for their ISP. The ISP service behavior is well suited for any environment in which subscribers connect directly to their ISP.
 - Cable behavior—The cable behavior is provided for a PCMM environment in which an application creates a subscriber session.
- (Optional) Set up subscriber authentication through RADIUS at portal login.
- (Optional) Customize how the sample residential portal handles unrecognized IP subscribers.

Configuring Equipment Registration Behavior

To configure a Merit RADIUS server to demonstrate equipment registration:

1. Move to the *radius/etc* directory.

```
cd /opt/UMC/radius/etc
```

2. Copy *authfile.equipment* to *authfile*.

```
cp authfile.equipment authfile
```

With equipment registration, a subscriber registers equipment to the SAE only once. At registration, the system caches the media access control (MAC) address of the device; thereafter, the MAC address identifies the device to the SAE, and an authenticated IP address is returned to the device.

When the MAC address of the subscriber's equipment is associated with a user profile, the subscriber login can be configured as persistent. With a persistent login, the subscriber does not need to log in again as long as the registered MAC address remains the same. This process lets non-HTML-capable devices, such as IP phones and set-top boxes, to be registered to the network. If subscribers do not have a persistent login configured, the portal detects that the subscriber is not authenticated and directs the subscriber to a login page.

Configuring ISP Service Behavior

To configure a Merit RADIUS server to demonstrate the ISP service behavior:

1. Move to the *radius/etc* directory.

```
cd /opt/UMC/radius/etc
```

2. Copy the *authfile.isp* to *authfile*.

```
cp authfile.isp authfile
```

This connection can be to a wireless device or over physical connection media. In this scenario, subscribers can log in to their ISP from any device; there is no need to bind a particular subscriber to a particular PC or workstation (equipment registration).

The ISP service model applies to subscribers who log in to a specific provider. To switch between providers, subscribers can log out from one and then log in to another.

Configuring Cable Behavior

For a PCMM environment, you can create an application to create a subscriber session by either:

- Using the event API to integrate an IP address manager such as a DHCP server or a RADIUS server.
- Having the application provide the IP address, the associated interface name, and virtual router name for the subscriber making the request. Typically, the IP address is used to identify the associated virtual router.

If the application provides the subscriber IP address and associated information, you can configure the portal application to locate the SAE that manages the subscriber session by configuring one of the following:

- Network information collector (NIC)
 - NIC host that resolves a subscriber IP address to name of the virtual router managing the IP address and an SAE interoperable object reference (IOR)
 - NIC proxy for the application to communicate with the NIC host
- A local feature locator in the properties for the residential portal. See *WEB-INF/portalBehavior.properties* on page 307.

Authenticating Subscribers Through RADIUS

If you use RADIUS to manage subscriber data, you can use RADIUS to authenticate subscribers when they log in to a residential portal. You configure RADIUS authentication plug-ins to provide RADIUS authentication or authorization. In the configuration for the plug-in, you specify how the SAE handles RADIUS attributes received from the RADIUS server.

Because the SAE rather than a JUNOS router receives the authentication response, you can specify that the response include attributes other than serviceBundle and class, and you can specify more than value for the RADIUS class attribute.

To authenticate subscribers through RADIUS at portal login:

1. Create a RADIUS authorization plug-in to authenticate subscriber sessions.
2. Configure the RADIUS authorization plug-in to specify:
 - The RADIUS attributes to be set in an authorization response
 - The action to be taken in response to the attribute values received

For example, you could create a RADIUS authorization plug-in to:

- Authenticate a PPP subscriber session on a JUNOSe router
- Specify the `setLoadServices` value for the `serviceBundle` attribute

By default, the flexible RADIUS authentication plug-in defines this attribute as:

```
RadiusPacket.stdAuth.userresp.vendor-specific.Juniper.Service-Bundle =
setLoadServices
```

For more information about RADIUS authentication plug-ins, see *Chapter 8, Overview of Plug-Ins Included with the SAE*.

Customizing How the Sample Residential Portal Handles Unrecognized IP Subscribers

By default, the sample residential portal sends unrecognized IP subscribers to a login page rather than to an error page.

To customize how unrecognized IP subscribers are handled:

- Edit the *struts-config.xml* file.

Overview of Configuration Files for the Sample Residential Portal

The *ssportal.war* file contains the following configuration files in the *WEB-INF* directory:

- *portalBehavior.properties*—Specifies properties to configure the `portalBehavior` servlet that determines the behavior of the sample residential portal.

Modify this file to run the sample residential portal. See *WEB-INF/portalBehavior.properties* on page 307.

- *web.xml*—Specifies the deployment descriptor for the sample residential portal. It describes the servlets, other components, and initialization parameters.



NOTE: We recommend that you do not change the deployment descriptor.

- *jboss-web.xml*—Contains one configuration property that defines the Web context of the sample residential portal as the root context.

Modify this file to run the sample residential portal in a context other than root. The *WEB-INF/jboss-web.xml* file is proprietary to the JBoss application server.

- *struts-config.xml*—Contains the configuration for the struts action servlet. See *WEB-INF/struts-config.xml* on page 309.
- *tiles-defs.xml*—Contains the definitions of the tiles template system. The definitions describe the general layout of every Web page used in the sample residential portal. See *WEB-INF/tiles-defs.xml* on page 311.

WEB-INF/portalBehavior.properties

Set the following properties to configure the portalBehavior servlet to determine the behavior of the sample residential portal, and to connect to the LDAP server.

In addition, configure the other properties listed in the file for the network information collector (NIC) proxy configuration. For information about the values to configure for NIC properties, see *SRC-PE Network Guide, Chapter 13, Configuring Applications to Communicate with an SAE*.

Factory.behavior

- Model for handling subscribers who connect using DHCP.
- Value
 - net.juniper.smgmt.ssp.model.EquipmentRegistrationBehavior
 - net.juniper.smgmt.ssp.model.ISPServiceBehavior
 - net.juniper.smgmt.ssp.model.CableBehavior
- Guidelines—For information about the behaviors, see *Installing the Sample Residential Portal* on page 312.

Factory.locator

- Method that the portal uses to locate the SAE that is managing the subscriber who tries to access the application.
- Value
 - net.juniper.smgmt.ssp.LocalFeatureLocator—Uses the locally configured object reference
 If you specify net.juniper.smgmt.ssp.LocalFeatureLocator, configure a value for LocalFeatureLocator.objectRef.
 - net.juniper.smgmt.ssp.DistributedFeatureLocator—Uses NIC configuration

LocalFeatureLocator.objectRef

- CORBA object reference for the single SAE whose address is resolved by the locator. Specify the object reference if you set net.juniper.smgmt.ssp.LocalFeatureLocator for Factory.locator.
- Value—A reference to the CORBA object in one of the following formats:
 - The absolute path to the IOR file in the form file:// <absolutePath>
 - The corbaloc URL in the format:
 corbaloc:: <host> : <port> /SAE
 - <host> — IP address or host on which the SAE is installed.
 - <port> — TCP/IP port number for the SAE. The default is 8801.

- COS naming service in the format:
corbaname:: <host> [: <port>][/NameService]# <key>

where <key> is provided by the publisher of the IOR to the COSnaming service.
- The actual IOR in the form IOR: <objectReference>
- Guidelines—Configure this property to use the portal as a demonstration application in a small environment that does not use NIC.
By default, the SAE does not publish its IOR to a COSnaming service.
- Example
 - Absolute path—file:///opt/UMC/sae/var/run/sae.ior
 - corbaloc URL—corbaloc::10.10.6.171:8801/SAE
 - Actual IOR—
IOR:0000000000000002438444C3A736D67742E6A756E697...

LocalFeatureLocator.vrName

- Virtual router to use in a Packet Cable Multimedia (PCMM) environment as the virtual router on the local machine.
- Value—Name of virtual router
- Guidelines—Configure this property only if you configured a value for LocalFeatureLocator.objectRef.
- Default—default@simJunos

DistributedFeatureLocator.locName

- Namespace for the NIC proxy configuration.
- Value— <namespace>
- Guidelines—For the cable behavior to create an assigned IP subscriber, the NIC must resolve an IP address to both the SAE IOR and the name of the virtual router that manages the IP address.
- Default—/ which indicates the root namespace
- Example—DistributedFeatureLocator.locName = /nicProxy indicates that the NIC proxy configuration is in /nicProxy.

Config.java.naming.provider.url

- Location of the LDAP server.
- Value—ldap:// <IP address> : <port number>
- Example—ldap://127.0.0.1:389 (default location if you are using the default OpenLDAP installation from the SRC installation).

Config.net.juniper.smgmt.des.backup_provider_urls

- Location of a backup LDAP server.
- Value—ldap:// < IP address > : < port number >

WEB-INF/struts-config.xml

The *WEB-INF/struts-config.xml* file contains the following settings. The file has multiple sections.

data-sources

- Not used by the sample residential portal.

form-beans

- Holds data entered in an HTML form and makes it available to the associated action.

global-exceptions

- Specifies that the sample residential portal declare one global exception handler, which is invoked for any exception raised during action processing.

global-forwards

- Global forwards for handling error situations. The sample residential portal declares a number of global forwards.
- Value
 - unknownUser—Used when an action is processed for a subscriber who is not known by the system. The possible pages are either *.error.unknownUser.page*, which displays an error message, or *.login.page*, which asks the user to log in.
 - nonUniqueUser—Used when a request cannot be mapped to a single subscriber session.
The sample residential portal uses the IP address of the subscriber, preventing this error.
 - unknownService—Used when a request refers to a service that is not loaded by the SAE. This can happen if services are modified while subscribers are connected to the portal.
 - unknownSubscription—Used when a request refers to a service to which the current subscriber is not subscribed.
 - serviceAuthError—Used if authorization for a service is denied; for example, because mutex group restrictions are violated or a plug-in has denied authorization.
 - loginError—Used if login was unsuccessful.
 - saeError—Used for SAE internal errors.
 - error—Used for any other problem.

action-mappings

- Actions that each correspond to an interaction of the subscriber with the portal page. The sample residential portal declares a number of actions.
- Value
 - `/index`—Displays the main page of the portal; collects information about the subscriber requesting the page and forwards it to the `.index.page`.
 - `/services`—Gets information about the subscribed services and forwards to the `.services.page`.
 - `/activate`—Checks whether authentication is required and forwards the request either to the `.service.auth.page` or back to the `.services.page`.
Called when the subscriber wants to activate a service.
 - `/deactivate`—Forwards the request back to the `.services.page`.
Called when the subscriber wants to deactivate an active service.
 - `/schedules`—Gets information about the service schedule. Allows the subscriber to view and change service schedules. The action forwards the request to the `.schedules.page`.
 - `/scheduleOperation`—Forwards the request back to the `.schedules.page`.
Called when the subscriber wants to change the service schedule.
 - `/usage`—Collects statistics for currently active services and forwards them to the `.usage.page`.
 - `/account`—Allows modification of the `activationTrigger` property of currently subscribed services. After a change of the `activationTrigger` property has been processed, the action forwards subscribers to the `.account.page`.
 - `/subscribe`—Allows the subscriber to subscribe to and unsubscribe from services. After processing the subscription change, the action forwards subscribers to the `.subscribe.page`.
 - `/register`—Allows subscribers to register MAC addresses for authenticated DHCP addresses. The action checks whether the subscriber has provided a username and password and forwards the request to the `.register.auth.page` to enter the username and password or to the `.register.page` displaying the currently registered equipment.
 - `/unregister`—Allows subscribers to remove MAC addresses that are registered for DHCP addresses. The action checks whether the subscriber provided a username and password and forwards the request to the `.unregister.auth.page` to enter the username and password or to the `.unregister.page` displaying the currently registered equipment.
 - `/login`—Allows the subscriber to log in to the system. If the login causes a switch of the DHCP IP address, the request is forwarded to the `.wait.page`. If the DHCP IP address remains the same after the login, the request is forwarded to the `.index.page`.
 - `/logout`—Allows the subscriber to log out of the system. If the logout causes a switch of the DHCP IP address, the request is forwarded to the `.wait.page`. If the DHCP IP address remains the same after the login, the request is forwarded to the `.index.page`.

- `/wait`—Checks whether the IP address of the current subscriber is authenticated or unauthenticated. If the address is of the wrong type, the request is forwarded to the `.wait.page`, which will renew itself automatically. If the address is of the expected type, the request is forwarded to `.index.page`.
- `/accessDenied`—Processes a captive portal request. The request is forwarded only to the `.error.accessDenied.page`.

controller

- Ensures generation of the correct headers for disabling caching of the generated pages.
- Value—`nocache`

message-resources

- Base name of the resource bundle. The resource bundle contains message strings in different languages.
- Value
 - `WEB-INF/classes/net/juniper/smgmt/ssp/ApplicationResources.properties`
The location of the resource file containing messages in English that is shipped with the sample residential portal.
 - `WEB-INF/classes/net/juniper/smgmt/ssp/ApplicationResources_xx.properties`
where `xx` is the two-letter ISO language code, optionally followed by an underline and the two-letter country code; for example, `en_CA` for English/Canada or `zh_TW` for Chinese/Taiwan.

To create a sample residential portal that supports other languages, translate the messages and store the translated file in the above location.

plug-in

- Processes templates.

WEB-INF/tiles-defs.xml

The `WEB-INF/tiles-defs.xml` file contains the following settings.

site.layout

- Main definition that specifies the general structure of all pages. The layout is based on a common template file, `/layouts/common.jsp`. The definition contains values for template variables shared by all page definitions.
- Value
 - `title`—Common title of all pages.
 - `header`—Page fragment displaying the header section of the pages.
 - `menu`—Page fragment displaying the menu bar.
 - `footer`—Page fragment displaying the footer section of the pages.

- body—Page fragment displaying the content of the pages. The default setting is empty and should be overwritten by individual page definitions.
- color—Color scheme used the by pages. A color scheme consists of a style sheet (*style_sheets/color.css*) and a set of images (stored in *images/color*). The predefined color schemes are blue and green.
- menuTag—Action name of the current page. The menu bar code uses this tag to highlight the action associated with the current page.

site.layout.nomenu

- Provides an extension of the main layout that defines a version of the page without a menu bar.

.*.page

- Provides the definition of portal pages. These pages are used for forwards in the action-mappings section of the *struts-config.xml* file. The page definitions extend one of the common layouts and define the value of the body variable as appropriate.

Installing the Sample Residential Portal

The sample residential portal is a Web application. The application is packaged as a standard Web application archive (WAR file) in the *webapp* subdirectory in the SRC software distribution.

Before you install the sample residential portal:

- Install a Web application server on the machine on which you want to install the sample residential portal.

We provide the JBoss Web application server in the SRC software distribution. For information about installing this software, see *SRC-PE Getting Started Guide, Chapter 33, Installing Web Applications*.

- Install the sample data from the SRC software distribution (see *SRC-PE Getting Started Guide, Chapter 29, Defining an Initial Configuration on a Solaris Platform*).
- Set up the RADIUS *authfile* for the user scenario you want to demonstrate. See *Installing the Sample Residential Portal* on page 312.

Tasks to install the sample residential portal are:

1. Preparing the Application for Customization on page 313
2. Configuring the Sample Residential Portal on page 313
3. Deploying the Updated WAR File on page 314



NOTE: The sample residential portal can be installed by root or authorized nonroot users.

Preparing the Application for Customization

When you customize the sample residential portal, copy the WAR file to a temporary folder and work in that folder. To do so:

1. Login as `root` or another authorized user.
2. Create a temporary folder in which you will work on the WAR file.

`mkdir ssportal`

3. Access the temporary folder.

`cd ssportal`

4. Copy the WAR file to the temporary folder.

`cp /cdrom/cdrom0/webapp/ssportal.war.`

Configuring the Sample Residential Portal

To configure the sample residential portal:

1. Access the temporary folder to which you copied the WAR file.

`cd ssportal`

2. Extract the files from the WAR file.

`unzip -qo ssportal.war`

3. With a text editor, edit the *portalBehavior.properties* file and other files in the *WEB-INF* directory as needed. See *Overview of Configuration Files for the Sample Residential Portal* on page 306.

Use *WEB-INF/portalBehavior.properties* on page 307 as a guideline for editing the *portalBehavior.properties* file to use properties specific to your environment.

4. Replace the *portalBehavior.properties* and any other updated files in the WAR file.

`zip -u ssportal.war`

Deploying the Updated WAR File

To deploy the updated WAR file:

- Copy the WAR file to the deployment directory for your Web server.

If you are using JBoss, copy the file to `/opt/UMC/jboss/server/default/deploy` directory. JBoss automatically starts the Web application when a new WAR file is copied into the deployment directory.

By default the sample residential portal is deployed into the root context ("/"). You can access the portal through `http://server:8080`. If you want to deploy the sample residential portal into something other than the root context, modify the `WEB-INF/jboss-web.xml` configuration file.

Testing a Portal Application

Simulated router drivers allow you to create subscriber sessions without connecting to a router. You can use a simulated router drive when you want to test your portal application. See *SRC-PE Monitoring and Troubleshooting Guide, Chapter 5, Configuring a Simulated Router Driver for Testing with the SRC CLI* or *SRC-PE Monitoring and Troubleshooting Guide, Chapter 6, Configuring a Simulated Router Driver for Testing with SDX Configuration Editor*.

Removing Access to the Sample Residential Portal

To remove access to the sample residential portal:

- Remove the `ssportal.war` file from the deployment directory.

Chapter 17

How Subscribers Use the Sample Residential Portal

This chapter describes how to log in to the sample residential portal and how to use it. The chapter contains the following sections:

- Overview of the Sample Residential Portal on page 315
- Before You Use the Sample Residential Portal on page 315
- Logging In to the Sample Residential Portal Using a Simulated User Profile on page 316
- Managing Services from the Sample Residential Portal on page 318
- Logging Out of the Sample Residential Portal on page 332
- Using the Sample Residential Portal from PDAs on page 333

Overview of the Sample Residential Portal

The sample residential portal allows subscribers to manage subscriptions to services that supplement their basic Internet services. The sample residential portal shows how subscribers could log in to a portal, start and stop supplementary services, and manage subscriptions for their special services. The services available in the sample residential portal are configured in the sample data.

If you are a portal developer and want to view the Javadoc documentation for the sample portal, you can access the documentation from the Welcome page of the sample residential portal after you log in to the portal.

Before You Use the Sample Residential Portal

Before you can log in to the sample residential portal, the portal must be configured for use in your environment. For information about installing and configuring the sample residential portal, see *Chapter 16, Installing and Configuring the Sample Residential Portal*.

Logging In to the Sample Residential Portal Using a Simulated User Profile

Logging in to the sample residential portal requires that you enter the username and password for a subscriber. You can log in to the sample residential portal by using a simulated user profile in a test environment, or you can log in as a subscriber in an environment that includes a JUNOSe router or a JUNOS routing platform. If you add a subscriber to the directory, do so under a retailer below the folder *o = Users*, *o = umc*.

If you want to use a simulated user profile to log in to the sample residential portal, you can use one of the subscribers in the sample data, or a subscriber that you create. Before you can log in to the sample residential portal, you log the subscriber in to a simulated user session from the SRC CLI. For information about using a simulated user profile, see *SRC-PE Monitoring and Troubleshooting Guide, Chapter 7, Using Simulated Subscribers for Testing with the SRC CLI*.

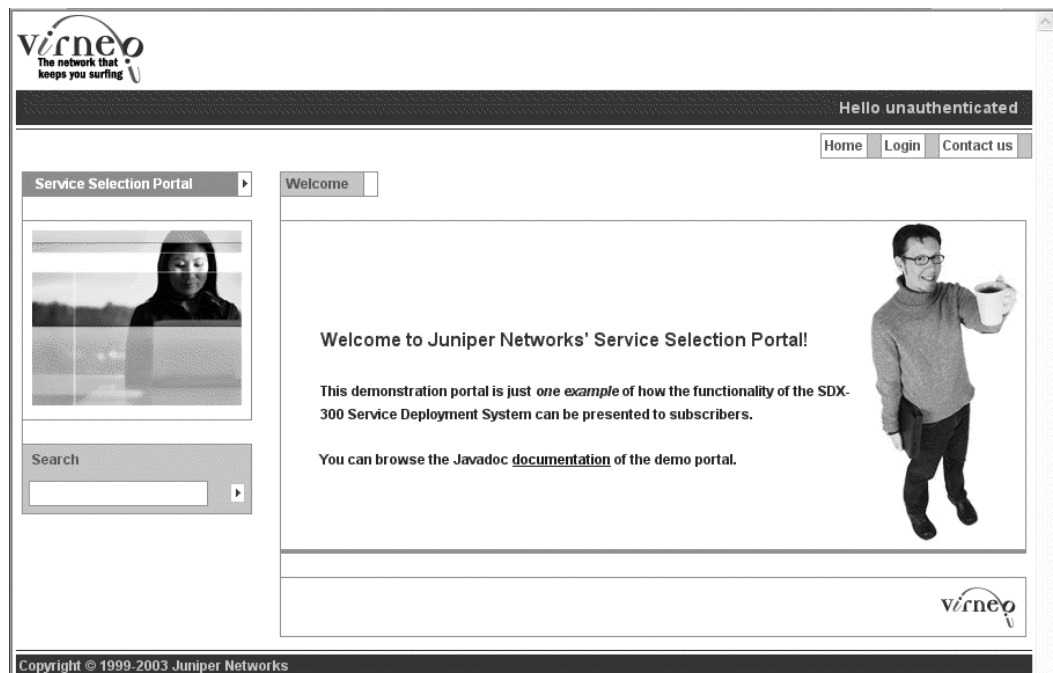
Logging In to the Sample Residential Portal

To log in to the sample residential portal:

1. Connect to the sample residential portal from a Web browser.

The default URL for the sample residential portal is `http:// < IP address of Web server > :8080`.

The Welcome page appears.



2. Click **Login**.

The Login page appears.



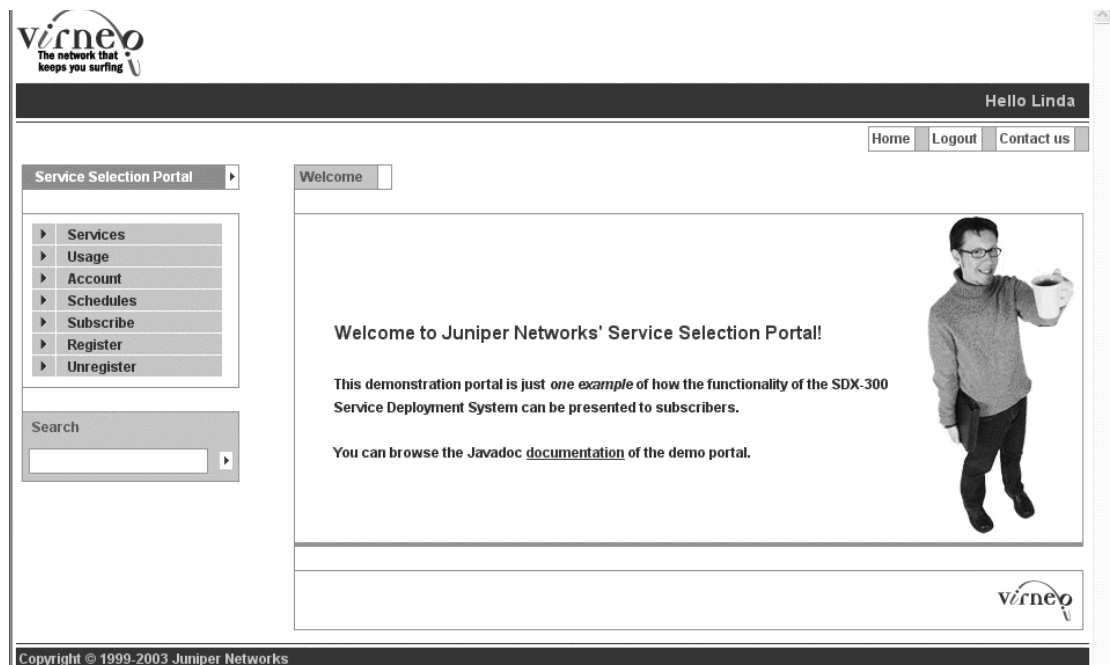
The screenshot shows the Virneo login page. At the top left is the Virneo logo with the tagline "The network that keeps you surfing". A dark banner at the top right says "Hello unauthenticated". Below this are links for "Home", "Login", and "Contact us". The main content area is divided into two columns. The left column has a "Service Selection Portal" dropdown menu, a placeholder image of a woman, and a "Search" input field. The right column features a "Login" link, a form titled "Please enter your SSP Username and Password." with "Username:" and "Password:" labels and corresponding input fields, and a "Login" button. To the right of the form are links for "Not registered yet? Sign up now!" and "Forgot your password? Click here for help." Below the form is a small image of a man at a laptop. The footer contains the Virneo logo and the copyright notice "Copyright © 1999-2003 Juniper Networks".



NOTE: The Sign up, Click here, and Search links are not operational in the sample portal.

3. Enter your username and password; then click **Login**.

Your personalized Welcome page appears.



Managing Services from the Sample Residential Portal

After you log in to the portal, you can use the portal in the same way that a subscriber would use it. This section describes how to use the sample residential portal from a subscriber's viewpoint.

Use the navigation pane on the left side of the page to move from one page to another.

You can set up, activate, and schedule additional services. These services supplement your basic Internet services, and may carry additional fees.

If you use DHCP to receive an IP address, you can also manage equipment registration.

Table 27 describes the tasks that you can perform in the sample residential portal and shows which item to select in the navigation pane to display the page that lets you perform the task.

Table 27: Navigation Pane for the Sample Residential Portal

To Do This	Select This Item in the Navigation Pane
Start and stop supplementary services. View the price of a supplementary service.	Services
View service statistics for traffic sent and received during your login session.	Usage
View the list of services made available to you by the Internet service provider. The list shows whether a service is automatically activated at login or whether you need to activate the service from the portal. Change the type of service activation from this page.	Account
Specify a schedule that indicates when a specified service should be activated and/or deactivated.	Schedules
View and change the services to which you subscribe.	Subscribe
If you are a DHCP user, register your DHCP equipment to always obtain an authenticated IP address.	Register
If you have equipment registration enabled, disable it.	Unregister

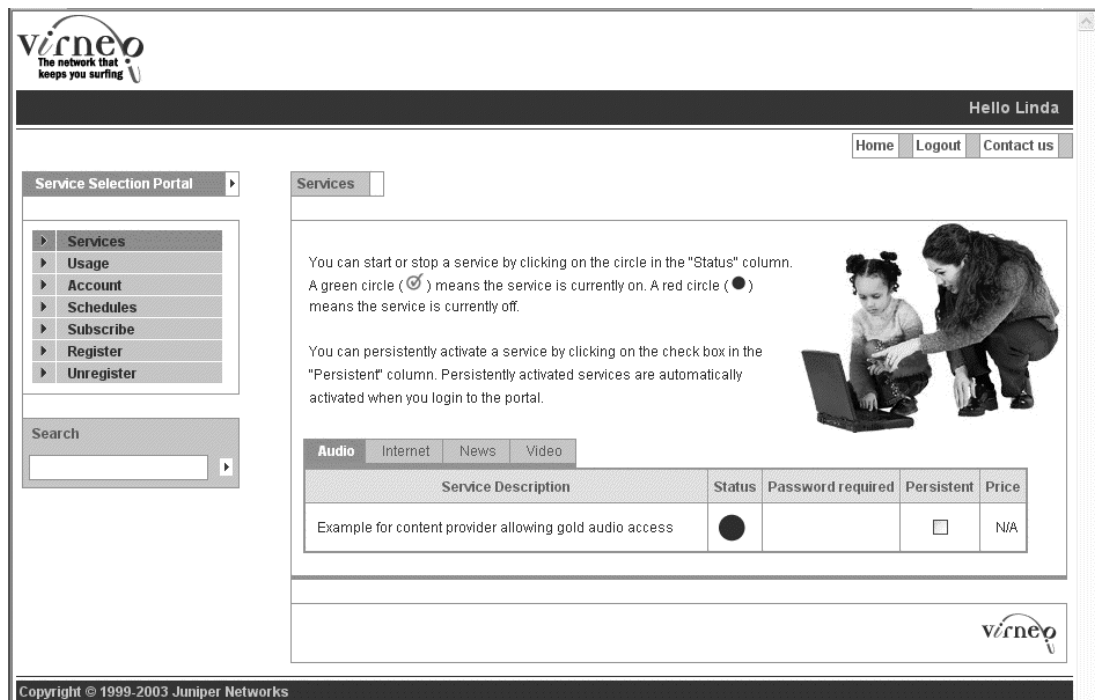
Starting and Stopping Services

You can start and stop services to which you have a subscription. You can view which supplementary services the Internet service provider makes available to you in the Subscribe page, and subscribe to services there. After you subscribe to a service, the Services page lists the service. See *Subscribing to Services* on page 327.

To start or stop services:

1. In the navigation page, click **Services**.

The Services page appears.



2. Click the tab that specifies the type of service to start or stop.
3. In the page that lists the service:
 - To start a service, click the red circle under Status.
 - To stop a service, click the green check mark under Status.
4. If a password is required to start a service, enter your password at the prompt.
5. To have a service become active when you log in to the portal again, click **Persistent** before you start the service.

If you specify a schedule for a service, that service is active as defined in the schedule and may remain active after you log out of the portal. See *Setting Up Service Schedules* on page 323.

Getting Usage Information

From the portal, you can view information about how long a service has been active and can view traffic statistics for your current login session. Internet service providers could use this type of information to generate accounting data for specified services, such as a video gold service that would support video on demand.

To get usage information for your current login session:

1. In the navigation pane, click **Usage**.

The Usage page appears.

virneo
The network that keeps you surfing

Hello Linda

Home Logout Contact us

Service Selection Portal Usage

- Services
- Usage
- Account
- Schedules
- Subscribe
- Register
- Unregister

Search

Accounting data for each of your subscribed services is listed below.

This information describes your *most recent* use of each service during your *current* login session. The status column shows a green circle for an active service or a red circle for a non active service. The time column shows the time at which the data was collected from the network.

Audio Internet News Video

Service description	Status	Been active for	Time	Bytes out	Bytes in	Packets out	Packets in
Example for content provider allowing gold audio access	●	0 sec	Never				

virneo

Copyright © 1999-2003 Juniper Networks

2. Click the tab that specifies the type of service for which you want usage information for your current login session.

Setting Up the Type of Service Activation

You can have a service activated every time you log in to the portal, or you can activate it from the Services page when needed.

To view information about service activation and change how a service is activated:

1. In the navigation pane, click **Account**.

The Account page appears.

The screenshot shows the Virneo web portal interface. At the top left is the Virneo logo with the tagline "The network that keeps you surfing". On the right, it says "Hello Linda" and has links for "Home", "Logout", and "Contact us". A left-hand navigation pane titled "Service Selection Portal" contains links for "Services", "Usage", "Account" (which is highlighted), "Schedules", "Subscribe", "Register", and "Unregister". Below this is a search box. The main content area is titled "Account" and contains the text "Your subscribed services are listed below." followed by instructions: "To have a service automatically activated every time you log in, select 'automatic' for that service and press the 'Update' button." There is an illustration of a woman sitting in a chair using a laptop. Below the text is a table with tabs for "Audio", "Internet", "News", and "Video". The "Audio" tab is selected. The table has columns for "Service description", "Manual", and "Automatic". One row is visible with the description "Example for content provider allowing gold audio access". The "Manual" column has a radio button that is selected, and the "Automatic" column has an unselected radio button. Below the table are "Update" and "Cancel" buttons. The Virneo logo is in the bottom right corner, and the footer text "Copyright © 1999-2003 Juniper Networks" is at the very bottom.

Service description	Manual	Automatic
Example for content provider allowing gold audio access	<input checked="" type="radio"/>	<input type="radio"/>

2. Click the tab that specifies the type of service that you want to view or for which you want to change the type of activation:
 - To start a specified service when you connect to your Internet service provider, click **Automatic**.
 - To start a specified service only when you want it to become active, click **Manual**.
3. Click **Update**.

Setting Up Service Schedules

You can set up schedules to activate specified services and deactivate specified services at fixed times. The schedules operate independently of whether you are logged in to the portal. For example, you could set up a schedule that activates a video gold service at 12 noon on every Saturday and deactivates the service at 12 midnight on the same day.

To create a service schedule:

1. In the navigation pane, click **Schedules**.

The Schedules page appears.

virneo
The network that keeps you surfing

Hello Linda

Home Logout Contact us

Service Selection Portal

- Services
- Usage
- Account
- Schedules**
- Subscribe
- Register
- Unregister

Search

Schedules

Your current schedule is shown below.

You can add new events to your schedule, or delete scheduled events. You can also view the detail information about each of your scheduled events.

ThisMonth EventList

Schedule Name	Action
You have no schedules events for the given period.	

Main

Name:

Schedule Cancel

Schedule

	Year	Month	Day	DOW		TZ
from	2004	9	23	*		*
	Hour: *	Minute: 0,30				
to	Year: *	Month: *	Day: *	DOW: *		TZ: *
	Hour: *	Minute: *				

Actions

Order	Operation	Service
0	Please Select	Please Select

2. In the Name field, specify a name for the schedule.
3. Under Schedule, specify the time to start the service under *from*, and the time to stop the service under *to*.

For information about the type of information to enter in these fields, see *Specifying Values for Times* on page 324 and *Setting Times* on page 325.

4. Under Actions, specify the operation to be performed for the service that you select under **Service**.

For information about the type of information to enter in these fields, see *Setting Actions* on page 326.

5. After you finish making all schedule entries, click **Schedule**.

The schedule appears under EventList, and the schedule of actions for this month appears under ThisMonth.

Specifying Values for Times

When you create or change schedules, you can use the values in the following list to make entries in the from and to sections in the Schedules page. See *Setting Times* on page 325 for a description of each entry field under the Schedule area of the page.

- Asterisks (*) are interpreted differently depending on the field in which you enter one as a value. The following list describes how the SRC software interprets an * as a value for the various fields:
 - Minutes and hours—0 (zero)
 - Time zones—Local SAE time zone
 - All other fields—First through last
 - For fields in the To section of the schedule area, * for the end time is equivalent to “deny service activation after this start date.”
 - For dates in the From section of the schedule area, * is equivalent to “deny service activation anytime before this end date.”
- Range of numbers or letters separated by a hyphen—The range is inclusive; for example, 1-5 for the hour specifies hours 1, 2, 3, 4, and 5. A range of mon-wed specifies Monday, Tuesday, and Wednesday.
- List of numbers, letters, or ranges separated by commas—For example, 1,2,5,9 or 0-4,8-12 or mon-wed,fri-sat.
- Skip values in ranges.
 - Skip a number’s value through the range, follow a range with / < number > . For example, 0-23/2 used in the hours field specifies that the event occurs every other hour.
 - Skip values with *. If you want to specify every two hours, use */2.



NOTE: If you set both a day of the month and a day of the week, the day of the month is used.

Setting Times

Use the following field definitions when you make entries in the from and to sections in the Schedules page. For information about general guidelines that apply to these entry fields, see *Specifying Values for Times* on page 324.

Year

- Year in which to schedule an action.
- Value—Four integers that indicate the year
- Default— *

Month

- Month of the year in which to schedule an action.
- Value
 - 1–12
 - First three letters of the name of the month
- Default— *
- Example—For January, specify one of the following:
 - jan
 - 1

Day

- Day of the month in which to schedule an action.
- Value—1–31
- Default— *

Hour

- Hour of the day in the indicated month in which to schedule an action.
- Value—0–23
- Default— *

Minute

- Number of minutes past the indicated hour in which to schedule an action.
- Value—0–59
- Default— *

DOW

- Day of the week in which to schedule an action.
- Value
 - 0–6, with 0 representing Sunday, and each subsequent number representing the next day of the week.
 - First three letters of the name of the day
- Default—*
- Example—For Saturday and Sunday, specify one of the following:
 - sat, sun
 - 6, 0

TZ

- Time zone to use in the schedule.
- Value
 - * —Local time zone of the SAE.
 - An offset to Greenwich Mean Time (GMT) in the format:
 GMT (+ | -) (hh:mm | hh mm | hh)

 hh— < hour >

 mm— < minute >
- Default—Time zone specified by the Internet service provider
- Example
 - Canada/Eastern or America/New York
 - GMT + 5 sets the time zone to 5 hours behind GMT.

Setting Actions

In the Actions area, specify the type of action to be taken for a specified service.

Operation

- Type of action to be taken at the indicated time.
- Value—Menu of actions to be taken
 - deactivate—Deactivates the specified service at the indicated time.
 - activate—Activates the specified service at the indicated time.
 - deny—Does not allow activation of the specified service at the indicated time.
 - deny and deactivate—Deactivates the service if it is currently active and does not allow activation of the indicated service at the specified time.
- Guidelines—For deactivate and activate, specify times only in the from fields; any entries in the to fields are ignored.

Service

- Service for the schedule.
- Value—Menu of services to which you have a subscription

Subscribing to Services

After you subscribe to a service, you can activate the service to use it. Your Internet service provider decides which services are available to you for subscription. For information about activating a service, see *Starting and Stopping Services* on page 319.

To manage subscriptions to services:

1. In the navigation pane, click **Subscribe**.

The Subscribe page appears.

virneo
The network that keeps you surfing

Hello Linda

Home Logout Contact us

Service Selection Portal

- ▶ Services
- ▶ Usage
- ▶ Account
- ▶ Schedules
- ▶ **Subscribe**
- ▶ Register
- ▶ Unregister

Search

Subscribe

All available services are listed below.

It may take a minute for your new subscriptions to take effect.

Audio **Video** Internet News

Service Name	Service description	Subscribed	Unsubscribed
Video-Bronze	Example for content provider allowing bronze video access	<input type="radio"/>	<input checked="" type="radio"/>
Video-Gold	Example for content provider allowing high speed access	<input checked="" type="radio"/>	<input type="radio"/>
Video-Silver	Example for content provider allowing silver video access	<input type="radio"/>	<input checked="" type="radio"/>

OK Cancel

virneo

Copyright © 1999-2003 Juniper Networks

2. Click the tab that specifies the type of service to which you want to subscribe or unsubscribe.
 - To subscribe to a specified service, click **Subscribed**.
 - To stop a subscription to a specified service, click **Unsubscribed**.
3. After you finish making all schedule entries, click **OK**.

Registering Equipment for DHCP Login

If your Internet service provider assigns an IP address by using DHCP, you can register your equipment to automatically obtain an authenticated IP address when you log in to the portal. Your equipment can be a device other than a PC, such as an IP phone or a set-top box.

To register your equipment:

1. In the navigation pane, click **Register**.

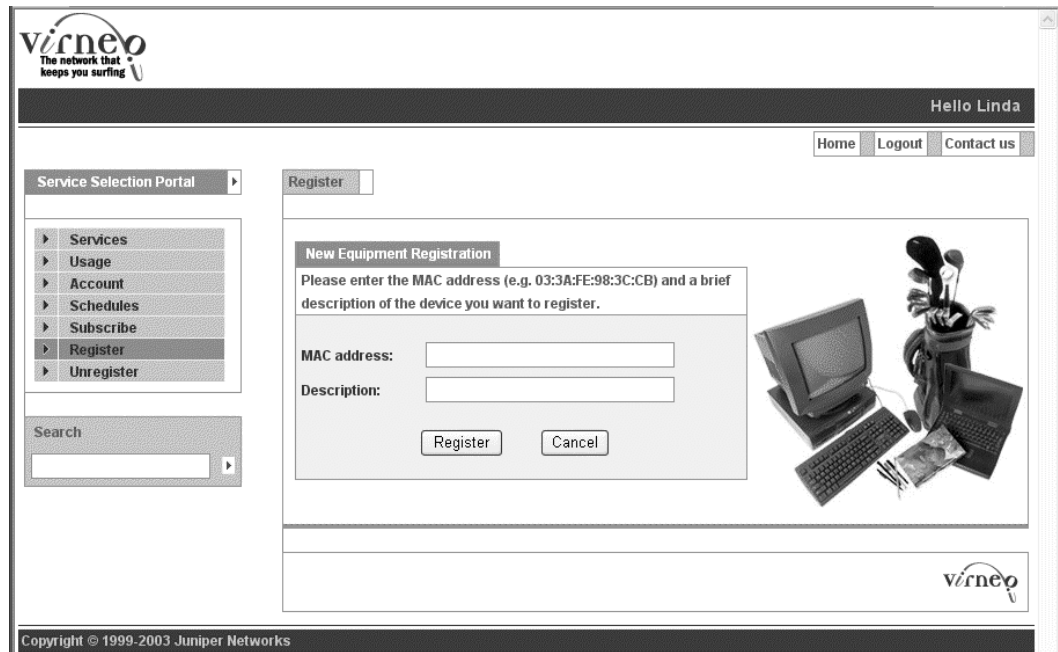
The Register page appears.



The screenshot shows the Vireo web portal interface. At the top left is the Vireo logo with the tagline "The network that keeps you surfing". At the top right, it says "Hello Linda" and has links for "Home", "Logout", and "Contact us". On the left side, there is a "Service Selection Portal" with a list of options: Services, Usage, Account, Schedules, Subscribe, Register (highlighted), and Unregister. Below this is a search bar. The main content area is titled "Register" and contains the following text: "You may register your DHCP equipment so that it always obtains a public IP address. The first step is to supply the credentials that will authorize your equipment to receive a public IP address." Below this text is a section titled "Equipment Credentials" with the instruction "Please enter your username and password for the Equipment Registration:". There are two input fields: "Username:" and "Password:". A "Continue" button is located below the password field. To the right of the input fields is an image of a computer monitor, keyboard, and a golf bag. At the bottom right of the main content area is the Vireo logo. The footer of the page reads "Copyright © 1999-2003 Juniper Networks".

2. Specify the username and password to use for equipment registration, and click **Continue**.

3. In the page that appears, specify the media access control (MAC) address of the equipment to be registered, provide a brief description of this equipment, and click **Register**.



The screenshot displays the Virneo Service Selection Portal. At the top left is the Virneo logo with the tagline "The network that keeps you surfing". A dark navigation bar at the top right says "Hello Linda" and contains links for "Home", "Logout", and "Contact us". On the left side, there is a "Service Selection Portal" menu with options: Services, Usage, Account, Schedules, Subscribe, Register (highlighted), and Unregister. Below this menu is a search bar. The main content area is titled "Register" and features a "New Equipment Registration" form. The form instructions state: "Please enter the MAC address (e.g. 03:3A:FE:98:3C:CB) and a brief description of the device you want to register." It includes input fields for "MAC address:" and "Description:", followed by "Register" and "Cancel" buttons. To the right of the form is an illustration of a computer setup with a monitor, keyboard, mouse, and a golf bag. The footer of the page contains the copyright notice "Copyright © 1999-2003 Juniper Networks" and the Virneo logo.

The page displays the registration information.

Disabling Equipment Registration

If you previously registered your equipment to obtain an authenticated IP address, you can change your configuration to disable equipment registration.

To disable registration of your equipment:

1. In the navigation pane, click **Unregister**.

The Unregister page appears.

virnet
The network that keeps you surfing

Hello Linda

Home Logout Contact us

Service Selection Portal

- Services
- Usage
- Account
- Schedules
- Subscribe
- Register
- Unregister

Search

Unregister

You may unregister your DHCP equipment so that it does not automatically obtain a public IP address. The first step is to supply the same credentials that you entered when you registered your equipment.

Equipment Credentials

Please enter your username and password for the Equipment Registration:

Username:

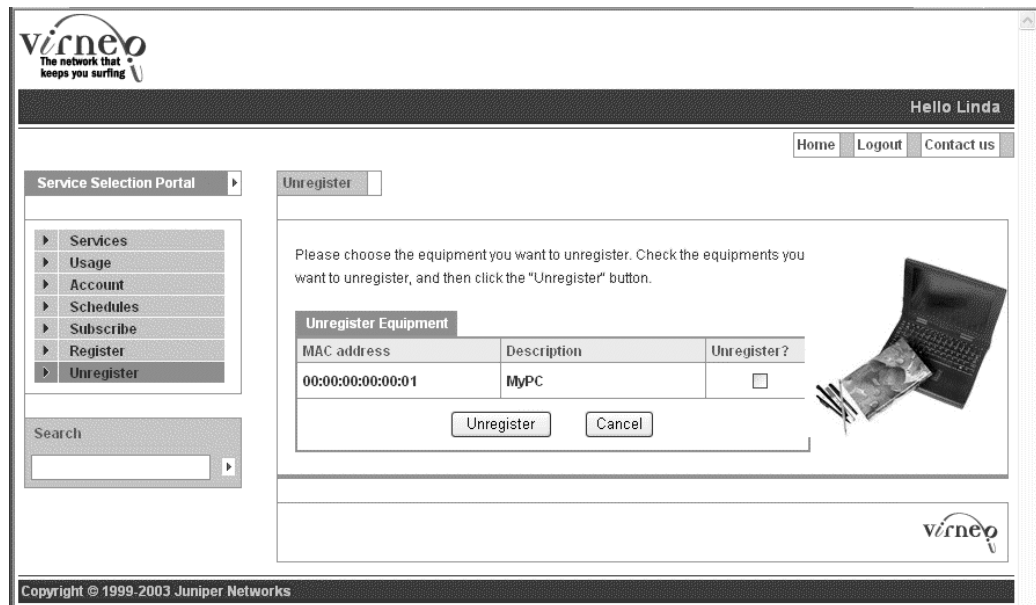
Password:

virnet

Copyright © 1999-2003 Juniper Networks

2. Enter your username and password, and click **Continue**.

A page appears that shows the equipment that you have registered.



The screenshot shows the Vireo Sample Residential Portal. The header includes the Vireo logo with the tagline "The network that keeps you surfing" and a greeting "Hello Linda". Navigation links for "Home", "Logout", and "Contact us" are present. A "Service Selection Portal" menu on the left lists options: Services, Usage, Account, Schedules, Subscribe, Register, and Unregister. The "Unregister" option is selected. The main content area is titled "Unregister" and contains instructions: "Please choose the equipment you want to unregister. Check the equipments you want to unregister, and then click the 'Unregister' button." Below this is a table titled "Unregister Equipment" with columns for "MAC address", "Description", and "Unregister?". The table lists one item: MAC address "00:00:00:00:01" and Description "MyPC". The "Unregister?" column has an unchecked checkbox. "Unregister" and "Cancel" buttons are at the bottom of the table. An image of a laptop with a stack of cash next to it is on the right. The footer shows the Vireo logo and copyright information: "Copyright © 1999-2003 Juniper Networks".

MAC address	Description	Unregister?
00:00:00:00:01	MyPC	<input type="checkbox"/>

3. Select the Unregister check box, and click **Unregister**.

The Welcome page for the portal appears.

You can also disable equipment registration when you log out of the portal; see *Logging Out of the Sample Residential Portal* on page 332.

Logging Out of the Sample Residential Portal

When you finish using subscriptions to services, log out of the sample residential portal.

To log out of the sample residential portal:

1. On any portal page, click **Logout**.

The Logout page appears.



2. If you want to disable equipment registration, select **Unregister my PC**.
3. Click **Logout**.

The Welcome page appears again.

Using the Sample Residential Portal from PDAs

You can also access the sample residential portal from a personal digital assistant (PDA).

To use the sample residential portal from a PDA:

1. Start the sample residential portal from a PDA in the same way that you start the portal from a Web browser running on your PC. See *Logging In to the Sample Residential Portal Using a Simulated User Profile* on page 316.

The Welcome page appears.



2. Click **Login**.

The login page appears.

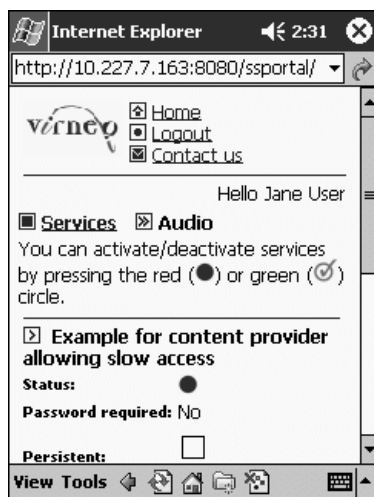


3. Enter your username and password.

After you log in, you can view the available services.



4. Navigate through the menus to activate and deactivate services.



Chapter 18

Developing a Residential Portal

This chapter provides an overview of the SRC residential portal. The chapter contains the following sections:

- Before You Develop a Residential Portal on page 335
- Development Tools to Create a Residential Portal on page 336
- Virtual IP Address for Policies on page 337
- Redirecting Traffic to a Captive Portal Web Page on page 338
- Managing Security for Public Wireless LAN Applications on page 339
- Developing a Portal Based on the Sample Residential Portal on page 340

Before You Develop a Residential Portal

You can develop a residential portal based on the sample residential portal that accompanies the SRC software, or you can create a new one. Before you set up a residential portal, the SAE configuration for the retailers, services, subscribers, and basic subscriber services should already be in place.

Before you start to develop a portal, make sure that you understand the SAE configuration and how subscribers are expected to log in to the portal. See the following sources for information about the SAE and its configuration:

- *SRC-PE Network Guide, Chapter 1, Overview of the SAE*
- *SRC-PE Services and Policies Guide, Chapter 14, Using the CLI to Configure SRC Applications to Communicate with an SAE*

or

SRC-PE Services and Policies Guide, Chapter 2, Managing Services on a Solaris Platform

- *Chapter 3, Subscriber Logins and Service Activation*

When you are planning an SRC network that uses residential portals, consider how many instances of the portals you need. For example, if your network includes a number of different retailers, you could create different portals for different retailers. Residential portals use CORBA to connect to the SAEs, allowing you to create distributed Web applications. These applications can be deployed in clusters for load sharing.

Development Tools to Create a Residential Portal

The SRC software provides the following tools for service providers to make residential portals available to residential customers:

- CORBA remote API—Provides remote access to the SAE core API

The CORBA remote API is the preferred interface to use between external applications and the SRC software. See the following sources for more information:

- *SRC-PE Network Guide, Chapter 1, Overview of the SAE.*
- SAE CORBA remote API documentation in the SRC software distribution in the folder *SDK/doc/idl* or on the Juniper Networks Web site at

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

- Javadoc documentation for the sample residential portal—Provides information about the Java interface

You can access the Javadoc documentation for the sample portal from the Welcome page of the sample portal after you log in to the portal. See *Chapter 17, How Subscribers Use the Sample Residential Portal*.

- Sample residential portal

You can customize and extend the sample residential portal included with this release or create your own portal based on the sample. For information about the sample residential portal, see *Chapter 16, Installing and Configuring the Sample Residential Portal* and *Chapter 17, How Subscribers Use the Sample Residential Portal*.

Virtual IP Address for Policies

You can configure a virtual IP address to specify an IP address that policies use as a substitution to send traffic to a captive portal.

For information about how to configure a virtual IP address from the SRC CLI, see *SRC-PE Network Guide, Chapter 5, Using JUNOSe Routers in the SRC Network with the SRC CLI*.

Configuring a Virtual Portal Address with SDX Configuration Editor

To configure a virtual portal address:

1. In SDX Configuration Editor, select the configuration for the SAE.
2. Click the **Routers** tab, and in the Routers pane.



The screenshot shows a configuration field labeled "Virtual Portal Address" with the value "192.168.254.1" entered. To the right of the text box is a button labeled "Disable".

3. Enter a value for the virtual portal address.

See *Virtual Portal Address Field* on page 337.

4. Select **File > Save**, then select **SDX System Configuration > Export to LDAP Directory**.

Virtual Portal Address Field

In SDX Configuration Editor, you can modify the following field in the Routers pane in an SAE configuration file.

Virtual Portal Address

- IP address of the portal server that is published to subscribers and used in router policies.
- Value—IP address
- Default—192.168.254.1
- Property name—Router.virtual.portal.address

Redirecting Traffic to a Captive Portal Web Page

A captive portal Web page is a page that receives redirected HTTP requests. You can use a captive portal page as the initial page a subscriber sees after logging in to a subscriber session and as a page used to receive and manage HTTP requests to unauthorized Web resources.

The type of information available from a captive portal page depends on the portal design. The page can provide informational messages or can let subscribers perform actions such as activating a service to which they have a subscription. For example, if a subscriber requests access to a service that the subscriber has not activated, the portal could display a captive portal page that tells the subscriber that the service is not available, or the page could prompt the subscriber to activate the requested service.

Implementing a captive portal requires the following:

- An instance of the redirect server installed on a host in the same network as a JUNOSe router. The redirect server redirects HTTP requests received from IP Filter to a captive portal page.
- When the SRC software is installed on a Solaris platform, the IP Filter tool installed and configured on the same host as the redirect server. This tool redirects incoming HTTP requests to the redirect server.
- Default policies installed on the JUNOSe router. The default policies on the JUNOSe router must include a forwarding or rate-limiting policy that permits access to the portal server and a next-hop rule to intercept the unauthorized access request packets. The target of the next-hop rule is the host on which the redirect server resides.
- A portal server for serving the captive portal pages.

For a sample captive portal, see the sample residential portal.

For information about configuring the redirect server, see the following chapters:

- *Chapter 20, Configuring Traffic Redirection with the SRC CLI*
- *Chapter 21, Configuring Traffic Redirection on a Solaris Platform*

Sequence for Redirecting Traffic

The following list describes the sequence of events that occurs when a subscriber tries to access a restricted service:

1. A subscriber opens a Web browser and attempts to access a restricted server; for example, `http://a.com`.
2. A next-hop policy on the JUNOSe router sends this request to the redirect server instead of to the requested server.

The policy does not affect the destination address (resolved from `a.com`) in the IP packets.

3. For environments that have the SRC software installed on a Solaris platform, the IP Filter process running on the same host as the redirect server filters traffic and redirects traffic arriving on port 80 on the host's incoming interface.
4. The captured request is redirected to an address and a port where the redirect server listens.
5. The redirect server opens a TCP port (8800 by default) and sends the type of response configured—an HTTP 200 (OK) or a small HTML document that encodes a refresh in the meta header of the file—to the subscriber's browser for the requests.
6. The subscriber browser follows the redirect request and opens the captive portal page on the portal server.

Configuring the SRC Software in a Multihop Environment

The captive portal system implemented by the HTTP redirect server requires a single-hop connection; that is, the router accessed by the subscriber cannot be more than one hop away from the redirect server. However, some networking environments will require a multihop connection—through more than one router—to the redirect server.

You can use any of several methods to get around the intermediate, next-hop routers, such as IP-in-IP tunneling, deployment of a NAT device, and dynamic DNS. Contact Juniper Networks Professional Services for assistance with these methods.

Managing Security for Public Wireless LAN Applications

You can include in a residential portal a Web page that automatically refreshes itself and provides a keepalive application that verifies the HTTP session. If the keepalive application cannot verify the HTTP session, the portal terminates the subscriber session. This feature improves security for public wireless LAN applications.

If you include this Web page in a residential portal, the following sequence of events occurs:

1. When a subscriber logs in through the portal, the SRC software starts the keepalive application.
2. The keepalive application creates a session key and sends it to the residential portal.
3. The residential portal stores the session key in its corresponding HTTP session.
4. The keepalive application sets the timeout for the subscriber session to a value greater than the refresh time.
5. When the Web page refreshes itself, the keepalive application sends the session key to the residential portal.

6. The portal responds as follows:
 - If the session key matches the value in the portal's HTTP session, the portal updates the timeout for the subscriber session, creates a new session key, and sends the new key to the keepalive page.
 - If the session key does not match the value in the portal's HTTP session, the portal terminates the subscriber session.
7. If the Web page does not refresh itself before the timeout expires (for example, if the subscriber closes the Web browser or turns off the PC without logging out), the portal terminates the subscriber session.

Developing a Portal Based on the Sample Residential Portal

The source code is included with the sample residential portal. To modify the behavior of the portal beyond a simple configuration, install a Java development environment. You can find the source code of the sample residential portal in the directory *WEB-INF/src*. The portal pages are stored in the layout and tiles directories.

The sample residential portal does not require any specific environment, but the procedures below assume that you use the Eclipse platform. A servlet container is required to run the portals during development. We recommend that you use Tomcat and its Eclipse plug-in.

For information about your development environment, see the documentation for the product you are using.

Preparing to Develop a Portal Based on the Sample Residential Portal

The following instructions describe how to set up a development environment that uses Eclipse and Tomcat on a Solaris platform. If you want to use Eclipse and Tomcat on a different operating system, see the following Web sites:

- For Eclipse:
<http://www.eclipse.org>
- For Tomcat:
<http://jakarta.apache.org/tomcat>

To get ready to develop a portal based on the sample residential portal:

1. Download and install Eclipse from
<http://www.eclipse.org>
2. Download the Tomcat plug-in for Eclipse from
<http://www.sysdeo.com/eclipse/tomcatPlugin.html>
3. Unzip the plug-in into the Eclipse installation directory.

- Download Tomcat from
<http://jakarta.apache.org/tomcat>

- Install Tomcat:

```
mkdir $HOME/eclipse
cd $HOME/eclipse
unzip /tmp/eclipse-SDK-2.0.2-solaris-motif.zip
unzip /tmp/tomcatPluginV201.zip
cd $HOME
gzip -dc /tmp/tomcat-4.1.18.tar.gz | tar xvf -
```

- Start Eclipse.
- Configure the Tomcat plug-in.

Select **Window > Preferences > Tomcat**, and configure the Tomcat version and the path where you installed Tomcat.

Creating a Portal Project

To create a new Tomcat project inside Eclipse:

- Select **File > New > Project > Java > Tomcat Project**, enter the name of the project, and click **Finish**.
- Select **File > Import... > Zip File**, enter the path for *ssportal.war*; and click **Finish**.
- Select **File > Properties > Java Build Path > Libraries > Add Jars**, open the sample project, navigate to *WEB-INF/lib*, and select all JAR files in the *WEB-INF/lib* directory.
- Select **File > Properties > Tomcat**, and click **Can update server.xml file**.

Building the Portal

Eclipse automatically rebuilds the project when you save a modified source file.

To test or debug the project, run the code inside Tomcat.

To start Tomcat:

- Select **Tomcat > Start Tomcat**.

You can set break points in your code to debug the code.

Deploying the Portal

To create a new Web application, set the name of the target WAR file.

- Select **File > Properties > Tomcat**.
- Enter the path of the target WAR file in the field WAR file for export.

3. Right-click the portal project, and select **Tomcat Project > Export to the WAR file set** in project properties.
4. Copy the WAR file to the final deployment location; for example, */opt/UMC/jboss/server/default/deploy* on your portal server.

Testing a Portal Application

Simulated router drivers allow you to create subscriber sessions without connecting to a router. You can use a simulated router drive when you want to test your portal application. See *SRC-PE Monitoring and Troubleshooting Guide, Chapter 5, Configuring a Simulated Router Driver for Testing with the SRC CLI* or *SRC-PE Monitoring and Troubleshooting Guide, Chapter 6, Configuring a Simulated Router Driver for Testing with SDX Configuration Editor*.

Part 3

Redirecting Subscriber Traffic Through Redirect Server

Chapter 19

Redirecting Subscriber Traffic

This chapter describes the redirect server and contains the following sections:

- Overview of Traffic Redirection on page 345
- Proxy Request Management on page 345
- Redirect Server Redundancy on page 347
- Before You Configure Redundancy for the Redirect Server on page 348
- Protection Against Denial-of-Service Attacks on page 348

Overview of Traffic Redirection

The redirect server is part of a captive portal system that redirects subscribers' Web requests to a captive portal page. You can use a captive portal page as the initial page a subscriber sees after logging in to a subscriber session and as a page used to receive and manage HTTP requests to unauthorized Web resources.

If you run the SRC software on Solaris platforms, a captive portal uses an instance of the redirect server installed on a host in the same network as a JUNOSe router. Your network configuration must not have any routers between the JUNOSe router and the redirect server. An intermediate router would look at the destination address that is still present in the packets and would route the packets there rather than to the SAE. One way to overcome this limitation is to set up a tunnel between the JUNOSe router and the redirect server.

Proxy Request Management

The redirect server examines requested paths and detects proxy HTTP requests by the proxy prefix "< scheme >:" followed by the address of the requested host. If the requested URL is served by the captive portal server:

1. The redirect server opens a TCP connection to the captive portal and forwards the request for the URL. The redirect server adds to the request an X-Forwarded-For header that specifies the IP address of the client.

2. The captive portal server inspects the incoming request for the X-Forwarded-For header for the IP address. The captive portal server uses this address instead of the source IP address to determine the originator of the request.
3. If the captive portal authorizes the client and activates a service that enables a direct connection between the client and the proxy, the redirect server then sends the returned data to the subscriber's Web browser.

or

If the requested URL is not served by the captive portal server, the redirect server opens a TCP port (8800 by default) and sends the type of response configured to a subscriber's browser in response to a captured request:

- HTTP 200 OK response with an HTML document that includes the < HTTP-Equiv = "Refresh" > header (default)
- HTTP 302 Found response to a subscriber's browser in response to a captured request

The subscriber browser follows the redirect request, and the proxied request is served by the redirect server again, which opens a connection to the captive portal.

Support for HTTP proxy requests requires the following:

- A local HTTP proxy server that can handle the traffic from all clients configured with a proxy.
- A location for the local HTTP proxy server that is one IP hop from each access router.
- A proxy service that the captive portal server can activate to send proxy requests to the local HTTP proxy server when the portal server authorizes proxy clients.
- A proxy service activation policy that includes a next-hop policy that points to the local HTTP proxy server, and a classifier that matches the client's IP address and the address of the proxy server configured on the client.

Services that the client accesses through the proxy server, such as HTTP and FTP, cannot be activated based on destination address.

You must redirect all ports to the redirect server because you cannot know which ports are configured on the client for the proxy. Consequently, the redirect server receives non-HTTP requests as well as HTTP requests. The non-HTTP requests generate error log entries. To reduce overhead, HTTP error messages are logged as system log debug messages.

HTTP Proxy and DNS

Make sure that your network includes a domain name service (DNS) server to resolve unknown names to a fixed IP address. A DNS server is required because proxy servers can be configured with DNS names in private domains that are not valid in the public environment. You can use the DNS server included with the redirect server, or another DNS server on your network.

The DNS server can be configured on a client with DHCP. Alternatively, the service provider can set up a transparent DNS proxy by configuring a next-hop policy on the JUNOS router for UDP and TCP port 53 traffic. The policy redirects traffic on these two ports to the redirect server's DNS server.

Because proxy addresses must be resolved even if general access to the Internet is enabled, the DNS server must continue to resolve all client requests for proxy clients. Nonproxy clients can use their regular DNS server after the initial service has been activated.

The redirect server's DNS server either forwards the request to a set of configured DNS servers or resolves the request by using the root domain name server. If a request for an IPv4 address cannot be resolved and the request results in an NXDOMAIN error, the DNS server returns a configurable IP address. The redirect server returns an error message to the clients for any other type of request that cannot be resolved.

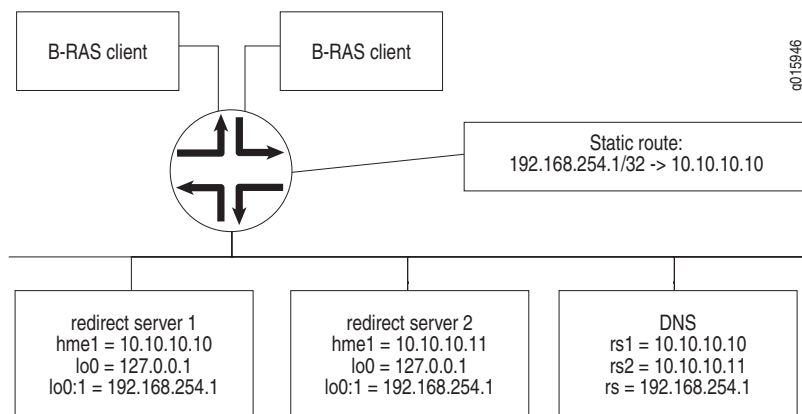
Redirect Server Redundancy

You can configure the redirect server to provide redundancy to help ensure that a redirect server is always available. You install the redirect server software on two different hosts; then you configure one redirect server as the primary redirect server, and the other as the redundant redirect server. The active and redundant redirect servers regularly poll each other to confirm each other's availability. If the primary redirect server becomes unavailable, the redundant server assumes the active role.

When a redirect server assumes the primary role, it configures on the router a static route from the virtual IP address to the server's real IP address. Clients send requests to the virtual IP address, and the router automatically sends the request to the active redirect server through a static route. The virtual IP address is used only in the static route configured on the router and the next-hop policy installed by SAE. End users do not see the virtual IP address.

Figure 28 shows a configuration in which two redirect servers use the same virtual IP address, 192.168.254.1.

Figure 28: Failover of Redirect Server



Before You Configure Redundancy for the Redirect Server

If you plan to use a redundant configuration for the redirect server, ensure that:

- The virtual IP address to be used is also the next-hop address for policies that capture web traffic and send it to the redirect server.
- The redirect server has SNMP write access to the virtual routers connected to it. Each VR must have at least a write community configured. (The static route from the virtual IP address to the server's real IP address is installed on the router through SNMP.)
- If additional access controls are enabled on the JUNOS router, the hosts on which the redirect server runs must be included.

Protection Against Denial-of-Service Attacks

The redirect server incorporates a number of properties to protect against denial-of-service attacks. The following list shows the default values set for these properties:

- The redirect server can serve no more than 12,000 requests per minute, with a burst of 18,000 requests.
- The redirect server can serve no more than 25 requests per client per minute, with a burst of 50 requests.
- Incoming requests can be no larger than 4 KB.
- Incoming requests have a time limit of 2 seconds.

You can change the values for any of these properties.

Chapter 20

Configuring Traffic Redirection with the SRC CLI

This chapter describes how use the SRC CLI to configure the redirect server for a C-series platform. Topics include:

- Configuration Statements for the Redirect Server on page 350
- Before You Configure the Redirect Server on a C-Series System on page 351
- Configuring the Redirect Server on page 351
- Configuring General Properties for the Redirect Server on page 352
- Configuring a Connection Between the Redirect Server and the Directory on page 353
- Defining Traffic to Transmit to the Redirect Server on page 354
- Changing the Number of Requests That the Redirect Server Accepts on page 354
- Specifying Extensions for Files That the Redirect Server Accepts on page 356
- Verifying Configuration for the Redirect Server on page 357
- Configuring the DNS Server for the Redirect Server on page 357
- Configuring the Redirect Server to Support HTTP Proxies on page 358
- Configuring a Redundant Redirect Server on page 359
- Configuring Logging for the Redirect Server on page 360
- Changing the Configuration for the Redirect Server on page 361
- Assessing Load for Redirect Server on page 361

For information about the redirect server, including information about what you should do before using the redirect server, see *Chapter 19, Redirecting Subscriber Traffic*.

Configuration Statements for the Redirect Server

Use the following configuration statements to configure the redirect server at the [edit] hierarchy level.

```

redirect-server {
    tcp-port tcp-port;
    destination-url destination-url;
    proxy-support;
    proxy-destination-url proxy-destination-url;
    refresh;
    request-rate request-rate;
    request-burst-size request-burst-size;
    client-rate client-rate;
    client-burst-size client-burst-size;
    check-file-extensions;
    file-extensions file-extensions;
    redundancy;
}

redirect-server ip-redirect{
    interface interface;
    port port;
}

redirect-server ldap {
    url url;
    bind-dn bind-dn;
    bind-password bind-password;
    base-dn base-dn;
}

redirect-server dns {
    enable;
    tcp-port tcp-port;
    udp-port udp-port;
    forwarder forwarder;
    error-ip-address error-ip-address;
}

redirect-server monitor {
    redundant-host-ip-address redundant-host-ip-address;
    virtual-ip-address virtual-ip-address;
    real-ip-address real-ip-address;
    primary-server;
    check-interval check-interval;
    virtual-routers virtual-routers;
}

```

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

Before You Configure the Redirect Server on a C-Series System

Before you configure the redirect server on a C-series platform:

- Configure policies on a B-RAS to define which traffic to send to the redirect server; typically, a next-hop policy specifies a destination address that is the virtual IP address of the active redirect server.
- If you plan to configure a redundant redirect server, make sure that you are familiar with the network configuration required.

See *Chapter 19, Redirecting Subscriber Traffic*.

Configuring the Redirect Server

The redirect server on a C-series platform manages IP layer redirection.

To configure the redirect server:

1. Configure general properties for the redirect server.

See *Configuring General Properties for the Redirect Server* on page 352.

2. Configure a connection from the redirect server to the directory.

See *Configuring a Connection Between the Redirect Server and the Directory* on page 353.

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 platform.

See *Defining Traffic to Transmit to the Redirect Server* on page 354.

4. (Optional) Configure the number of requests that the redirect server accepts.

See *Changing the Number of Requests That the Redirect Server Accepts* on page 354.

5. (Optional) Configure the types of files for which the redirect server accepts requests.

See *Specifying Extensions for Files That the Redirect Server Accepts* on page 356.

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* on page 357.

7. (Optional) Configure support for HTTP proxies.

See *Verifying Configuration for the Redirect Server* on page 357.

8. (Optional) Configure a redundant redirect server.

See *Configuring a Redundant Redirect Server* on page 359.

Configuring General Properties for the Redirect Server

Use the following configuration statements to configure general properties for the redirect server:

```
redirect-server {
    destination-url destination-url;
    tcp-port tcp-port;
    refresh;
}
```

To configure properties for the redirect server:

1. From configuration mode, access the configuration statement that configures the redirect server.

```
user@host# edit redirect-server
```

2. Specify the URL to which to send subscriber traffic.

```
[edit redirect-server]
user@host# set destination-url destination-url
```

3. (Optional) Specify the TCP port on which the redirect server listens for requests.

```
[edit redirect-server]
user@host# set tcp-port tcp-port
```

4. (Optional) Specify whether the redirect server sends an HTTP 200 OK response with an HTML document that includes the < HTTP-Equiv = "Refresh" > header to a subscriber's browser in response to a captured request.

```
[edit redirect-server]
user@host# set refresh
```


If you do not use the `refresh` option, the redirect server sends an HTTP 302 Found response to a subscriber's browser in response to a captured request.

By setting the `refresh` option, the load on the Web server is decreased because non-browser (or non-HTML) client applications that use HTTP do not follow this refresh message; however, most client applications do follow HTTP 302 messages.

Configuring a Connection Between the Redirect Server and the Directory

Use the following configuration statements to configure a connection between the redirect server and the directory:

```
redirect-server ldap {
    url url;
    bind-dn bind-dn;
    bind-password bind-password;
    base-dn base-dn;
}
```

To configure a connection between the redirect server and the directory:

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

```
user@host# edit redirect-server ldap
```

2. List the URLs for directories employed by the redirect server.

```
[edit redirect-server ldap]
user@host# set url url
```

For each URL, use the format:

```
ldap:// <host> : <portNumber>
```

where `<host>` is the IP address or hostname of the directory host and `<portNumber>` is the TCP port

3. Specify the DN that the redirect server uses to authorize connections to the directory.

```
[edit redirect-server ldap]
user@host# set bind-dn bind-dn
```

The DN must have authorization to read from `o = network`, `o = umc` in the directory.

4. Specify the password that the redirect server uses to bind to the directory.

```
[edit redirect-server ldap]
user@host# set bind-password bind-password
```

5. Specify the base DN that is the root of the directory tree.

```
[edit redirect-server ldap]
user@host# set base-dn base-dn
```

Defining Traffic to Transmit to the Redirect Server

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 system 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.

Use the following configuration statements to define traffic to transmit to redirect server:

```
redirect-server ip-redirect{
  interface interface;
  port port;
}
```

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. From configuration mode, access the configuration statement that configures IP redirection for the redirect server.

```
user@host# edit redirect-server ip-redirect
```

2. Specify one or more interfaces on which subscriber traffic is forwarded from the B-RAS to the C-series platform.

```
[edit redirect-server ip-redirect]
user@host# interface interface
```

If you do not specify an interface, the C-series platform system accepts traffic from all interfaces.

3. Specify the TCP port of the redirected traffic. If you do not specify a port, the redirect server uses port 80 (HTTP).

```
[edit redirect-server ip-redirect]
user@host# port port
```

Changing the Number of Requests That the Redirect Server Accepts

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.

Use the following configuration statements to configure the number of requests that the redirect server accepts:

```
redirect-server {
    request-rate request-rate;
    request-burst-size request-burst-size;
    client-rate client-rate;
    client-burst-size client-burst-size;
}
```

To configure the number of redirection requests that the redirect server can accept:

1. From configuration mode, access the configuration statement that configures the redirect server.

```
user@host# edit redirect-server
```

2. Specify the number of requests that the redirect server can accept per minute from all clients (global sustained rate).

```
[edit redirect-server]
user@host# set request-rate request-rate
```

3. Specify the maximum number of requests that the redirect server can accept from all clients (burst size).

```
[edit redirect-server]
user@host# set request-burst-size request-burst-size
```

This value should exceed the value for the request rate. If the value for the request rate exceeds this value, the redirect server drops the excess requests.

4. Specify the number of requests that the redirect server can accept per minute for a single client (per-client sustained rate).

```
[edit redirect-server]
user@host# set client-rate client-rate
```

5. Specify the maximum number of requests that the redirect server can accept for a single client (per client burst size).

```
[edit redirect-server]
user@host# set client-burst-size client-burst-size
```

This value should exceed the value for the client rate.

Specifying Extensions for Files That the Redirect Server Accepts

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.

Use the following configuration statements to configure the file extensions that the redirect server accepts:

```
redirect-server {
    check-file-extensions;
    file-extensions file-extensions;
}
```

To specify the extensions for the types of files accepted by the redirect server:

1. From configuration mode, access the configuration statement that configures the redirect server.

```
user@host# edit redirect-server
```

2. Specify whether the redirect server should accept only URLs that point to files that have standard file extensions— < empty > , .asp, .htm, .html, .jsp, .php, .sh, .shtml, and .xml.

```
[edit redirect-server]
user@host# set check-file-extensions
```

If you enable `check-file-extensions` and the file does not have a standard file extension, the redirect server returns an HTTP 403 Forbidden message.

3. List file extensions to augment the standard file extensions configured in Step 3. Precede each extension with a period. Make sure that you specify the correct case for each character; entries are case-sensitive.

```
[edit redirect-server]
user@host# set file-extensions file-extensions
```

Separate each file extensions by a comma. For example:

```
set file-extensions .cgi,.aspx
```

Verifying Configuration for the Redirect Server

To verify the configuration for redirect server:

- At the [edit redirect-server] hierarchy level, enter the **show** command:

```
[edit redirect-server]
user@host# show
tcp-port 8800;
destination-url ;
refresh;
refresh-document etc/refresh.html;
user-name nobody;
request-rate 12000;
request-burst-size 18000;
client-rate 25;
client-burst-size 50;
```

For information about monitoring redirect server, see *SRC-PE Monitoring and Troubleshooting Guide, Chapter 9, Monitoring Redirect Server with the SDX CLI*.

Configuring the DNS Server for the Redirect Server

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.

If you plan to use an external DNS server, you can skip this section. This section describes how to configure the DNS server that is included with the redirect server.

Use the following configuration statements to configure the DNS server that is included with the redirect server:

```
redirect-server dns {
  enable;
  tcp-port tcp-port;
  udp-port udp-port;
  forwarder forwarder;
  error-ip-address error-ip-address;
}
```

To configure DNS for the redirect server that is included with the redirect server:

1. From configuration mode, access the configuration statement that configures DNS for the redirect server.

```
user@host# edit redirect-server dns
```

2. Enable DNS for the redirect server.

```
[edit redirect-server dns]
user@host# set enable
```

3. Specify the TCP port on which the DNS server listens:

If you set the value to 0, no TCP socket is opened.

```
[edit redirect-server dns]
user@host# set tcp-port tcp-port
```

4. Specify the UDP port on which the DNS server listens.

```
[edit redirect-server dns]
user@host# set udp-port udp-port
```

5. Specify the IP addresses of DNS servers to which resolution requests are forwarded; use commas to separate addresses, but do not add a space after the comma.

```
[edit redirect-server dns]
user@host# set forwarder forwarder
```

For example:

```
[edit redirect-server dns]
user@host# set forwarder 192.0.2.24,192.0.4.25
```

If you do not specify DNS servers, DNS resolves incoming requests by using the normal DNS method.

6. Specify the IP address that is returned when a DNS request results in an unknown name (NXDOMAIN) error.

```
[edit redirect-server dns]
user@host# set error-ip-address error-ip-address
```

Configuring the Redirect Server to Support HTTP Proxies

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.

For information about configuring the DNS server included with the SRC software, see *Configuring the DNS Server for the Redirect Server* on page 357.

Use the following configuration statements to configure the redirect server to support HTTP proxies:

```
redirect-server {
  proxy-support;
  proxy-destination-url proxy-destination-url;
}
```

To configure the redirect server to support HTTP proxies:

1. From configuration mode, access the configuration statement that configures the redirect server.

```
user@host# edit redirect-server
```

2. Enable HTTP proxy support.

```
[edit redirect-server]
user@host# set proxy-support
```

3. Specify the URL sent as a response to proxy requests.

```
[edit redirect-server]
user@host# set proxy-destination-url proxy-destination-url
```

If you do not configure a value, then the URL defaults to the `redir.url` value. You can use this property to send proxy requests to a page different from the direct request page on the captive portal.

Configuring a Redundant Redirect Server

Although configuration of a redundant redirect server is optional, we recommend that you configure redundancy to maintain high availability for the server.

Use the following configuration statements to configure redundancy for the redirect server:

```
redirect-server {
    redundancy;
}

redirect-server monitor {
    redundant-host-ip-address redundant-host-ip-address;
    virtual-ip-address virtual-ip-address;
    real-ip-address real-ip-address;
    primary-server;
    check-interval check-interval;
    virtual-routers virtual-routers;
}
```

To configure redundancy for the redirect server:

1. From configuration mode, access the configuration statement that configures the redirect server.

```
user@host# edit redirect-server
```

2. Enable redundancy for the redirect server.

```
[edit redirect-server]
user@host# set redundancy
```

3. Configure redundancy properties for the redirect server.

```
[edit redirect-server]
user@host# edit redirect-server monitor
```

4. Configure the IP address or hostname of the redundant redirect server.

```
[edit redirect-server]
user@host# set redundant-host-ip-address redundant-host-ip-address
```

5. Configure the virtual IP address of the redirect server.

```
[edit redirect-server]
user@host# set virtual-ip-address virtual-ip-address
```

6. Configure the real IP address of the redirect server.

```
[edit redirect-server]
user@host# set real-ip-address real-ip-address
```

When a primary redirect server is started, it dynamically establishes and maintains a static route on the client router to which it connects. The static route directs traffic destined for the virtual IP address of the server to the real IP address of the active redirect server.

7. (Optional) Set the system on which you enter the command as the primary redirect server.

```
[edit redirect-server]
user@host# set primary-server
```

8. (Optional) Set the interval at which the redirect server polls the redundant redirect server.

```
[edit redirect-server]
user@host# set check-interval check-interval
```

A shorter time in the range leads to faster detection of problems and results in higher consumption of CPU resources.

9. List of virtual routers to which the redirect server connects.

```
[edit redirect-server]
user@host# set virtual-routers vrName@routerName, vrName@routerName ...
```

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.

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.

Assessing Load for Redirect Server

You can 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.

To view statistics for redirect server:

```
user@host> show redirect-server statistics
Redirect Server
Uptime                        849767.841
Accepted requests             0
Rejected requests             0
Number of user limit leaky buckets 0
Number of user limits reached  0
Number of global limits reached 0
```

You can also obtain statistics for redirect server through SNMP. The name of the MIB for redirect server is Juniper-SDX-REDIRECTOR-MIB.

Chapter 21

Configuring Traffic Redirection on a Solaris Platform

This chapter describes how to redirect subscriber traffic by using redirect server on a Solaris platform. The chapter contains the following sections:

- Installing the Redirect Server on page 363
- Configuration Overview for Redirect Server on page 364
- Configuring IP Filter on page 364
- Configuring Redirect Server from the `redir.properties` File on page 366
- Configuring Logging for Redirect Server on page 372
- Changing the Configuration for Redirect Server on page 372

Installing the Redirect Server

To install and configure the redirect server on a Solaris platform:

1. Install the redirect server software as follows:
 - If you want to configure redundancy for the redirect server, install the software on two hosts.
 - If you do not want to configure redundancy for the redirect server, install the software on one host.

For information about installing the Web redirect component of the captive portal system, see *SRC-PE Getting Started Guide, Chapter 27, Before You Install the SRC Software on a Solaris Platform*.

2. (Optional) Configure DNS.

Configuration Overview for Redirect Server

To configure the redirect server on a Solaris platform:

1. Configure IP Filter to define which traffic to redirect to the redirect server.

See *Configuring IP Filter* on page 364.

2. If you plan to configure a redundant redirect server, make sure that you are familiar with the network configuration required.

See *Chapter 19, Redirecting Subscriber Traffic*.

3. Configure how you want the redirect server to work in your environment:

See *Configuring Redirect Server from the `redir.properties` File* on page 366.

Configuring IP Filter

If you run the SRC software on a Solaris platform, you use IP Filter to redirect subscriber requests for inappropriate or unsubscribed Web access. You specify Network Address Translation (NAT) rules in a configuration file that IP Filter uses to redirect traffic. When a packet arrives that matches a rule, its destination address is mapped as specified in the rule.

To install and configure IP Filter:

1. Install IP Filter on each server in which you want it to operate.

For information about installing the IP Filter component of the captive portal system, see *SRC-PE Getting Started Guide, Chapter 28, Installing the SRC Software on a Solaris Platform*.

2. Access the IP Filter directory.

`cd /etc/opt/ipf`

3. Create the NAT file `/etc/opt/ipf/ipnat.conf`.
4. Add a rule to the `ipnat.conf` file to direct unauthorized traffic, and other rules, as needed to specify which traffic is to be redirected and to specify the destination for the redirected traffic.

Create one rule for every interface on which redirected traffic can be received. For example, if you install the redirect server in a central location and set up multiple tunnel interfaces, you create one redirect rule for each tunnel interface. When you add rules to the `ipnat.conf` file, add a rule for authorized traffic followed by a rule for unauthorized traffic.

You can issue the **ifconfig -a** command to determine which network interfaces are configured on the host. You cannot use localhost (127.0.0.1) as a destination.

See the UNIX **man** pages for **ipnat** and **ipf** for more information about configuring IP Filter.

5. Update and start IP traffic filtering.

/etc/init.d/ipfboot start

6. View active rules and sessions.

/sbin/ipnat -l

The following sections give examples of the types of rules that you can configure by using IP Filter.

Example: Creating a Rule to Redirect Traffic to a Different Port Number

To enable subscribers to connect to the Web using the standard port, 80, for a Web server running on nonstandard port 8080, edit the *ipnat.conf* file on each Web server host to create a rule in the following format:

```
rdr ifName IpAddress/32 port 80 -> IpAddress port 8080 tcp
```

For example:

```
rdr hme0 192.168.1.1/32 port 80 > 192.168.1.1 port 8080 tcp
```

This rule filters legitimate traffic destined for the Web server and redirects it as follows:

1. Filters HTTP traffic that has a destination of standard port 80 and that meets the following criteria:
 - Has a destination of the specified masked IP address (the publicly known address for the Web server, stored in the JUNOS router IP routing table).
 - Arrives on the primary network interface on the SAE host that receives traffic by means of the JUNOS router.
2. Redirects filtered traffic to the specified target IP address on nonstandard port 8080.

The target IP address must be an address that exists on the Web server and must be different from localhost (127.0.0.1).

Example: Creating a Rule to Redirect Unauthorized Traffic

To redirect invalid traffic, on each host in which you have installed the redirect server, add a rule to the *ipnat.conf* in the following format:

```
rdm ifName 0.0.0.0/0 port 80 -> IpAddress port 8800 tcp
```

For example:

```
rdm hme0 0.0.0.0/0 port 80 > 10.227.1.163 port 8800 tcp
```

This rule redirects unauthorized traffic as follows:

1. Filters all HTTP packets that have the destination port of 80 and that meet the following criteria:
 - Has a destination of any IP address.
 - Arrives on the primary network interface on the redirect server host that receives traffic by means of the JUNOS router.
2. Redirects packets to the specified target IP address on port 8800. The redirect server listens on this port and redirects subscribers to the captive portal page that you define to handle this traffic.

Configuring Redirect Server from the *redir.properties* File

If you run the SRC software on a Solaris platform, you configure the redirect server by editing the *redir.properties* file.

To configure the redirect server from the *redir.properties* file:

1. On each host on which you installed the redirect server software, access the directory in which you installed the redirect server, and run the configuration script.

```
# cd /opt/UMC/redir
# etc/config
```

2. Follow the instructions on the screen to configure the redirect server.

Because the script includes some error checking, we recommend that you follow the instructions on the screen rather than directly editing the */opt/UMC/redir/etc/redir.properties* file.

For information about the properties to be configured, see *Configuration Properties for the Redirect Server* on page 367.

If you are configuring redundancy for the redirect server, assign one redirect server as the primary server, and the other as the redundant server.

For information about getting information about the requests the redirect server is receiving and processing, see *Chapter 20, Configuring Traffic Redirection with the SRC CLI*.

Configuration Properties for the Redirect Server

You can modify the following properties for the redirect server from the configuration script that saves changes to the */etc/redirect.properties* file.

redir.port

- TCP port on which the redirect server listens for requests.
- Value—Integer; valid port number in the range 1024–65535
- Default—8800

redir.url

- URL sent as a response to redirect requests. If *redir.proxyurl* is not configured, this URL is used for both proxied and nonproxied requests.
- Value—`http:// <serverHost> /accessDenied.do?url = %(url)`
 - `<serverHost>` —Valid URL; string of ASCII characters.
- Guidelines—The URL can contain the special strings “%(url)s” and “%(proxy)s.” If the HTTP request is sent to a proxy, the “%(url)s” string is replaced with the originally requested URL, and the “%(proxy)s” string is replaced with the proxy’s “<ipAddress> : <port>”. If the request is sent directly, the string is replaced with “None.”
- Default—`http:// <serverHost> /accessDenied.do?url = %(url)`

redir.proxy

- Configures proxy support. If you do not enable proxy support, the redirect server handles proxy requests in the same manner as direct requests.
- Value
 - Y—Proxy support is enabled.
 - N—Proxy support is disabled.
- Default—N

redir.proxyurl

- URL sent as a response to proxy requests. If you do not configure a value, then the URL defaults to the *redir.url* value. You can use this property to send proxy requests to a page different from the direct request page on the captive portal.
- Value—Valid URL; string of ASCII characters in URL string format
- Default—No value

redir.user

- Name of the user who owns the UNIX processes for the redirect server.
- Value—Text string
- Default—Nobody

redir.reqrate

- Number of requests that the redirect server can accept per minute from all clients (global sustained rate).
- Value—Integer in the range 0–2147483647
- Default—12000

redir.reqburst

- Maximum number of requests that the redirect server can accept from all clients (burst size). This value should exceed redir.reqrate. If the value for redir.reqrate exceeds this value, the redirect server drops the excess requests.
- Value—Integer in the range 0–2147483647
- Default—18000

redir.clientrate

- Number of requests that the redirect server can accept per minute for a single client (per client sustained rate).
- Value—Integer in the range 0–2147483647
- Default—25

redir.clientburst

- Maximum number of requests that the redirect server can accept for a single client (per client burst size). This value should exceed redir.clientrate.
- Value—Integer in the range 0–2147483647
- Default—50

redir.ext

- Specifies whether the redirect server should accept only URLs that point to files that have standard file extensions— < empty > , .asp, .htm, .html, .jsp, .php, .shtm, .shtml, and .xml. If you specify Y and the file does not have a standard file extension, the redirect server returns an HTTP 403 Forbidden message.
- Value
 - Y—Accepts only standard file extensions.
 - N—Accepts all file extensions.
- Default—N

redir.extensions

- List of additional file extensions. Employed only if you specified Y for redir.ext.
- Value—Text string consisting of acceptable file extensions separated by commas
- Default—No value

redir.monitor

- Configures redundancy for the redirect server.
- Value
 - Y—Enables redundancy
 - N—Specifies that only a single redirect server is used
- Default—N

monitor.host

- IP address or hostname for the redundant redirect server.
- Value—Fully qualified IP address or string
- Default—No value

monitor.virtuallp

- Configures virtual IP address of the redirect server. You must configure primary and redundant redirect servers to share this address under a common name in the DNS. Clients access the redirect server through this virtual IP address.
- Value—Fully qualified IP address
- Default—192.168.254.1

monitor.reallp

- Real IP address of the redirect server. When a primary redirect server is started, it dynamically establishes and maintains a static route on the client router to which it connects. The static route directs traffic destined for the virtual IP address of the server to the real IP address of the active redirect server.
- Value—Fully qualified IP address
- Default—Host IP address

monitor.master

- Specifies whether the redirect server identified in *monitor.realIP* is the primary redirect server.
- Value—Y or N
- Default—Y

monitor.checkInt

- Interval at which the redirect server polls the redundant redirect server.
- Value—Number of seconds in the range 60/< clientRate > –2147483647
where < clientRate > is the number of requests per minute that the redirect engine accepts from one client
- Guidelines—Specifying a shorter time in the range leads to faster detection of problems and results in higher consumption of CPU resources.
- Default—30

ldap.url

- List of the URLs for directories employed by the redirect server.
- Value—Text string consisting of acceptable LDAP URLs in the format
`ldap://<host>:<portNumber>`
 where <host> is the IP address or hostname of the directory host and
 <portNumber> is the TCP port
- Default—`ldap://localhost`

ldap.binddn

- Distinguished name (DN) that the redirect server uses to authorize connections to the directory.
- Value—Text string in LDAP format
- Default—`cn = ssp, ou = components, o = operators, o = umc`

ldap.bindpw

- Password that the redirect server uses to bind to the directory.
- Value—Text string
- Default—`ssp`

ldap.basedn

- Base DN that is the root of the directory tree.
- Value—Text string in LDAP format
- Default—`o = umc`

monitor.vrs

- Comma-separated list of virtual routers to which the redirect server connects.
- Value—Text string in the format
`<vrName>@<routerName>,<vrName>@<routerName>`
 where <vrName> is the name of the virtual router and <routerName> is the
 name of the router on which the VR is configured
- Default—No value

dns.enable

- Controls the DNS server that is included with the redirect server.
- Value
 - Y—Starts the DNS server (only if proxy support is enabled)
 - N—Disables the DNS server
- Guidelines—Use this property only if you want to use the DNS server that is included with the redirect server. If you want to use another DNS server, do not enable the DNS server included with redirect server.
- Default—Y

dns.errorip

- IP address that is returned when a DNS request results in an unknown name (NXDOMAIN) error.
- Value—Fully qualified IP address
- Default—192.168.254.2

dns.forwarder

- DNS servers to which requests are forwarded.
- Value—Text string consisting of fully qualified IP addresses separated by commas
- Default—No value

dns.tcpport

- TCP port on which the DNS server listens.
- Value—Integer; valid port number in the range 1024–65535
If you set the value to 0, no TCP socket is opened.
- Default—8853

dns.udpport

- UDP port on which the DNS server listens.
- Value—Integer; valid port number in the range 1024–65535
If you set the value to 0, no UDP socket is opened.
- Default—8853

agent.path

- Path to the SNMP agent.
- Value— < directory path >
- Guidelines—If you install SRC components into the default directory structure, you do not need to change this value. You can change this value only by editing the */opt/UMC/redirect.properties* file.
- Default—.../agent/var

redir.refresh

- Specifies whether the redirect server sends an HTTP 200 OK response or an HTML document that includes the `< HTTP-Equiv = "Refresh" >` header to a subscriber's browser in response to a captured request.
- Value
 - Y—Sends an HTTP 200 OK response with an HTML document that includes the `< HTTP-Equiv = "Refresh" >` header to a subscriber's browser in response to a captured request.
 - N—Sends an HTTP 302 Found response to a subscriber's browser in response to a captured request.
- Guidelines—By selecting Y, the load on the Web server is decreased because non-browser (or non-HTML) client applications that use HTTP do not follow this refresh message; however, most client applications do follow HTTP 302 messages.
- Default—Y

redir.refreshDoc

- Directory path to a local HTML file that the redirect server returns to a subscriber's browser in response to a captured request.
- Value—`< path to HTML file >`
- Guidelines—This property is used only if the `redir.refresh` property is set to Y. If you enter an invalid path, the redirect server uses a default file. This file can contain the string `"%(url)s"` which is replaced with the URL of the local HTML file to be returned to the subscriber's browser.
- Default—`etc/refresh.html`

Configuring Logging for Redirect Server

The redirect server logs incoming HTTP requests through the UNIX **syslog** command with a priority of INFO and log facility of LOCAL7. See *SRC-PE Monitoring and Troubleshooting Guide, Chapter 4, Configuring Logging for SRC Components on a Solaris Platform* for information about system logging.

Changing the Configuration for Redirect Server

If you change values set in the `/opt/UMC/redir.properties` file, restart redirect server.

To restart redirect server:

1. Stop redirect server:

```
/etc/rc2.d/S99UMCredirect stop
```

2. Start redirect server:

```
/etc/rc2.d/S99UMCredirect start
```

Part 4

**Designing Services for Enterprise
Manager Portal**

Chapter 22

Reviewing and Configuring Policies and Services for Enterprise Manager Portal

This chapter provides a high-level overview of the tasks to provision services that service providers make available through Enterprise Manager Portal application. The chapter contains the following sections:

- Overview of Services for Enterprise Manager Portal on page 375
- Before You Configure Services for Enterprise Manager Portal on page 377
- Configuring Firewall Policies and Services for Enterprise Manager Portal on page 377
- Configuring NAT Policies and Services for Enterprise Manager Portal on page 386
- Configuring Bandwidth Policies and Services for Enterprise Manager Portal on page 388
- Enabling Schedules for Subscriptions for Enterprise Manager Portal on page 396
- Configuring VPNs for Enterprise Manager Portal on page 396
- Billing Subscribers Through SCU/DCU for JUNOS Routing Platforms on page 398

Overview of Services for Enterprise Manager Portal

Enterprise Manager Portal is an application that lets service providers provision services for enterprise subscribers. For more information about Enterprise Service Manager, see *Chapter 29, Managing Services with Enterprise Manager Portal*.

Enterprise Manager Portal can apply the types of services listed in Table 28 to enterprise traffic as specified on JUNOS routing platforms or JUNOSe routers.

Table 28: Services Available from Enterprise Manager Portal

Types of Service	Types of Router
Firewalls—stateful or stateless	JUNOS routing platforms
Network Address Translation (NAT)	JUNOS routing platforms
Bandwidth on demand (BoD)	JUNOS routing platforms or JUNOSe routers
BoD for traffic routed to specified layer 3 VPNs	JUNOS routing platforms

The service provider uses services and policies in the SRC directory to manage traffic on a JUNOS routing platform or on a JUNOSe router. IT managers in enterprises that are customers of the service provider subscribe to these services through Enterprise Manager Portal.

Some of the services and policies are defined in the sample data and require little or no customization. You can, however, create some new services and policies, such as those for BoD.

Directory Structure

Use the directory structure in the sample data to organize services and policies. The following list shows the location of the policies and services in the directory:

- Services—*l = entJunos, o = Scopes, o = umc*
- Policies—*ou = entJunos, o = Policies, o = umc*

Although the scope that includes services for Enterprise Manager Portal is named *entJunos*, the policies for the BoD services have policy rules for both JUNOSe routers as well as JUNOS routing platforms.

Priorities for Subscriptions

Each subscription to a service has a priority that is identified by a service parameter named *priority*. A subscription with a lower priority setting takes precedence over a subscription with a higher priority setting. The SAE uses the priorities to determine the order in which it applies subscriptions to a particular type of service to traffic. For example, if the same traffic is affected by subscriptions to several firewall services on a JUNOS routing platform, the SAE applies those subscriptions in a prioritized order. Priorities of different types of service are independent of each other; for example, for JUNOS routing platforms, priorities of NAT services are independent of priorities for BoD services.

Depending on the type of service, you must specify either an explicit priority or a range of priorities in the service or the policy rules. When you specify a range of priorities, the IT manager selects an explicit priority in this range through Enterprise Manager Portal. The sample data includes definitions of priorities for each type of service; however, you can modify the priorities if you want to provide different ranges of priorities.

A substitution in a subscription provides the value for the service parameter named priority. This parameter is in the precedence policy rule field to control the ordering of policies when a subscription is activated.

Before You Configure Services for Enterprise Manager Portal

Before you configure services for use by Enterprise Manager Portal:

1. Install the SRC software, and configure the SAE (see *SRC-PE Getting Started Guide, Chapter 28, Installing the SRC Software on a Solaris Platform* and *SRC-PE Getting Started Guide, Chapter 30, Setting Up an SAE on a Solaris Platform*).
2. If you are managing services on JUNOS routing platforms, configure the JUNOS routing platform, and enable it to interact with the SRC software (see the JUNOS documentation set and *SRC-PE Network Guide, Chapter 9, Locating Subscriber Information with the NIC*).
3. If you are managing services on JUNOSe routers, configure the JUNOSe router, and enable it to interact with the SRC software (see the JUNOSe documentation set and *SRC-PE Network Guide, Chapter 5, Using JUNOSe Routers in the SRC Network with the SRC CLI* or *SRC-PE Network Guide, Chapter 6, Using JUNOSe Routers in the SRC Network with a Solaris Platform*).
4. Install the sample data (see *SRC-PE Getting Started Guide, Chapter 29, Defining an Initial Configuration on a Solaris Platform*).
5. For prerequisites to using policy rules on JUNOS routing platforms and JUNOSe routers, see *SRC-PE Services and Policies Guide, Chapter 6, Policy Management Overview*.
6. For general information about configuring services, see *SRC-PE Services and Policies Guide, Chapter 1, Managing Services with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 2, Managing Services on a Solaris Platform*.

Configuring Firewall Policies and Services for Enterprise Manager Portal

The SRC software represents a JUNOS firewall as two types of SRC services:

- Basic firewall service—Defines the action that the firewall takes and specifies the types of traffic that the firewall affects.
- Services to provide firewall exceptions—Defines exception rules to block traffic that otherwise would be permitted to traverse the firewall, or to admit traffic that would otherwise be blocked. Exceptions specify criteria against which packets and application flows are inspected.

For example, to configure an access only to accept e-mail from a specific IP address, you can use a basic firewall service that blocks all incoming and outgoing traffic; then you can use a firewall exception that allows incoming e-mail traffic from that IP address.

The SRC software supports the following types of firewalls on JUNOS routing platforms:

- Stateless firewalls—Inspect each packet in isolation; do not evaluate the traffic flow.
- Stateful firewalls—Inspect track traffic flows and conversations between applications, and evaluate this information when applying exception rules to the traffic.

An application is typically associated with a stateful firewall rule. After a flow or conversation meets firewall criteria, packets in that flow can pass through the firewall. For example, when an FTP control connection requests a file download, the stateful firewall knows to expect and allows a TCP data connection to start.

The same criteria may not be applied to each packet. For example for a TCP application, the criteria changes when a new TCP session is initiated to allow subsequent packets in the flow.

You can make either stateless firewalls or stateful firewalls available from Enterprise Manager Portal.

Overview of Basic Firewall Services and Policies

You can create as many basic firewall services in the directory as you want. Table 29 shows the names of the services and policies associated with the basic firewall services in the sample data.

Table 29: Basic Firewall Services and Policies

Name of Service	Name of Policy Group	Function of Firewall
BrickWall	brickwall	Blocks all incoming and outgoing traffic
EmailAndWeb	emailweb	Blocks all incoming traffic and allows only outgoing e-mail and HTTP traffic
Multiservice	multiservice	Blocks all incoming traffic and allows outgoing e-mail, HTTP, FTP, telnet, and Real-Time Streaming Protocol (RTSP) traffic

The services are located under *l = entjunos*, *o = Scopes*, *o = umc* in the sample data.

The policies are located under *ou = entjunos*, *o = Policies*, *o = umc* in the sample data.

You can use these services and their associated policies as a starting point for developing your own basic firewall services.

Tasks to Configure Firewall Policies and Services

The tasks to configure policies and services for firewalls are:

1. Configuring Basic Firewall Policies on page 379
2. Configuring Basic Firewall Services on page 380
3. For stateful firewalls:
 - a. Reviewing the fwrule Policy Group for Exceptions to Stateful Firewalls on page 380
 - b. Reviewing the FirewallRule Service for Exceptions to Stateful Firewalls on page 380
4. For stateless firewalls:
 - a. Reviewing Services for Exceptions to Stateless Firewalls on page 381
 - b. Parameter Values Used by Services for Exceptions to Stateless Firewalls on page 382
 - c. Planning Services for Custom Firewall Exceptions on page 382
 - d. Configuring Policies for Custom Firewall Exceptions on page 383
 - e. Configuring Services for Custom Firewall Exceptions on page 384

Configuring Basic Firewall Policies

You can create policies from Policy Editor. For information about creating firewall policies, including prerequisites on the JUNOS routing platform, see *SRC-PE Services and Policies Guide, Chapter 11, Configuring and Managing Policies with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 7, Using Policy Editor*.

To create a basic firewall policy:

1. Create a policy group and associated policy rules in *ou = entjunos, o = Policies, o = umc*.
2. Specify a precedence for the policy rules.

All basic firewall services should have a similar value that is higher than the range of precedences you configure for firewall exceptions. In the sample data, we use precedences of 600 and 601 for basic firewall policies.

Ensure that the precedence for basic firewall policies integrate with other policies that affect the same traffic. See *Configuring Priorities for Stateless or Stateful Firewall Services* on page 384.

For a sample basic firewall policy, see *policyGroupName = brickwall, ou = entjunos, o = Policies, o = umc* in the sample data.

Configuring Basic Firewall Services

You can create services from SDX Admin. For information about creating services in SDX Admin, see *SRC-PE Services and Policies Guide, Chapter 11, Configuring and Managing Policies with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 7, Using Policy Editor*.

To create a basic firewall service:

1. Create a service.
2. Specify the following values for the service:
 - Category—Text string basicFirewall (service's LDAP attribute sspCategory)
 - Description—Summary of what the firewall service does (service's LDAP attribute description)

This description will appear on the portal, and subscribers will use the description to select a firewall service. Although there is no upper limit for the length of this attribute, the portal will display the text in one paragraph.
 - Policy Group—Policy group configured for use with this service

For a sample firewall service, see *serviceName = BrickWall, l = entJunos, o = Scopes, o = umc* in the sample data.

Reviewing the fwrule Policy Group for Exceptions to Stateful Firewalls

The policy group *policyGroupName = fwrule, ou = entJunos, o = Policies, o = umc* is predefined in the sample data. Do not modify any settings or substitutions for this service.

Reviewing the FirewallRule Service for Exceptions to Stateful Firewalls

The SRC sample data provides one service for firewall exceptions, *serviceName = FirewallRule, l = entJunos, o = Scopes, o = umc*, that is designed to work with Enterprise Manager Portal. Do not modify the definition for this service or its associated policy.

You can modify the allowed priority ranges for the service. See *Configuring Priorities for Stateless or Stateful Firewall Services* on page 384.

Each subscription to this service adds a rule to the stateful firewall. The FirewallRule service and its associated policy are general and contain many parameters, such as the priority of the firewall exception and the action that the firewall should take. IT managers supply actual values for these parameters through Enterprise Manager Portal.

You can modify the priority ranges for this policy group if necessary; do not modify any other settings. The values for these parameters must be lower than the precedence settings for the policy rules in the basic firewall policy groups. This distinction allows the firewall exception to take priority over the basic firewalls. In the sample data, the FirewallRule service has priorities in the range 500–579.

Reviewing Services for Exceptions to Stateless Firewalls

Review the services that Enterprise Manager Portal requires to ensure that configuration of these services works in your environment. These services are firewall exceptions—services that define the types of traffic that a firewall admits or blocks.

Enterprise Manager Portal requires that specific services be configured to cover each of the following traffic actions:

- Allow
- Reject
- Discard

These actions are required for each traffic direction; that is, traffic:

- Entering the network
- Exiting the network
- Entering and exiting the network

Table 30 lists the names of services required by Enterprise Manager Portal. The naming convention for the services specifies both action and direction; for example, for the FWR_Fwd_Out service:

- Action—allow (forward)
- Direction—Outgoing (from the enterprise)

Services configured to reject traffic return a “network-unreachable” ICMP message.

Table 30: Stateless Firewall Services in Sample Data

	Traffic Entering the Enterprise	Traffic Exiting from the Enterprise	Traffic Entering and Exiting the Enterprise
Traffic Allowed	FWR_Fwd_In	FWR_Fwd_Out	FWR_Fwd_Both
Traffic to Be Discarded	FWR_Filter_In	FWR_Filter_Out	FWR_Filter_Both
Traffic Rejected	FWR_Rej_In	FWR_Rej_Out	FWR_Rej_Both

The services are located under *l = entJunosStatelessFW*, *o = Scopes*, *o = umc* in the sample data. These services and the associated policies configured in the sample data are designed for a subscriber-facing interface on a provider edge device.

In most cases you can use the services as configured. If needed—for example, for a service provider-facing interface in a customer edge device—you can customize the services listed in Table 30, but do not change the names.

To customize services for an enterprise-facing interface, change the configuration for:

- Source IP addresses and ports
- Destination IP addresses and ports

You can also create services that provide custom exceptions to a firewall. Portal users can select custom exceptions under Firewall actions on the Firewall page in Enterprise Manager Portal.

Parameter Values Used by Services for Exceptions to Stateless Firewalls

Table 31 lists the parameters for which Enterprise Manager Portal provides values. The parameter names start with “fw” (service’s LDAP attribute parameterSubstitution). The services listed in *Before You Configure Services for Enterprise Manager Portal* on page 377 use these parameters.

Table 31: Parameters for Stateless Firewall Services for Enterprise Manager Portal

To Specify this Value	Use This Parameter
Protocol	fwProtocol
Source network	fwSrcIp
Source port	fwSrcPort
Destination network	fwDestIp
Destination port	fwDestPort
TOS byte	fwTosByte
TOS byte mask	fwTosByteMask
TCP flags	fwTcpFlags
TCP flags mask	fwTcpFlagsMask
IP flags	fwIpFlags
IP flags mask	fwIpFlagsMask
Fragmentation offset	fwIpFragOffset
ICMP type	fwIcmpType
ICMP code	fwIcmpCode
Packet length	fwPacketLength

Planning Services for Custom Firewall Exceptions

Typically, you use custom exceptions to provide bandwidth management as well as firewall exceptions. Using custom exceptions that do both simplifies the way you integrate BoD and firewall services. For example, you can create custom exceptions to police traffic or to assign a traffic class to the traffic and to specify firewall behavior.

See examples of services for custom exceptions in the sample data:

- `l = Limit1Mbs, l = entJunosStatelessFW, o = Scopes, o = umc`
- `l = Limit2Mbs, l = entJunosStatelessFW, o = Scopes, o = umc`
- `l = Limit5kbs, l = entJunosStatelessFW, o = Scopes, o = umc`

The sample services and the associated policies are designed for a subscriber-facing interface on a provider edge device. When you create policies, policy direction (input or output) can map to incoming or outgoing traffic depending on whether the SRC-managed interface is a subscriber-facing interface on a service provider edge device, or a service-provider facing interface on the customer edge device in an enterprise. When you configure policies for services designed for use through the Enterprise Management Portal, you typically assume that:

- Source IP addresses and ports are inside an enterprise
- Destination IP addresses and ports are outside an enterprise

Configuring Policies for Custom Firewall Exceptions

You can create policies from Policy Editor. For information about creating policies in Policy Editor, see *SRC-PE Services and Policies Guide, Chapter 11, Configuring and Managing Policies with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 7, Using Policy Editor*. For information about managing policies, see *SRC-PE Services and Policies Guide, Chapter 6, Policy Management Overview*.

To configure a policy for a custom firewall exception:

1. Create a stateless firewall policy group and associated policy rules.
2. Specify parameters for the following properties for each policy rule:
 - IP protocol
 - TOS byte in the IP header
 - Source IP addresses
 - Source TCP/UDP ports
 - Destination IP addresses
 - Destination TCP/UDP ports
 - TCP flags
 - IP flags (fragmentation flags)
 - Fragmentation offset
 - Packet length

- ICMP type
- ICMP code

For a sample policy, see *policyGroupName = custom_policer*,
ou = entjunos_statelessfw, *o = Policies*, *o = umc* in the sample data.

Configuring Services for Custom Firewall Exceptions

You can create services from SDX Admin. For information about creating services in SDX Admin, see *SRC-PE Services and Policies Guide, Chapter 1, Managing Services with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 5, Scheduling Services on a Solaris Platform*. You can create services that take actions such as those listed in Table 30.

To configure a service for a custom firewall exception:

1. Create a service for each traffic action listed in Table 30. Specify a name that provides meaningful information to a user, including information about the forwarding treatment for traffic. The name appears in the Firewall Action field on the Firewall tab in Enterprise Manager Portal.
2. Specify the following values for the service:
 - Category—customFWRule (the service's LDAP attribute sspCategory)
 - Policy Group—Policy group that supports custom firewall exceptions
3. Specify substitutions for the service.

Configuring Priorities for Stateless or Stateful Firewall Services

If you design services to be accessed from Enterprise Manager Portal, you can configure ranges of priority values that are enterprise specific and ranges that are available to a number of enterprises. Setting the two ranges makes it possible for a service provider to specify firewall exceptions that an IT manager in an enterprise cannot override.

Configuring Priorities to Have Enterprise Services Work Together

You can configure the parameters in the following list as global parameters that apply to all subscribers, and as subscriber-specific parameters. If you configure both, the global range takes precedence over a subscriber-specific limit.

- fwMinPriority—Specifies the lower limit of the range of precedences available for subscriptions to firewall exceptions.
- fwMaxPriority—Specifies the upper limit of the range of precedences available for subscriptions to firewall exceptions.
- fwEnterpriseMinPriority—Specifies the lower limit of the range of precedences that an enterprise-specific manager can make available for subscriptions to firewall exceptions.

- `fwEnterpriseMaxPriority`—Specifies the upper limit of the range of precedences that an enterprise-specific manager can make available for subscriptions to firewall exceptions.

Ensure that:

- `fwMaxPriority` is greater than or equal to `fwEnterpriseMaxPriority`
- `fwEnterpriseMaxPriority` is greater than `fwEnterpriseMinPriority`
- `fwEnterpriseMinPriority` is greater than or equal to `fwMinPriority`

Configuring Global Priority Ranges from Policy Editor

Before you configure the global priority range, make sure that the sample data for Enterprise Manager Portal is loaded. If the sample data is not available, you must create a parameter similar to `fwEnterpriseMinPriority`.

To configure priorities for firewall policy rules from Policy Editor:

1. In Policy Editor, in the navigation pane select **Parameters**.
2. Under Parameters, select a priority, such as `fwEnterpriseMinPriority`, and on the General tab change the value for Default Value.

Configuring Global Priority Ranges from SDX Admin

Before you configure the global priority range, make sure that the sample data for Enterprise Manager Portal is loaded. If the sample data is not available, you must create a parameter similar to `fwEnterpriseMinPriority` in Policy Editor.

To configure priorities for firewall services from SDX Admin:

1. In SDX Admin, in the navigation pane select **Parameters**.
2. Under Parameters, select a priority, such as `fwEnterpriseMinPriority`, and on the Main tab change the value for Default Value.

Configuring Priorities for Individual Scopes by Defining Them in Services

You can use parameters to limit priority ranges for services within a scope. For stateful firewall services, you set parameters to limit priority ranges in the `FirewallRule` service. For stateless firewall services, you set parameters to limit priority ranges in the `FRW_Filter_Both` service.

You can use parameters to limit priority ranges for services within a scope in addition to using global ranges. For example, you can define a global range, and then define a different range that overrides the global range for specified subscribers.

To allow priority values for services in one scope to override the priority values for services in another scope:

1. In a service that resides in a service scope that has a low precedence (indicated by a higher number), define default values for parameters that limits a priority range.

2. Attach this scope to an entry at a high level in the subscriber folder; for example, to a retailer.
3. Create a second scope that has a higher precedence.
4. Create a service that uses parameters to limit priority ranges in the second scope.
5. Attach the second scope (which has a higher precedence) to the enterprise.

The services with the higher precedence override the services with a lower precedence.

Using Stateless Firewall and BoD Applications Together

In most cases, you can use the services listed in Table 30 on page 381 to provide bandwidth management and firewall support. However, if you want to design special services to have firewalls work with BoD services, use the following guidelines to design your services:

- Specify a higher priority in the BoD policies.
- Specify next-rule actions for the BoD policies.

After all the BoD policy rules are applied, the stateless firewall policy rules are applied. Packets are forwarded or dropped as appropriate.

Configuring NAT Policies and Services for Enterprise Manager Portal

The NAT policy groups and services provided in the sample data are designed to work with Enterprise Manager Portal and require little configuration. Table 32 shows the names of the policy groups and services associated with each type of NAT that the SRC software supports.

Table 32: NAT Services and Policies

Type of NAT	Name of Policy Group	Name of Service
Dynamic source NAT	dynsrcnat	DynSrcNat
Static destination NAT	staticdstnat	StaticDstNat
Static source NAT	staticsrcnat	StaticSrcNat

The services are located under *l = entjunos*, *o = Scopes*, *o = umc* in the sample data.

The policies are located under *ou = entjunos*, *o = Policies*, *o = umc* in the sample data.

For information about creating NAT policies, including prerequisites on the JUNOS routing platform, see *SRC-PE Services and Policies Guide, Chapter 1, Managing Services with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 2, Managing Services on a Solaris Platform*.

Configuring the dynsrcnat Policy Group

You can modify the precedence settings in the policy rules for the dynsrcnat policy group. Use the following guidelines if you make changes to the precedence settings:

- The precedence settings for the policy rules in the dynsrcnat policy group must be higher than the precedence settings for the policy rules in the staticsrcnat policy group. This distinction allows static source NAT rules to take priority over dynamic source NAT rules.
- The value for this setting must be higher than the precedence of any firewall exception. This distinction ensures that the SAE activates the artificial firewall rule first.

Reviewing the DynSrcNat Service

The DynSrcNat service is predefined in the sample data. Do not modify any settings or substitutions for this service.

Configuring the staticdstnat Policy Group

This policy group contains two policy rules:

- SFWR —Acts as an artificial firewall rule that ensures that the SAE activates a basic firewall service for the access before activating a NAT service; the JUNOS software requires that a firewall be active before you implement a NAT rule.
- PR—Defines the policy for the static destination NAT service.

The only setting you can modify for this policy group is the precedence setting for the SFWR policy rule. The value for this setting should be higher than the precedence of any other firewall exception. This distinction ensures that the SAE activates the artificial firewall rule first.

Configuring the StaticDstNat Service

You can modify the following substitutions for the StaticDstNat service; do not modify any other settings for this service.

- staticDestNatMinPriority—Lower limit of the range of precedences available for subscriptions to static destination NAT rules
- staticDestNatMaxPriority—Upper limit of the range of precedences available for subscriptions to static destination NAT rules

Configuring the staticsrcnat Policy Group

This policy group contains two policy rules:

- SFWR—Acts as an artificial firewall rule that ensures that the SAE activates a basic firewall service for the access before activating a NAT service; the JUNOS software requires that a firewall be active before you implement a NAT rule.
- PR—Defines the policy for the static source NAT service.

The only setting you can modify for this policy group is the precedence setting for the SFWR policy rule. The value for this setting should be higher than the precedence of any other firewall exception. This distinction ensures that the SAE activates the artificial firewall rule first.

Configuring the StaticSrcNat Service

You can modify the following substitutions for the StaticSrcNat service; do not modify any other settings or substitutions for this service.

- staticSrcNatMinPriority—Lower limit of the range of precedences available for subscriptions to static source NAT rules
- staticSrcNatMaxPriority—Upper limit of the range of precedences available for subscriptions to static source NAT rules

The values for these parameters must be lower than the precedence settings for the policy rules in the dynsrcnat policy group. This distinction allows static source NAT rules to take priority over dynamic source NAT rules.

Configuring Bandwidth Policies and Services for Enterprise Manager Portal

You can make bandwidth available on demand to IT managers by creating the following types of services:

- Basic BoD service—Specifies the bandwidth level available to an access link.
- BoD service—Classifies traffic and assigns a service level that specifies the forwarding treatment for the traffic class.

BoD and basic BoD services allow billing for subscriptions to supplementary services.

You can create services to provide JUNOS class of service (CoS) or JUNOSe quality of service (QoS) by configuring BoD and basic BoD services that interact with each other. You can provide different service levels to different traffic by specifying traffic classification criteria.

You can create any number of basic BoD services and any number of BoD services. Only one basic BoD service, but numerous BoD services can be assigned to an access link.

BoD services can be configured to provision bandwidth provided by basic BoD services for a link. For example, you could provide a basic BoD service that provides 1 Mbps to the access link, and two video services as BoD services, each with different characteristics.

When you configure BoD and basic BoD services, they are available to IT managers through Enterprise Manager Portal. For information about how IT managers configure BoD and basic BoD services through Enterprise Manager Portal, see *Chapter 28, Managing Enterprise Service Portals*.

Parameter Values Used by BoD Services

Table 33 lists the parameters for which Enterprise Manager Portal provides values. The parameter names start with “bod” (service’s LDAP attribute parameterSubstitution).

Table 33: Parameters for BoD Services for Enterprise Manager Portal

To Specify This Value	Use This Parameter
Protocol	bodProtocol
TOS byte	bodTosByte
TOS byte mask	bodTosByteMask
Source network	bodSrcIp
Source port	bodSrcPort
Destination network	bodDestIp
Destination port	bodDestPort
TCP flags	bodTcpFlags
TCP flags mask	bodTcpFlagsMask
IP flags	bodIpFlags
IP flags mask	bodIpFlagsMask
Fragmentation offset	bodIpFragOffset
Packet length	bodPacketLength
ICMP type	bodIcmpType
ICMP code	bodIcmpCode

Bandwidth Policies for Different Routing Platforms

If you support environments that include both JUNOS routers and JUNOS routing platforms, you can configure policies to have policy rules for JUNOS filters and JUNOS filters. This way, if the service is activated on a JUNOS router, the JUNOS rule is used, and if the service is activated on a JUNOS routing platform, the JUNOS policies are used.

When Enterprise Manager Portal has JUNOS compatibility enabled, the portal allows:

- Single subnets for source and destination addresses
- Single ports or single port ranges for source and destination ports

In addition, with JUNOS compatibility enabled, Enterprise Manager Portal does not show the following configuration fields for BoD services:

- TCP flags
- IP flags
- Fragment offset
- Packet length
- ICMP type
- ICMP code

You should be familiar with the types of bandwidth management policies available for the type of router for which you are configuring policies. See *SRC-PE Services and Policies Guide, Chapter 6, Policy Management Overview*.

Configuring Basic BoD Policies

You can create policies from Policy Editor. For information about creating policies in Policy Editor, see *SRC-PE Services and Policies Guide, Chapter 11, Configuring and Managing Policies with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 7, Using Policy Editor*.

To configure a basic BoD policy:

1. Create a policy group and associated policy rules.

Typically the policy rules include JUNOS schedulers, JUNOS policers, JUNOS filters, or JUNOS filters that specify a traffic classification, and basic rules that define best-effort forwarding and drop behavior.

2. Include parameters in the classify-traffic conditions of the policer. Use parameter names from Table 33 on page 389.
3. Specify a precedence for the policy rules.

Structure the precedence for policies to ensure that policy rules for JUNOS schedulers and JUNOS policers have a higher precedence, and therefore a lower number, than default policy rules. If the configuration includes BoD services, the policies to support BoD services should have a higher precedence, indicated by a lower number.

For a sample basic BoD policy, see *policyGroupName = basicBod*, *ou = entjunos*, *o = Policies*, *o = umc* in the sample data.

Configuring Basic BoD Services

You can create services from SDX Admin. For information about creating services in SDX Admin, see *SRC-PE Services and Policies Guide, Chapter 1, Managing Services with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 2, Managing Services on a Solaris Platform*.

Basic BoD services do not have service parameters.

To configure a service that uses basic BoD:

1. Create a service.
2. Specify the following values for the service:
 - Category—basicBod (service's LDAP attribute sspCategory)
 - Description—Description of the bandwidth provided by the service

If you plan to integrate a basic BoD service with a BoD service, the description for each basic BoD service should explain the bandwidth provided, and the relationship between this bandwidth level and the BoD service. The description should also explain the relationship between the service name, which is shown on the portal in the Bandwidth Level list, and the bandwidth provided. For example, for a service named 1 Mbps, the bandwidth provided could be 1 Mbps downstream and 500 Kbps upstream.

This description will appear in the online help for Bandwidth Level in Enterprise Manager Portal. Although there is no limit for the length of the text entered, the portal displays the text in one paragraph.

- Policy Group—Policy group that supports basic BoD services

For a sample BoD service, see *serviceName = 1.0 Mbps, l = EntJunos, o = Scopes, o = umc* in the sample data.

Configuring BoD Policies

When configuring BoD policies, you create rules that classify traffic. Make sure that the source and destination policy rules correspond to location of the enterprise relative to the subscriber interface that the SRC software manages. When configuring Enterprise Manager Portal, you follow the same rules for defining source and destination fields. See *SRC-PE Services and Policies Guide, Chapter 11, Configuring and Managing Policies with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 7, Using Policy Editor*.

You can create policies from Policy Editor. For information about creating policies in Policy Editor, see *SRC-PE Services and Policies Guide, Chapter 7, Using Policy Editor*.

To configure a BoD policy:

1. Create a BoD policy group and associated policy rules.

You can create some policy rules as JUNOS filters and others as JUNOSe filters.

Specify values or parameters for the following for each policy rule for the BoD service:

- TOS byte in the IP header
- Mask used for the ToS byte

- Source TCP/UDP port
 - Destination TCP/UDP port
 - IP address of source
 - IP address of destination
 - TCP flags
 - Fragmentation flags
 - Fragmentation offset
 - ICMP type
 - ICMP code
2. Specify a precedence for the policy rules.

If the configuration includes basic BoD services, the policies to support basic BoD services should have a lower precedence, indicated by a higher number.

For information about policy rules and precedences, see *See SRC-PE Services and Policies Guide, Chapter 11, Configuring and Managing Policies with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 7, Using Policy Editor*.

For a sample BoD policy, see *policyGroupName = bod, ou = entjunos, o = Policies, o = umc* in the sample data. In the sample BoD policies, substitutions in services rename policy parameters to names required by Enterprise Manager Portal.

The sample data is based on a scenario that has the SRC managed interface on a device with egress to the access link that leads to the enterprise.

Configuring BoD Services

You can create services from SDX Admin. For information about creating services in SDX Admin, see *SRC-PE Services and Policies Guide, Chapter 1, Managing Services with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 2, Managing Services on a Solaris Platform*.



NOTE: If you configure BoD services that use forwarding classes, take into consideration the number of forwarding classes supported on the router.

To configure a service for BoD:

1. Create a service.
2. Specify the following values for the service:
 - Category—bod (service's LDAP attribute sspCategory).

- **Description**—Description of how this service will affect traffic.

If you plan to integrate a basic BoD service with a BoD service, the description for each BoD service should take into consideration how the BoD service interacts with any basic BoD service selected. The description should also provide information about the forwarding treatment for traffic.

This description will appear in the online help for BoD services in Enterprise Manager Portal. Although there is no upper limit for the length of this attribute, the portal will display the text in one paragraph.

- **Substitutions**—Substitutions for the parameter names; these names start with “bod” (service’s LDAP attribute parameterSubstitution).

Note that the actual parameter names are required to be the service parameter names for Enterprise Manager Portal.

- **Policy Group**—Policy group that supports BoD services.

For a sample BoD service, see *serviceName = Gold, l = entJunos, o = Scopes, o = umc* in the sample data.

Using BoD Services to Assign Traffic to Bandwidth Categories

You can use BoD services to assign different classes of traffic to different bandwidth categories, with each category identified by a specified quantity of bandwidth.

For example, a configuration could provide two services:

- Silver—Bandwidth of 500,000 Mbps
- Gold— Bandwidth of 1,000,000 Mbps

Each service has the specified bandwidth available to specified traffic flows, based on the policy rules for traffic classification and policing.

Using BoD and Basic BoD Services Together to Supply Class of Service

You can use BoD and basic BoD services together to provide more sophisticated bandwidth level management to IT managers. For example, you can integrate these types of services to take advantage of the CoS features available on JUNOS routing platforms.

On the JUNOS routing platform, policers are applied before schedulers. The type of service defined by these settings is applied to traffic exiting from the JUNOS routing platform. For information about policing, scheduling, and queuing traffic on the JUNOS routing platform, see *JUNOS Network Interfaces and Class of Service Configuration Guide*.

If you want to integrate basic BoD services and BoD services, you can base your configuration on the implementation in the sample data. The sample services and data are designed to work with Enterprise Manager Portal and require little configuration.

You can also create a configuration to meet requirements specific to your environment. If you want to create a configuration that has both basic BoD and BoD services, carefully plan services and associated policies. Ensure that the bandwidth requirements for BoD services are in proportion to the bandwidth provided by the basic BoD services. See *Setting Up Forwarding Preferences—Example 2* on page 395 for another way to provide BoD to IT managers.



NOTE: When configuring services to use JUNOS CoS, take into consideration which interfaces on the router support CoS.

Setting Up Forwarding Preferences—Example 1

The sample data provides an implementation that supports CoS features on the JUNOS routing platform. This implementation provides:

- Basic BoD services to apply a JUNOS policer only to best-effort traffic
- BoD services to assign traffic to forwarding classes other than best-effort
- Policing for best-effort traffic

Table 34 lists the services and policies in the sample data. You can locate the services in *l = entjunos*, *o = Scopes*, *o = umc*. You can customize the policies and services as needed. For general information about configuring policies and services, see *Configuring Basic BoD Policies* on page 390 and *Configuring BoD Policies* on page 391.

Table 34: Integrated BoD and Basic BoD Services in Sample Data

Name of Service	Category of Service	Name of Policy Group	Description of Service
1.0 Mbps	basic BoD	basic BoD	Specifies that a bandwidth of 1.0 Mbps be available to a specified access link for best-effort traffic.
3.0 Mbps	basic BoD	basic BoD	Specifies that a bandwidth of 3.0 Mbps be available to a specified access link for best-effort traffic.
5.0 Mbps	basic BoD	basic BoD	Specifies that a bandwidth of 5.0 Mbps be available to a specified access link for best-effort traffic.
Silver	BoD	BoD	Marks associated traffic as belonging to an assured forwarding class.
Gold	BoD	BoD	Marks associated traffic as belonging to an expedited forwarding class.

Billing can be established for traffic in the assured forwarding class and in the expedited forwarding class because the SRC software can account for traffic in each of these forwarding classes separately from other forwarding classes. Traffic in the assured forwarding class and in the expedited forwarding class is not included in the accounting data for the currently selected basic BoD service.

Setting Up Forwarding Preferences—Example 2

The following example shows another way to use BoD and basic BoD services to provide BoD services. In this example, a percentage of an access link's bandwidth is allocated to a specified service.

This configuration provides:

- Three bandwidth levels available to access links: 1.0 Mbps, 1.5 Mbps, and 2.0 Mbps.
- Three service levels defined to use a specified percentage of the bandwidth set for the access link: best effort 20 %, Silver 30 %, and Gold 50 %.

Each traffic class uses only the bandwidth assigned to it and does not share bandwidth with other traffic classes.

For an SRC configuration to support this scenario, you could create policies such as the following and assign these policies to services:

- Policies that provide a local policy parameter, *bw*, whose value is set by the service that references the policy:

For policy 1.0 Mb, *bw* = 1000000

For policy 1.5 Mb, *bw* = 1500000

For policy 2.0 Mb, *bw* = 2000000

- The transmission rate, bandwidth allocation, and priority scheduling for specified forwarding classes as shown in Table 35.

Table 35: Policies to Specify Forwarding Treatment for Specified Traffic Classes

Forwarding Class	Transmission Rate	Exact	Priority Scheduling
Best effort	$bw * 0.2$ bps	true	Low
Silver (assured forwarding)	$bw * 0.3$ bps	true	Medium
Gold (expedited forwarding)	$bw * 0.5$ bps	true	High

By setting *exact* to true, you can ensure that the sum of the transmission rates is less than the bandwidth allocated to the access link.

Enabling Schedules for Subscriptions for Enterprise Manager Portal

You can add schedules to subscriptions from Enterprise Manager Portal for subscriptions to BoD and firewall services that have scheduling enabled. To enable scheduling:

1. In SDX Admin, select the service to be scheduling-enabled.
2. In the Parameter tab, add the Substitution **isSchedulable = 1**.

This substitution lets enterprise subscribers configure schedules for subscribers to this service.

Configuring VPNs for Enterprise Manager Portal

You can use the SRC software to allow IT managers to manage layer 3 VPNs on JUNOS routing platforms. This type of VPN supports membership based on filter-based forwarding policies.

You can configure Enterprise Manager Portal to display VPN features. IT managers can modify VPNs and send traffic associated with BoD subscriptions to specific VPNs. In addition, if you configure Enterprise Manager Portal to display extranet features, IT managers with privileges to configure VPNs can create extranets for other enterprises and retailers by exporting those VPNs. Enterprises and retailers who share VPNs that other subscribers own are called *extranet clients*.

To provide VPN services from Enterprise Manager Portal, you create corresponding VPN versions of the BoD services and their associated policies.

Before You Configure VPN Policies and Services

When you configure the SRC software to manage VPNs, you must perform some additional tasks to those listed in *Before You Configure Services for Enterprise Manager Portal* on page 377:

1. Configure the VPNs on the JUNOS routing platform (see *JUNOS VPNs Configuration Guide*).

All routing instances that implement a specific VPN must have the same name.

2. Add the VPNs to the directory (see *Chapter 24, Adding VPNs from JUNOS Routing Platforms*).

The identifier for a VPN in the directory must match the name of the routing instance configured on the JUNOS routing platform (see Step 1).

3. If you want to send traffic associated with BoD services to specific VPNs, configure policies and services for BoD traffic destined for VPNs (see *Configuring Policies for BoD Traffic Destined for VPNs* on page 397 and *Configuring Services for BoD Traffic Destined for VPNs* on page 397).
4. Implement an addressing scheme for VPNs that allows extranet clients to access the VPNs (see *Implementing a Routing Scheme for VPNs* on page 406).

Configuring Policies for BoD Traffic Destined for VPNs

You can manage policies from Policy Editor. For information about creating policies in Policy Editor, see *SRC-PE Services and Policies Guide, Chapter 11, Configuring and Managing Policies with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 7, Using Policy Editor*.

To configure a policy for a BoD service associated with a VPN (a VPN policy):

1. Copy the policy for the BoD service in the directory.
2. Rename the policy you copied to a similar name that indicates this policy is the VPN version; for example, you can use `< bodPolicy > Vpn`, where `< bodPolicy >` is the name of the BoD policy.

For example, if the name of the original policy is `bod`, rename the service you copied to `bodVpn`.

3. Add a new local parameter (the name is arbitrary, for example `vpnName`) of type Routing Instance to the VPN policy.
4. Add a new action of type `RoutingInstanceAction` to the input policy rule, and specify a Routing Instance of `vpnName` for this action.
5. Save the VPN policy.

For a sample VPN policy, see `policyGroupName = bodVpn, ou = entjunos, o = Policies, o = umc` in the sample data. In the sample BoD policies, substitutions in services rename policy parameters to names required by Enterprise Manager Portal.

Configuring Services for BoD Traffic Destined for VPNs

You can manage services from SDX Admin. For information about creating services in SDX Admin, see *SRC-PE Services and Policies Guide, Chapter 22, Reviewing and Configuring Policies and Services for Enterprise Manager Portal*.

To configure a BoD service that will be associated with a VPN (a VPN service):

1. Copy the BoD service in the directory.
2. Rename the service you copied to `< bodService > _VPN`, where `< bodService >` is the name of the original BoD service.

For example, if the name of the original BoD service is called `Gold`, rename the service you copied to `Gold_VPN`.

3. Add to the VPN service a parameter with a name that matches the parameter of type Routing Instance that you defined in the policy (see Step 3 of *Configuring Policies for BoD Traffic Destined for VPNs* on page 397).

`!vpnName=bodVpnName`

4. Modify the VPN service to use the corresponding VPN policy that you created.
5. Save the service.

For a sample VPN service, see *serviceName = Gold_VPN*, *l = entJunos*, *o = Scopes*, *o = umc* in the sample data.

Billing Subscribers Through SCU/DCU for JUNOS Routing Platforms

All services that you configure for JUNOS routing platforms support billing that uses the source class usage (SCU) and destination class usage (DCU) features for egress traffic on the JUNOS routing platform. The SRC software supports this feature through the SAE and policy engine, which match source and destination classes in JUNOS policy rules. To enable SCU/DCU-based billing:

1. Configure the JUNOS routing platforms in the network to support SCU/DCU accounting, ensuring that all traffic is tagged with the appropriate classes.

The classes depend on the routes that the routers use to forward the traffic. For information about configuring SCU/DCU accounting with the JUNOS software, see the JUNOS documentation set.

2. Configure policies that match the source and destination classes you defined and that contain accounting rules.
3. Configure the services to which enterprises subscribe to use these policies.

For example, a service provider may want to bill local and long-distance traffic at different rates. The service provider could achieve this goal as follows:

1. Configure the JUNOS routing platform to tag traffic that exits the SRC network with the class *netout* and traffic that stays within the network with the class *netin*.
2. Define a service called *LocalBestEffortData*, and associate with this service a policy that matches the destination class *netin* at output.
3. Define a service called *LongDistanceBestEffortData*, and associate with this service a policy that matches the destination class *netout* at input and output.

The service provider can monitor the use of each service and whether the traffic remains within the network. With this information, the service provider can bill the enterprise accordingly. An IT manager in the enterprise can subscribe to both services and can monitor the enterprise's use of each service through the portal.

Chapter 23

Adding VPNs from JUNOS Routing Platforms with the SRC CLI

This chapter describes how to represent virtual private networks (VPNs) in an SRC configuration, and how to view and update extranet configuration through the SRC CLI. Topics include:

- Before You Add a JUNOS VPN to the SRC Configuration on page 399
- Configuring VPNs to Integrate into an SRC Network on page 400
- Configuration Statements for Adding VPNs and Extranet Clients on page 400
- Adding VPNs for Retailers and Enterprises on page 401
- Verifying and Updating Configuration of Extranets for VPNs on page 402

Before You Add a JUNOS VPN to the SRC Configuration

Before you can add a VPN to an SRC configuration, you must configure the VPN. Before you configure the VPN, make sure that in the routing scheme in the VPN:

- All members in the VPN can reach other.
- No changes are needed as members are added to and removed from the VPN.

If a VPN is used as an intranet, you can ensure that the routing scheme meets these requirements by configuring either:

- Static routes in the VPN
- Appropriate routing protocols

If the VPN is exported as an extranet, some members of the VPN may use private or conflicting address schemes. In addition, if the VPN has a large number of potential members, configuring static routing or routing protocols for all potential members may not be a manageable proposition. In these last two cases, we recommend that you use public addresses in the VPN and have VPN members implement Network Address translation (NAT) for traffic destined for the VPN.

VPNs use private IP addresses. If, however, enterprises that you administer export VPNs to extranet clients, you must ensure that the extranet clients can reach the IP addresses that the VPNs use. To implement an address scheme that allows all subscribers who have access to a VPN, we recommend that you implement NAT on the JUNOS routing platform. IT managers in the retailers and enterprises who own the VPNs can then map private IP addresses in the VPNs to public IP addresses, which extranet clients can reach.

For information about configuring NAT, see *Chapter 30, Using NAT Address Management Portal*.

Before you can reference a JUNOS VPN from the SRC configuration:

1. Create one routing instance in each router where VPN members access the VPN.
2. Make sure that each routing instance in the VPN has the same name as the VPN. The VPN represents the collection of the routing instances, the VPN members, and the connections between those routing instances within the VPN. All routing instances share a VPN ID, which you use to add VPNs to an SRC configuration.
3. Connect the VPN through a tunnel such as an MPLS label-switched path or IP Security tunnel.

Configuring VPNs to Integrate into an SRC Network

For SRC configurations that support JUNOS routers, you can add VPNs and extranets for retailers and enterprises.

For C-series platforms, you add VPNs through the CLI and can manage the VPNs through an enterprise portal that runs on another system.

See *Chapter 29, Managing Services with Enterprise Manager Portal* and *Chapter 31, Using the Sample Enterprise Service Portal*.

Configuration Statements for Adding VPNs and Extranet Clients

Use the following configuration statements to add VPNs and extranet clients at the [edit] hierarchy level.

```
subscribers retailer name vpn vpn-id {
  description description;
  display-name display-name;
  extranet-client [extranet-client ...];
  imported-extranet [imported-extranet...];
}
```



```

subscribers retailer name subscriber-folder folder-name enterprise name vpn vpn-id {
  description description;
  display-name display-name;
  extranet-client [extranet-client ...];
  imported-extranet [imported-extranet...];
}

```

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

Adding VPNs for Retailers and Enterprises

When you add a VPN to the SRC configuration, you are creating a VPN configuration object that represents a VPN that is already configured in the network. You can add a VPN for a retailer or for an enterprise.

Before you add a VPN to the configuration, obtain the identifier for the VPN. This identifier is the name of the routing instances on a JUNOS routing platform that implements the VPN.

To add a VPN to subscriber configuration for a retailer or an enterprise:

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

```

[edit]
user@host# edit subscribers retailer name vpn vpn-id

```

or

```

[edit]
user@host# edit subscribers retailer name subscriber-folder folder-name
enterprise name vpn vpn-id

```

where *vpn-id* is the name of the routing instances on a JUNOS routing platform that implements the VPN.

2. (Optional) Provide a name to identify the VPN as it appears in other SRC components, such as the Enterprise Manager Portal or other login pages.

```

[edit subscribers retailer name vpn vpn-id]
user@host# edit display-name display-name

```

For example, to label the VPN as one used for video conferences with corporate partners:

```

[edit subscribers retailer name vpn vpn-id]
user@host# edit display-name "Partner Video Conference"

```

3. (Optional) Add a description of the VPN.

```
[edit subscribers retailer name vpn vpn-id]
user@host# edit description description
```

For example:

```
[edit subscribers retailer name vpn vpn-id]
user@host# edit description "VPN for video conference with partners"
```

4. Verify that the configuration is correct. For example:

```
[edit subscribers retailer Acme vpn 1234]
user@host# show
display-name "Partner Video Conference";
description "VPN for video conference with partners.";
```

Verifying and Updating Configuration of Extranets for VPNs

From the SRC CLI, you can correct errors in extranet configuration when these errors result from directory or portal errors. In the extranet configuration, an extranet client of an object must be imported by that object.

In the SRC configuration for a subscriber that is the client of an extranet client, you specify a VPN for the imported extranet client. Typically, you add the extranet client and specify the imported extranet from the Enterprise Manager Portal. You can use the SRC CLI to verify the configuration and to make updates to the existing configuration.

To view information about extranet configuration and update it:

1. From configuration mode, access the configuration statement that represents the configuration for the VPN.

```
[edit]
user@host# edit subscribers retailer name vpn vpn-id
```

or

```
[edit]
user@host# edit subscribers retailer name subscriber-folder folder-name
enterprise name vpn vpn-id
```

where *vpn-id* is the name of the routing instances on a JUNOS routing platform that implements the VPN.

2. View the configuration for the VPN. For example:

```
[edit subscribers retailer Acme vpn 1234]
user@host# show
extranet-client [ "enterpriseName=Acme, ou=local, retailername=default,
o=Users,
o=umc" "enterpriseName=WidgetCo, ou=local, retailername=default, o=Users,
o=UMC "];
```

3. (Optional) Change or add the distinguished name (DN) of a retailer or an enterprise that is an extranet client of this VPN.

```
[edit subscribers retailer name vpn vpn-id]
user@host# set extranet-client extranet-client
```

For example:

```
[edit subscribers retailer name vpn vpn-id]
user@host# set extranet-client
enterpriseName=Acme2,ou=local,retailername=default, o=Users, o=umc
```

4. (Optional) Change or add extranets to be imported by specifying the DN of the extranet.

```
[edit subscribers retailer name vpn vpn-id]
user@host# set imported-extranets imported-extranets
```

You can specify one or more extranets.

5. Verify that the updated configuration is correct.

```
[edit subscribers retailer name vpn vpn-id]
user@host# show
[edit subscribers retailer Acme vpn 1234]
user@host# show
extranet-client [ "enterpriseName=Acme, ou=local, retailername=default,
o=Users,
o=umc" "enterpriseName=Acme2, ou=local, retailername=default, o=Users,
o=umc""enterpriseName=WidgetCo, ou=local, retailername=default, o=Users,
o=UMC "];
```


Chapter 24

Adding VPNs from JUNOS Routing Platforms

This chapter describes how to manage virtual private networks (VPNs) in the directory and contains the following sections:

- Overview of VPNs in the SRC Network on page 405
- Implementing a Routing Scheme for VPNs on page 406
- Configuring VPNs to Integrate into an SRC Network on page 406
- Modifying VPNs on page 408
- Adding Extranet Clients to VPNs on page 409
- Removing Extranet Clients on page 411
- Locating and Removing Inactive Subscriptions to a VPN on page 411
- Deleting VPNs from the Directory on page 412

Overview of VPNs in the SRC Network

For SRC configurations that support JUNOS routers, retailers and enterprises can support one or more VPNs. A VPN is an object in the directory that represents a virtual private network in an organization and has the object class `umcVpn`, which can be subordinate to the object classes `umcRetailer` and `umcEnterprise`.

For information about the object classes and their associated attributes, see the LDAP schema in the SRC software distribution in the folder *SDK/doc/ldap* or on the Juniper Networks Web site at

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

Implementing a Routing Scheme for VPNs

You must configure a routing scheme in the VPN that ensures that all members in the VPN can reach other and that does not require changes as members are added to and removed from the VPN. If a VPN is used as an intranet, you can achieve this goal by configuring static routes in the VPN or by configuring routing protocols appropriately.

If, however, the VPN is exported as an extranet, some members of the VPN may use private or conflicting address schemes. In addition, if the VPN has a large number of potential members, configuring static routing or routing protocols for all potential members may not be a manageable proposition. In these last two cases, we recommend that you use public addresses in the VPN and have VPN members implement NAT for traffic destined for the VPN (see *Overview of Services for Enterprise Manager Portal* on page 375).

VPNs use private IP addresses. If, however, enterprises that you administer export VPNs to extranet clients, you must ensure that the extranet clients can reach the IP addresses that the VPNs use. To implement an address scheme that allows all subscribers who have access to a VPN, we recommend that you implement NAT on the JUNOS routing platform. IT managers in the retailers and enterprises who own the VPNs can then map private IP addresses in the VPNs to public IP addresses, which extranet clients can reach.

Configuring VPNs to Integrate into an SRC Network

The administrator of a retailer can add and modify VPNs with an LDAP client, a data integrator, or SDX Admin. IT managers with the appropriate privileges can modify VPN properties through Enterprise Manager Portal.

For information about managing VPNs through Enterprise Manager Portal, see *Chapter 29, Managing Services with Enterprise Manager Portal*.

For information about managing VPNs from the SRC CLI, see *Chapter 23, Adding VPNs from JUNOS Routing Platforms with the SRC CLI*.

Adding VPNs with a Data Integrator

You can develop a data integrator that reads data from a storage medium, such as a database or a directory that does not use the SRC LDAP schema and that writes the data to the directory in a format that complies with the LDAP schema.

We provide a sample data integrator, VPN Directory Updater, which reads data about VPNs from a database and writes the data to a directory. If you want to use this data integrator, you need to understand how it works, and customize it for your specific application.

For information about data integrators and VPN Directory Updater, see *SRC-PE Integration Guide, Chapter 9, Integrating Data with the LDAP Directory*.

Adding VPNs with SDX Admin

To use SDX Admin add a VPN:

1. In the navigation pane, right-click the retailer or enterprise to which you want to add the new VPN, and select **New > VPN**.

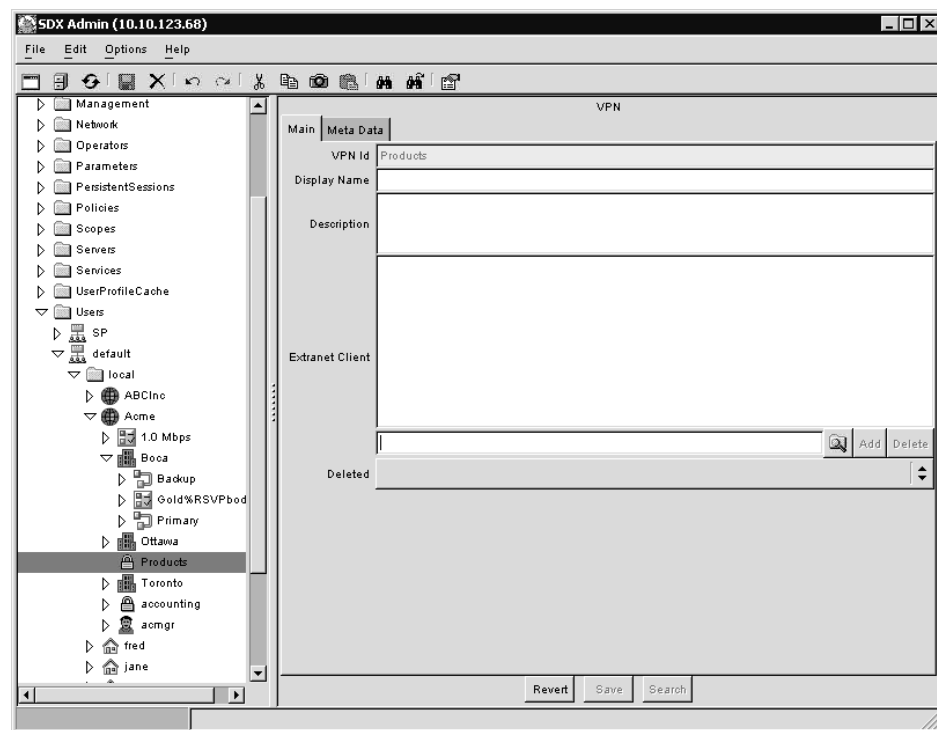
The New VPN dialog box appears.

2. Enter the names of the routing instances, as defined on the JUNOS routing platform, that implement the VPN in the network, and click **OK**.

For more information about routing instances and JUNOS routing platforms, see the JUNOS Internet Software documentation.

An object for the new VPN appears in the navigation pane, and the Main tab of the VPN pane appears.

Figure 29: VPN Pane



3. Edit or accept the default values for the VPN fields.

See *VPN Fields* on page 408.

4. Click **Save**.

VPN Fields

In SDX Admin, you can modify the following fields in the content pane for a VPN (*retailername* = < *retailer name* > , *o* = *Users*, *o* = *umc* or *enterprisename* = < *enterprise name* > , *ou* = < *foldername* > , *retailername* = < *retailer name* > , *o* = *Users*, *o* = *umc*).

Display Name

- Name of the VPN that appears in other SRC components, such as the Enterprise Manager Portal.
- Value—Text string
- Default—No value
- Example—Products VPN

Description

- Description of the VPN.
- Value—Text string
- Default—No value
- Example—VPN for sales representatives

Extranet Client

- Extranet client for this VPN.
- Value—Retailer or enterprise
- Default—No value
- Guidelines —For information about completing this field, see *Adding Extranet Clients to VPNs* on page 409.

Deleted

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

Modifying VPNs

IT managers with the appropriate permissions can display names and modify the descriptions of VPNs through the Enterprise Manager portal. Service providers can modify VPNs with an LDAP client or SDX Admin.

Adding Extranet Clients to VPNs

Retailers and enterprises can be extranet clients. Service providers can add extranet clients to VPNs with an LDAP client or SDX Admin. IT managers add extranet clients to their VPNs through Enterprise Manager Portal.

For information about adding extranet clients through Enterprise Manager Portal, see *Chapter 29, Managing Services with Enterprise Manager Portal*.

Two LDAP attributes specify information about extranet clients:

- The object classes `umcRetailer` and `umcEnterprise` have an LDAP attribute called `ImportedExtranet` that defines the DNSs of the imported VPNs.
- The object class `umcVPN` has an attribute called `extranetClient` that defines the DNSs of extranet clients of the VPN.

To use SDX Admin to add an extranet client:

1. In the navigation pane, select the VPN you want to export to the extranet client.

The VPN pane appears (see Figure 29 on page 407).

2. Click the magnifying glass below the Extranet Client field.

The Select Object dialog box appears and displays a list of subscribers.

3. Navigate to the retailer or enterprise who will be the extranet client.

- To navigate to a subordinate subscriber, double-click on a subscriber in the list.
- To navigate to a subscriber at a higher level in the directory, use the menu at the top of the Select Object dialog box.
- To select multiple options, shift-click or control-click the subscribers.

4. Click **OK**.

The extranet clients appear in the VPN pane.

5. Click **Add**.

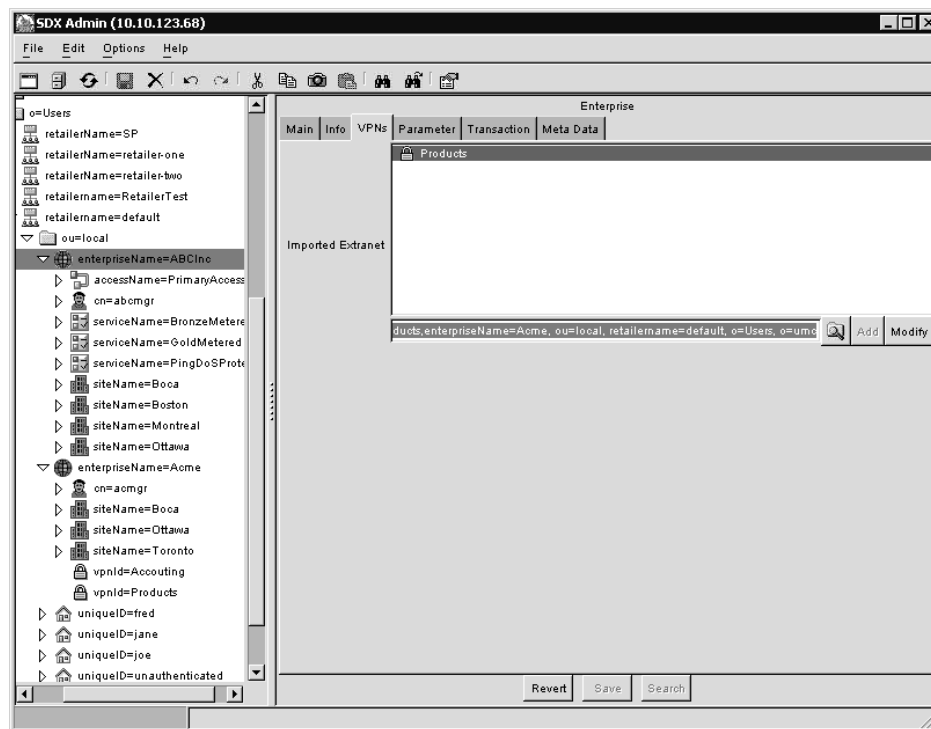
The extranet clients appear in the Extranet Client field of the VPN pane.

6. Click **Save** in the VPN pane.

7. In the navigation pane, highlight the subscriber for whom you want to import the VPN.

The subscriber's pane appears.

8. Click the **VPNs** tab for this subscriber.

Figure 30: Enterprise Pane

9. Click the magnifying glass below the Imported Extranet field.

The Select Object dialog box appears and displays a list of subscribers.

10. Navigate to the VPN you want to import.

- To navigate to a subordinate VPN, double-click on a subscriber in the list.
- To navigate to a VPN at a higher level in the directory, use the menu at the top of the Select Object dialog box.
- To select multiple options, shift-click or control-click the subscribers.

11. Click **OK**.

The VPN appears in the subscriber's pane.

12. Click **Add**.

The VPN appears in the Extranet Client field of the subscriber's pane.

13. Click **Save** in the subscriber's pane.

Removing Extranet Clients

Service providers can remove extranet clients to VPNs with an LDAP client or SDX Admin. IT managers can remove extranet clients through Enterprise Manager Portal.

For information about removing extranet clients with Enterprise Manager Portal, see *Chapter 29, Managing Services with Enterprise Manager Portal*.

To use SDX Admin to remove an extranet client:

1. In the navigation pane, select the subscriber who is the extranet client.
2. Click the VPN tab for this subscriber.

The subscriber's pane appears (for example, see Figure 30 on page 410).

3. Right-click the VPN in the Imported Extranet field, and select **Delete**.
4. Click **Save** in the subscriber's pane.
5. In the navigation pane, select the VPN.

The VPN pane (see Figure 29 on page 407) appears.

6. Right-click the extranet client in the Extranet Client field, and select **Delete**.
7. Click **Save** in the VPNs pane.

Locating and Removing Inactive Subscriptions to a VPN

When an IT manager cancels the export of a VPN, the Enterprise Manager Portal automatically deactivates any active subscriptions to that VPN for the associated extranet client. If an IT manager cancels the export of a VPN at the same time that the extranet client activates a subscription to this VPN, there is a remote possibility that the Enterprise Manager portal will maintain the active subscription.

We recommend that you periodically check for and deactivate these types of invalid subscriptions to prevent this type of invalid subscription. We provide a data integrator, VPN Subscription Deactivator, for this purpose. This data integrator works with the Enterprise Service Portal audit plug-in. For more information on data integrators and VPN Subscription Deactivator, see *SRC-PE Integration Guide, Chapter 9, Integrating Data with the LDAP Directory*.

To use this data integrator:

1. Install and configure the Enterprise Service Portal audit plug-in with the Enterprise Manager portal (see *Chapter 27, Installing and Configuring Enterprise Service Portals*).
2. Install the Data Integration package (see *SRC-PE Getting Started Guide, Chapter 28, Installing the SRC Software on a Solaris Platform*).
3. Run the script `/opt/UMC/datint/etc/vpndatamgt` with the check option, or configure a utility, such as a crontab file, to run this script at a defined time (see *SRC-PE Integration Guide, Chapter 9, Integrating Data with the LDAP Directory*).

Deleting VPNs from the Directory

Service providers can delete VPNs in the directory.

To delete VPNs:

1. Delete subscriptions to BoD services associated with the VPN.

Subscriptions to BoD services associated with a particular VPN all contain the substitution

`bodVpnName=<vpnID>`

where `<vpnID>` is the DN of the VPN to be deleted.

You can delete subscriptions with the specified substitution through an LDAP client. You can also delete individual subscriptions with SDX Admin (see *Modifying and Deleting Subscribers and Subscriptions* on page 271), although this solution is not practical for large numbers of subscribers. As a third option, you can develop a data integrator to delete the subscriptions (see *SRC-PE Integration Guide, Chapter 9, Integrating Data with the LDAP Directory*).

2. Remove all extranet clients (see *Removing Extranet Clients* on page 411).
3. Delete the VPN object from the directory.

For information about deleting entries with SDX Admin, see *SRC-PE Getting Started Guide, Chapter 38, Using SDX Admin*.

If you also want to delete the VPNs from the JUNOS routing platform, delete the routing instances that implement the VPN in the network. For complete information about configuring JUNOS routing platforms, see the JUNOS Internet Software documentation.

Part 5

**Managing Access Portals for Enterprise
Subscribers**

Chapter 25

Overview of Enterprise Service Portals

This chapter provides an overview of enterprise service portals and contains the following sections:

- Function of Enterprise Service Portals on page 415
- Enterprise Service Portals Provided with the SRC Software on page 417
- Enterprise Service Portal Audit Plug-In on page 419
- Network Information Collector with Enterprise Service Portals on page 419
- Service Parameters on page 420
- Substitutions and the Parameter Acquisition Path on page 420
- Managing Subscriptions to Aggregate Services on page 423
- Configuring Your Web Browser to Use an Enterprise Service Portal on page 423
- Accessing Enterprise Service Portals on page 423

Function of Enterprise Service Portals

The SRC software enables service providers to use enterprise service portals to provision services to enterprise subscribers who connect to the SRC network by means of a JUNOSe router or a JUNOS routing platform. An enterprise service portal is a standalone Web application that runs in a Java 2 Platform, Enterprise Edition (J2EE)-compliant Web application server. An enterprise service portal must have a corresponding configuration in the directory. Typically, a service provider provisions the router and configures the initial directory structure.

IT managers in an enterprise log in to the SRC network through an enterprise service portal. The managers can then activate services and perform some administrative tasks associated with their enterprises. When an IT manager requests an action through an enterprise service portal, the enterprise service portal uses the SRC software's enterprise service portal application programming interface (API) to interact with the SAE and to update data in the directory.

More specifically, the enterprise service portal calls methods in this API to:

- Authenticate IT managers in an enterprise.
- Create, delete, and modify accounts for IT managers.
- Navigate among retailers, enterprises, sites, and accesses.
- Create, delete, activate, and deactivate subscriptions to services.
- Get feedback from the sessions that a subscription generates. This feedback, which comes directly from the SAE managing the session, indicates whether the session is active in the network and provides the values used for the service parameters.
- Get feedback about the use of resources, such as the number of bytes and packets the SAE has sent or received for a particular service.
- Configure values for service parameters.

Consistency of Data in the Directory

Enterprise service portals can monitor the consistency of data as you enter it through the portal; for example, an enterprise service portal can prevent you from deleting a subscription if that subscription depends on other data in the directory. Enterprise service portals do not constantly monitor the consistency of existing data in the directory for all subscribers, however, because doing so would consume significant network resources. Consequently, if you use an LDAP browser to modify data in the directory that was entered through a portal, you must be sure that the data in the directory is consistent.

Privileges of IT Managers

The enterprise service portal API controls the privileges that determine how IT managers can manipulate subscribers, subscriptions, and services associated with a retailer or enterprise. All IT managers in an enterprise share the same connections to the directory.

Developing and Customizing Enterprise Service Portals

You can customize enterprise service portals to provide customer-specific Web pages and supply specified services. By modifying JavaServer pages (JSP), which use a set of customized tags to call methods in the enterprise service portal API, you can customize an enterprise service portal to suit a customer's environment.

For information about the JSP tags that you can use to customize an enterprise service portal, see the documentation for the enterprise tag library in the SRC software distribution in the folder */SDK/doc/ent/tagDocs* or on the Juniper Networks Web site at

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

Identifying the SAE

An enterprise service portal handles a request from an IT manager by communicating with the SAE that manages the subscriber affected by the IT manager's request. You can use the following methods to allow the enterprise service portal to identify which SAE manages a subscriber:

- For SRC implementations that use more than five SAEs, configure a network information collector (NIC) that takes the distinguished name (DN) of an access as the key and returns the corresponding SAE as the value.
- For SRC implementations that use five or fewer SAEs, you can use directory eventing to identify the SAEs. If you configure this option, SAEs update the addresses of their external interfaces in the directory at a specified time interval. Each update triggers an event that is sent to the enterprise service portal to confirm that the corresponding SAE is available. If the enterprise service portal does not receive the update event within a certain time, the enterprise service portal assumes that the SAE is not available and subsequently does not send any service activation or feedback requests to that SAE. When the SAE becomes available and starts to manage subscribers again, the enterprise service portal sends new requests to that SAE.

Enterprise Service Portals Provided with the SRC Software

We provide several enterprise service portals in the SRC software distribution in the folder *webapp*. Some of the enterprise service portals we provide are intended for demonstration purposes or as a basis for developing a customized enterprise service portal for your SRC implementation. Other enterprise service portals are intended to serve a specific purpose and require little customization. The WAR files for the enterprise service portals contain all required libraries and Web contents.

The following enterprise service portals are available:

- Sample enterprise service portal
- Enterprise Manager Portal
- NAT Address Management Portal

Sample Enterprise Service Portal

The sample enterprise service portal incorporates many of the features that the enterprise service portal API offers. You can use the sample enterprise service portal to demonstrate the functionality available, and you can customize the sample enterprise service portal to create a portal for your own SRC implementation. The source code for the sample enterprise service portal is in its JSP pages; the code was created with the tags in the enterprise portal tag library.

For information about the JSP tags that you can use to customize an enterprise service portal, see the documentation for the enterprise tag library in the SRC software distribution in the folder */SDK/doc/ent/tagDocs* or on the Juniper Networks Web site at

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

Enterprise Manager Portal

Service providers can deploy Enterprise Manager Portal to provision services for enterprise subscribers. IT managers can access the SRC network through this portal and select the services they require. Enterprise Manager Portal is a complete application for which you need to customize only style sheets and icons.

NAT Address Management Portal

Service providers can deploy this enterprise service portal to manage public IP addresses for use with NAT services on JUNOS routing platforms. IT managers make requests about public IP addresses through Enterprise Manager Portal. The service provider responds to these requests through NAT Address Management Portal. This enterprise service portal is a complete application for which you need to customize only style sheets and icons.

When an IT manager makes a request about public IP addresses through Enterprise Manager Portal, Enterprise Manager Portal sends an e-mail to a human administrator or a machine. For small installations or demonstration purposes, a human administrator can manage the public IP addresses; however, for large installations, public IP addresses are managed by machines. NAT Address Manager handles two operations: the supply of new IP addresses and the return of unwanted public IP addresses.

If a human administrator provides the IP addresses, the administrator can access the Address Manager portal by clicking the portal address that is included in the e-mail from Enterprise Manager Portal. The administrator can then use NAT Address Management Portal to make a change to the IT manager's public IP addresses in the directory. The IT manager can view the changes through Enterprise Manager Portal and can use the assigned IP addresses in subscriptions to NAT services.

If you use a machine to manage public IP addresses, you must write an application that allows the machine to handle the e-mails that Enterprise Manager Portal sends. The e-mails contain XML code that NAT Address Management Portal and the machine must interpret. The following sequence of events describes how the machine interacts with the portals.

1. The IT manager requests one or more IP addresses through Enterprise Manager Portal.
2. Enterprise Manager Portal sends an e-mail to the machine that administers IP addresses.

The subject line of the e-mail contains the URL of NAT Address Management Portal. The body of the e-mail contains an SDXNATStatusRequest message—XML code that contains a request for information about the status of a particular access.

3. The machine forwards the e-mail to the URL in the subject line of the e-mail.
4. The machine extracts the SDXNATStatusRequest message from the e-mail and sends it by means of HTTP to NAT Address Management Portal.
5. NAT Address Management Portal analyzes the SDXNATStatusRequest message and returns an SDXNATStatusResponse message to the machine.

6. The machine analyzes the response and determines the next action, such as providing an IP address for the enterprise.
7. The machine sends the appropriate information in an SDXNATOperationRequest message to NAT Address Management Portal.
8. NAT Address Management Portal updates the directory and returns an SDXNATOperationResponse message to the machine.

When NAT Address Management Portal updates the directory, the IT manager can view the new status in Enterprise Manager Portal and can use the assigned IP addresses in subscriptions to NAT services.

The XML messages described above contain subordinate elements that depend on whether the IT manager's request is to obtain or return IP addresses. The document type definition (DTD) for the XML messages describes these subordinate elements. You can find the DTD in the SRC software distribution in the folder called *SDK/dtd*.

Enterprise Service Portal Audit Plug-In

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

You can write audit plug-in event listeners by implementing the callback interface. A listener performs tasks such as processing received events and then publishing the events to one or more event handlers, such as a log file, system log, or database. Events are sent after the corresponding operations have been completed. The plug-in processes events, which are sent synchronously, and then returns control to the enterprise service portal. Future events are blocked from being processed until the listener returns the thread.

Network Information Collector with Enterprise Service Portals

You can improve the performance of service activation for an enterprise service portal by implementing the NIC in your network. In this case, the enterprise service portal uses the NIC to locate the SAE managing a particular session. If you do not configure a NIC for your network, the enterprise service portal locates the managing SAE by polling all the SAEs in the network. See *SRC-PE Network Guide, Chapter 9, Locating Subscriber Information with the NIC*.

Service Parameters

Subscribing to and activating services are only part of the functionality available through the enterprise service portal API. An enterprise service portal can also expose the power of service parameters.

An enterprise service is, at its core, a set of policies that affect network traffic when they are applied to the router interfaces associated with some subset of an enterprise's accesses. When these service policies are defined by the service provider, they can contain parameters. For example, a service that provides protection against denial-of-service attacks may limit the traffic on a specific port to a specific percentage of the bandwidth available on a router interface. Both the port and the percentage can be expressed as parameters in the service's network policies.

Service parameters allow for some very powerful functionality. For example, they allow the service provider to define a generic service that can be customized for specific enterprises or for specific sites or accesses within an enterprise. The enterprise customer can perform this customization at any time (even while the service is active) through an enterprise service portal. The enterprise service portal must invoke a method in the enterprise API to provide the value for each parameter.

For an enterprise service portal to detect service parameters configured for fragment services for an aggregate service, the parameters must be defined in the configuration for the aggregate service. See *Chapter 29, Managing Services with Enterprise Manager Portal*.

Substitutions and the Parameter Acquisition Path

Each parameter in a service policy requires that a value be obtained. In the example above, the denial-of-service protection policies have two parameters: port number and bandwidth percentage. Each of those parameters in a service's network policies results in the creation of a variable. Policy configuration specifies the name of a variable.

Each of these variables must have a value assigned to it (unless it already has a default value). The enterprise service portal can obtain that value from the enterprise customer. The enterprise service portal must then call a method in the API to assign that value to the variable. The API will record this value by writing a substitution into an LDAP entry. A substitution is an LDAP entry attribute that, at its simplest, just assigns a value to a variable.

More than one substitution can exist for a given variable. Substitutions for a given variable can exist in any LDAP entry on the acquisition path. The acquisition path is a path through a sequence of LDAP entries. It begins with a most specific entry and ends with a most general entry. When the value for a given variable is specified through substitution attributes in multiple LDAP entries on this path, only the most specific entry's substitution is actually used.

The ordering of the LDAP entries in the acquisition path is always the same. Starting from the most specific, they are the:

1. SSP subscription entry under the access entry (if one exists for the service in question)
2. Access entry
3. SSP subscription entry under the site entry (if one exists for the service in question)
4. Site entry
5. SSP subscription entry under the enterprise entry (if one exists for the service in question)
6. Enterprise entry
7. Relevant localized version of the SSP service entry (if one exists)
8. SSP service entry

The acquisition path allows values assigned to variables at a more general place in the acquisition path to be overridden by values assigned at a more specific place in the acquisition path. This method enables an enterprise to subscribe to a given service, to specify values for that service's parameters at a more general place in the acquisition path, and then to override those values at a more specific level according to the needs of local enterprise IT managers who control a given site or access.



NOTE: Each session of a subscription uses a different acquisition path (because each is associated with a different access). This means that each session of a subscription may end up with different values for a given service parameter. For each session, the enterprise API exposes detailed information about the actual values used for every service parameter.

Power of Substitutions

In addition to assigning values to the variables that are used as service parameters, a substitution can declare that the value it assigns is fixed. When a fixed value is declared, substitutions for the same variable that exist in more specific places in the acquisition path are ignored (that is, the fixed value cannot be overridden). More important, a substitution can specify the value for a variable as an expression that includes other variables. A substitution can also introduce new variables. The new variables are then available for use in other substitutions at any more specific point on the acquisition path. Enterprise service portals that expose these features allow enterprises to define their own way of presenting and managing service parameters. For more detail on service parameters, the acquisition path, and the uses of substitutions, see the *SRC-PE Services and Policies Guide, Chapter 15, Defining and Acquiring Values for Parameters*.

Substituting Values for Policy Parameters

The value substitution feature of an enterprise service portal gives the enterprise IT manager the ability to customize subscribed services in his or her sphere of control. The enterprise IT manager can be required to provide a set of substitutions that define the values for the parameters of the underlying service policies everywhere the policies are applied. Sample parameter types that might require value substitution include:

- Network—Address/prefix length pairs that denote networks
- Interface—Router interface specifications
- Protocol—Eight-bit unsigned integers enumerating protocols such as IP, TCP, and UDP
- Rate—32-bit unsigned integers used for rate-limit and burst-size calculations

For example, the service provider could offer a service to the enterprise that applies a firewall policy. The firewall policy could screen ingress traffic from a source network and redirect the screened traffic to a specific destination. The enterprise IT manager might want to specify at the time of subscription or subscription activation which source networks are involved. The service provider establishes a general policy template, in this case configuring the destination. The enterprise IT manager modifies the template by means of value substitution for the particular needs of the enterprise, such as providing a range of IP addresses for one or more source networks.

A different service might have an egress rate-limit policy with policy rules to screen egress traffic from the source network, by protocol, or according to a traffic rate limit. Value substitution for the parameters defined in the generic policy template enables the manager to define the policy to match the needs of the enterprise.

Note that parameter names provided to one customer can be renamed by the service provider to suit the needs of another customer. For example, one customer might prefer a parameter named “department” to one named “network” because that name better fits the enterprise hierarchy.

The service provider can specify whether all parameters or only certain ones can be modified in the enterprise service portal by the enterprise IT manager by means of value substitution. Likewise, an IT manager can determine whether subordinate managers have the ability to modify a given service parameter. Parameters for which values cannot be substituted at a given level are said to be fixed at some higher level. For example, in the sample portal, the enterprise service portal populates drop-down lists from which the manager at that level can select values to substitute. If a parameter substitution is fixed at a higher management level, lower-level managers will not see options for substituting for that parameter in the drop-down lists on their instance of the enterprise service portal. See *SRC-PE Services and Policies Guide, Chapter 15, Defining and Acquiring Values for Parameters* for more information.

Managing Subscriptions to Aggregate Services

If an enterprise service portal manages subscriptions to aggregate services, ensure that each parameter defined for a fragment service is also defined in the aggregate service. For information about aggregate services, see *SRC-PE Services and Policies Guide, Chapter 1, Managing Services with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 2, Managing Services on a Solaris Platform*.

To review parameter definitions and define parameters used by a fragment service for an aggregate service from SDX Admin:

1. Select the aggregate service to be managed by an enterprise service portal.
2. Click the **Aggregate** tab for the service, and review the parameters listed under Expression and Substitution for each service fragment.
3. Click the **Parameters** tab, and review the list of Substitutions. If a substitution is not listed for one of the parameters referenced on the Aggregate tab, add it.

The value for each of the parameter substitutions should not be Fixed.

Configuring Your Web Browser to Use an Enterprise Service Portal

Before you can use an enterprise service portal, you must enable your Web browser to:

- Allow cookies from the enterprise service portal.
- (Enterprise Manager Portal and NAT Address Management Portal only) Use JavaScript.

Accessing Enterprise Service Portals

When viewing the enterprise service portals, take care to open only one browser window yourself. The portals automatically open pop-up windows for various operations. If you open more than one browser window yourself, the information in the original window may not be updated correctly when you complete an operation in a pop-up window.

To access an enterprise service portal:

1. Enter the URL of the portal in your Web browser, and press Enter. For example, to access Enterprise Manager Portal, type:

`http://192.0.2.1:8080/entmgr`

The enterprise service portal displays the login page.

2. Select your service provider from the Retailer menu.
3. Enter your username in the Login ID field and your password in the Password field.

The enterprise service portal displays your Welcome page. On the left of the page is a navigation pane for the objects in the service provider's directory over which you have control. Your login identity is the root of this navigation pane.

Chapter 26

Planning Deployment for Enterprise Service Portals

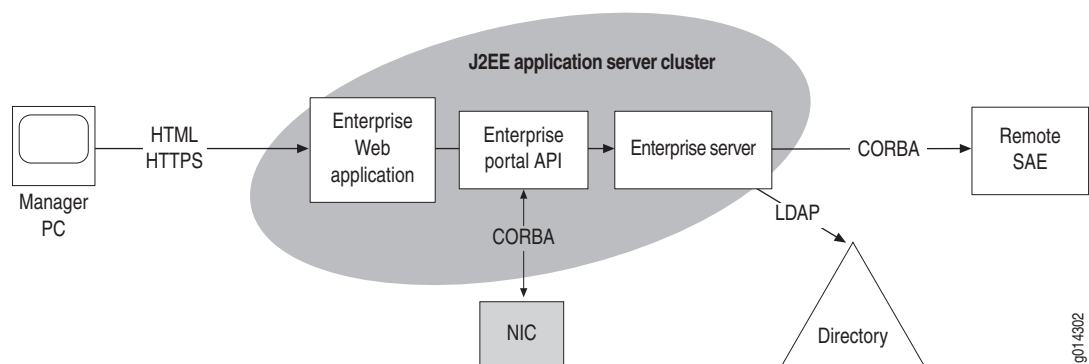
This chapter provides information to help you plan a deployment for enterprise service portals. The chapter contains the following sections:

- Architecture of Enterprise Service Portals on page 425
- Deployment Scenario for an Enterprise Service Portal on page 427
- Deciding Which Enterprise Service Portal to Use on page 428
- Planning Number of Instances of an Enterprise Service Portal on page 428
- Planning Namespace Hierarchy for an Enterprise Service Portal on page 428

Architecture of Enterprise Service Portals

Figure 31 shows the basic elements and communication protocols of an enterprise service portal.

Figure 31: Elements and Communication Protocols for an Enterprise Service Portal



Elements for an Enterprise Service Portal

An enterprise service portal consists of a server cluster that communicates with the following network elements:

- Directory system—A distributed set of directories with information shadowing and chaining agreements between master and slave servers
- (Optional) Network information collector

For SRC implementations that use more than five SAEs, an enterprise service portal requires a NIC to identify which SAE is managing a subscriber. This NIC takes the distinguished name (DN) of an access as the key and returns the corresponding SAE as the value. For SRC implementations that use five or fewer SAEs, you can use directory eventing to identify the SAEs.

- Remote SAE
- Manager PC—A client PC on which a person managing an enterprise runs a Web browser to communicate with an enterprise service portal

Internally, an enterprise service portal consists of a J2EE application server cluster that implements an Enterprise API or Enterprise Tags Library, an enterprise Web application that uses one of these interfaces, and an enterprise server. The enterprise server requires persistent sessions in the cluster. That is, the cluster member that receives the first manager session request must receive all subsequent requests for the same session.

Communication Protocols

Table 36 describes the communication protocols that are used between elements in the enterprise service portal network.

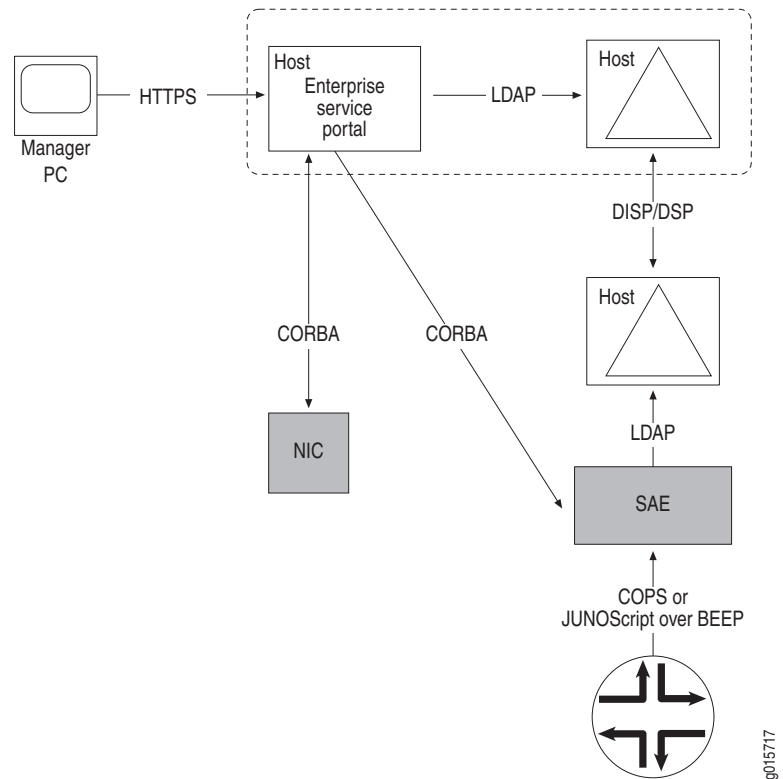
Table 36: Communication Protocols for an Enterprise Service Portal

Protocol	Used for Communication Between
HTML/HTTPS (HyperText Markup Language over Secure HyperText Transmission Protocol)	Enterprise manager's Web browser and the enterprise portal Web application running in the enterprise service portal
Enterprise Portal API	Enterprise Web application and the enterprise server
CORBA	Enterprise server and remote SAEs running in a different Web application server than the enterprise server
LDAP	Enterprise server and SRC directories

Deployment Scenario for an Enterprise Service Portal

Figure 32 shows component interactions for a sample deployment of an enterprise service portal.

Figure 32: Deployment for an Enterprise Service Portal



The directory servers are synchronized by means of server-to-server protocols, such as DISP and DSP in the case of X.500 directories, and DirX and equivalent protocols in the case of native LDAP directories, such as Sun ONE Directory Server.

In this configuration, bulk service session requests and implicit subscription reactivation caused by substitution changes are made through replication of directory information. The enterprise service portal writes new information to its local directory, and the server-to-server protocols transfer the information to the SAE's local directory. Then the SRC directory eventing system notifies the SAE of the new information, and the SAE reacts by activating and deactivating subscriptions.

The enterprise service portal receives feedback on the session state and parameter values of a session using remote procedure calls through the CORBA connection directly to the SAE managing the session.

Deciding Which Enterprise Service Portal to Use

Table 37 describes which application to use in your organization.

Table 37: Enterprise Service Applications

To Perform This Task	Use This Application
Provide services to a number of enterprises, and let IT managers at the enterprises manage services for their enterprise	Enterprise Manager Portal
Manage address allocation	NAT Address Management Portal with Enterprise Manager Portal
Provide custom management functions through an enterprise service portal	Customized version of the sample Enterprise Service Portal

Planning Number of Instances of an Enterprise Service Portal

When you are planning an SRC network that uses enterprise service portals, consider how many instances of the enterprise service portal you need. For example, if your network has multiple points of presence (POPs), you may want to install an enterprise service portal in each POP.

Planning Namespace Hierarchy for an Enterprise Service Portal

Each enterprise service portal that you install must have a namespace that defines the location of its configuration in the directory. The namespaces form a hierarchy of LDAP entries, and a namespace inherits all the properties defined in its parent namespaces. Properties defined in subordinate namespaces override properties of the same name inherited from parent namespaces. Multiple enterprise service portals can use the same namespace if all the properties in the configurations are identical.

For example, in the sample data, the namespaces for Enterprise Manager Portal and NAT Address Management Portal are subordinate to the namespace for the sample Enterprise Service Portal (see Table 38). Consequently, the subordinate configurations inherit property definitions from the sample Enterprise Service Portal configuration, unless specific settings in the subordinate configurations override those in the sample Enterprise Service Portal configuration.

Table 38: Namespaces for Enterprise Service Portals

Name of Enterprise Service Portal	Namespace
Sample Enterprise Service Portal	<i>l = EASP, ou = staticConfiguration, ou = Configuration, o = Management, o = umc</i>
Enterprise Manager Portal	<i>l = ENT-MGR, l = EASP, ou = staticConfiguration, ou = Configuration, o = Management, o = umc</i>
NAT Address Management Portal	<i>l = ADDR-MGR, l = EASP, ou = staticConfiguration, ou = Configuration, o = Management, o = umc</i>

You can use the hierarchy of namespaces to minimize the number of properties you configure for a particular instance of an enterprise service portal. For example, suppose you want to deploy two instances of Enterprise Manager Portal in different POPs—Ottawa and Montreal. The POPs use the same directory for services; however, each POP uses its own directory for subscribers.

To minimize the number of properties you configure for the enterprise service portal, you can:

1. Create the following two namespaces subordinate to *l = ENT-MGR*, *l = EASP*, *ou = staticConfiguration*, *ou = Configuration*, *o = Management*, *o = umc*:
 - *l = ENT-MGR-Ottawa*
 - *l = ENT-MGR-Montreal*
2. Configure information about the service directory in *l = ENT-MGR*, *l = EASP*, *ou = staticConfiguration*, *ou = Configuration*, *o = Management*, *o = umc*.
3. Configure information about the respective subscriber directories in *l = ENT-MGR-Ottawa* and *l = ENT-MGR-Montreal*.

Chapter 27

Installing and Configuring Enterprise Service Portals

This chapter describes how to install and configure the enterprise service portals, and contains the following sections:

- Before You Install an Enterprise Service Portal on page 431
- Installing Enterprise Service Portals on page 432
- Writing an Application to Allow a Machine to Provide Public IP Addresses for NAT on page 441
- Configuring an Enterprise Service Portal on page 442
- Configuring an Enterprise Service Portal Audit Plug-In on page 452

Before You Install an Enterprise Service Portal

Before you install the enterprise service portal:

- Identify the machine on which you want to install the application.

If you plan to use Enterprise Manager Portal and NAT Address Management Portal, which work together but serve different purposes, you must install both portals. You can install these portals on the same or different machines.

- Install a Web application server on the machine on which you want to install the enterprise service portal.

We provide the JBoss Web application server in the SRC software distribution. For information about installing this software, see *SRC-PE Getting Started Guide, Chapter 33, Installing Web Applications*.

- If you use JBoss or another Web application server that performs load balancing, you must configure the Web application server to use *sticky sessions* to process requests to the enterprise service portal.

Sticky sessions are sessions between a server and client in which information is preserved between different transactions in an activity. When a server establishes a session for an activity with a particular client, the Web application server preserves session information by sending subsequent requests from the client to the same server. For enterprise service portals, use of sticky sessions ensures that the Web application server always routes requests from IT managers to the same instance of the enterprise service portal that they logged into.

For information about configuring sticky sessions for the Web application server, see the documentation for your Web application server.

- Determine how you will identify the SAE that manages a subscriber who connects to the SRC network through an enterprise service portal (see *Identifying the SAE* on page 417). If you will use a network information collector (NIC) for this purpose, configure a NIC that takes the distinguished name (DN) of an access and returns the corresponding SAE reference (for more information about the NICs, see *SRC-PE Network Guide, Chapter 9, Locating Subscriber Information with the NIC*).
- Install the sample data from the SRC software distribution (see *SRC-PE Getting Started Guide, Chapter 29, Defining an Initial Configuration on a Solaris Platform*).
- In the directory, create any new namespaces for the enterprise service portals you will install. For information about namespaces, see *Chapter 26, Planning Deployment for Enterprise Service Portals*. To create a namespace, you can copy one of the enterprise service portal configurations included with the same data to another location in the directory.

Installing Enterprise Service Portals

Tasks to install an enterprise service portal are:

1. Preparing the Web Applications for Customization on page 433
2. Configuring Connections to the Directory on page 433
3. (Enterprise Manager Portal only) Configuring Deployment Settings for Enterprise Manager Portal on page 435
4. Deploying the Enterprise Service Portals on page 441
5. Configuring the URL for an Enterprise Service Portal on page 441

After you install an enterprise service portal:

- If you use a machine to administer public IP addresses in conjunction with NAT Address Management Portal, write an application to handle the interaction between the machine and this portal. See *Writing an Application to Allow a Machine to Provide Public IP Addresses for NAT* on page 441.
- If you use Enterprise Manager Portal, NAT Address Management Portal, or an application that uses a configuration file based on the `easp_conf` template, see *Configuring an Enterprise Service Portal* on page 442.

Preparing the Web Applications for Customization

When customizing the Web applications, copy the WAR files to a temporary folder and work in that folder.

To copy the WAR file to a temporary folder:

1. Login as `root` or another authorized user.
2. Create a temporary folder in which you will work on the WAR file. For example:

```
mkdir tempWar
```

3. Access the temporary folder. For example:

```
cd tempWar
```

4. Copy the WAR file to the temporary folder.

```
cp /cdrom/cdrom0/webapp/<filename>
```

`<filename>` —Name of the WAR file; for example, *entmgr.war*

Configuring Connections to the Directory

To configure a connection between the Web application and the directory that contains the configuration for the enterprise service portal:

1. Access the temporary folder to which you copied the WAR file.

```
cd tempWar
```

2. Extract the *boot.props* file from the WAR file.

```
jar xvf <filename> WEB-INF/boot.props
```

`<filename>` —Name of the WAR file; for example, *entmgr.war*

3. Edit the *boot.props* file with any text editor; use the following property descriptions as guidelines.
4. Replace the *boot.props* file in the WAR file.

```
jar uvf <filename> WEB-INF/boot.props
```

Initialization Properties for Enterprise Service Portals

In the boot properties file for an enterprise service portal, you can modify the following fields.

Config.java.naming.provider.url

- URL of the primary directory in URL string format.
- Value—ldap:// <host> : <portNumber> /
 - <host> —IP address or name of the host that supports the directory
 - <portNumber> —Number of the TCP port
- Default—ldap://127.0.0.1:389/

Config.java.naming.security.credentials

- Password that the Web application server uses to authenticate and authorize access to the directory.
- Value— <password>
- Guidelines—The password can be encoded in base64 and not visible in plain text. To use an encoded value, use the format {BASE64} <encoded-value> .
- Default—ent

Config.java.naming.security.principal

- DN that contains the username that the Web application server uses to authenticate and authorize access to the directory.
- Value—DN of the object that contains the username
- Default—cn = ent-admin, o = operators, o = umc

Config.net.juniper.smgmt.des.backup_provider_urls

- Redundant directories that store configuration information.
- Value—List of URLs in URL string format separated by semicolons (see description for the property Config.java.naming.provider.url)
- Default—ldap://127.0.0.1:389/; ldap://127.0.0.1:389/

Config.net.juniper.smgmt.des.<propertySuffix>

- Set of properties that specify how the Web application interacts with the directory.
- Value—See *SRC-PE Getting Started Guide, Chapter 32, Distributing Directory Changes to SRC Components on a Solaris Platform*.
- Default—See *SRC-PE Getting Started Guide, Chapter 32, Distributing Directory Changes to SRC Components on a Solaris Platform*.

Config.net.juniper.smgmt.lib.config.staticConfigDN

- Root of the static configuration properties.
- Value—DN of the object that contains the username
- Default—ou = staticConfiguration, ou = configuration, o = Management, o = umc

Config.EASP.namespace

- Location of the enterprise service portal's configuration in the directory.
- Value—Path, relative to the root of the static configuration properties, that defines the location
- Guidelines—If you are using the enterprise service portals we provide, use the defaults, which match the locations of the configurations in the sample data.
- Default—Depends on the enterprise service portal:
 - Sample Enterprise Service Portal—/EASP
 - Enterprise Manager Portal—/EASP/ENT-MGR
 - NAT Address Management Portal—/EASP/NAT-ADDR

Configuring Deployment Settings for Enterprise Manager Portal

You configure deployment settings for Enterprise Manager Portal. You do not need to configure deployment settings for the sample Enterprise Service Portal or NAT Address Management Portal.

To configure deployment settings for Enterprise Manager Portal:

1. Access the temporary folder to which you copied the WAR file.

cd tempWar

2. Extract the *web.xml* file from the WAR file.

jar xvf entmgr.war WEB-INF/web.xml

3. Edit the *web.xml* file in the *entmgr.war* file with any text editor; use the following property descriptions as guidelines.

This file specifies which applications Enterprise Manager Portal displays and specifies how to generate e-mails when IT managers request public IP addresses through this enterprise service portal.

4. Replace the *web.xml* file in the WAR files.

jar uvf entmgr.war WEB-INF/web.xml

Deployment Properties for Enterprise Manager Portal

In the *web.xml* deployment properties file for Enterprise manager Portal, you can modify the following fields.

showBasicBandwidthOnDemand

- Whether or not the enterprise service portal displays basic bandwidth-on-demand (BoD) features.
- Value
 - True—Displays the basic BoD features
 - False—Hides the basic BoD features

- Guidelines—Specify True if you want to provision basic BoD with a JUNOS routing platform. When enabled, service providers can offer basic BoD services to IT managers as service options that affect all traffic on an access link, including customizing the amount of bandwidth provided to meet their traffic requirements.

To make class of service (CoS) services available, BoD services and basic BoD services must be enabled. If both are enabled, IT managers must select a basic BoD service before they can subscribe to BoD services.

- Default—True

showBandwidthOnDemand

- Whether or not the enterprise service portal displays BoD features.
- Value
 - True—Displays the BoD features
 - False—Hides the BoD features
- Guidelines—Specify True if you want to provision BoD with a JUNOS routing platform. To make CoS services available, BoD services and basic BoD services must be enabled. If both are enabled, IT managers must select a basic BoD service before they can subscribe to BoD services.
- Default—True

showFirewall

- Whether or not the enterprise service portal displays firewall features.
- Value
 - True—Displays the firewall features
 - False—Hides the firewall features
- Guidelines—Specify True if you want to provision firewall services with a JUNOS routing platform.
If you set showFirewall to True and statelessFirewall to False, the portal provides support for stateful firewalls on JUNOS routing platforms.
- Default—True

statelessFirewall

- Whether or not the enterprise service portal displays stateless firewall features.
- Value
 - True—Displays the stateless firewall features
 - False—Hides the stateless firewall features

- Guidelines—Specify True if you want to provision firewall services on a JUNOS routing platform. The showFirewall field must also be set to True.

When you set statelessFirewall to True, the Firewall tab but not the Application tab appears in Enterprise Manager Portal.

You can configure either stateless firewalls or stateful firewalls from Enterprise Manager Portal. If you set showFirewall to True and statelessFirewall to False, the portal provides support for stateful firewalls on JUNOS routing platforms.

- Default—True

showNat

- Whether or not the enterprise service portal displays NAT features.
- Value
 - True—Displays the NAT features
 - False—Hides the NAT features
- Guidelines—Specify True if you want to provision NAT services with a JUNOS routing platform. If this property is set to True, the enterprise service portal always displays the firewall features, regardless of the value of the showFirewall property.
- Default—True

showSchedule

- Whether or not the enterprise service portal displays scheduling features for services.
- Value
 - True—Displays the scheduling features
 - False—Hides the scheduling features
- Default—True

showVpn

- Whether or not the enterprise service portal displays VPN features.
- Value
 - True—Displays the VPN features
 - False—Hides the VPN features
- Guidelines—Specify True if you want to provision VPNs with a JUNOS routing platform. If you set this property to True, you must also set the showBandwidthOnDemand property to True.
- Default—True

showExtranet

- Whether or not the enterprise service portal displays VPN extranet features.
- Value
 - True—Displays the VPN extranet features
 - False—Hides the VPN extranet features
- Guidelines—Specify True if you want to provision VPN extranets with a JUNOS routing platform. If you set this property to True, you must also set the showVPN property to true.
- Default—True

junoseCompatibleBoD

- Whether or not the enterprise service portal can be used to configure BoD services on JUNOSe routers.
- Value
 - True—Provides configuration for BoD services on JUNOSe routers
 - False—Does not provide configuration for BoD services on JUNOSe routers
- Guidelines—If set to true, this field allows BoD services to be configured for JUNOSe routers as well as JUNOS routing platforms. This setting limits the configuration for IP protocol, source IP address, source port or port range, destination IP address, and destination port or port range for a BoD rule to one each for JUNOS routing platforms as well as JUNOSe routers. The online help indicates that users can specify one value for these fields if **junoseCompatibleBoD** is set to True, and that users can specify more than one value for these fields if **junoseCompatibleBoD** is set to False.

Consider that if both JUNOS routing platforms and JUNOSe routers exist in an enterprise's network, IT managers who are using the enterprise service portal to configure their SRC-managed environment do not know which routers are JUNOSe routers and which are JUNOS routing platforms.
- Default—False

machineReadableNotifications

- Format of the e-mails that indicate that public addresses have been requested or released for a particular access link.
- Value
 - True—E-mails contain XML code and will be handled by a machine.
 - False—E-mails contain ordinary text and will be handled by a human administrator.
- Default—False

renotificationInterval

- Minimum time between e-mails that notify the service provider about outstanding requests for IP addresses.
- Value—Number of seconds in the range 1–2147483647
- Guidelines—For actual SRC implementations that use a human administrator, we recommend a value of 86400 seconds (1 day). For demonstrations of the SRC software that use a human administrator, we recommend a value of 240 seconds. For actual SRC implementations that use machines, the value depends on how you design an application to handle the e-mails; a value of 600 seconds (10 minutes) may be a good starting point.
- Default—120
- Example—200

addressManagerUrl

- URL of NAT Address Management Portal that the service provider uses to manage public IP addresses for enterprises. This value is included in the e-mails about IP addresses.
- Value—URL in the format
http://<host>:<port><path>
 - <host> —Name or IP address of the machine on which you install the Web application for NAT Address Management Portal
 - <port> —TCP/UDP port for HTTP traffic
 - <path> —Path to location of the Web application
- Default—http://example.com:8080/nataddr/AddressManager

mail.smtp.host

- SMTP mail server that Enterprise Manager Portal uses to send e-mails about requests for or release of public IP addresses.
- Value—Name or IP address of the mail server
- Default—mailhost

notificationFrom

- Sender's address in e-mails that Enterprise Manager Portal sends about public IP addresses.
- Value—Text string that specifies the sender's name and e-mail address in XML format
- Guidelines—Be sure to use the correct XML escape sequences for any special characters in the value.
- Default—"Enterprise Portal" <entMgrPortal@example.com >

notificationTo

- Human administrator or machine to which Enterprise Manager Portal should send e-mails about requests for or release of public IP addresses.
- Value—Text string that specifies the name and e-mail address of the human administrator or machine in XML format
- Guidelines—Be sure to use the correct XML escape sequences for any special characters in the value.
- Default—"Public IP Address Manager"
<ipManager@example.com >

notificationSubject

- Text used for the subject of e-mails about requests for or release of public IP addresses.
- Value—Text string that specifies the subject of the e-mail in XML format
- Guidelines—This value is not used if you configure e-mails to be machine-readable notifications. Be sure to use the correct XML escape sequences for any special characters in the value.
- Default—An IP request or release needs your attention.

renotificationSubject

- Text used for the subject of reminders to administrators about requests for or release of public IP addresses.
- Value—Text string that specifies the subject of the e-mail in XML format
- Guidelines—This value is ignored if you configure e-mails to be machine-readable notifications. Be sure to use the correct XML escape sequences for any special characters in the value.
- Default—REMINDER: An IP request or release still needs your attention.

notificationText

- Text that appears in the body of the e-mail.
- Value—Text string in XML format that specifies the body of the e-mail message
- Guidelines—This text and the URL appear in the body of the message if you specify that the e-mails are not machine-readable notifications. Otherwise, the URL appears in the subject, and the body is an XML document indicating which access needs attention. Be sure to use the correct XML escape sequences for any special characters in the value.
- Default—Please click on the link in this e-mail to go to a Web page where you will be able to fulfill a customer's request for public IP addresses, or acknowledge a customer's release of public IP addresses.

maxIpPoolSize

- Maximum number of public IP addresses that you can include in the pool that is used for the dynamic source NAT service.
- Value—Integer in the range 0–2147483647
- Guidelines—Configure this property if you want to provide NAT addresses through NAT Address Management Portal. Consult the JUNOS documentation for information about the maximum for each JUNOS routing platform.
- Default—32

Deploying the Enterprise Service Portals

The way you deploy the enterprise service portals depends on your Web application server.

If you are using a Web application server other than JBoss, see the documentation for your Web application server for information about the deployment.

For information about installing the enterprise service portal inside the JBoss Web application server, see *SRC-PE Getting Started Guide, Chapter 33, Installing Web Applications*.

Configuring the URL for an Enterprise Service Portal

By default, the name of the WAR file determines the URL that you use to access the enterprise service portal. For example, if the name of the WAR files is *entmgr.war*, the URL for the enterprise service portal is `http:// <host> : <port> /entmgr`.

- <host> —Name or IP address of the machine on which you install the enterprise service portal
- <port> —TCP/UDP port for HTTP traffic

If you want use a different URL, you must modify the relevant configuration file for your Web application server. For information about this task, see the documentation for your Web application server.

Writing an Application to Allow a Machine to Provide Public IP Addresses for NAT

If you use Enterprise Manager Portal and NAT Address Management Portal, and you use a machine to administer public IP addresses that you provide to enterprises.

To use a machine to administer public IP addresses:

1. Write an application that handles:
 - E-mails from Enterprise Manager Portal
 - XML messages that NAT Address Management Portal uses to communicate with the software that manages the IP addresses

For information about the XML messages, see *NAT Address Management Portal* on page 418.

2. Install the application that you created in Step 1 on a machine that contains the software for managing IP addresses.

Configuring an Enterprise Service Portal

Follow the configuration instructions in this section for:

- Enterprise Manager Portal
- NAT Address Management Portal
- An application that uses a configuration file based on the `easp_conf` template

Tasks to configure an enterprise service portal are:

1. Accessing the Configuration Files on page 442
2. Configuring Connections to the Subscriber Directory on page 443
3. Configuring Connections to the Service Directory on Solaris Platforms on page 446
4. Configuring Search Bases for Each Directory on page 449
5. Configuring the Logging Properties on page 450
6. (Optional) Configure a NIC proxy if you use a NIC to identify the SAEs that manage subscribers. See Configuring a NIC Proxy on page 451.
7. (Optional) Configure directory eventing if you use directory eventing to identify the SAEs that manage subscribers. See Configuring Directory Eventing for SAE Identification on page 451.
8. Exporting the Configuration to the Directory on page 452

If you use an enterprise service portal audit plug-in with your application, also complete the following task:

- Configuring an Enterprise Service Portal Audit Plug-In on page 452

Accessing the Configuration Files

On a Solaris platform, use SDX Configuration Editor to configure properties for enterprise service portals. For information about using SDX Configuration Editor, see *SRC-PE Getting Started Guide, Chapter 39, Using SDX Configuration Editor*.

To access the enterprise service portal configuration:

1. Start SDX Configuration Editor.
2. Import the sample data from the directory.
3. Open the folder called enterprise service portal.

4. Open the file for the enterprise service portal that you want to configure.

Configuring Connections to the Subscriber Directory

To use SDX Configuration Editor to configure the connections to the directory that contains information about subscribers:

1. Click the **LDAP** tab in the configuration file.

The LDAP pane appears.

The screenshot shows the LDAP configuration interface. The 'User Data' section is expanded, revealing the following fields and values:

- Server Address:** 127.0.0.1
- Server Port:** 389
- Authentication DN:** cn=ent-admin,o=operators,o=umc
- Password:** *** (with a 'Show' button)
- Enable SNMP Monitoring:** No
- Secured LDAP protocol:** Checked (with a 'Disable' button)
- Filter for loading subscriptions:** Subscriber Reference Filter
- Session Usage Refresh Time Interval:** 900

The 'Service Data' and 'Search Base' sections are currently collapsed.

2. Expand the entry called **User Data**, and configure the properties for the directory that contains information about subscribers.
3. Save the file.

Server Address

- List of subscriber directories. The first entry is the primary directory, and the rest are backup directories.
- Value—Space-separated list of IP addresses or names of hosts that support subscriber directories
- Guidelines—If one directory contains both subscribers and services, be sure to use the same value for this field in both the User Data entry and the Service Data entry.
- Default—127.0.0.1
- Property name—ent.repository.ldap.subscriber.server.address

Server Port

- Port number for the subscriber directory servers. The primary host and all backup directory hosts must use this port.
- Value—TCP port
- Guidelines—If one directory contains both subscribers and services, be sure to use the same value for this field in both the User Data entry and the Service Data entry.
- Default—389
- Property name—ent.repository.ldap.subscriber.server.port

Authentication DN

- DN for authentication with the subscriber directory.
- Value—DN
- Default—*cn = ent-admin, o = operators, o = umc*
- Property name—ent.repository.ldap.subscriber.manager.authDN

Password

- Password for authentication with the subscriber directory.
- Value—Text string
- Default—ent
- Property name—ent.repository.ldap.subscriber.manager.password

Enable SNMP Monitoring

- Whether or not information about enterprise service portal directory connections to the SNMP directory connection table if an SRC SNMP agent is running on the same host as the enterprise service portal.
- Value
 - Yes—Enable SNMP monitoring.
 - No—Do not enable SNMP monitoring.
- Default—No
- Property name—ent.repository.ldap.subscriber.des.enable_sysman

Secured LDAP Protocol

- Security protocol that the enterprise service portal uses to connect to the subscriber directory.
- Value—ldaps
- Default—ldaps
- Property name—ent.repository.ldap.subscriber.manager.security.protocol

Filter for Loading Subscriptions

- Filter that the SAE uses when it loads sample enterprise data from the subscriber directory.
- Value—One of the following filters:
 - Subscriber Reference Filter—The SAE runs a search based on the subscriberRef attribute in the umcServiceProfile object class, which is the base object class of the service profile hierarchy. The subscriberRef attribute contains a DN that points to the parent of the subscriber object.
 - Subscription Objectclass Filter—The SAE performs a one-level search with the directory entry, which represents the subscriber folder as the base DN. The search filter is (objectClass = sspServiceProfile). This method can be slow if you have a large number of subscription entries within the subscriber folder subtree.
- Guidelines—If you use a directory that does not search efficiently for large numbers of subscribers, specify the Subscriber Reference Filter. Otherwise, use the Subscription Objectclass Filter.
- Default—Subscription Objectclass Filter
- Property name—ent.repository.ldap.subscriber.server.loadSubscriptionFilter

Session Usage Refresh Time Interval

- How often the enterprise service portal contacts the SAE to obtain updates for usage data. The SAE obtains this data from the router.
- Value—Number of seconds in the range 0 to 2147483647
- Guidelines—If you specify a lower value than the default, you may cause a denial-of-service attack on the router.
- Default—900
- Example—1200

Configuring Connections to the Service Directory on Solaris Platforms

To configure the connections to the directory that contains information about subscribers:

1. Click the **LDAP** tab in the configuration file.

The LDAP pane appears.

The screenshot shows the LDAP configuration interface. It has a title bar 'LDAP' and three main sections: 'User Data', 'Service Data', and 'Search Base'. The 'Service Data' section is expanded, revealing several configuration fields. The 'Server Address' field contains '127.0.0.1', 'Server Port' contains '389', and 'Authentication DN' contains 'cn=ent-admin,o=operators,o=umc'. The 'Password' field is masked with '***' and has a 'Show' button. 'Enable SNMP Monitoring' is set to 'No', 'Secured LDAP protocol' is checked with a 'Disable' button, 'Enable Directory Eventing' is set to 'Yes', and 'Polling Interval' is set to '60'.

2. Expand the entry called **Service Data**, and configure the properties for the directory that contains information about subscribers.
3. Save the file.

Server Address

- List of service directories. The first entry is the primary directory, and the rest are backup directories.
- Value—Space-separated list of IP addresses or names of hosts that support service directories
- Guidelines—If one directory contains both subscribers and services, be sure to use the same value for this field in both the User Data entry and the Service Data entry.
- Default—127.0.0.1
- Property name—ent.repository.ldap.service.server.address

Server Port

- Port number for the service directory servers. The primary host and all backup directory hosts must use this port.
- Value—TCP port number
- Guidelines—If one directory contains both subscribers and services, be sure to use the same value for this field in both the User Data entry and the Service Data entry.
- Default—389
- Property name—ent.repository.ldap.service.server.port

Authentication DN

- DN for authentication with the service directory.
- Value—DN
- Default—*cn = ent-admin, o = operators, o = umc*
- Property name—ent.repository.ldap.service.manager.authDN

Password

- Password for authentication with the service directory.
- Value—Text string
- Default—ent
- Property name—ent.repository.ldap.service.manager.password

Enable SNMP Monitoring

- Whether or not to add Information about enterprise service portal directory connections to the SNMP directory connection table if an SRC SNMP agent is running on the same host as the enterprise service portal.
- Value—Yes or No
- Default—No
- Property name—ent.repository.ldap.service.des.sysman

Secured LDAP protocol

- Whether or not the enterprise service portal uses a security protocol to connect to the service directory.
- Value—LDAPS
- Guidelines—If the connection to the directory is secure, click Enable to enforce use of LDAPS. Click Disable if the connection to the directory is not secure.
- Default—ldaps
- Property name—ent.repository.ldap.service.manager.security.protocol

Enable Directory Eventing

- Whether or not enterprise service portal uses directory eventing to identify the SAE that manages a subscriber.
- Value
 - Yes—Enterprise service portal uses directory eventing to identify the SAE.
 - No—Enterprise service portal does not use directory eventing to identify the SAE.
- Guidelines—Set this property to Yes if you use directory eventing to identify the SAE that manages a subscriber. Set this property to No for NAT Address Management Portal, and for other enterprise service portals if you use a NIC to identify the SAE that manages a subscriber.
- Default—Yes
- Property name—ent.repository.ldap.service.des.enable_eventing

Polling Interval

- Time between polls that the enterprise service portal sends to the directory to obtain changes to the addresses of the SAEs' external interfaces.
- Value—Number of seconds in the range 15–2147483647
- Guidelines—Use the default value unless the response time of the directory is unacceptably long. In this case, use a higher value than the default. Do not use a lower value than the default.
- Default—60
- Property name—ent.repository.ldap.service.des.pollinginterval

Configuring Search Bases for Each Directory

You configure the base DN of information that the enterprise service portal uses in each directory.

To configure the search bases (the base DN in the directory that store particular types of information):

1. Click the **LDAP** tab in the configuration file.

The LDAP pane appears.

The screenshot shows the LDAP configuration interface. It has a title bar 'LDAP' and three main sections: 'User Data', 'Service Data', and 'Search Base'. 'User Data' and 'Service Data' are collapsed, while 'Search Base' is expanded. Under 'Search Base', there are six rows, each with a label and a text input field: 'Subscribers', 'Services', 'Global Parameters', 'Operators', 'Service Scopes', and 'Network'.

2. Expand the entry called **Search Base**, and configure the properties under this entry.
3. Save the file.

Subscribers

- Base DN of subscribers in the directory.
- Value—DN
- Default—*o = users, o = umc*
- Property name—*ent.repository.subscribers.base.dir*

Services

- Base DN of services in the directory.
- Value—DN
- Default—*o = services, o = umc*
- Property name—*ent.repository.services.base.dir*

Global Parameters

- Base DN of the global parameters for policies in the directory.
- Value—DN
- Default—*o = parameters, o = umc*
- Property name—ent.repository.parameters.base.dir

Operators

- Base DN of operators in the directory.
- Value—DN
- Default—*o = operators, o = umc*
- Property name—ent.repository.managers.base.dir

Service Scopes

- Base DN of service scopes in the directory.
- Value—DN
- Default—*o = scopes, o = umc*
- Property name—ent.repository.scopes.base.dir

Network

- Base DN of networks in the directory.
- Value—DN
- Default—*o = network, o = umc*
- Property name—ent.repository.network.base.dir

Configuring the Logging Properties

To use SDX Configuration Editor to configure logging properties:

1. Click the **Logging** tab in the configuration file.

The Logging pane appears.

2. Configure the logging properties.

You can see default settings for logging in this file. For information about configuring logging, see *SRC-PE Monitoring and Troubleshooting Guide, Chapter 4, Configuring Logging for SRC Components on a Solaris Platform*.

3. Save the file.

Configuring a NIC Proxy

If you use a NIC to identify the SAEs that manage subscribers, configure a NIC proxy for the enterprise service portal. Do not configure a NIC proxy for NAT Address Management Portal, because it does not need to identify the SAEs that manage subscribers.

To use SDX Configuration Editor to configure a NIC proxy:

1. Click the **SAE Resolution** tab in the configuration file.
2. Expand the entry called **NIC Proxy**, and configure the properties under this entry.

For information about configuring NIC proxies, see *SRC-PE Network Guide, Chapter 13, Configuring Applications to Communicate with an SAE*.

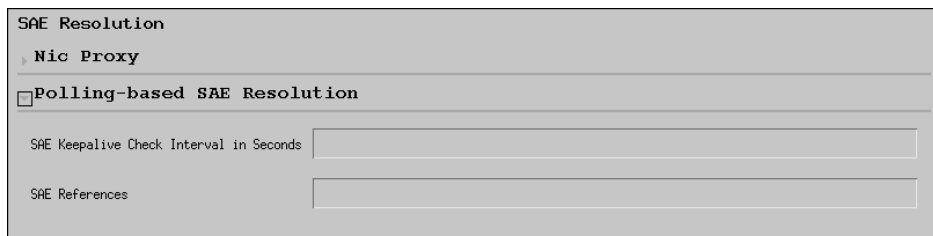
3. Save the file.

Configuring Directory Eventing for SAE Identification

For SRC implementations that use five or fewer SAEs, you can configure the enterprise service portal to use directory eventing to identify the SAEs that manage subscribers. Do not configure this feature for NAT Address Management Portal, because it does not need to identify the SAEs that manage subscribers.

To use the SDX Configuration Editor to configure directory eventing for SAE identification:

1. Click the **SAE Resolution** tab in the configuration file.



2. Expand the entry called **Polling-based SAE Resolution**, and configure the properties under this entry.
3. Save the file.
4. Be sure that the property `ent.feedback.urlupdateinterval` is configured in the SAE configuration (see *Modifying the SAE Property File* on page 57).

SAE Keepalive Check Interval in Seconds

- Time interval at which the enterprise service portal polls the SAE.
- Value—Number of seconds in the range 0–2147483647
- Guidelines—Specify a value that exceeds the interval at which the SAE updates the address of its external interface (configured in the property `ent.feedback.urlupdateinterval` in SAE properties).
- Default—5400
- Example—6000
- Property name—`ent.saewatchdog_timeout`

SAE References

- DN of the subtree that contains the addresses of the external interface of remote SAEs.
- Value—DN
- Default—`ou = sspadmurls, o = servers, o = umc`.
- Property name—`ent.feedback.admin.baseDN`

Exporting the Configuration to the Directory

For information about exporting the configuration to the directory, see *SRC-PE Getting Started Guide, Chapter 39, Using SDX Configuration Editor*. Enterprise service portal configurations are exported to `l = EASP, ou = staticConfiguration, ou = Configuration, o = Management, o = umc`.

Configuring an Enterprise Service Portal Audit Plug-In

The SRC software provides a sample event listener, `DefaultAuditEventListener`. You can use the sample listener, customize it, or use the information in the sample to create another audit plug-in. The sample event listener is in the SRC software distribution in the directory `/SDX/doc/ent/plugin/doc/net/juniper/smg/ent/plugin`. The sample listener sends output to a log file. See the documentation for the plug-in in the SRC software distribution in the folder `/SDX/doc/ent/plugin/doc` or on the Juniper Networks Web site at

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

If you create an audit plug-in, you add the plug-in class to the WAR file for the enterprise service portal.

Table 39 shows the common information that is provided by every enterprise service portal audit plug-in event.

Table 39: Common Audit Plug-In Information

Information	Description
Manager DN	Distinguished name that identifies the manager's profile in the directory; for example: <i>cn = unimgr, enterprisename = jnpr, ou = local, retailername = default, o = users, o = umc</i>
Manager principle	Manager's fully qualified log-in principle for logging in to the enterprise portal. For example, the equivalent principle for the Manager DN above is: <i>unimgr@jnpr/local.default</i>
Operation time	Time when the corresponding operation was successfully completed.

Table 40 describes the events that an audit plug-in listener can listen for and the information reported in those events.

Table 40: Events Reportable to the Audit Plug-In

Event	IT Manager Action That Initiates Event	Information Reported
ManagerLoginEvent	Logs in to an enterprise service portal.	Common information only.
ManagerLogoutEvent	Logs out of an enterprise service portal.	Common information only.
SubscribeAuditEvent	Subscribes to a service.	Common information plus: <ul style="list-style-type: none"> ■ DN of the new subscription object in the directory. ■ Attributes of the new subscription, including <i>sspState</i>, <i>sspAction</i>, and <i>parameterSubstitution</i>.
UnsubscribeAuditEvent	Unsubscribes from a service.	Common information plus: <ul style="list-style-type: none"> ■ DN of the subscription object removed from the directory. ■ Attributes of the removed subscription, including <i>sspState</i>, <i>sspAction</i>, and <i>parameterSubstitution</i>.
SubscriberUpdateAuditEvent	Changes the <i>parameterSubstitution</i> attribute of a subscriber object, such as adding or removing a substitution from the IT manager's enterprise object.	Common information plus: <ul style="list-style-type: none"> ■ DN of the subscriber object that is changed. ■ Attributes changed in the operation, including the old values and new values of the attributes.
SubscriptionUpdateAuditEvent	Changes the <i>parameterSubstitution</i> attribute of a subscription object; suspends, resumes, activates, or deactivates a subscription.	Common information plus: <ul style="list-style-type: none"> ■ DN of the subscription object that is changed. ■ Old and new values of the changed attributes: <ul style="list-style-type: none"> ■ <i>parameterSubstitution</i> attribute when subscriber object is changed. ■ <i>sspState</i> attribute when subscription is suspended or resumed. ■ <i>sspAction</i> attribute when subscription is activated or deactivated.

Table 40: Events Reportable to the Audit Plug-In (continued)

Event	IT Manager Action That Initiates Event	Information Reported
ServiceOpStateAuditEvent	Changes the operational state of a session. NOTE: Because changing the operational state of the session—such as dynamically activating or deactivating a subscription session—does not change the directory entry, the change is not persistent, and the subscription session returns to its administrative state after the subscriber's interface is restarted. Changes to the administrative state of a subscription are reported with the SubscriptionUpdateAuditEvent.	Common information plus: <ul style="list-style-type: none"> ■ DN of the subscriber that owns the subscription session. The subscriber must be a leaf in the subscriber tree in the enterprise scenario. ■ DN of the subscription object where the subscription session comes from. ■ Operational state of the session after the IT manager's action.
ExportAuditEvent	Exports a VPN.	Common information plus: <ul style="list-style-type: none"> ■ DN of VPN that is exported. ■ DN of the subscriber to which the VPN is exported.
UnexportAuditEvent	Cancels the export of a VPN.	Common information plus: <ul style="list-style-type: none"> ■ DN of VPN for which export is canceled. ■ DN of the subscriber for which export of the VPN was canceled.

Overview of Configuration for an Enterprise Service Portal Audit Plug-In

You must configure the properties for an enterprise service portal audit plug-in in configuration for an enterprise service portal. If you use the sample or create a plug-in based on the sample, use SDX Configuration Editor to configure the plug-in. If you customize the plug-in to use additional API properties, use an LDAP browser or SDX Admin to customize the plug-in.

Configuring the Sample Enterprise Service Portal Audit Plug-In

Use SDX Configuration Editor to configure properties for an enterprise service portal audit plug-in, also referred to as the Enterprise Service Portal audit plug-in, based on the sample.

Before you configure the properties, define the Java class for the plug-in. You can also configure the Java logging utility provided by JDK 1.4 to record the log messages. For more information about this utility, see

<http://java.sun.com/j2se/1.4.1/docs/api/java/util/logging/FileHandler.html>

To configure the audit plug-in:

1. Start SDX Configuration Editor.

For information about using SDX Configuration Editor, see *SRC-PE Getting Started Guide, Chapter 39, Using SDX Configuration Editor*.

2. Import the SRC system configuration from the directory.

3. Open a file for an enterprise service portal:
 - *ENT-MGR.xml* in the *EASP* folder
 - *NAT-ADDR.xml* in the *EASP* folder
 - File that uses the *easp_conf* template
4. Click the **EASP Audit Plug-In** tab.

The EASP Audit Plug_In pane appears.

5. Use the following descriptions to complete the fields in the Audit Plug-in area.
6. Save the file.
7. Export the SRC system configuration from the directory.



NOTE: You can also use SDX Admin to modify Enterprise Service Portal audit plug-in properties. See *Configuring a Customized Enterprise Service Portal Audit Plug-In* on page 456.

Plug-in Class

- Fully qualified name of the Java class for the Enterprise Service Portal audit plug-in event listener. If you implement your own plug-in event listener, set this property to the Java class of your listener. This property is mandatory for all Enterprise Service Portal audit plug-ins.
- Value—Text string
- Default—`net.juniper.smgmt.ent.plugin.DefaultAuditEventListener`
- Property name—`Plugin.EASPAudit.class`

Log Destination

- Path to the log file (relative to the folder where you installed the Enterprise Service Portal audit plug-in) and the pattern of the filename.
- Value—Text string, with the following special characters:

- /—Separator for names in the path
- %t—System's temporary folder
- %h—Current user's home folder
- %g—Generated number for this log file
- %u—Unique number for this log file
- %%—Percent sign
- Default—audit %g/log
- Property name—Plugin.EASPAudit.log.file.pattern

Maximum File Size

- Maximum number of bytes that the event listener can write to a file.
- Value—Number of bytes in the range 0–2147483647
- Default—10000
- Property name—Plugin.EASPAudit.log.file.limit

Log File Count

- How many log files the event listener should use.
- Value—Integer in the range 0–2147483647
- Default—3
- Property name—Plugin.EASPAudit.log.file.count

Log File Append Mode

- Whether or not the event listener should add to or replace the exiting information in the log file.
- Value
 - Append—Event listener should add new information to existing information.
 - Overwrite—Event listener should replace existing information.
- Default—Append
- Property name—Plugin.EASPAudit.log.file.append

Configuring a Customized Enterprise Service Portal Audit Plug-In

If you have customized the Enterprise Service Portal audit plug-in to use additional properties in the API, you must configure the plug-in with an LDAP browser or SDX Admin. To do so:

1. Start the LDAP browser or SDX Admin.
2. Access the file *I = EASP, ou = StaticConfiguration, ou = Configuration, o = Management, o = umc*.
3. Find the section that contains the properties with the prefix Plugin.EASPAudit.

4. Modify the existing properties in the file.

Each field description in the previous section includes a property name for the existing properties.

5. Add the properties that you included in the customized portal; be sure to include the prefix `Plugin.EASPAudit` for each property.
6. Specify appropriate values for the custom properties.
7. Save the file.

Chapter 28

Managing Enterprise Service Portals

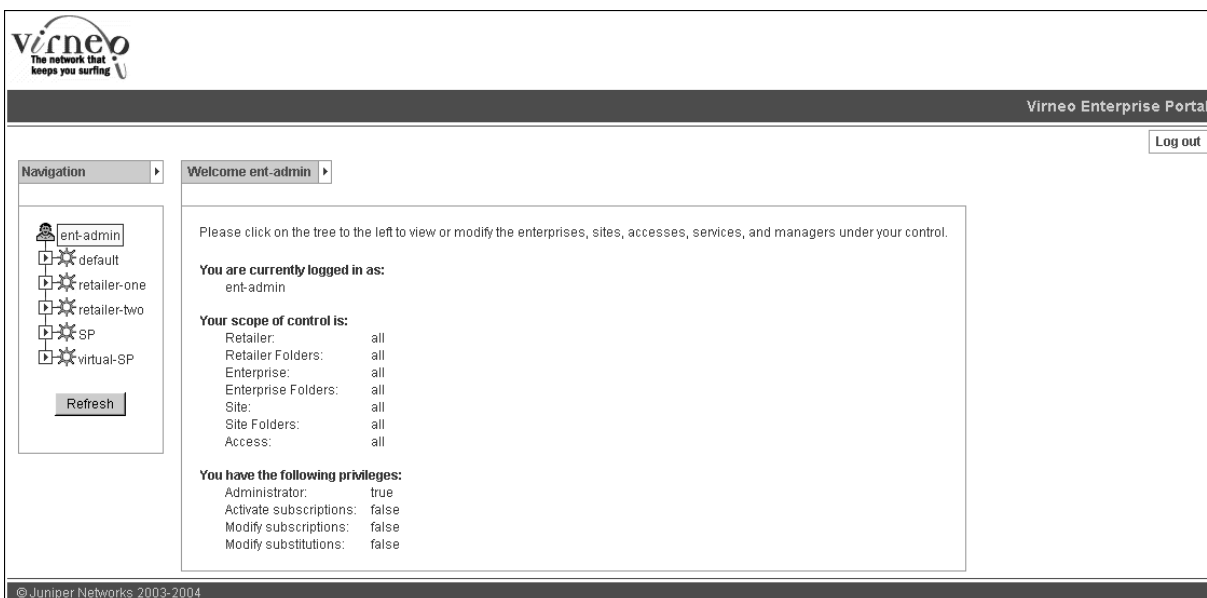
This chapter describes how IT managers and service providers can use enterprise service portals to log in to the SRC networks. The information in this chapter applies to Enterprise Manager Portal and to the sample enterprise service portal.

The chapter contains the following sections:

- Displaying Information About Your Control in the Enterprise on page 459
- Updating Data That the Enterprise Service Portal Displays on page 460
- Managing Operators on page 460

Displaying Information About Your Control in the Enterprise

To display information about your scope of control and permissions in the enterprise, click the icon for the manager at the root of the navigation pane. The portal displays your Welcome page.



Updating Data That the Enterprise Service Portal Displays

To update the data that the enterprise service portal displays, click Refresh in the navigation pane. This action deletes data from the enterprise service portal cache and causes the enterprise service portal to display new data from the directory. If you refresh a Web page in the portal with the Web browser's refresh utility, the Web browser displays data from the cache, and you may not see the latest data.

Managing Operators

Typically, a service provider uses an LDAP client or SDX Admin to create one operator for each enterprise. This operator, or manager, represents the primary IT manager for the enterprise.

For information about adding an operator from SDX Admin, see *Chapter 14, Configuring Subscribers and Subscriptions with the SRC CLI* or *Chapter 13, Configuring Subscribers and Subscriptions with SDX Admin*.

The primary IT manager uses the enterprise service portal to create other managers in the directory and gives those managers privileges to manage specific sites and accesses. IT managers can perform the following tasks to manage operators with the enterprise service portals we provide:

- Creating Managers on page 461
- Modifying Managers on page 463
- Deleting Managers on page 463

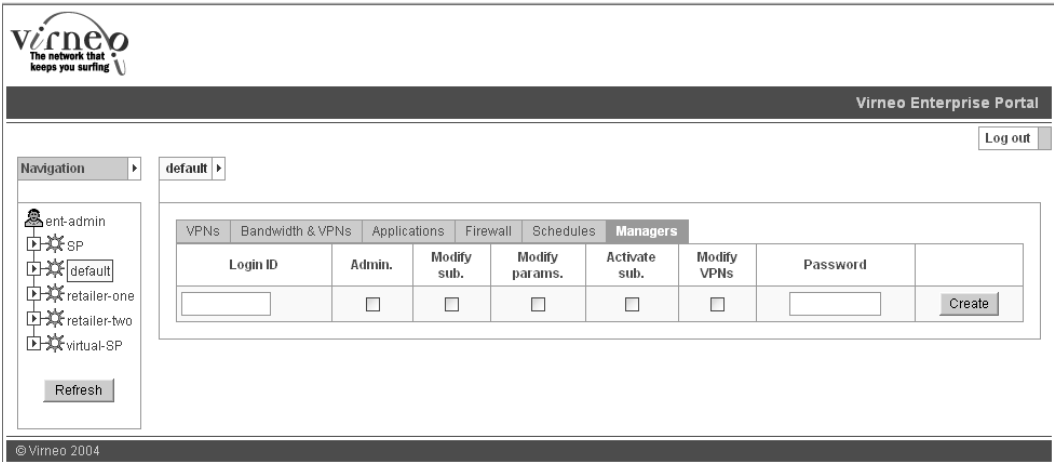
Creating Managers

To create managers through the enterprise service portal:

- 1. In the navigation pane of the enterprise service portal, click the object that you want the manager to control.
- 2. Click the **Managers** tab in the portal.

The portal displays the Manager's page for the object.

Figure 33: Manager's Page



- 3. Complete the fields in a new line of the table.

See *Managers Fields* on page 461.

- 4. Click **Create**.

The portal adds the new manager to the table.

Managers Fields

In the Managers tab of an enterprise service portal, you can modify the following fields to control privileges for managers.

Login ID

- Name that this manager uses to access the enterprise portal.
- Value—Text string
- Guidelines—Login IDs for enterprises must be unique within the whole enterprise; retailer-level login IDs must be unique to the retailer.
- Default—No value
- Example—Operator1

Admin.

- Whether or not the manager has complete control over managers, subscribers, subscriptions, substitutions, subscription sessions, and virtual private networks (VPNs) for this object and its subordinate objects.
- Value
 - Enabled—Checked box
 - Disabled—White box
- Default—Disabled

Modify sub.

- Whether or not the manager has complete control over subscriptions and subscription sessions for this object and its subordinate objects.
- Value
 - Enabled—Checked box
 - Disabled—White box
- Default—Disabled

Modify params.

- Whether or not the manager can configure substitutions in subscribers and subscriptions for this object and its subordinate objects.
- Value
 - Enabled—Checked box
 - Disabled—White box
- Default—Disabled

Activate sub.

- Whether or not the manager can configure automatic activation of subscriptions and manually activate and deactivate subscription sessions for this object and its subordinate objects.
- Value
 - Enabled—Checked box
 - Disabled—White box
- Default—Disabled

Modify VPNs

- Whether or not the manager can modify, export, and cancel the export of VPNs in the enterprise.
- Value
 - Enabled—Checked box
 - Disabled—White box

- Guidelines—This field appears only if the service provider configures the portal to display the VPN features.
- Default—Disabled

Password

- Password that this manager uses to access the enterprise portal.
- Value—Text string
- Default—No value
- Example—Secret

Modifying Managers

To modify a manager's privileges:

1. Start at the Manager's page (see Figure 33 on page 461).
2. Change the values in the fields for this manager.
3. If you want to revert to the original values, click **Reset**.
4. Click **Apply**.

Deleting Managers

To delete a manager:

1. Start at the Manager's page (see Figure 33 on page 461).
2. Click **Delete** for the manager.

Chapter 29

Managing Services with Enterprise Manager Portal

This chapter describes how IT managers and service providers can use Enterprise Manager Portal to manage subscribers, services, and subscriptions in their enterprises. The chapter contains the following sections:

- Overview of Enterprise Manager Portal on page 465
- Getting Help on Enterprise Manager Portal on page 466
- Setting the Configuration Level for Enterprise Manager Portal on page 466
- Managing Schedules on page 467
- Managing Subscriptions to Bandwidth-on-Demand Services on page 474
- Integrating VPNs into an SRC Network on page 487
- Classifying Traffic for Stateful Firewall Exceptions and NAT Rules on page 491
- Subscribing to Firewall Services on page 496
- Working with IP Addressing and NAT Services on page 513
- Monitoring the Status of Subscriptions on page 520

Overview of Enterprise Manager Portal

IT managers who connect to the SRC network through a JUNOS routing platform or JUNOSe router can use Enterprise Manager Portal to activate services, subscribers, and subscriptions for that enterprise. The services that IT managers can use depend on those that the service provider offers (see *Chapter 27, Installing and Configuring Enterprise Service Portals*). In SRC-managed environments that include both JUNOS routing platforms and JUNOSe routers, the router type determines which types of services can be configured on a system. The portal does not indicate whether a router is a JUNOS routing platform or a JUNOSe router. Table 41 lists the types of services that can be configured from Enterprise Manager Portal for JUNOSe routers and JUNOS routing platforms.


Table 41: Portal Configuration Support for Services on Routers

Type of Service	JUNOSe Router	JUNOS Routing Platform
BoD services	Yes	Yes
VPNs	No	Yes
Applications	No	Yes
Firewall services	No	Yes
NAT services	No	Yes

If you offer Network Address Translation (NAT) services, IT managers can also use the portal to request public IP addresses for use with NAT services on an access.

Getting Help on Enterprise Manager Portal

Most fields in the portal offer tool tips. To view tool tips for a field in the portal, hold the cursor over that field in the portal.

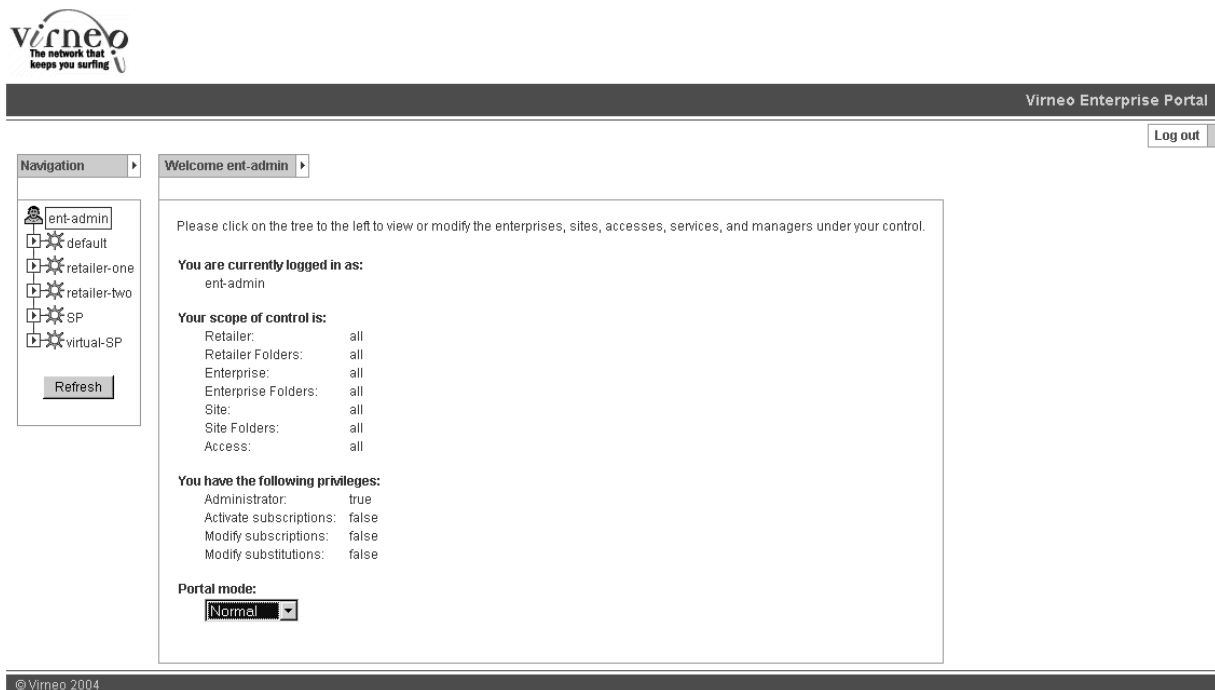
Some fields and pages in the portal offer more extensive online help. To view this help, click the help icon .

Setting the Configuration Level for Enterprise Manager Portal

The default setting for the configuration level is Normal. With this setting you can configure most services on a JUNOS routing platform. If you want to configure more advanced features, such as static source NAT rules, you must change the configuration level of the portal. To do so:

1. Click the operator icon in the navigation pane.

The operator's Welcome page appears.



2. Select **Advanced** from the Portal mode drop-down list.

Managing Schedules

An IT manager can configure schedules to be applied to BoD or firewall services for a specified enterprise subscriber. From Enterprise Manager Portal, you can establish schedules that identify the times when a specified BoD or firewall service can be activated or deactivated. Schedules are configured on a per-subscriber basis; they cannot be shared with other subscribers. Schedules are, however, inherited by subscribers subordinate to the subscriber for which the schedule is configured.



NOTE: NAT services cannot be scheduled.

Whether or not scheduling is available depends on the configuration for Enterprise Manager Portal and for the service.

To enable scheduling:

1. Edit the *web.xml* file for the portal to enable scheduling. See *Chapter 27, Installing and Configuring Enterprise Service Portals*.

When scheduling is enabled for the portal, a Schedules tab appears on Enterprise Manager Portal page.

2. Enable scheduling for the BoD or firewall service to be scheduled from Enterprise Manager Portal. See *Chapter 22, Reviewing and Configuring Policies and Services for Enterprise Manager Portal*.

If you plan to schedule BoD or firewall service subscriptions, you can configure the schedules first so that you can assign schedules at the time that you configure the subscription. If the subscriptions are already configured, you can edit the service definition to assign a schedule. The Schedules page lets you create new schedule definitions and view and change existing ones.

Each subscription, whether to the same service or to another one, can have its own schedule.

To use a schedule:

1. Create the schedule. See *Creating a Schedule* on page 468.
2. Apply the schedule to a subscription. See *Applying a Schedule to a Service* on page 472.

Creating a Schedule

To create a schedule:

1. Click the **Schedules** tab.

The Schedules page appears.

default ▶ local ▶ Acme ▶ Boca ▶ Primary ▶

Bandwidth & VPNs	Applications	Firewall	Addresses	NAT	Schedules	Managers
Schedule Name	Definition					
Promotional	Occurs on 02/07/2005 from 00:00 for 1 week(s)	Edit Delete				
GoldVideo	Occurs every Sunday, Saturday effective 02/01/2005 until 06/01/2005 from 00:01 for 23 hour(s)	Edit Delete				
		Create				

2. In the Schedules page, click **Create**.

The Schedule Definition Page appears.

- Using the field descriptions below, define a schedule, and click **Save**.

A description of the schedule appears in the Schedules page.



NOTE: The system generates the description of the service. If you want a page to display a different description, you can edit the JSP page and change and compile the Java classes found in the WAR file.

If you need assistance to make these changes, contact Juniper Professional Services.

Schedule Name

- Name of the schedule.
- Value—Text string
- Default—No value

Subscription is

- Whether or not the subscription can be activated during or outside the scheduled time.
- Value
 - Enabled during schedule—Service can be activated during the scheduled time.
 - Enabled outside schedule—Service can be activated outside the scheduled time.
- Default—No value

Start Time

- Time that a scheduled activity is to start.
- Value—Time of day in the format hh:mm, where hh indicates the hour and mm indicates the minute. The range is 00:00 to 23:59.
- Default—No value
- Example—13:15

Time Zone

- Time zone for which the schedule is defined.
- Value—Name of time zone
- Default—Local time zone

Duration

- Length of time after the start time that a scheduled activity is allowed.
- Value—Length of time in minutes, hours, days, or weeks
- Guidelines—The length of time should be more than 15 minutes; using a shorter time could adversely affect system performance. Table 42 shows the maximum duration for specified recurrence patterns.

Table 42: Maximum Duration for Recurrence Patterns

For This Recurrence Pattern	Duration Must Be Less Than
Daily	24 hours
Weekly	24 hours
Monthly	28th day of the month
Yearly	365 days

- Default—No value
- Example—2 hours

During the interval from the start time to 2 hours after the start time, the action (defined on the Schedule Definition Page under the *During schedule subscription is* field) is available.

Once

- Date on which the scheduled activity is to occur.
- Value—Date in the format mm/dd/yyyy, where mm indicates the month, dd indicates the day, and yyyy indicates the year
- Default—No value
- Example—12/10/2005

Daily

- Whether or not the scheduled activity is to occur every day of the week or every weekday.
- Value
 - day—Scheduled activity is to occur on every day of the week
 - weekday—Scheduled activity is to occur on each day Monday through Friday
- Default—No value

Weekly

- Scheduled activity occurs on a specified day or days during a week.
- Value—Name of day(s) of the week
- Default—No value

Monthly

- Scheduled activity occurs on the indicated day every month
- Value—Day of the month
- Default—No value

Yearly

- Scheduled activity occurs on a specified day each year
- Value—Month and day
- Default—No value

Range of recurrence Start by

- Date on which a schedule starts for a recurring action.
- Value—Date in the format mm/dd/yyyy, where mm indicates the month, dd indicates the day, and yyyy indicates the year
- Default—No value

The default indicates that the recurring schedule starts immediately—the next time the recurrence pattern applies.
- Example—12/10/2005

Range of recurrence End by

- Date on which a schedule ends for a recurring action.
- Value—Date in the format mm/dd/yyyy, where mm indicates the month, dd indicates the day, and yyyy indicates the year
- Default—No value
The default indicates that the schedule has no end date and remains in place indefinitely.
- Example—12/10/2005

Applying a Schedule to a Service

Before you can schedule a subscription, you must define a schedule. See *Creating a Schedule* on page 468.

To apply a schedule to a service that was configured earlier:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber for which you want to schedule a service.
2. Click the tab for the type of service to be scheduled:
 - Bandwidth or Bandwidth & VPNs
 - Firewall



NOTE: If VPN features are not configured, the tab is named Bandwidth.

3. On the same line as the service to be assigned to a schedule, select the name of a schedule under Schedule, and click **Apply**.

The service provider controls which services can be scheduled. Text on the page indicates which services cannot be scheduled.

default ▶ local ▶ Acme ▶ Boca ▶ Primary ▶

Bandwidth & VPNs Applications Firewall Addresses NAT Schedules Managers

Bandwidth Level ?

1.0 Mbps

Inherited from site "Boca"
Status...
Usage data...

Name	Affected Traffic	BoD Service ?	Destination VPN ?	Schedule ?	Enabled	
Rule1	Source IPs: 192.0.2.1/22 Destination IPs: 192.0.2.22/22 <input type="button" value="Edit"/>	Gold <input type="button" value="Apply"/>	None <input type="button" value="Apply"/>	GoldVideo <input type="button" value="Apply"/>	<input type="checkbox"/>	<input type="button" value="Delete"/> Status... Usage data...
Rule2	Source IPs: 10.10.10.168/24 Destination IPs: 10.10.10.100/24 <input type="button" value="Edit"/>	Silver <input type="button" value="Apply"/>	None <input type="button" value="Apply"/>	No schedule <input type="button" value="Apply"/>	<input type="checkbox"/>	<input type="button" value="Delete"/> Status... Usage data...

Disabling a Schedule for a Service

When you disable a schedule for a subscription, the service remains in the same state as when the schedule was disabled. For example, if the service is inactive at the time the schedule is removed, the service remains inactive. This state can be different from the one indicated by the Enabled check box. After disabling a schedule for a service, ensure that the status of the service is the same as indicated by the Enabled check box.

To disable a schedule for a service:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber for whom you want to remove a schedule that is assigned to a service, and then click the **Bandwidth & VPNs** (or **Bandwidth**) or **Firewall** tab.
2. On the line for the service select **No Schedule**, and then in the last column click the **Status** link.
3. On the Subscription Status page, check the status of the sessions listed. If a session status is different from what it should be—for example if it is inactive instead of active—click **Fix Problems** to activate or deactivate the session.

See *Monitoring the Status of Subscriptions* on page 520.

Changing Schedules

You can change a schedule at any time. Before you delete a service schedule, however, you must make sure that the schedule is not being used by any service.

To modify a schedule:

1. Click the **Schedules** tab; then on the line that describes the schedule that you want to change, click **Edit**.
2. On the Schedule Edit page, change values using the field descriptions under *Creating a Schedule* on page 468, and click **Apply**.

To delete a schedule:

1. Before you delete a schedule, make sure that none of the services reference this schedule:
 - Go to the Bandwidth (or Bandwidth & VPNs) page and review the names of schedules listed under Schedule. If the name of the service to be changed is listed, change the schedule to another one or to Any.
 - Go to the Firewall page and review the names of schedules listed under Schedule. If the name of the service to be changed is listed, change the schedule to another one or to Any.
2. Click the **Schedules** tab; then on the line that describes the schedule that you want to delete, click **Delete**.

The Schedules page no longer lists the schedule.

Managing Subscriptions to Bandwidth-on-Demand Services

The service provider makes bandwidth services available to enterprises. IT managers can use these services to provision bandwidth within an enterprise to meet the forwarding requirements for subscriber traffic. The service provider can make the following types of bandwidth services available:

- Bandwidth-level allocation for an Internet access link

Only one subscription to one bandwidth level is supported for an access link.

- BoD services that classify traffic and assign different classes of traffic to different BoD services

You can classify traffic by source IP address, destination IP address, source Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port, destination TCP or UDP port, or type-of-service (ToS) byte, and assign that traffic to a service level.



NOTE: Enterprise Manager Portal supports only services that have policies configured.

When both of these services are available, you can provide subscribers with class of service (CoS)—the method of classifying traffic on a packet-by-packet basis with information in the ToS byte to provide different service levels to different traffic.

Whether bandwidth level (a basic BoD service), BoD services, or both are available depends on the configuration for the portal. See *Chapter 27, Installing and Configuring Enterprise Service Portals*.

Planning Subscriptions to BoD Services

When planning subscriptions, consider the following factors:

- In a configuration that includes both a subscription to a bandwidth level and subscriptions to BoD services, the bandwidth level must be set before BoD services can be configured.

If a subscription to a bandwidth level needs to be deleted or moved, all subscriptions to BoD services for subscribers in the same container must be disabled or deleted first.

- BoD services are inherited by subscribers who are subordinate in the navigation pane.
- A rule for a BoD service specifies which fields in the IP header to match—protocol, source IP address, destination IP address, source TCP or UDP port, destination TCP or UDP port, or ToS byte—and the BoD service to assign to packets that match the conditions. If configured, a destination VPN can also be assigned.

If a packet matches more than one rule for BoD services, which rule is applied is unpredictable. For example, if the destination IP address matches a rule for a Gold BoD service, but the destination port matches the source TCP port for a Silver BoD service, and the rules have no other conditions, which rule is applied is uncertain.

Plan rules for BoD services so that a packet matches all the following conditions—protocol, source IP address, destination IP address, source TCP or UDP port, destination TCP or UDP port, or ToS byte—for only one BoD service.

Creating a Subscription to BoD Services

When you create a subscription to a BoD service, you initially set a bandwidth level if available and not previously set.

Setting a Bandwidth Level

To create a subscription to a bandwidth level:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber for whom you want to provision bandwidth.

- Click the **Bandwidth & VPNs** tab.



NOTE: If VPN features are not configured, the tab is named Bandwidth.

The Bandwidth & VPNs page appears.

Figure 34: Bandwidth & VPNs Page

retailer-one ▾

VPNs **Bandwidth & VPNs** Applications Firewall Schedules Managers

Welcome to Virneo's Bandwidth and VPN services.

Please select a Bandwidth Level from the list below. Click on the help icon ⓘ to see a description of how each Bandwidth Level would affect your network traffic. The Bandwidth Level that you select here will be enforced on all internet access links at or below the location you have currently selected in the tree on the left side of this page.

Consider carefully the locations at which you will subscribe to a Bandwidth Level service. A Bandwidth Level subscription affects all accesses underneath the subscription location, and you are only allowed to have one Bandwidth Level subscription affect a given access. For example, if you subscribe a site to a Bandwidth Level service, you can not subscribe the enterprise that contains that site to a Bandwidth Level service, because the two subscriptions would affect the same accesses in the site.

Bandwidth Level ⓘ

Default ▾ Apply

- Using the field description below, select a bandwidth level, and click **Apply**.

The bandwidth level becomes available, and the fields for setting BoD services appear on the Bandwidth page.

Bandwidth Level

- Bandwidth assigned to an access link (the basic BoD service in the directory). The bandwidth level governs the overall bandwidth available on the link.
- Value—Menu of bandwidth levels in the directory available for this subscriber. See the online help ⓘ for information about the menu entries.
- Guidelines—A subscriber can be assigned to up to one bandwidth level on an access link.

In the navigation pane, a subscriber subordinate to the one who has the bandwidth level subscription inherits the subscription. A subordinate subscriber cannot subscribe to another bandwidth level.

If you select default for the value, all traffic is treated the same.

- Default—Bandwidth level specified as the default by the service provider.

Adding Subscriptions to BoD Services

To add a subscription to a BoD service:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber to assign to a BoD service.
2. Click the **Bandwidth & VPNs** tab.
3. If a bandwidth level has not been set, specify a bandwidth level.

The bandwidth level becomes available, and the fields for setting BoD services appear on the Bandwidth & VPNs page.

Figure 35: Bandwidth & VPNs Page with a Bandwidth Level Set

default > local > Acme > Boca > Primary >

Bandwidth & VPNs Applications Firewall Addresses NAT Schedules Managers

Bandwidth Level ?

1.0 Mbps ▾ Apply

Inherited from enterprise "Acme"
Status...
Usage data...

Name	Affected Traffic	BoD Service ?	Destination VPN ?	Schedule ?	Enabled	
Rule1	IP Protocol tcp Source Address 192.0.2.0/24 Edit Destination Address 192.0.2.0/24	Gold ▾	None ▾	No schedule ▾	<input type="checkbox"/>	Delete

Apply

Create Bandwidth Rule

Status...
Usage data...

4. Click **Create Bandwidth Rule**.

The Create Rule dialog box appears.

Create Rule	
Rule Name	<input type="text"/>
IP Protocols	<input type="text"/>
ToS Byte	<input type="radio"/> DiffServ <input type="text"/> <input type="radio"/> Precedence <input type="text"/> <input type="radio"/> Free Format (e.g. 110101xx) <input type="text"/>
Source IP Addresses	<input type="text"/>
Source Ports	<input type="text"/>
Destination IP Addresses	<input type="text"/>
Destination Ports	<input type="text"/>
TCP Flags	<input type="text"/>
Fragmentation Flags	<input type="text"/>
Fragment Offset	<input type="text"/>
Packet Length	<input type="text"/>
ICMP Type	<input type="text"/>
ICMP Code	<input type="text"/>
BoD Service	Gold <input type="button" value="v"/>
Destination VPN	None <input type="button" value="v"/>
Enabled	<input type="checkbox"/>
<input type="button" value="Create"/> <input type="button" value="Cancel"/> <input type="button" value="Reset"/>	

- Using the field descriptions below, configure subscriptions for BoD services.

You can configure any number of subscriptions by assigning different traffic flows, identified by rules under Affected Traffic on the Bandwidth & VPNs page (see Figure 35 on page 477), to different BoD services.

- Click **Create**.

The subscription appears in the Bandwidth & VPNs page.

Rule Name

- Name of the BoD rule.
- Value—Alphanumeric characters without spaces
- Default—No value
- Example—SalesVideoConference

IP Protocols

- IP protocol associated with traffic affected by this bandwidth rule.
- Value—One of the following:
 - ah—authentication header
 - egp—exterior gateway protocol
 - esp—Encapsulating Security Payload
 - gre—generic routing encapsulation
 - icmp—Internet Control Message Protocol
 - igmp—Internet Group Management Protocol
 - ipip—IP over IP
 - ospf—Open Shortest Path First
 - pim—Protocol Independent Multicast
 - rsvp—Resource Reservation Protocol
 - sctp—Stream Control Transmission Protocol
 - tcp—Transmission Control Protocol
 - udp—User Datagram Protocol
 - < ipProtocolNumber >
- Guidelines—Specify an IP protocol or its corresponding number if you want to enable BoD for a certain type of traffic. If you want to enable BoD for all IP protocols, leave this field empty. If you specify an IP protocol other than TCP or UDP, the port fields will dim, and you will not be able to specify port numbers for this subscription.
- Default—No value
- Example—tcp

ToS Byte

- ToS byte in the header of the IP datagram associated with traffic affected by this bandwidth rule.
- Value
 - DiffServ—DiffServ is used to classify packets by the selected value.
 - Precedence—Value of the drop precedence.
 - Free Format—ToS byte in binary format.
Use an x to indicate a bit to be ignored.

- Guidelines—You can configure the ToS byte only if the configuration level is set to Advanced (see *Setting the Configuration Level for Enterprise Manager Portal* on page 466).

Specify the ToS byte in this field if you want to enable BoD for a specific type of service. If you want to enable BoD for all types of service, leave this field empty.

- Default—No value
- Example—Free Format 000010xx

Source IP Addresses

- Source IP address(es) (contained in the IP packets) of traffic affected by this bandwidth rule.
- Value—[not] < networkAddress > / < networkMask >
 - not—Address, or set of IP addresses as expressed by the netmask, for which the BoD service is not available
 - < networkAddress > —IP address of the network
 - < networkMask > —Netmask expressed as an integer 0–32, which specifies how many of the first bits in the address specify the network
- Guidelines—To specify traffic not from a source IP address or not from a set of IP addresses as expressed by the netmask, precede the IP address with the keyword **not**. To specify traffic with any source IP address, leave the field empty.

The order in which you list prefixes, identified by the IP address–netmask pair, is not significant. They are all evaluated to determine whether a match occurs. If prefixes overlap, longest-match rules are used to determine whether a match occurs. For an address to be considered a match, it must match one of the rules in the list.

For information about how JUNOS routing platforms evaluate prefixes, see the *JUNOS Policy Framework Configuration Guide*.

- Default—No value
- Example—In this example for a JUNOS routing platform, all IP addresses on the subnet 172.16.0.0/10 are specified, except for those on the subnet 172.16.2.0/16.
172.16.0.0/10, not 172.16.2.0/16

Source Ports

- Source TCP/UDP port(s) (contained in the IP packets) of traffic affected by this bandwidth rule.
- Values
 - Port number
 - Comma-separated list of port numbers and ranges of port numbers (JUNOS routing platforms)
 - Ranges of port numbers separated by two dots (..)

- Guidelines— To specify all ports, leave this field empty. If you specify an IP protocol other than TCP or UDP for this subscription, the port field will dim, and you will not be able to specify port numbers in this field.
- Default—No value
- Example
 - 2
 - 2, 3, 45..55

Destination IP Addresses

- Destination IP addresse(s) (contained in the IP packets) of traffic affected by this bandwidth rule.
- Value—[not] < networkAddress > / < networkMask >
 - not—Address, or set of IP addresses as expressed by the netmask, for which the BoD service is not available
 - < networkAddress > —IP address of the network
 - < networkMask > —Netmask expressed as an integer 0–32, which specifies how many of the first bits in the address specify the network
- Guidelines—To specify traffic not to a destination IP address or not to a set of IP addresses as expressed by the netmask, precede the IP address with the keyword **not**.

The order in which you list prefixes, identified by the IP address–netmask pair, is not significant. They are all evaluated to determine whether a match occurs. If prefixes overlap, longest-match rules are used to determine whether a match occurs. For an address to be considered a match, it must match one of the rules in the list.

For information about how JUNOS routing platforms evaluate prefixes, see the *JUNOS Policy Framework Configuration Guide*.

- Default—No value
- Example—192.0.2.0/24

Destination Ports

- Destination TCP/UDP port(s) (contained in the IP packets) of traffic affected by this bandwidth rule.
- Value
 - Port number
 - Comma-separated list of port numbers and ranges of port numbers (JUNOS routing platforms)
 - Ranges of port numbers separated by two dots (..)
- Guidelines—To specify all ports, leave this field empty. If you specify an IP protocol other than TCP or UDP for this subscription, the port field will dim, and you will not be able to specify port numbers in this field.

- Default—No value
- Example
 - 2
 - 2, 3, 45..55

TCP Flags

- Conditions in the TCP flags in the TCP message header. This field is enabled when the TCP protocol is selected.
- Value—Expression or text synonym that identifies the TCP flags
- Guidelines—You can enter a value for TCP flags only if you select TCP as the IP protocol.

You can enter a logical expression that contains the symbols for the six TCP flags: urgent, ack, push, rst, syn, and fin. You can use the following logical operators in the list of flags:

- &—And. Separates flag settings in the list.
- !—Not. Flags preceded by ! are cleared; flags not preceded by ! are set.

You can use the following expression instead of the entire expression:

- tcp-initial—syn & !ack

The interface displays text synonyms for expressions if stored data matches the expression.

This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—No value
- Example
 - syn
 - tcp-initial

Fragmentation Flags

- Logical expression using the dont-fragment, more-fragments, and reserved IP fragmentation flags.
- Value—Flags expression
- Guidelines—The expression can also contain the following logical operators:
 - &—And. Separates flag settings in the list.
 - !—Not. Flags preceded by ! are cleared; flags not preceded by ! are set.
- Default—No value
- Example
 - more-fragments
 - ! dont-fragment

Fragment Offset

- IP fragment offset—a value that defines the order in which to assemble fragments for an IP datagram.
- Value—One of the following:
 - Number in the range 0–8191
 - Range of numbers separated by two dots (..) within the range 0–8191
- Default—No value
- Example
 - 50
 - 50 .. 76

Packet Length

- Length of packets.
- Value—One of the following:
 - Number in the range 0–65536
 - Range of numbers separated by two dots (..) within the range 0–65536
- Default—No value
- Example
 - 15000
 - 15000 .. 30000

ICMP Type

- Type of message for Internet Control Management Protocol (ICMP).
- Value—Type of ICMP message in the following formats:
 - Number of the ICMP message type in the range 0–255
 - Symbolic name for an ICMP message type
 - Comma-separated list of ICMP types and ranges of ICMP types
 - Ranges of ICMP types separated by two dots (..) within the range 0–255
 - Blank—Any ICMP type
- Guidelines—You can enter a value for this field only if you select the icmp protocol (protocol number 1).

The following list shows the symbolic name and associated numbers for ICMP types. The ICMP types are the same as those on JUNOS routing platforms with the addition of traceroute.

- 0—echo-reply
- 8—echo-request
- 16—info-reply
- 15—info-request
- 18—mask-reply

- 17—mask-request
- 12—parameter-problem
- 5—redirect
- 9—router-advertisement
- 10—router-solicit
- 4—source-quench
- 11—time-exceeded
- 13—timestamp
- 14—timestamp-reply
- 30—traceroute
- 3—unreachable

This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—Any
- Example—10 .. 25, 27


ICMP Code

- Code for ICMP.
- Value—Type of ICMP code in the following formats:
 - Number of ICMP code in the range 0–255
 - Comma-separated list of code numbers and ranges of code numbers
 - Ranges of code numbers separated by two dots (..) within the range 0–255
 - Blank—Any ICMP code
- Guidelines—You can enter a value for this field only if you select particular protocols.

This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—Any
- Example—75

BoD Service

- Name of the BoD service in the directory that will be applied to the subscription.
- Value—Menu of BoD services available for this subscriber. See the online help  for information about the menu entries.

- Guidelines—How BoD services define bandwidth allocation depends on whether or not a bandwidth level is set:
 - On a link that has a bandwidth level set, the BoD service defines the transmission service and the forwarding priority of the traffic for the subscription—for example, expedited or best-effort.
 - On a link that does not have bandwidth allocated, the BoD service typically specifies the fixed bandwidth level available to the traffic type for the subscription.

For more information about the interaction between the bandwidth level and BoD services, see *Chapter 22, Reviewing and Configuring Policies and Services for Enterprise Manager Portal*.

- Default—BoD service with lowest alphanumeric name in the directory
- Example—Gold

Destination VPN

- Configured VPN to use.
- Value—Name of VPN
- Guidelines—This field appears if configuration for VPNs is enabled for the portal. For more information about VPNs, see *Modifying Subscriber VPN Configuration* on page 487.
- Default—No value

Enabled

- Status of the subscription.
- Value
 - Gray box—Subscription is inherited from a parent subscriber
 - White box—Subscription is configured for this subscriber
 - Box with check mark—Subscription is enabled
 - Empty box—Subscription is disabled
- Guidelines—Click box to enable or disable a subscription.
- Default—Subscription is disabled

Modifying Rules for a Subscription to a BoD Service

To modify rules for a subscription to a BoD service:

1. Start at the subscriber's Bandwidth page (see Figure 35 on page 477).
2. Change the values in the fields for this rule.
3. Click **Apply** for the subscription.

Modifying the Bandwidth Level

To modify a bandwidth level:

1. Start at the subscriber's Bandwidth page (see Figure 35 on page 477).
2. Disable all BoD services that this subscriber inherits from parent subscribers.
3. Disable all BoD services defined for this subscriber's subordinate subscribers.
4. Select a new value from the Bandwidth Level menu.
5. Click **Apply**.
6. If needed, enable BoD services that this subscriber inherits from parent subscribers.
7. If needed, enable BoD services defined for this subscriber's subordinate subscribers.

Moving the Bandwidth Level

To move the bandwidth level to another subscriber:

1. Delete the bandwidth level. See *Deleting the Bandwidth Level* on page 486.
2. Set a bandwidth level for another subscriber. See *Creating a Subscription to BoD Services* on page 475.
3. Create BoD services. See *Creating a Subscription to BoD Services* on page 475.

Deleting a Subscription for a BoD Service

To delete a subscription to a BoD service:

1. Start at the subscriber's Bandwidth page (see Figure 35 on page 477).
2. Click **Delete** for the subscription.

Deleting the Bandwidth Level

To delete the bandwidth level:

1. Start at the subscriber's Bandwidth page (see Figure 35 on page 477).
2. Disable all BoD services that this subscriber inherits from parent subscribers.
3. Disable all BoD services defined for this subscriber's subordinate subscribers.
4. Select **Default** from the Bandwidth Level menu.
5. Click **Apply**.

Monitoring Use of Subscriptions to BoD Services

To monitor the use of a bandwidth subscription:

1. Start at the subscriber's Bandwidth page (see Figure 35 on page 477).
2. Click **Usage Data** for the bandwidth level or subscription.

The Service Usage page appears.



Service Usage

Service Usage Data

This data is for the subscription **Rule1** to service **Gold**.

Access Link	Usage Data					
	For Period From	For Period To	Incoming Bytes	Outgoing Bytes	Incoming Packets	Outgoing Packets
primary.boca.acme.local/default	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown
<input type="button" value="Refresh"/>						

The table above shows usage data for the service. The usage data covers the period starting when the service was most recently activated on the access link, and ending when the usage data was most recently collected from the network infrastructure. Usage data is collected periodically (e.g. once an hour). No usage data is available for subscriptions that are not active on the access link.

Usage data may be shown as "Unknown". Usage data may be unknown because no data has yet been collected for the access link, or because the access link is currently down, or because the usage data collection mechanism is temporarily unavailable.

© Virneo 2004

Integrating VPNs into an SRC Network

The service provider creates VPNs in the directory for specific subscribers. If the service provider configures the portal to display VPN features, IT managers with privileges to configure VPNs (see *Chapter 28, Managing Enterprise Service Portals*) can make modifications to VPNs that a subscriber owns.

Modifying Subscriber VPN Configuration

To modify a VPN:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber who owns the VPN that you want to modify.
2. Click the **VPNs** tab.

The VPNs page appears and displays the Available VPNs area. If the service provider configures the portal to display extranet features, this page also displays the Expose VPNs area.

Figure 36: VPNs Page

Virneo Enterprise Portal

Log out

Navigation

ent-admin

SP

default

local

Acme

ABCInc

Boca

Ottawa

Toronto

retailer-one

retailer-two

virtual-SP

Refresh

default > local > Acme >

VPNs Bandwidth & VPNs Applications Firewall Schedules Managers

Available VPNs

Name	VPN ID	Description	Source
Accounting	accounting	VPN for accounting group	Owned by this location

Apply

Expose VPNs

Name	VPN ID	Description	Exposed to:
Accounting VPN 1	accounting	VPN for accounting group	

Add

This location's ID is: acme.local/default

© Virneo 2004

- Using the field descriptions below, modify the VPN.
- Click **Apply**.

Name

- Name of the VPN that appears in other pages of Enterprise Manager Portal.
- Value—Text string
- Guidelines—Enter a name that summarizes the application of this VPN.
- Default—Value of the VPN ID field
- Example—Accounting VPN

VPN ID

- Unique identifier for the VPN.
- Value—Text string
- Guidelines—You cannot modify this value.
- Default—Specified by the service provider
- Example—Accounting

Description

- Description of the VPN.
- Value—Text string
- Default—Specified by the service provider
- Example—VPN for accounting in Boca

Source

- Whether or not the subscriber owns, imports, or inherits the VPN.
- Value—Text string
- Guidelines—You cannot modify this value.
- Default—Determined by the configuration of this VPN
- Example—Owned by this location

Creating Extranets

If the service provider configures the portal to display extranet features, IT managers with privileges to configure VPNs in their scope of control (see *Chapter 28, Managing Enterprise Service Portals*) can create extranets for other enterprises and retailers by exporting those VPNs. Enterprises and retailers who share VPNs that other subscribers own are called *extranet clients*.

To create an extranet:

1. Obtain a location identifier from the extranet client.

When you click an enterprise or retailer in the navigation pane of Enterprise Manager Portal, the location identifier for that subscriber appears at the bottom of the VPNs page (see Figure 36 on page 488). The default format of the location identifier is:

[< enterpriseName > . < subscriberFolderName > /] < retailerName >

- enterpriseName—Name of the enterprise in the directory
 - subscriberFolderName—Name of the subscriber folder that contains the directory
 - retailerName—Name of the retailer in the directory
2. Start at the VPN page for the subscriber who owns the VPN.
 3. In the field called Exposed to in the Expose VPNs area, enter the location identifier for the extranet client.
 4. Click **Add**.

The VPN page for the subscriber who owns the VPN displays the updated status of the VPN, and the extranet client now has access to the VPN.

Deleting Extranets

You can delete an extranet by canceling the export of a VPN. To do so:

1. Start at the VPN page for the subscriber who owns the VPN.
2. In the Expose VPNs area, identify the VPN and the extranet client for whom you want to delete the extranet.

3. Click **Delete** for the extranet client in the field Exposed to.

This action will deactivate all subscriptions to this VPN for the extranet client, and the extranet client will not be able to reactivate subscriptions to the VPN.

Sending Traffic to a VPN

If the service provider makes VPN features visible to subscribers, the name of the Bandwidth tab in the portal changes to Bandwidths & VPNs, and you can send traffic associated with BoD services to VPNs. To do so:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber for whom you want to send traffic to a VPN.
2. Click the **Bandwidth and VPNs** tab.
3. Follow the instructions in *Managing Subscriptions to Bandwidth-on-Demand Services* on page 474 to configure the BoD service.
4. From the menu in the Destination VPN field for that subscription, select the VPN to which you want to send the traffic.
5. Click **Create** for the subscription.

Modifying the VPN to Which the Router Sends Traffic

To modify the VPN to which the router sends traffic:

1. Start at the subscriber's Bandwidth & VPN page (see Figure 34 on page 476).
2. From the menu in the Destination VPN field for the subscription, select a different VPN from the menu.
3. Click **Apply** for the subscription.

Stopping the Router from Sending Traffic to VPNs

To stop a router from sending traffic to a VPN:

1. Start at the subscriber's Bandwidth & VPNs page (see Figure 34 on page 476).
2. From the menu in the Destination VPN field for the subscription, select **None**.
3. Click **Apply** for the subscription.

Classifying Traffic for Stateful Firewall Exceptions and NAT Rules

You can create for a subscriber a list of application objects that can be used to classify the traffic affected by a firewall exception to a stateful firewall or by a NAT rule. These application objects are based on application protocols—protocols that are categorized in the application layer of the TCP/IP reference model—or IP protocols that the JUNOS routing platform supports. Subordinate subscribers inherit application objects configured for parent subscribers.

An application protocol defines how a client and a server communicate during a *conversation*—a particular activity between the client and the server, such as an FTP session. A conversation in the application layer consists of multiple *flows*. A flow is one element of the conversation; for example, in an FTP session, the initial TCP control connection or a subsequent UDP traffic connection. You can apply a NAT rule or a firewall exception to the initial flow in a conversation by defining an application object. The NAT rule or firewall exception then applies to all subsequent flows in that conversation.

In the FTP example, the client may create a TCP connection to the server and send the server a UDP port number in the initial flow. The server may then start sending UDP traffic to the UDP port specified in the initial flow. If the initial flow matches a defined application object that a firewall allows, the firewall will allow the UDP traffic in the second flow and in all subsequent flows in the conversation.

Certain application protocols, such as FTP, are supported explicitly, and you can select them for your application object. These application protocols usually have an associated IP protocol that the portal selects automatically. If you want to create an application object for an application protocol that is not explicitly supported, such as HTTP, you can create an application object based on an IP protocol only. For example, you could create an application object called HTTP, specify no application protocol, and select TCP as the IP protocol. You can then specify 8080 for the source and destination ports in the application protocol to identify the HTTP traffic.

Classifying Traffic

To create an application protocol:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber to whom you want to assign the application object.
2. Click the **Applications** tab.

The Applications page appears. This page displays the application protocols that the subscriber inherits from parent subscribers and application protocols configured explicitly for the subscriber.

Figure 37: Applications Page

default ▾ local ▾ Acme ▾ Boca ▾ Primary ▾

Bandwidth & VPNs	Applications	Firewall	Addresses	NAT	Schedules	Managers
Name	Application Protocol	IP Protocol	Details			
bootp_boca_primary	bootp	udp	Inactivity timeout: 25 Destination port: 8067		<div>EditDelete</div>	
ftp_boca_primary	ftp	tcp	Inactivity timeout: 30 Destination port: 8098		<div>EditDelete</div>	
<div>Create Application</div>						

3. Click **Create Application**.

The Create Application page appears.

Create Application - Microsoft Internet Explorer

Create Application

Application Name: (Must be unique.)

Application Protocol:

IP Protocol:

Source Port:

Destination Port:

SNMP Command:

ICMP Type:

ICMP Code:

TTL Threshold:

RPC Program Number:

UUID:

Inactivity Timeout:

Create Cancel

4. Using the following field descriptions, specify details for the application protocol.

Some fields are available only for certain applications. When a field is unavailable, the box in which you enter information is dimmed, and you cannot enter information in it.

5. Click **Apply**.

Application Name

- Name for this application protocol.
- Value—Text string
- Default—No value
- Example—bootp-boston

Application Protocol

- Application protocol.
- Value—Type of application protocol or None
- Guidelines—Select a protocol from the menu to specify that the application uses a particular application protocol. Depending on the application protocol you choose, some fields in the application object are irrelevant (and disabled) or restricted to specific values. If the application protocol you want is not available, you can select the option **None** and base the application object on an IP protocol. If you select this option, the NAT rule or firewall exception affects only the first flow in a conversation. Consequently, you can deny or discard a conversation, but you cannot allow a complete conversation.
- Default—Any
- Example—bootp

IP Protocol

- IP protocol.
- Value—Type of IP protocol or number of IP protocol in the range 0–255
- Guidelines—The names of the allowed IP protocols are shown in the tool tips for this field. The portal automatically selects an IP protocol for certain application protocols.
- Default—No value
- Example—tcp

Source Port

- Source TCP/UDP ports (as contained in the IP packets) of traffic for this application object.
- Value—Integer in the range 0–65535
- Guidelines—Enter either a single port number or a range of port numbers separated by two dots (..). To specify all ports, leave this field empty.
- Default—No value
- Example—25..35

Destination Port

- Destination TCP/UDP ports (as contained in the IP packets) of traffic for this application object.
- Value—Integer in the range 0–65535
- Guidelines—Enter either a single port number or a range of port numbers separated by two dots (..). To specify all ports, leave this field empty.
- Default—No value
- Example—25..35

SNMP Command

- Type of command for Simple Network Management Protocol (SNMP).
- Value—Type of SNMP command
- Guidelines—Select a type of command from the menu.
- Default—Any
- Example—get-next

ICMP Type

- Type of message for Internet Control Management Protocol (ICMP).
- Value—Type of ICMP message
- Guidelines—Select a type of message from the menu.
- Default—Any
- Example—info-reply

ICMP Code

- Code for ICMP.
- Value—Type of ICMP code
- Guidelines—Select a type of code from the menu.
- Default—Any
- Example—host-precedence-violation

TTL Threshold

- Depth of network penetration for the traceroute application protocol.
- Value—Integer in the range 0–255 or unspecified
 - Unspecified—Allows traceroutes up to a depth of 255.
- Default—Unspecified
- Example—5

RPC Program Number

- Program number for the remote procedure call (RPC) application protocol.
- Value—A single program number or range of program numbers separated by two dots (.). Program numbers are integers in the range 100000–400000.
- Guidelines—Specify the RPC program numbers to which the NAT rule or firewall exception applies. To specify all RPC program numbers, leave this field empty.
- Default—No value
- Example—7..12

UUID

- Universal unique identifier (UUID) for the Distributed Computing Environment (DCE) RPC application protocol.
- Value—Hexadecimal number in the format
xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
- Guidelines—Specify a number of a specific DCE RPC object to which the NAT rule or firewall exception applies. To specify all DCE RPC objects, leave this field empty.
- Default—No value
- Example—1f356a25-ce67-73ad-2187-631ec8ae1bd6

Inactivity Timeout

- Time for which a conversation associated with the identified application protocol can be inactive before the JUNOS routing platform terminates the conversation.
- Value—Number of seconds in the range 0–2147483647
- Guidelines—Specify a time, or leave this field empty to use the default setting.
- Default—30 seconds
- Example—45

Modifying Values for Traffic Classifications

To modify values for an application object:

1. Start at the Applications page (see Figure 37 on page 492).
2. Click **Edit** for the application object.

The Edit Application page appears.

3. Change the values in the fields for this application object.
4. Click **Apply**.

Deleting Traffic Classifications

To delete an application protocol:

1. Start at the Applications page (see Figure 37 on page 492).
2. Click **Delete** for the application protocol.

Subscribing to Firewall Services

The basic firewall that you configure will be enforced on all Internet access links subordinate to the subscriber you select in the navigation pane. When you have configured a basic firewall, you can create firewall exceptions—variances from the basic firewall—for specific categories of traffic.

Firewall exception rules block traffic that otherwise would be permitted to traverse the firewall, or to admit traffic that would otherwise be blocked. Exceptions specify criteria against which each packet is inspected.

How you configure firewall exceptions depends on which type of firewall service the ISP enabled. Enterprise Manager Portal can support one of the following:

- Stateless firewalls—Inspect each packet in isolation; they do not evaluate the traffic flow.

With stateless firewalls, you can configure exceptions to take customized actions, such as policing specified traffic at a specified rate, or setting the ToS byte. By using customized actions, you can allow traffic from a specified IP address or for a specified IP protocol to traverse the firewall. In addition, you can specify quality of service (QoS) properties such as values for the type of service (ToS) byte.

- Stateful firewalls—Track traffic flows and conversations between applications and evaluate this information when applying exception rules.

An application is typically associated with a stateful firewall rule. After a flow or conversation meets firewall criteria, packets in that flow can pass through the firewall. For example for an FTP connection, when an FTP control connection requests a file download, the stateful firewall knows to expect and allows a TCP data connection to start. You can also create firewall exceptions for traffic associated with a particular application protocol, such as FTP, that originates at a particular address in the enterprise. See *Classifying Traffic for Stateful Firewall Exceptions and NAT Rules* on page 491 for information about defining an application object, which defines traffic associated with a particular application protocol.

Before You Configure Firewall Exception Rules

Before you configure firewall exception rules, make sure that you understand which types of packets you want to pass through a firewall.

Enterprise Manager Portal must be set to Advanced configuration mode to configure some of the properties for a firewall. If the portal is not in Advanced mode, some of the settings appear as read-only fields. For information about setting the portal mode, see *Setting the Configuration Level for Enterprise Manager Portal* on page 466.

Creating Subscriptions to Firewall Services

To create a subscription to a basic firewall service:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber for whom you want to create a subscription to a basic firewall service.
2. Click the **Firewall** tab.

The Firewall page appears.

default > local > Acme > Boca > Primary >

Bandwidth & VPNs Applications **Firewall** Addresses NAT Schedules Managers

Welcome to Virneo's Firewall Services.


Please select one firewall from the list below. Click on the help icon ⓘ to see a description of how each firewall would affect your network traffic. The firewall that you select will be enforced on all internet access links at or below the location you have currently selected in the tree on the left side of this page.

Consider carefully the locations at which you will subscribe to a firewall service. A firewall affects all accesses underneath the subscription location, and you are only allowed to have one firewall affect a given access. For example, if you subscribe a site to a firewall service, you can not subscribe the enterprise that contains that site to a firewall service, because the two firewall subscriptions would affect the accesses in the site.

After selecting a firewall, you will be able to specify exceptions to the firewall's normal behaviour. For example, you could open a hole in the firewall for specific traffic at a specific site.

Firewall Service ⓘ

No firewall ▾ Apply

3. Click the help icon  above the firewall service to review information about the available firewalls.
4. Select a firewall service from the menu, and click **Apply**.

The Firewall page changes to allow you to create firewall exceptions.

Firewall Service

- Name of the firewall service.
- Value—Menu of firewall services in the directory available for this subscriber
- Default—No Firewall
- Example—BasicFW1

Creating Firewall Exceptions for Stateless Firewalls

To create a firewall exception for a subscriber:

1. Access the subscriber's Firewall page (see Figure 40 on page 508).
2. In the Firewall page, click **Create Firewall Exception**.

The Create Exception dialog box appears. Figure 38 shows the appearance of the dialog box when Enterprise Manager Portal is set to Advanced mode.

Figure 38: Create Exception Dialog Box for Stateless Firewalls

Using the field descriptions below, configure the values for the firewall exception. Which protocols you select determines which associated protocol fields are available for editing.



NOTE: If a user changes the value for a protocol when the configuration level for the portal is set to Normal mode, values for the following fields may be deleted: TCP Flags, Fragmentation Flags, Fragmentation Offset, Packet Length, ICMP Type, and ICMP Code.

If the value of a protocol is changed to the original setting, the portal restores the associated field values that were previously removed.

3. Click **Create**.

The Firewall page shows the exception configured. Figure 39 shows three exceptions configured for a brickwall firewall service. The exceptions appear in priority order.

Figure 39: Firewall Page with Firewall Service Applied and Exceptions Configured

Bandwidth & VPNs
Firewall
Addresses
NAT
Schedules
Managers

Firewall Service

BrickWall
Apply

Status...

Usage data...

Exceptions to Firewall Service							
Name	Affected Traffic	Priority	Direction	Firewall Action	Schedule	Enabled	
tcpProto1	<div> IP Protocol tcp ToS Byte precedence: internet_control Source Address 10.10.10.0/24 Destination Address 10.11.12.0/24 Destination Port 6789 TCP Flags tcp-initial Fragmentation Flags dont-fragment Fragment Offset 100..170 Packet Length 60..70 </div> <div>Edit</div>	4	Incoming	Allow	No schedule	<input checked="" type="checkbox"/>	Delete Status... Usage data...
		<div>Apply</div>					
tcpRule2	<div>All Traffic</div> <div>Edit</div>	7	Incoming	Allow	No schedule	<input type="checkbox"/>	Delete Status... Usage data...
		<div>Apply</div>					
icmpRule	<div> IP Protocol icmp Source Address 1.1.1.0/24 Destination Address 2.2.2.0/24 Fragmentation Flags reserved Fragment Offset 5000 Packet Length 65535 ICMP Type info-reply ICMP Code 50..100 </div> <div>Edit</div>	10	Outgoing	Discard	No schedule	<input type="checkbox"/>	Delete Status... Usage data...
		<div>Apply</div>					
tcpProtocol	<div> IP Protocol tcp ToS Byte precedence: immediate Source Address 10.10.10.0/24 Source Port 23456 Destination Address 10.11.12.0/24 Destination Port 6789 TCP Flags fin & tsyn & rst & lpush & ack & urgent Fragmentation Flags dont-fragment Fragment Offset 100..170 Packet Length 60..70 </div> <div>Edit</div>	45	Incoming	Allow	No schedule	<input checked="" type="checkbox"/>	Delete Status... Usage data...
		<div>Apply</div>					

Create Firewall Exception

Rule Name

- Name of the subscription to the firewall service.
- Value—Alphanumeric string
- Guidelines—You must specify a name for the rule. Do not use spaces, dots, or punctuation characters in the name.
- Default—No value
- Example—WebAccess

IP Protocols

- IP protocol associated with this rule.
- Value—Type of IP protocols separated by commas, with the protocol specified by:
 - Number of IP protocol in the range 0–255
 - The following abbreviations:
 - ah—authentication header
 - egp—exterior gateway protocol
 - esp—Encapsulating Security Payload
 - gre—generic routing encapsulation
 - icmp—Internet Control Message Protocol
 - igmp—Internet Group Management Protocol
 - ipip—IP over IP
 - ospf—Open Shortest Path First
 - pim—Protocol Independent Multicast
 - rsvp—Resource Reservation Protocol
 - sctp—Stream Control Transmission Protocol
 - tcp—Transmission Control Protocol
 - udp—User Datagram Protocol
 - Blank—Any IP protocol
- Default—No value
- Example—tcp

ToS Byte

- ToS byte in the header of the IP datagram associated with traffic affected by this rule.
- Value
 - DiffServ—DiffServ is used to classify packets by the selected value.
 - Precedence—Value for the drop precedence.
 - Free Format—ToS byte in binary format.
Use an x to indicate a bit to be ignored.
- Guidelines—You can configure the ToS byte only if the configuration level is set to Advanced.
Specify the ToS byte in this field if you want to specify a specific type of service. If you want to specify all types of service, leave this field empty.
- Default—No value
- Example—Free Format 000010xx

Source IP Addresses

- IP addresses (as contained in the IP packets) of traffic to which the rule applies.
- Value—[not] < networkAddress > / < networkMask >
 - not—All addresses except the listed addresses
 - < networkAddress > —IP address of the network
 - < networkMask > —Subnet mask
- Guidelines—To specify traffic with a particular source IP address, enter an IP address. To specify all traffic except that with a particular source IP address, precede the IP address with the keyword **not**. To specify traffic with any source IP address, leave the field empty. To specify multiple source IP addresses, enter multiple addresses on different lines. You can specify multiple source IP addresses only if the configuration level is set to Advanced.
- Default—No value
- Example—192.0.2.0/24

Source Ports

- Source TCP/UDP port(s) (contained in the IP packets) of traffic affected by this rule.
- Values
 - Port number
 - Comma-separated list of port numbers and ranges of port numbers (JUNOS routing platforms)
 - Ranges of port numbers separated by two dots (..)
- Guidelines— To specify all ports, leave this field empty. If you specify an IP protocol other than TCP or UDP for this subscription, the port field will dim, and you will not be able to specify port numbers in this field.
- Default—No value
- Example
 - 2
 - 2, 3, 45..55

Destination IP Addresses

- Destination IP addresse(s) (contained in the IP packets) of traffic affected by this rule.
- Value—[not] < networkAddress > / < networkMask >
 - not—Address, or set of IP addresses as expressed by the netmask, for which the firewall service is not available
 - < networkAddress > —IP address of the network
 - < networkMask > —Netmask expressed as an integer 0–32, which specifies how many of the first bits in the address specify the network
- Guidelines—To specify a netmask for a destination IP address or a set of IP addresses that should not be included, precede the IP address with the keyword **not**. The order in which you list prefixes, identified by the IP address–netmask pair, is not significant. They are all evaluated to determine whether a match occurs. If prefixes overlap, longest-match rules are used to determine whether a match occurs. For an address to be considered a match, it must match one of the rules in the list.

For information about how JUNOS routing platforms evaluate prefixes, see the *JUNOS Policy Framework Configuration Guide*.

- Default—No value
- Example—192.0.2.0/24

Destination Ports

- Destination TCP/UDP port(s) (contained in the IP packets) of traffic affected by this rule.
- Value
 - Port number
 - Comma-separated list of port numbers and ranges of port numbers (JUNOS routing platforms)
 - Ranges of port numbers separated by two dots (..)
- Guidelines—To specify all ports, leave this field empty. If you specify an IP protocol other than TCP or UDP for this subscription, the port field will dim, and you will not be able to specify port numbers in this field.
- Default—No value
- Example
 - 2
 - 2, 3, 45..55

TCP Flags

- Conditions in the TCP flags in the TCP message header. This field is enabled when the TCP protocol is selected.
- Value—Expression or text synonym that identifies the TCP flags
- Guidelines—You can enter a value for TCP flags only if you select TCP as the IP protocol.

You can enter a logical expression that contains the symbols for the six TCP flags: urgent, ack, push, rst, syn, and fin. You can use the following logical operators in the list of flags:

- &—And. Separates flag settings in the list.
- !—Not. Flags preceded by ! are cleared; flags not preceded by ! are set.

You can use the following expression instead of the entire expression:

- tcp-initial—syn & !ack

The interface displays text synonyms for expressions if stored data matches the expression.

This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—No value
- Example
 - syn
 - tcp-initial

Fragmentation Flags

- Logical expression using the dont-fragment, more-fragments, and reserved IP fragmentation flags.
- Value—Flags expression
- Guidelines—The expression can also contain the following logical operators:
 - &—And. Separates flag settings in the list.
 - !—Not. Flags preceded by ! are cleared; flags not preceded by ! are set.
- Default—No value
- Example
 - more-fragments
 - ! dont-fragment

Fragment Offset

- IP fragment offset—a value that defines the order in which to assemble fragments for an IP datagram.
- Value—One of the following:
 - Number in the range 0–8191
 - Range of numbers separated by two dots (..) within the range 0–8191
- Default—No value
- Example
 - 50
 - 50 .. 76

Packet Length

- Length of packets.
- Value—One of the following:
 - Number in the range 0–65536
 - Range of numbers separated by two dots (..) within the range 0–65536
- Default—No value
- Example
 - 15000
 - 15000 .. 30000

ICMP Type

- Type of message for Internet Control Management Protocol (ICMP).
- Value—Type of ICMP message in the following formats:
 - Number of the ICMP message type in the range 0–255
 - Symbolic name for an ICMP message type
 - Comma-separated list of ICMP types and ranges of ICMP types
 - Ranges of ICMP types separated by two dots (..) within the range 0–255
 - Blank—Any ICMP type
- Guidelines—You can enter a value for this field only if you select the icmp protocol (protocol number 1).

The following list shows the symbolic name and associated numbers for ICMP types. The ICMP types are the same as those on JUNOS routing platforms with the addition of traceroute.

- 0—echo-reply
- 8—echo-request
- 16—info-reply
- 15—info-request
- 18—mask-reply

- 17—mask-request
- 12—parameter-problem
- 5—redirect
- 9—router-advertisement
- 10—router-solicit
- 4—source-quench
- 11—time-exceeded
- 13—timestamp
- 14—timestamp-reply
- 30—traceroute
- 3—unreachable

This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—Any
- Example—10 .. 25, 27

ICMP Code

- Code for ICMP.
- Value—Type of ICMP code in the following formats:
 - Number of ICMP code in the range 0–255
 - Comma-separated list of code numbers and ranges of code numbers
 - Ranges of code numbers separated by two dots (..) within the range 0–255
 - Blank—Any ICMP code
- Guidelines—You can enter a value for this field only if you select particular protocols.

This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—Any
- Example—75

Priority

- Numeric value that indicates which firewall exception takes precedence if a subscriber has multiple exceptions for a firewall service.
- Value—Integer in the range specified by the online help for this field

- Guidelines—You must specify a priority for the firewall exception. A lower number indicates a higher priority. Use a unique priority for each firewall exception that relates to the same traffic. If two rules have the same priority, they will be applied to traffic in an unpredictable order.
- Default—No value
- Example—5

Direction

- Direction, with respect to the enterprise, of the traffic.
- Value
 - Incoming—Applies to traffic that starts outside the enterprise
 - Outgoing—Applies to traffic that starts inside the enterprise
 - Both—Applies to traffic flows that start inside or outside the enterprise
 - Guidelines—If you select a custom firewall rule, you cannot specify a direction. Custom firewall rules should have names that reflect what the rule does.
- Default—Incoming
- Example—Both

Action

- Way in which the firewall should handle the incoming or outgoing traffic.
- Value
 - Allow—Let the traffic through the firewall.
 - Reject—Send an ICMP reply that explains why the firewall blocked the traffic.
 - Discard—Drop the traffic without sending any reply.
 - A custom value configured by the service provider.
- Guidelines—Other actions may be available—one for each custom firewall rule.
- Default—Allow
- Example—Discard

Enabled

- Status of the rule.
- Value
 - Gray box—Rule is inherited from a parent subscriber or the rule is scheduled
 - White box—Rule is configured for this subscriber
 - Box with check mark—Rule is enabled
 - Empty box—Rule is disabled
- Guidelines—Click box to enable or disable a rule.
- Default—Rule is disabled

Creating Firewall Exceptions for Stateful Firewalls

To create a firewall exception for a subscriber:

- 1. If you want to create a firewall exception for a particular application object, first create that object (see *Classifying Traffic for Stateful Firewall Exceptions and NAT Rules* on page 491).
- 2. Access the subscriber’s Firewall page.

Figure 40: Firewall Page with Firewall Service Applied

default ▸ local ▸ Acme ▸ Boca ▸ Primary ▸

Bandwidth & VPNsApplicationsFirewallAddressesNATSchedulesManagers

Firewall Service ⓘ

EmailAndWeb ▾ApplyStatus...

Priority	Name	Affected Traffic				Firewall Action	Schedule ⓘ	Enabled	
		Direction	Source IPs	Destination IPs	Application				
<input type="text"/>	<input type="text"/>	Incoming ▾	<input type="text"/>	<input type="text"/>	Any ▾	Allow ▾		<input type="checkbox"/>	Create

- 3. Using the field descriptions below, configure the values for the firewall exception.
- 4. Click **Create**.

Priority

- Numeric value to indicate which firewall exception takes precedence if a subscriber has multiple exceptions for a firewall service.
- Value—Integer in the range specified by the online help for this field
- Guidelines—You must specify a priority for the firewall exception. A lower number indicates a higher priority. Use a unique priority for each firewall exception that relates to the same traffic. If two rules have the same priority, they will be applied to traffic in an unpredictable order.
- Default—No value
- Example—5

Name

- Name of the subscription to the firewall service.
- Value—Text string
- Guidelines—You must specify a name for the firewall exception.
- Default—No value
- Example—videoConference

Direction

- Direction, with respect to the enterprise, of the initial traffic flow in a conversation.
- Value
 - Incoming—Applies to an initial traffic flow that starts outside the enterprise
 - Outgoing—Applies to an initial traffic flow that starts inside the enterprise
 - Both—Applies to initial traffic flows that start inside or outside the enterprise
- Default—Incoming
- Example—Both

Source IPs

- Source IP addresses (as contained in the IP packets) of traffic to which the firewall exception applies.
- Value—[not] < networkAddress > / < networkMask >
 - not—All addresses except the listed addresses
 - < networkAddress > —IP address of the network
 - < networkMask > —Subnet mask
- Guidelines—To specify traffic with a particular source IP address, enter an IP address. To specify all traffic except that with a particular source IP address, precede the IP address with the keyword **not**. To specify traffic with any source IP address, leave the field empty. To specify multiple source IP addresses, set the configuration level of the portal to Advanced (see *Setting the Configuration Level for Enterprise Manager Portal* on page 466), and enter multiple addresses on different lines.
- Default—No value
- Example—192.0.2.0/24

Destination IPs

- Destination TCP/UDP ports (as contained in the IP packets) of traffic to which this firewall exception applies.
- Value—[not] < networkAddress > / < networkMask >
 - not—All addresses except the listed addresses
 - < networkAddress > —IP address of the network
 - < networkMask > —Subnet mask
- Guidelines—To specify traffic with a particular destination IP address, enter an IP address. To specify all traffic except that with a particular destination IP address, precede the IP address with the keyword **not**. To specify multiple destination IP addresses, set the configuration level of the portal to Advanced (see *Setting the Configuration Level for Enterprise Manager Portal* on page 466), and enter multiple addresses on different lines.
- Default—No value
- Example—192.0.2.0/24

Application

- Application object to which the firewall applies.
- Value—Application object you defined
- Guidelines—Select an application object from the menu. For information about specifying an application object, see *Classifying Traffic for Stateful Firewall Exceptions and NAT Rules* on page 491.
- Default—Any
- Example—ftp

Firewall Action

- The way in which the firewall should handle the incoming or outgoing traffic.
- Value
 - Allow—Let the traffic through the firewall
 - Reject—Send an ICMP reply that explains why the firewall blocked the traffic
 - Discard—Drop the traffic without sending any reply
- Default—Allow
- Example—Discard

Schedule

- Configured schedule to use.
- Name of the schedule
- Guidelines—This field appears if scheduling is enabled for the portal. For more information about schedules, see *Managing Schedules* on page 467.
- Default—No value

Enabled

- Status of the firewall exception.
- Value
 - Gray box—Firewall exception is inherited from a parent subscriber
 - White box—Firewall exception is configured for this subscriber
 - Box with check mark—Firewall exception is enabled
 - Empty box—Firewall exception is disabled
- Guidelines—Click box to enable or disable a firewall exception.
- Default—Firewall exception is disabled

Adding a Schedule to a Firewall Exception

A schedule must be configured before you can apply one to a firewall exception. For information about configuring schedules in Enterprise Manager Portal, see *Managing Schedules* on page 467.

To add a schedule to a firewall exception:

1. Access the subscriber's Firewall page (see Figure 39 on page 500).
2. In the Firewall page, select a schedule from the Schedule menu for the exception. See the following field description for details.

Schedule

- Configured schedule to use.
- Name of the schedule
- Guidelines—This field appears if scheduling is enabled for the portal.
- Default—No value

Modifying Firewall Exceptions

To modify a firewall exception:

1. Start at the Firewall page for the subscriber (see Figure 40 on page 508).
2. Change the values in the fields for this firewall exception.
3. For stateless firewalls, to change the values for affected traffic, click Edit under Affected Traffic, make changes in the Edit Exception dialog box, and click **Apply**.

or

For stateful firewalls, click **Apply** for the application protocol.

Deleting Firewall Exceptions

To delete a firewall exception:

1. Start at the Firewall page for the subscriber (see Figure 40 on page 508).
2. Click **Delete** for the firewall exception.

Deleting Basic Firewalls

To delete a basic firewall:

1. Disable all firewall exceptions and NAT rules configured for this subscriber.

For information about disabling these values, see the field descriptions in *Creating Firewall Exceptions for Stateful Firewalls* on page 508 and *Applying NAT Rules to Traffic* on page 516.

2. Disable all firewall exceptions and NAT rules that this subscriber inherits from parent subscribers.
3. Disable all firewall exceptions and NAT rules defined for this subscriber's subordinate subscribers.
4. Access the Firewall page for the subscriber for which you configured the firewall (see Figure 40 on page 508).
5. Select **No Firewall** from the Firewall Service menu.
6. Click **Apply**.

Monitoring the Use of Subscriptions to Firewall Services

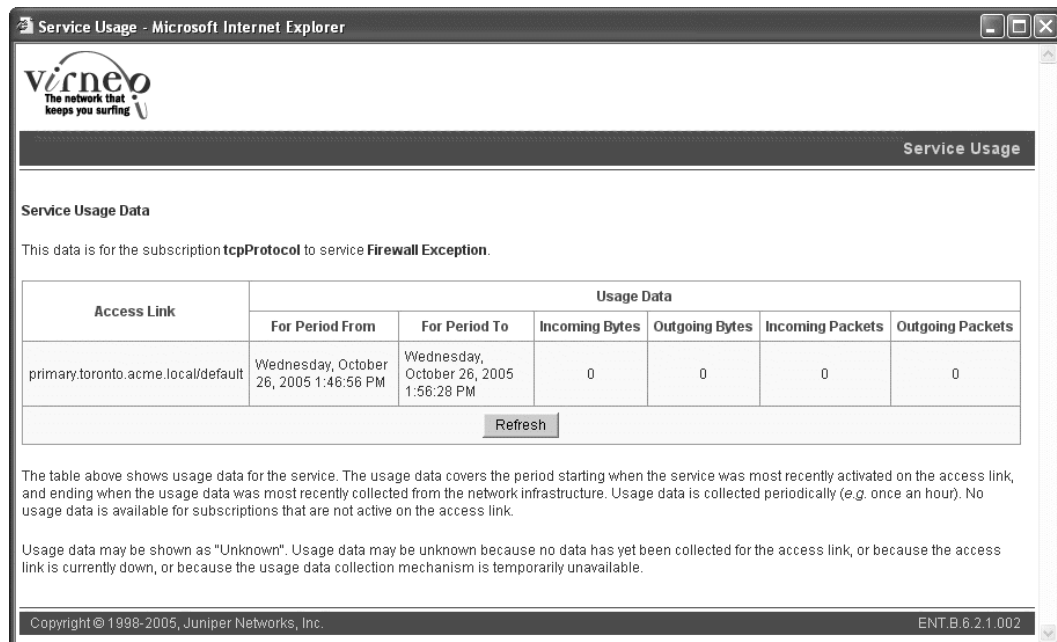
To monitor the use of firewall subscriptions:

1. Access the subscriber's Firewall page (see Figure 40 on page 508).
2. In the Firewall page, click the **Usage Data** link in the last column.

or

Click the **Usage Data** link under Firewall Service.

The Service Usage Data page appears.



Working with IP Addressing and NAT Services

You can configure NAT addressing and services from Enterprise Manager Portal. For information about NAT services and policies, see *Chapter 22, Reviewing and Configuring Policies and Services for Enterprise Manager Portal*.

Requesting Public IP Addresses for NAT Services

To request one or more IP addresses:

1. In the navigation pane of Enterprise Manager Portal, click the access to which you want to request an IP address.
2. Click the **Addresses** tab.

The Addresses page appears.

Figure 41: Addresses Page Before Requesting Addresses

default ▶ local ▶ Acme ▶ Boca ▶ Primary ▶

Bandwidth & VPNsApplicationsFirewall**Addresses**NATSchedulesManagers

Public IP Addresses

No public IP addresses have been assigned to this access link.

Request More Public IP Addresses

Number of Addresses	Contiguous	
1	<input type="checkbox"/>	Request

Outstanding Requests for Public IP Addresses

No outstanding requests for public IP addresses exist.

3. In the Number of Addresses field, enter the number of addresses that you want.
4. (Optional) If you specify multiple IP addresses and you want the addresses to be sequential, select **Contiguous**.
5. Click **Request**.

Enterprise Manager Portal sends a request to the service provider for the IP addresses and displays the number of outstanding requests. When the service provider allocates the IP addresses, Enterprise Manager Portal displays the public IP addresses assigned to this access and makes the addresses visible in the menus on the NAT page for that access, as shown in Figure 42 on page 514. If a request for an IP address is outstanding for a certain period of time, Enterprise Manager Portal automatically sends a reminder to the service provider.

Figure 42: Addresses Page After Requesting Addresses

Acme ▶ Boca ▶ Primary ▶

Bandwidth & VPNsApplicationsFirewall**Addresses**NATSchedulesManagers

Public IP Addresses		
Address	Used By	
165.165.165.165		<input type="checkbox"/>
165.165.165.166		<input type="checkbox"/>
165.165.165.167		<input type="checkbox"/>
165.165.165.168		<input type="checkbox"/>
165.165.165.169		<input type="checkbox"/>
165.165.165.170		<input type="checkbox"/>
Release selected public IPs:		Release

Request More Public IP Addresses

Number of Addresses	Contiguous	
1	<input type="checkbox"/>	Request

Outstanding Requests for Public IP Addresses

No outstanding requests for public IP addresses exist.

514 ■ Working with IP Addressing and NAT Services

Number of Addresses

- Number of IP addresses that you want the service provider to supply.
- Value—Integer in the range 1–2147483647
- Default—1

Contiguous

- Whether or not requested multiple IP addresses should be sequential.
- Value
 - Checked box—IP addresses must be contiguous
 - Empty box—IP address need not be contiguous
- Default—IP address need not be contiguous

Canceling Requests for Public IP Addresses

To cancel a request:

- Click **Cancel** for that request in the Outstanding Requests for IP Addresses table.

Returning Public IP Addresses to Service Providers

To return one or more IP addresses to the service provider:

1. Start at the Addresses page for the subscriber (see Figure 42 on page 514).
2. In the Public IP Addresses table, click in the small box in the last column for each address that you want to return.

If an enabled NAT rule is using an address, the box for that address is dimmed, and you cannot release that address until you disable or delete the NAT rule listed in the Used By field.

3. Click **Release**.

Applying NAT Rules to Traffic

After you protect an access with a firewall and have obtained one or more public IP addresses for the access, you can apply the following types of NAT rules to traffic on the access.

- Public addresses for outgoing traffic

Also known as *dynamic source NAT*, this type of NAT allows computers with private IP addresses in a private network to share a small set of public IP addresses for outgoing connections. For example, employees in an enterprise can use these public IP address for browsing the Web. You can specify the source IP addresses and, optionally, the ports that the outgoing traffic will use.

- Public addresses for incoming traffic

Also known as *static destination NAT*, this type of NAT allows you to expose to the world a server, such as a Web server, that has a private IP address in your private network. You specify a public IP address, and incoming connections destined for that public IP address will be received by your server at its private IP address.

- Fixed public addresses for outgoing traffic

Also known as *static source NAT*, this type of NAT allows you to specify the public source IP to be used for specific outgoing traffic. To specify this type of NAT you must set the configuration level of the portal to Advanced (see *Setting the Configuration Level for Enterprise Manager Portal* on page 466).

Enterprise Manager Portal ensures that the SAE activates a basic firewall service before it activates a NAT service.

To apply NAT rules to traffic on JUNOS routing platforms:

1. In the navigation pane of Enterprise Manager Portal, click the access that connects to the router.
2. Click the **NAT** tab.

The NAT page appears.

Figure 43: NAT Page

Virneo Enterprise Portal

Log out

Navigation

ent-admin

- default
- local
 - ABCInc
 - Acme
 - Boca
 - Backup
 - Primary
 - Ottawa
 - Toronto
- retailer-one
- retailer-two
- SP
- virtual-SP

Refresh

default local Acme Boca Backup

Bandwidth & VPNs Applications Firewall Addresses NAT Schedules Managers

Public Addresses for Outgoing Traffic

Address Range	Port Range	Enabled	
From: 192.0.2.22	From:	<input type="checkbox"/>	Create
To: 192.0.2.22	To:		

Public Addresses for Incoming Traffic

Priority	Name	Public IP	Private IP	Application	Enabled	
		192.0.2.22		Any	<input type="checkbox"/>	Create

Fixed Public Addresses for Outgoing Traffic

Priority	Name	Private IP	Public IP	Application	Enabled	
			192.0.2.22	Any	<input type="checkbox"/>	Create

© Virneo 2004

3. See the following sections for information about configuring NAT for incoming and outgoing interfaces on the router.

Configuring Public IP Addresses for Outgoing Traffic

To configure public IP addresses for outgoing traffic:

1. Locate the area called Public Addresses for Outgoing Traffic in the NAT page.
2. Using the field descriptions below, specify how the router will apply the NAT rule to outgoing traffic.
3. Select **Enabled**.
4. Click **Create**.

Address Range

- Contiguous range of public IP addresses to which the source addresses of clients in the enterprise are translated.
- Value—Public IP addresses
- Guidelines—Select the starting and ending IP addresses in the From and To menus. For one IP address, select the same address in the From and To menus.
- Default—No value

Port Range

- Range of ports that are used as the source ports in outgoing IP packets after the NAT translation.
- Value—Integers in the range 0–65535
- Guidelines—Specify the starting and ending port numbers in the From and To fields. Be sure to use a port range big enough to allow all the private addresses to share the limited set of public addresses. To specify all ports in the range 1024–65535, leave these fields empty.
- Default—No value

Enabled

- Whether or not the router applies NAT to outgoing traffic on this access.
- Value
 - Enabled—Checked box
 - Disabled—White box
- Default—Disabled

Configuring Public IP Addresses for Incoming Traffic

To configure public IP addresses for incoming traffic:

1. Locate the area called Public Addresses for Incoming Traffic in the NAT page.
2. Using the field descriptions below, specify how the router will apply the NAT rule to incoming traffic.
3. Click Create.

Priority

- Numeric value that indicates which NAT rule takes precedence if you specify more than one NAT rule for an IP address.
- Value—Integer in the range specified by the online help for this field
- Guidelines—You must specify a priority for the NAT rule. A lower number indicates a higher priority. Use a unique priority for each NAT rule that relates to the same traffic. If two rules have the same priority, they will be applied to traffic in an unpredictable order.

- Default—No value
- Example—5

Name

- Name of the NAT rule
- Value—Text string
- Default—No value
- Example—rule1

Public IP

- Public IP address that the router translates to a private address in the enterprise.
- Value—IP address
- Guidelines—Select the public destination address that is to be translated into a private destination address inside the enterprise.
- Default—No value

Private IP

- Private IP address to which the router translates the public IP address.
- Value—IP address
- Guidelines—Enter the private address of the host you wish to make available outside the enterprise.
- Default—No value

Application

- Application object to which the router will apply NAT.
- Value
 - < application > —An application object that you created (see *Classifying Traffic for Stateful Firewall Exceptions and NAT Rules* on page 491)
 - Any—Any application
- Guidelines—Select a value from the menu.
- Default—Any
- Example—myVideoConference

Enabled

- Whether or not the router applies NAT to incoming traffic on this access.
- Value
 - Enabled—Checked box
 - Disabled—White box
- Default—Disabled

Configuring Fixed Public Addresses for Outgoing Traffic

To configure fixed public IP addresses for outgoing traffic:

1. Set the portal configuration level to Advanced (see *Setting the Configuration Level for Enterprise Manager Portal* on page 466).
2. Locate the area called Fixed Public Addresses for Outgoing Traffic in the NAT page (see Figure 43 on page 517).
3. Click **Create**.

Modifying NAT Rules

To modify a NAT rule:

1. Modify the entry in the appropriate table.
2. Click **Apply**.

Deleting NAT Rules

To delete a public IP address for outgoing traffic, click delete for the address range in the Public Addresses for Outgoing Traffic table.

Monitoring the Status of Subscriptions

To monitor the status of a subscription:

1. Start at the page that lists information about the subscription.

For an example, see Figure 35 on page 477, which shows BoD subscriptions.

2. In the last cell of the row of data for the subscription, click **Status**.

The Subscription Status page appears.

The Subscription Status page displays the status of this subscription for all accesses subordinate to this subscriber. The page appearance varies depending on whether the subscription is scheduled. You can click the Refresh button to update status information.

The following Subscription Status page shows the status for an unscheduled subscription.



Subscription Status

The status of the **enabled** subscription to service **1.0 Mbps**.

Access Link	As Of	Status
backup.boca.acme.local/default	Thu Jan 06 10:11:13 EST 2005	Unknown
primary.boca.acme.local/default	Thu Jan 06 10:11:13 EST 2005	Unknown
primary.ottawa.acme.local/default	Thu Jan 06 10:11:14 EST 2005	Inactive (should be active)
backup.toronto.acme.local/default	Thu Jan 06 10:12:32 EST 2005	Unknown
primary.toronto.acme.local/default	Thu Jan 06 10:12:32 EST 2005	Unknown

[Refresh](#) [Fix Problems](#)

Each row in the table above shows the status of the subscription on one internet access link. For each access link, the status displayed is valid as of the given time. You can press the refresh button to get more current information.

The status is either active or inactive. If you see that an enabled subscription is inactive or a disabled subscription is active on some access links, you will also see a button which you can press to fix these problems. If the system is unable to automatically fix the problems, you will be provided with further information that you or your service provider can use to fix the problems.

The status may be shown as "Unknown". The status may be unknown because the access link is currently down, or because the status checking mechanism is temporarily unavailable.

© Virneo 2004

The following Subscription Status page shows the status for a scheduled subscription.

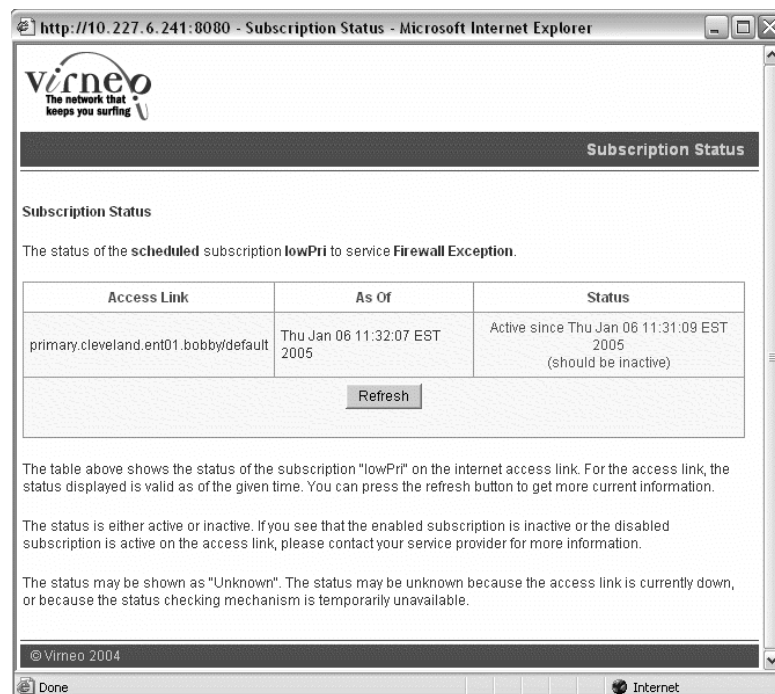


Table 43 shows the possible status for subscriptions.

Table 43: Statuses of Subscriptions

Status	Meaning	Category
Active	Subscription is enabled and is operative.	Subscription is functioning correctly.
Inactive	Subscription is disabled.	Subscription is functioning correctly.
Active (should be inactive)	Subscription is disabled but is operative.	Subscription is not functioning correctly.
Inactive (should be active)	Subscription is enabled but is inoperative.	Subscription is not functioning correctly.
Unknown	Enterprise manager Portal cannot currently communicate with the SAE, typically because the access is not functioning correctly or the checking mechanism is temporarily unavailable.	Subscription may be functioning correctly, but another problem exists.

Troubleshooting Subscriptions That Are Not Functioning Correctly

If one or more subscriptions are not functioning correctly, the Fix Problems link appears in the Subscription Status page. To troubleshoot the problems with the nonfunctioning subscriptions, click **Fix Problems**. This action causes Enterprise Manager Portal to attempt to resolve the problems with the subscriptions.

If Enterprise Manager Portal succeeds in resolving the problems, the Subscription Status page displays the new settings. Otherwise, the Subscription Status page displays more information about the problems.

Troubleshooting Subscriptions of Unknown Status

If subscriptions of unknown status and subscriptions that are not functioning correctly exist, the software will also attempt to update the unknown subscriptions when you click Fix Problems. If Enterprise Manager Portal cannot resolve the status, it will remain unknown.

If you have subscriptions of unknown status and either the Fix Problems link is not available or using the link does not resolve the status, click **Subscription Status** page. If this action does not solve the problem, check the status of the subscription later.

Chapter 30

Using NAT Address Management Portal

This chapter describes how to use NAT Address Management Portal to manage requests about public IP addresses. The chapter contains the following sections:

- Overview of NAT Address Management Portal on page 525
- Assigning IP Addresses on page 526
- Acknowledging the Release of IP Addresses on page 527

Overview of NAT Address Management Portal

Service providers use NAT Address Management Portal to manage requests about public IP addresses from IT managers. When an IT manager sends a request about IP addresses through Enterprise Manager Portal, the portal sends an e-mail to the service provider that contains a link to NAT Address Management Portal.

For demonstration purposes or for small service providers, a human administrator can deal with this e-mail manually. In a large production environment, however, the e-mail will be sent to a machine that automatically assigns addresses to accesses. For information about how a machine manages IP addresses, see *NAT Address Management Portal* on page 418.

Assigning IP Addresses

To assign IP addresses to accesses manually:

1. Click the link to NAT Address Management Portal in the e-mail.

NAT Address Management Portal appears and displays the status of IP addresses for this link.

Assigned IP Addresses			
No public IP addresses have been assigned to this access link			

Released IP Addresses			
No public IP addresses have been released by this access link			

Outstanding Requests for Public IP Addresses			
Request Time	Number of Addresses	Must be Contiguous	
Jun 30, 2004 4:03 PM	1	false	<input type="button" value="Assign IPs"/>

Copyright Juniper Networks 2004

2. Click **Assign IPs**.


The Assign Public IP Addresses window appears.

Assign Public IP Addresses (Contiguous)	
	IP Address
1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>
<input type="button" value="Assign"/>	

3. Enter an IP address in each line of this window.
4. Click **Assign**.

Acknowledging the Release of IP Addresses

When an IT manager returns an IP address through Enterprise Manager Portal, NAT Address Management Portal displays the returned IP address. You must acknowledge release of the IP Address to the IT manager. To do so, click **Acknowledge** in the Released IP Addresses table.



NAT Address Management

default ▾local ▾Acme ▾Boca ▾Primary ▾

Assigned IP Addresses

No public IP addresses have been assigned to this access link

Released IP Addresses

Release Time	Released IPs
Jul 19, 2004 6:40 PM	192.0.2.22

Acknowledge

Outstanding Requests for Public IP Addresses

Request Time	Number of Addresses	Must be Contiguous	
Jul 18, 2004 2:55 PM	1	false	Assign IPs

Copyright Juniper Networks 2004

Chapter 31

Using the Sample Enterprise Service Portal

This chapter describes how IT managers and service providers can use an enterprise service portals to manage services, subscriptions, and departments in their enterprises. The chapter contains the following sections:

- Overview of the Sample Enterprise Service Portal on page 529
- Starting the Sample Enterprise Service Portal on page 530
- Subscribing to Services on page 531
- Activating Subscriptions on page 532
- Deactivating Subscriptions on page 533
- Suspending Subscriptions on page 533
- Canceling Suspensions of Subscriptions on page 533
- Monitoring Use of Subscriptions on page 533
- Specifying Values for Service Parameters in Subscriptions on page 534
- Restoring Default Values for Service Parameters In Subscriptions on page 534
- Deleting Subscriptions on page 535
- Monitoring Service Sessions for a Subscription on page 535
- Defining Networks for Departments in an Enterprise on page 536
- Modifying Network Definitions for Departments in an Enterprise on page 537
- Deleting Network Definitions for Departments in an Enterprise on page 537

Overview of the Sample Enterprise Service Portal

The sample Enterprise Service Portal illustrates how service providers can make their services available to IT managers in an enterprise and that provides developers with a starting point from which they can create their own service portal.

Starting the Sample Enterprise Service Portal

The WAR file for the sample Enterprise Service Portal, *tagsEntDemo.war*, is in the */webapp* directory in the SRC software distribution. You deploy this file to an application server, such as JBoss.

When you view the sample portal, take care to open only one browser window yourself. The portal automatically opens pop-up windows for various operations. If you open more than one browser window yourself, the information in the original window may not be updated correctly when you complete an operation in a pop-up window.

To start the sample Enterprise Service Portal:

1. Enter the URL of the portal in your Web browser, and press Enter. For example:

`http://192.0.2.1:8080/tagsEntDemo`

The login page appears.

2. Select a retailer, or leave the entry blank to view all retailers.
3. Enter your username in the Login ID field and your password in the Password field.

The Welcome page appears. On the left of the page is a navigation pane for the objects in the service provider's directory over which you have control. Your login identity is the root of this navigation pane.

Subscribing to Services

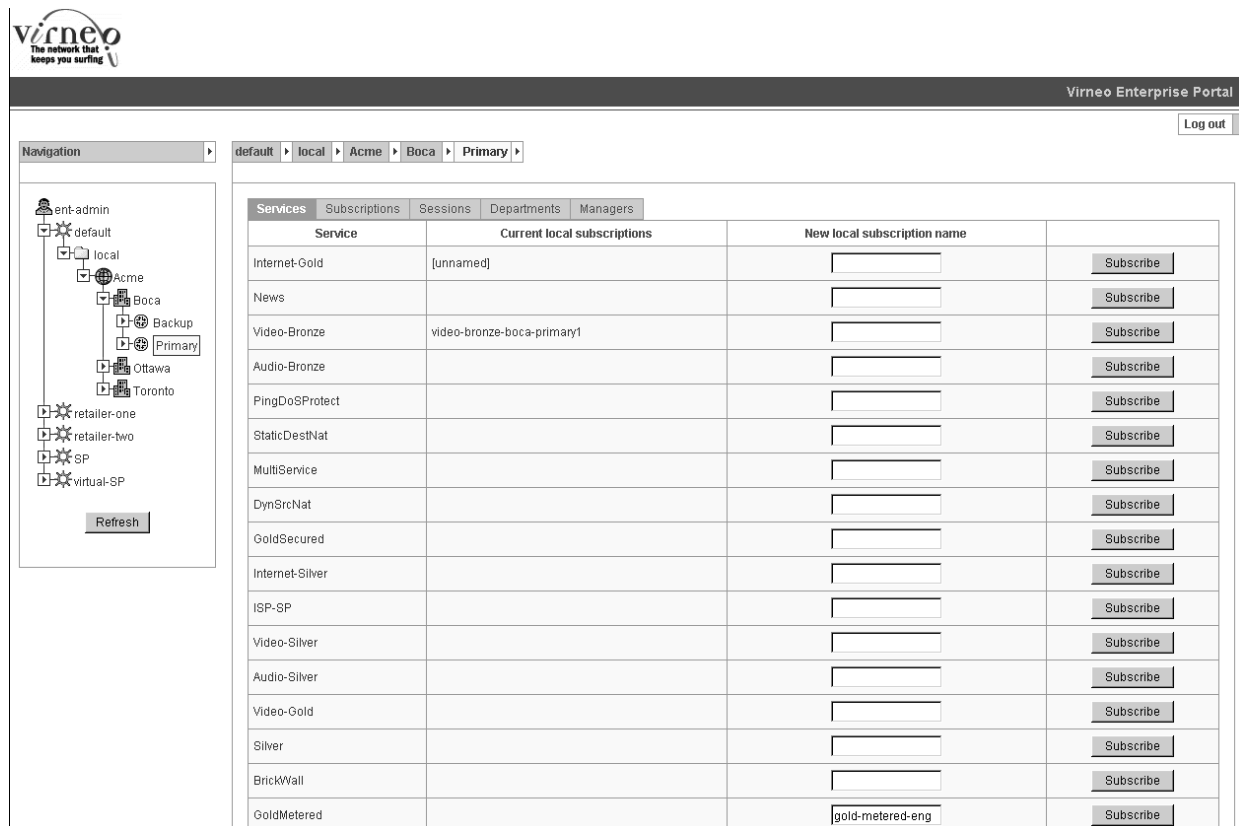
To subscribe to a service:

1. In the navigation pane of the sample Enterprise Service Portal, click the subscriber for whom you want to create a subscription to a service.

The portal displays the information for that subscriber.

2. Click the **Services** tab.

The Services page appears and displays the list of services available to this subscriber and the subscriber's current subscriptions.



The screenshot shows the Virneo Enterprise Portal interface. On the left is a navigation pane with a tree structure showing the hierarchy: ent-admin > default > local > Acme > Boca > Primary. The main content area has a breadcrumb trail: default > local > Acme > Boca > Primary. Below the breadcrumb is a tabbed interface with tabs for Services, Subscriptions, Sessions, Departments, and Managers. The 'Services' tab is active, displaying a table of services.

Service	Current local subscriptions	New local subscription name	
Internet-Gold	[unnamed]	<input type="text"/>	Subscribe
News		<input type="text"/>	Subscribe
Video-Bronze	video-bronze-boca-primary1	<input type="text"/>	Subscribe
Audio-Bronze		<input type="text"/>	Subscribe
PingDoSPProtect		<input type="text"/>	Subscribe
StaticDestNat		<input type="text"/>	Subscribe
MultiService		<input type="text"/>	Subscribe
DynSrcNat		<input type="text"/>	Subscribe
GoldSecured		<input type="text"/>	Subscribe
Internet-Silver		<input type="text"/>	Subscribe
ISP-SP		<input type="text"/>	Subscribe
Video-Silver		<input type="text"/>	Subscribe
Audio-Silver		<input type="text"/>	Subscribe
Video-Gold		<input type="text"/>	Subscribe
Silver		<input type="text"/>	Subscribe
BrickWall		<input type="text"/>	Subscribe
GoldMetered		gold-metered-eng	Subscribe

3. In the New local subscription name field, enter a name for the subscription to the service.

You can have one unnamed subscription to a service; if you have multiple subscriptions to a service, only one can be unnamed.

4. Click **Subscribe**.

Activating Subscriptions

To activate a subscription:

1. In the navigation pane of the sample Enterprise Service Portal, click the subscriber for whom the subscription is configured.
2. Click the **Subscriptions** tab.

The Subscriptions page appears. Note that inherited subscriptions cannot be modified.

Figure 44: Subscriptions Page

The screenshot shows the Virneo Enterprise Portal interface. The top navigation bar includes the Virneo logo and the text 'The network that keeps you surfing'. The main header area displays 'Virneo Enterprise Portal' and a 'Log out' button. The left navigation pane shows a tree view of the network hierarchy, with the 'Primary' subscription under the 'Boca' site selected. The main content area is divided into two sections: a table of subscriptions and a details panel for the selected subscription.

Service	Subscription
BronzeMetered	[unnamed] (From site Boca)
GoldMetered	[unnamed] (From enterprise ABCInc)
PingDoSPProtect	[unnamed] (From enterprise ABCInc)

The details panel for the selected subscription shows the following information:

- Subscription Status:** Administratively inactive. Actions: **Activate**, **Deactivate**.
- Not suspended.** Actions: **Unsuspend**, **Suspend**.
- Usage:** **Reporting**.
- Service Parameters:** (use checkbox to lock value). **dept =** ☐. (From subscription in enterprise ABCInc). Actions: **Apply**, **Delete**, **Reset**.
- Unsubscribe** button.

3. In the Subscription column, click the subscription that you want to activate.
4. In the Subscription details area, click **Activate**.

Deactivating Subscriptions

To deactivate a subscription:

1. Start at the subscriber's Subscriptions page (see Figure 44 on page 532).
2. In the Subscription column, click the subscription you want to deactivate.
3. Click **Deactivate**.

Suspending Subscriptions

You can prevent a subscriber from inheriting a subscription by suspending that subscription. To do so:

1. Start at the subscriber's Subscriptions page (see Figure 44 on page 532).
2. In the Subscription column, click the subscription you want to suspend.
3. Click **Suspend**.

Canceling Suspensions of Subscriptions

If you suspend a subscription for a subscriber, you can restore the inherited subscription for that subscriber. You can also maintain the suspension for that subscriber and restore the inherited subscription for that subscriber's subordinate subscribers. To do so:

1. Start at the Subscriptions page (see Figure 44 on page 532) for the subscriber for which you want to restore the inherited subscription.
2. In the Subscription column, click the subscription you want to allow.
3. Click **Unsuspend**.

Monitoring Use of Subscriptions

To monitor the use of a subscription:

1. Start at the subscriber's Subscriptions page (see Figure 44 on page 532).
2. In the Subscription column, click the subscription you want to view.

3. Click **Reporting**.

The Usage Reporting page appears. If the enterprise service portal cannot contact the relevant SAE to obtain data for this subscriber, the page displays the statistics as Unknown.

EmailAndWeb%EmailAndWeb1 Service Session under	Usage Information					
	In Bytes	Out Bytes	In Packets	Out Packets	Update Time	Start Time
Primary.Boca.Acme.local/default	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown
<div>Reload</div>						

To update the data on this page, click **Reload**.

Specifying Values for Service Parameters in Subscriptions

On the Subscriptions page, the Service Parameters column lists the parameters you can specify for this subscription. Subscriptions inherit values for service parameters from subscriptions of parent subscribers. If the parameter is locked by the parent subscriber, the value appears dimmed in the portal, and you cannot modify the value. If the parameter is not locked by a parent subscriber, you can modify the value.

To specify a value for a parameter:

1. Start at the subscriber's Subscriptions page (see Figure 44 on page 532).
2. Locate the parameter in the Service Parameters column.
3. Provide a value for this parameter.
4. (Optional) Select **Locked** to prevent managers of subordinate subscribers from changing this value.
5. If you want to revert to the original values, click **Reset**.
6. Click **Apply**.

Restoring Default Values for Service Parameters In Subscriptions

To restore the default value for a service parameter:

1. Start at the subscriber's Subscriptions page (see Figure 44 on page 532).
2. Locate the parameter in the Service Parameters column.
3. Click **Delete**.

Some services may have parameters without a default value. If you do not supply values for these parameters, the SAE cannot perform the substitutions when it tries to activate a service, and the activation will fail.

Deleting Subscriptions

To delete a subscription:

1. Start at the subscriber's Subscriptions page (see Figure 44 on page 532).
2. Click the subscription you want to delete.
3. Click **Unsubscribe**.

Monitoring Service Sessions for a Subscription

To monitor the service sessions for a subscription:

1. In the navigation pane of the sample Enterprise Service Portal, click the subscriber for which you want to monitor the sessions.

The portal displays the information for that subscriber.

2. Click the **Sessions** tab.

The portal displays the status of each subscription and the parameters associated with each subscription.

The screenshot shows the Virneo Enterprise Portal interface. On the left is a navigation tree with a 'Refresh' button at the bottom. The main content area has a breadcrumb trail: default > local > ABCInc > Boca > Primary. Below the breadcrumb are tabs for Services, Subscriptions, Sessions (selected), Departments, and Managers. The Sessions tab displays a table with the following data:

Service Name	Oper Active	Service Parameter		
		Name	Admin Value	Op Value
PingDoSProtect	unknown	dept	0.0.0.0/0	Unknown
GoldMetered	unknown	dept	208.93.36.64/28	Unknown
BronzeMetered	unknown	dept	208.93.36.80/28	Unknown

Below the table is a 'Reload' button. The footer of the page reads '© Juniper Networks 2003-2004'.

To update the data on this page, click **Reload**.

Defining Networks for Departments in an Enterprise

To define the networks for departments in an enterprise:

1. In the navigation pane of the sample Enterprise Service Portal, click the subscriber for whom you want to define the department.

The portal displays the information for that subscriber.

2. Click the **Departments** tab.

The Departments page appears.

Figure 45: Departments Page

Virneo Enterprise Portal

Log out

Navigation

default local Acme Boca Primary

ent-admin
 default
 local
 Acme
 Boca
 Primary
 Backup
 Ottawa
 Toronto
 retailer-one
 retailer-two
 SP
 virtual-SP

Refresh

Services Subscriptions Sessions **Departments** Managers

Department	Department network	Locked	
eng	192.0.2.22/2	<input checked="" type="checkbox"/>	Apply Delete Reset
acct	192.0.2.22/3	<input type="checkbox"/>	Apply Delete Reset
		<input type="checkbox"/>	Create

© Juniper Networks 2003-2004

3. In the Department field, enter the name of the department.
4. In the Department network field, enter the network that this department uses, or leave this field empty to use the department name.
5. (Optional) Select **Locked** to prevent managers of subordinate subscribers from changing this value.
6. Click **Create**.

This feature illustrates how service providers can use parameters and substitutions in the portal. The fields called Department and Department network are a name and value for a substitution, respectively. These parameters are also defined in SRC objects such as services and policies. The IT manager provides actual values for the parameters through the portal. Service providers could use these parameters to track and charge each department for the volume of bandwidth it uses. For more information about parameters and substitutions, see *SRC-PE Services and Policies Guide, Chapter 15, Defining and Acquiring Values for Parameters*.

Modifying Network Definitions for Departments in an Enterprise

To modify a network definition for a department:

1. Start at the subscriber's Departments page (see Figure 45 on page 536).
2. Modify values for the department.
3. If you want to revert to the original values, click **Reset**.
4. Click **Apply**.

Deleting Network Definitions for Departments in an Enterprise

To delete a network definition for a department:

1. Start at the subscriber's Departments page (see Figure 45 on page 536).
2. Click **Delete** for the department.

Chapter 32

Developing an Enterprise Service Portal

This chapter describes how you can develop an enterprise service portal based on the sample Enterprise Service Portal. This chapter contains the following sections:

- Developing a Portal Based on the Sample Enterprise Service Portal on page 539
- Preparing to Develop a Sample-Based Enterprise Service Portal on page 540
- Creating a Portal Project for a Sample-Based Enterprise Service Portal on page 540
- Building a Sample-Based Enterprise Service Portal on page 541
- Deploying a Sample-Based Enterprise Service Portal on page 541
- Testing a Sample-Based Enterprise Service Portal on page 541
- Using a Virtual Address for the Portal on page 542

Developing a Portal Based on the Sample Enterprise Service Portal

The source code is included with the sample Enterprise Service Portal. To make complex changes to the portal, we recommend that you install a Java development environment.

The sample Enterprise Service Portal does not require any specific environment, but the procedures to develop a portal assume that you use the Eclipse platform. A servlet container is required to run the portals during development. We recommend that you use Tomcat and its Eclipse plug-in.

For information about your development environment, see the documentation for the product you are using.

Preparing to Develop a Sample-Based Enterprise Service Portal

The following instructions describe how to set up a development environment that uses Eclipse and Tomcat on a Solaris platform. If you want to use Eclipse and Tomcat on a different operating system, see the following Web sites:

- For Eclipse

<http://www.eclipse.org>

- For Tomcat

<http://jakarta.apache.org/tomcat>

To get ready to develop a portal based on the sample Enterprise Service Portal:

1. Download and install Eclipse from

<http://www.eclipse.org>

2. Download the Tomcat plug-in for Eclipse from

<http://www.sysdeo.com/eclipse/tomcatPlugin.html>

3. Unzip the plug-in into the Eclipse installation directory.

4. Download Tomcat from

<http://jakarta.apache.org/tomcat>

5. Install Tomcat:

```
mkdir $HOME/eclipse
cd $HOME/eclipse
unzip /tmp/eclipse-SDK-2.0.2-solaris-motif.zip
unzip /tmp/tomcatPluginV201.zip
cd $HOME
gzip -dc /tmp/tomcat-4.1.18.tar.gz | tar xvf -
```

6. Start Eclipse.

7. Configure the Tomcat plug-in.

Select **Window > Preferences > Tomcat**, and configure the Tomcat version and the path where you installed Tomcat.

Creating a Portal Project for a Sample-Based Enterprise Service Portal

To create a new Tomcat project inside Eclipse:

1. Select **File > New > Project > Java > Tomcat Project**, enter the name of the project, and press **Finish**.
2. Select **File > Import... > Zip File**, enter the path for *entmgr.war*, and click **Finish**.

3. Select **File > Properties > Java Build Path > Libraries > Add Jars**, open the sample Enterprise Service Portal portal project, and navigate to *WEB-INF/lib*. Select all JAR files in the *WEB-INF/lib* directory.
4. Select **File > Properties > Tomcat**, and click **Can update server.xml file**.

You can find the source code of the sample Enterprise Service Portal in the directory *WEB-INF/src*. The JSP pages are stored in the *layout* and *tiles* directories.

Building a Sample-Based Enterprise Service Portal

Eclipse automatically rebuilds the project when you save a modified source file.

To test or debug the project, you must run the code inside Tomcat.

To start Tomcat:

- Select **Tomcat > Start Tomcat**.

You can set break points in your code to debug the code.

Deploying a Sample-Based Enterprise Service Portal

To create a new Web application, set the name of the target WAR file.

1. Select **File > Properties > Tomcat**.
2. Enter the path of the target WAR file in the field **WAR file for export**.
3. Right-click the portal project, and select **Tomcat Project > Export to the WAR file set** in project properties.
4. Copy the WAR file to the final deployment location; for example, */opt/UMC/jboss/server/default/deploy* on your portal server.

Testing a Sample-Based Enterprise Service Portal

To test a sample-based Enterprise Service Portal:

1. Use a virtual address for the portal. See *Using a Virtual Address for the Portal* on page 542.
2. Test the portal. See *SRC-PE Monitoring and Troubleshooting Guide, Chapter 5, Configuring a Simulated Router Driver for Testing with the SRC CLI* or *SRC-PE Monitoring and Troubleshooting Guide, Chapter 6, Configuring a Simulated Router Driver for Testing with SDX Configuration Editor*.

Using a Virtual Address for the Portal

You can configure a virtual address for the portal under a common name in the Domain Name System (DNS) to specify the address through which client applications access the portal. For information about a virtual portal address, see *Virtual IP Address for Policies* on page 337.

Index

A

- access lines.....5, 12
 - description4, 5, 11
- access services
 - configuring subscriptions
 - SDX Admin261
- access subscribers10
 - configuring, SDX Admin236
- accesses
 - configuring subscriptions
 - SRC CLI292
- accounting
 - basic RADIUS accounting plug-in.....152, 192
 - custom RADIUS accounting plug-ins.....152, 192
 - flat file accounting plug-ins.....152, 192
 - flexible RADIUS accounting plug-ins.....152, 192
- action classes in the sample residential portal302
- APIs (application programming interfaces)
 - documentation336
- application protocols, managing491–496
- applications
 - SRC on CD.....xxi
- architecture
 - enterprise service portal.....425
- audience for documentationxix
- authentication plug-ins
 - configuring
 - SDX Configuration Editor160
 - SRC CLI203
 - types130
- authorization plug-ins
 - configuring
 - SDX Configuration Editor160
 - SRC CLI203
 - types130

B

- bandwidth on demand. *See* BoD
- basic RADIUS accounting plug-in152, 192
 - configuring
 - SDX Configuration Editor158
 - SRC CLI196
- basic RADIUS authentication plug-in.....161, 203
 - configuring
 - SDX Configuration Editor162
 - SRC CLI205
- BoD (bandwidth on demand)
 - services376, 388–395
 - subscriptions474–520

C

- callback interface419
- captive portal
 - implementing338
 - preventing access to resources338, 345
- classification scripts
 - conditions.....64
 - glob matching68
 - joining68
 - regular expression matching69
 - configuring
 - SDX Admin98
 - SRC CLI66
 - criteria
 - definition96
 - glob matching99
 - joining99
 - regular expression matching100
 - descriptions63, 95
 - DHCP classification, c-Series platform
 - conditions87
 - configuring86
 - description64
 - targets89
 - DHCP classification, Solaris platform
 - configuring117
 - criteria118
 - description96
 - targets119
 - interface classification, c-Series platform
 - conditions72
 - configuring70
 - description63
 - examples.....74
 - how it works64
 - targets74
 - interface classification, Solaris platform
 - configuring104
 - criteria104
 - description95
 - examples.....107
 - how it works96
 - targets106
- structure
 - SDX Admin98
 - SRC CLI66
- subscriber classification, c-Series platform
 - condition79
 - configuring76

description	63	CORBA (Common Object Request Broker Architecture)	
DHCP options	82	object reference in external plug-ins.....	145
enterprise subscriber example	84	plug-in interface	
how it works	65	enterprise service portal	426–427
static IP subscriber example.....	83	remote API	336
subscriber group example	84	crontab file	412
targets.....	83	custom RADIUS accounting plug-ins	152, 192
subscriber classification, Solaris platform		configuring	
configuring.....	108	SDX Configuration Editor	159
criteria	109	SRC CLI	200
description	96	custom RADIUS authentication plug-ins.....	161, 203
DHCP options	112	configuring	
enterprise subscriber example	115	SDX Configuration Editor	164
how it works	97	SRC CLI	209
static IP subscriber example.....	114	customer support.....	xxiv
subscriber group example	115		
targets.....	114	D	
wholesaler/retailer example	116	data integrators	
target, c-Series platform		adding VPNs.....	406
definition	64	deactivating invalid subscriptions to VPNs.....	411
expressions	67	DCU (destination class usage)	398
types	67	default retailer authentication plug-ins	
target, Solaris platform		configuring	
definition	96	SDX Configuration Editor	185
expressions	98	SRC CLI	225
types	98	default retailer DHCP authentication plug-ins	
component interactions		configuring	
DHCP		SDX Configuration Editor	186
initial login	23	SRC CLI	225
persistent login	26	denial-of-service attacks.....	348
subscriber account login	25	deployment scenarios	
subscriber logout.....	28	enterprise service portal	427
enterprise subscribers		destination class usage	398
login.....	32	DHCP (Dynamic Host Configuration Protocol)	
remote session activation.....	38	address assignment.....	132
PPP		classification scripts. <i>See</i> classification scripts	
login.....	19	options	90, 120
logout.....	21	profiles	92, 123
static IP subscribers.....	29	subscribers	
subscription activation	34	login process	22–27
subscription deactivation.....	36	logout process	28
configuration level in Enterprise Manager Portal.....	466	directory	
conventions defined		enterprise service portal	426
icons	xx	directory server	
text	xx	deployment with remote SAE.....	427
COPS (Common Open Policy Service)		DirX directory server	
DHCP interactions		deployment with remote SAE.....	427
initial login	24	documentation set, SRC. <i>See</i> SRC documentation set	
logout.....	28	domain name parsing	
persistent login	27	configuring, property file	60
subscriber account login	25		
interface startup interactions.....	22	E	
PPP interactions		embedded AdminServer authorization plug-in	187
login.....	20	enterprise	
logout.....	21	description	4, 11
static IP subscriber interactions.....	29	hierarchy	5, 12
subscription activation interactions	36	service parameters	420
subscription deactivation interactions	37	subscriptions	5, 12

- Enterprise Manager Portal
 - application protocols, managing 492–496
 - BoD subscriptions 474–520
 - configuration level 466
 - deployment settings 435
 - directory eventing 451
 - firewall exception rules
 - stateful firewalls 508
 - stateless firewalls 498
 - firewall subscriptions 496–513
 - fixed addresses for outgoing traffic 520
 - help 465
 - NAT
 - IP address 513, 515
 - rules for traffic 517
 - NAT Address Management Portal 441
 - NAT rules 516, 520
 - overview 418, 466
 - policies 375–398
 - public IP addresses, configuring
 - incoming traffic 518
 - outgoing traffic 517
 - schedules 467–474
 - services 375–398
 - Enterprise Service Portal audit plug-in 452–457
 - using with VPN Subscription Deactivator 411
 - enterprise service portals
 - accessing 424
 - architecture 425
 - communication protocols 426
 - configuring directory connections 433
 - data, displaying 459
 - deploying 441
 - improving performance 419
 - installing 432–441
 - IT Manager audit plug-in sample 454–457
 - locating in SRC software distribution 417
 - logging properties 450
 - managers 460, 463
 - NIC proxy 451
 - operators, managing 463
 - overview 415
 - performance 419
 - planning 428
 - prerequisites 423, 431, 459, 525, 539
 - properties 442
 - remote SAE properties 451
 - search bases 449
 - server description 426
 - service directory connection 446
 - subscriber directory connection 443
 - value substitution 422
 - value substitution for policy parameters 422
 - See also* Enterprise Manager Portal
 - enterprise subscribers 3, 9
 - adding
 - SRC CLI 283
 - adding, SDX Admin 246
 - enterprise subscribers, login process 32
 - enterprise tag library 416, 417
 - equipment registration
 - description 301
 - See also* sample residential portal
 - event publishers
 - configuring
 - property file 149
 - SDX Configuration Editor 184
 - SRC CLI 224
 - default retailer authentication, configuring
 - SDX Configuration Editor 185
 - SRC CLI 225
 - default retailer DHCP authentication, configuring
 - SDX Configuration Editor 186
 - SRC CLI 225
 - description 130
 - retailer-specific 188, 227
 - service-specific 187, 227
 - virtual router-specific 188, 227
 - events, IT manager audit 452
 - external plug-ins
 - configuring
 - SDX Configuring Editor 144
 - SRC CLI 138
 - extranet clients
 - adding to VPNs
 - Enterprise Manager portal 409
 - LDAP clients 409
 - SDX Admin 409
 - removing from VPNs 411
- F**
- files
 - ipnat.conf 364
 - WEB-INF/jboss-web.xml 306
 - WEB-INF/portalBehavior.properties 306
 - WEB-INF/struts-config.xml 306, 309
 - WEB-INF/tiles-defs.xml 306, 311
 - WEB-INF/web.xml 306
 - firewall services
 - configuring 377, 380
 - description 496
 - managing in Enterprise Manager Portal 496–513
 - policies for 379
 - router support 376
 - flat file accounting plug-ins 152, 192
 - configuring
 - SDX Configuration Editor 153
 - SRC CLI 193
 - configuring headers
 - SDX Configuration Editor 156
 - SRC CLI 194
 - flexible RADIUS accounting plug-ins 152, 192
 - attributes, defining
 - SDX Configuration Editor 177
 - SRC CLI 215
 - configuring 198
 - SDX Configuration Editor 158
 - RADIUS packets, defining 176, 215
 - SDX Admin 149

flexible RADIUS authentication plug-ins.....	161, 203
attributes, defining	
examples	182, 222
SDX Configuration Editor	177
SRC CLI	215
configuring.....	163
SRC CLI	207
RADIUS packets, defining	
SDX Admin	149
SDX Configuration Editor	176
SRC CLI	215
setting responses	
SDX Configuration Editor	183
SRC CLI	223
forwarding preferences.....	393, 395

H

HTTP proxy	345, 347
------------------	----------

I

icons defined, notice	xx
ifconfig command	365
installing software	
enterprise service portals	432–441
interface classification scripts. <i>See</i> classification scripts	
interfaces	
callback	419
interim accounting, configuring on SAE	
SDX Configuration Editor	43, 52
internal plug-ins	
configuring	
SDX Configuring Editor	143
SRC CLI	137
IOR (interoperable object reference)	
external plug-ins.....	145
IP addresses	
acknowledging release	527
assigning in NAT Address Management Portal	525, 526
NAT services	513, 515
IP Filter.....	338, 364
IP-in-IP tunneling.....	339
ipnat.conf file	364
ISP service in sample residential portal.....	302, 304
IT manager	
audit plug-in	
configuring.....	454
events	452
operators, managing	460, 463

J

Jakarta Struts Web application framework	301
Java development environment, Tomcat.....	340, 539
Javadoc documentation for sample residential portal.....	336
JBoss	
installing Web applications.....	312, 431
JSP tag library. <i>See</i> enterprise tag library	

JUNOS routing platforms	
CoS (Class of Service)	388
forwarding preferences	395
managing traffic	376
policies	
basic BoD	390
BOD	391
BoD and VPNs.....	397
firewall	377–386
NAT	386
provisioning services	
prerequisites	377
routing preferences	393
services	398
basic BoD	390
BoD	392
BoD and VPNs.....	397
firewall	377–386
NAT	386

JUNOSe routers	
(QoS) quality of service.....	388
policies	
basic BoD	390
BOD	391
services	
basic BoD	390
BoD	392

L

LDAP	
models subscriptions.....	231
LDAP authentication plug-in	161, 204
configuring	
SDX Configuration Editor	166
SRC CLI	212
LDAP models	
operators.....	234
subscribers	229
limiting subscribers plug-in.....	161, 204
configuring	
SDX Configuration Editor	161
SRC CLI	204
listeners, defining	419
logging	
properties	
enterprise service portal	450
redirect server	360, 372
login events, description	16
login process	
enterprise	32
residential	17
DHCP	22–27
PPP	18–20
<i>See also</i> logout process, residential	
summary	16
login registration	
configuring	
SDX Configuration Editor	55
SRC CLI	46

logout process, residential	
DHCP	28
PPP	21
<i>See also</i> login process	

M

managers	
configuring	
SRC CLI	287
control over all retailers	7
management privileges	6
subscribers and subscriptions	6
manuals, SRC	
comments	xxiii
multihop environment	339

N

NAT (Network Address Translation)	
rules	520
services for Enterprise Manager Portal	386
services, IP address	513, 515, 526
types	516
VPNs	399, 406
<i>See also</i> NAT Address Management Portal	
NAT Address Management Portal	
acknowledging IP address release	527
assigning IP addresses	526
deployment settings	435
Enterprise Manager Portal	441
overview	525
network address translation. <i>See</i> NAT	
NIC (network information collector)	
enterprise service portals. with	419
NIC proxies	
enterprise service portals	451
notice icons defined	xx

O

objectives of guide	xix
operators	
adding	
SDX Admin	253
control over all retailers	234
LDAP model	234
management privileges	13, 233
subscribers and subscriptions	12, 232
outsourced services	
configuring subscriptions	258

P

parameters	
acquisition path and substitutions	420
sample enterprise service portal	537
performance	
enterprise service portals	419
plug-ins	
activating service sessions	135
audit plug-in, configuring	454
authentication	

configuring, SDX Configuration Editor	160
configuring, SRC CLI	203
authorization	
configuring, SDX Configuration Editor	160
configuring, SRC CLI	203
basic RADIUS accounting	152, 192
configuring, SDX Configuration Editor	158
configuring, SRC CLI	196
basic RADIUS authentication	161, 203
configuring, SDX Configuration Editor	162
configuring, SRC CLI	205
configuring	
SDX Configuration Editor	141
creating subscriber sessions	134
custom RADIUS accounting	152, 192
configuring, SDX Configuration Editor	159
configuring, SRC CLI	200
custom RADIUS authentication	161, 203
configuring	164
configuring, SRC CLI	209
defining RADIUS packets	
SDX Admin	149
SDX Configuration Editor	176
SRC CLI	215
DHCP address assignment	132
embedded AdminServer authorization	187
event publishers. <i>See</i> event publishers	
external	
configuring in SAE property file	148
configuring, SDX Configuration Editor	144
configuring, SRC CLI	138
CORBA object reference	145
flat file accounting	152, 192
configuring, SDX Configuration Editor	153
configuring, SRC CLI	193
flexible RADIUS accounting	152, 192
configuring	198
configuring, SDX Configuration Editor	158
flexible RADIUS authentication	161, 203
configuring, SDX Configuration Editor	163
configuring, SRC CLI	207
instances, creating	143
internal	130
authorization	130
configuring in SAE property file	148
configuring RADIUS peers, SDX Configuration Editor	175
configuring RADIUS peers, SRC CLI	190
configuring, SDX Configuration Editor	143
configuring, SRC CLI	137
customizing RADIUS packets	132
how they work	129
pool	129
RADIUS attributes, SDX Configuration Editor	177
RADIUS attributes, SRC CLI	215
tracking	131
LDAP authentication	161, 204
configuring, SDX Configuration Editor	166
configuring, SRC CLI	212

- limiting subscribers 161, 204
 - configuring, SDX Configuration Editor 161
 - configuring, SRC CLI 204
 - listeners 419
 - state synchronization
 - configuring, SDX Configuration Editor 146
 - configuring, SRC CLI 139
 - tracking
 - configuring, SDX Configuration Editor 152
 - configuring, SRC CLI 192
 - service sessions 135
 - subscriber sessions 134
 - See also* Enterprise Service Manager audit plug-in
 - policies
 - basic BoD 390
 - BoD 391
 - BoD and VPNs 397
 - NAT 386
 - parameters 422
 - PPP subscribers
 - login process 18–20
 - logout process 21
 - Web login 18
 - precedence
 - subscriptions 376
 - prevention, use of unauthorized resources 338, 345
 - privileges
 - IT managers 416
 - properties
 - remote SAE properties 451
 - subscriber information 443, 449
 - WEB-INF/portalBehavior.properties 307
 - protocols
 - communication 426
 - routing 399, 406
 - proxy HTTP 345, 347
 - proxy request management 339, 345
 - public addresses, VPNs 399, 406
 - public wireless LAN applications 339
- Q**
- QoS tracking plug-in 152, 192
- R**
- RADIUS
 - server and equipment registration 304
 - server with ISP service 304
 - RADIUS attributes
 - defining in RADIUS plug-ins
 - SDX Configuration Editor 177
 - SRC CLI 215
 - examples, defining in RADIUS plug-ins
 - SDX Configuration Editor 182
 - SRC CLI 222
 - RADIUS client library, custom RADIUS plug-ins 132
 - RADIUS packets, customizing in plug-ins 132
 - RADIUS peers
 - configuring in plug-ins
 - SDX Configuration Editor 175
 - SRC CLI 190
 - RADIUS plug-ins
 - authentication 161, 203
 - UDP port 174, 215
 - See also* plug-ins
 - RADIUS services
 - configuring subscriptions 264
 - redirect server
 - configuration prerequisites 351
 - configuration statements 350
 - configuring
 - C-series platform 351
 - Solaris platform 363
 - directory connection 353
 - failover 348
 - file extensions 356
 - logging 360, 372
 - number of requests 355
 - protection against denial-of-service attacks 348
 - redundancy 347, 348
 - traffic definition 354
 - redundancy
 - redirect server 347
 - release notes xxiii
 - residential portal
 - developing 300
 - overview 299, 335
 - prerequisites for development 335
 - RADIUS authentication for login 305
 - security 339
 - See also* sample residential portal
 - residential subscribers 3, 9
 - adding
 - SDX Admin 242
 - SRC CLI 279
 - login process. *See* login process
 - retailers
 - subscribers 3, 9
 - adding, SDX Admin 236
 - adding, SRC CLI 276
 - router subscribers 4, 10
 - adding
 - SDX Admin 251
 - SRC CLI 286
 - routing instances 396
 - routing instances, VPNs 400, 407
 - routing scheme 399, 406
 - rules, NAT 520
- S**
- SAE (service activation engine)
 - classification scripts. *See* classification scripts
 - identifying 417
 - login events 15
 - login process. *See* login process
 - logout process. *See* logout process

- property file
 - configuring external plug-ins 148
 - configuring internal and hosted plug-ins 148
- SAE (service activation engine), configuring
 - accepting login names with different formats
 - property file 60
 - interim accounting
 - SDX Configuration Editor 52
 - SRC CLI 43
 - loading subscriptions, RADIUS authorization
 - property file 58
 - login registration
 - SDX Configuration Editor 55
 - SRC CLI 46
 - multiple logins from same IP address
 - SDX Configuration Editor 54
 - SRC CLI 45
 - property file
 - modifying with SDX Admin 57
 - modifying with text editor 58
 - reduce reported session time
 - SDX Configuration Editor 53
 - SRC CLI 44
 - session reactivation timers
 - SDX Configuration Editor 56
 - SRC CLI 46
 - time for MAC address in cache
 - SDX Configuration Editor 50
 - SRC CLI 41
 - unauthenticated user DN
 - SDX Configuration Editor 51
 - SRC CLI 43
 - virtual portal address 337
 - See also* SAE (service activation engine)
- sample enterprise service portal
 - configuring 442–452
 - configuring connection to directory 433
 - customizing 433
 - privileges 416
 - data, displaying 460
 - managing services 531–533
 - monitoring
 - service sessions 535
 - subscriptions 533
 - networks for departments 536, 537
 - overview 417
 - parameters 537
 - service parameters 534
- sample residential portal
 - action classes 302
 - behaviors 302
 - customizing 313
 - developing portal based on the sample 340, 539
 - development tools 336
 - equipment registration 302, 304, 328
 - installing 312
 - login 316
 - model components 302
 - overview 315, 336
 - personal digital assistant (PDA) 333
 - prerequisites 312
 - schedules 323
 - service activation 322
 - services
 - management 318
 - schedules 323
 - subscriptions 327
 - usage
 - information 321
 - view components 302
 - Web application framework 301
 - security, residential portal 339
 - sending traffic to VPNs 490
 - service activation 419
 - service activation engine. *See* SAE
 - service parameters, enterprise 420
 - service schedules
 - Enterprise Manager Portal, in 467–474
 - sample residential portal, in 324
 - service scopes
 - assigning
 - subscribers, SDX Admin 240
 - service sessions
 - activate-on-login 38, 135
 - activating and tracking 135
 - activating with Web application 33
 - enterprise, remote activation 38
 - services
 - basic BoD 388, 391
 - BoD 392, 393, 474
 - JUNOS routing platforms 398
 - BoD and VPNs 397
 - NAT 386
 - sample enterprise service portal, managing 531
 - See also* firewall services
 - single-hop environment 339
 - sites 4, 5, 11, 12
 - subscriber
 - adding, SDX Admin 249
 - adding, SRC CLI 285
 - source class usage (SCU) 398
 - SRC documentation set
 - comments xxiii
 - obtaining xxiii
 - SRC documentation CD xxi
 - SRC single-hop requirement 339
 - SRC software distribution xxiii
 - state synchronization plug-in interface
 - configuring
 - SRC CLI 139
 - configuring, SDX Configuration Editor 146
 - static IP subscribers, login process 29–31
 - static routing 399, 406
 - subscriber classification scripts. *See* classification scripts
 - subscriber folders 4, 10
 - adding
 - SDX Admin 240
 - SRC CLI 278

subscriber sessions	
activating with Web application	34
creating and tracking.....	134
deactivating with Web application.....	36
enterprise, creating and activating	32
subscribers	
access	10
adding	
SDX Admin	236–252
SRC CLI	275–287
billing	398
directory connection properties	443, 449
enterprise.....	3, 9
adding, SDX Admin	246
adding, SRC CLI	283
inheriting properties.....	235, 274
inheriting subscriptions.....	235, 274
LDAP model	229
password encryption.....	235
residential	3, 9
adding, SDX Admin	242
adding, SRC CLI	279
retailer	3, 9
adding, SDX Admin	236
adding, SRC CLI	276
router	4, 10
adding, SDX Admin	251
adding, SRC CLI	286
service scopes, assigning	
SDX Admin	240
sites.....	3, 9
adding, SDX Admin	249
adding, SRC CLI	285
types	3, 9
subscriptions	4, 10, 230
access, configuring	
SDX Admin	261
SRC CLI	292
activation order, specifying	
SDX Admin	231
SRC CLI	274
enterprise hierarchy	423
hierarchy.....	5, 12
LDAP model	231
multiple per subscriber.....	258, 292
outsourced services, configuring	258
password encryption.....	235
priority	376
RADIUS, configuring.....	264
sample enterprise service portal, creating	531
value-added services, configuring.....	255
substitutions	
configuring.....	269
parameter acquisition path.....	420
sample enterprise portal.....	537
use	421
Sun ONE Directory Server	
enterprise service portal	427
support, requesting.....	xxiv
T	
targets. <i>See</i> classification scripts	
technical support, requesting.....	xxiv
text conventions defined	xx
Tomcat, as Java development environment	340, 539
tracking plug-ins	131
configuring	
SDX Configuration Editor	152
SRC CLI	192
U	
UDP ports	
RADIUS plug-ins	174, 215
User Datagram Protocol. <i>See</i> UDP	
V	
validating	
VPNs	411
value substitution.....	422
value-added services	
subscriptions	
configuring.....	255
virtual portal address	337
configuring.....	337
virtual private networks. <i>See</i> VPNs	
VPN Subscription Deactivator	411
VPNs (virtual private networks)	
adding	
data integrator	406
SDX Admin	407
SRC CLI	401
configuration requirements	399, 405, 406
configuration statements.....	400
definition.....	400, 405
deleting	412
directory.....	487
exporting.....	409
extranet clients, modifying	
SDX Admin	409, 411
SRC CLI	402
identifiers	396
invalid subscriptions.....	411
modifying.....	402, 408, 487
VPN to which router sends traffic.....	490
routing schemes	399, 406
sending traffic	490
stopping router from sending traffic.....	491
using NAT	399, 406
validating.....	411
W	
WEB-INF/jboss-web.xml.....	306
WEB-INF/portalBehavior.properties	306
WEB-INF/struts-config.xml.....	306, 309
WEB-INF/tiles-defs.xml	306, 311
WEB-INF/web.xml.....	306