



**SRC-PE Software**

## **Subscribers and Subscriptions Guide**

*Release 3.0.x*

**Juniper Networks, Inc.**

1194 North Mathilda Avenue  
Sunnyvale, California 94089  
USA

408-745-2000

**[www.juniper.net](http://www.juniper.net)**

Part Number: 530-026632-01, Revision 1

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

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

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

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

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

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

*SRC-PE Software Subscribers and Subscriptions Guide*  
Release 3.0.x  
Copyright © 2008, Juniper Networks, Inc.  
All rights reserved. Printed in USA.

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

Revision History  
15 August 2008—Revision 1

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

#### YEAR 2000 NOTICE

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

#### SOFTWARE LICENSE

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

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

For complete product documentation, please see the Juniper Networks Web site at [www.juniper.net/techpubs](http://www.juniper.net/techpubs).

## End User License Agreement

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# Abbreviated Table of Contents

About This Guide

xxiii

## Part 1

### Managing Subscribers and Subscriptions

---

Chapter 1	Overview of Subscribers and Subscriptions on a C-series Controller	3
Chapter 2	Subscriber Logins and Service Activation	9
Chapter 3	Configuring Subscriber-Related Properties on the SAE (SRC CLI)	33
Chapter 4	Classifying Interfaces and Subscribers (SRC CLI)	39
Chapter 5	Overview of Plug-Ins Included with the SAE	73
Chapter 6	Configuring Internal, External, and Synchronization Plug-Ins (SRC CLI)	81
Chapter 7	Configuring Accounting and Authentication Plug-Ins (SRC CLI)	85
Chapter 8	Configuring Subscribers and Subscriptions (SRC CLI)	125

## Part 2

### Redirecting Subscriber Traffic Through Redirect Server

---

Chapter 9	Redirecting Subscriber Traffic	149
Chapter 10	Configuring Traffic Redirection (SRC CLI)	153

## Part 3

### Designing Services for Enterprise Manager Portal

---

Chapter 11	Reviewing and Configuring Policies and Services for Enterprise Manager Portal	171
Chapter 12	Adding VPNs from JUNOS Routing Platforms (SRC CLI)	197

## Part 4

### Managing Access Portals for Enterprise Subscribers

---

Chapter 13	Overview of Enterprise Service Portals	205
Chapter 14	Planning Deployment for Enterprise Service Portals	215
Chapter 15	Installing and Configuring Enterprise Service Portals	221
Chapter 16	Managing Services with Enterprise Manager Portal	235
Chapter 17	Managing Enterprise Service Portals	301
Chapter 18	Using NAT Address Management Portal	307
Chapter 19	Using the Sample Enterprise Service Portal	311
Chapter 20	Developing an Enterprise Service Portal	321

## Part 5

### Index

---

Index	327
-------	-----



# Table of Contents

---

## About This Guide xxiii

---

SRC Guides and Release Notes .....	xxiii
Audience .....	xxiii
Documentation Conventions .....	xxiii
Related Juniper Networks Documentation .....	xxv
Obtaining Documentation .....	xxvii
Documentation Feedback .....	xxvii
Requesting Technical Support .....	xxvii

## Part 1

---

## Managing Subscribers and Subscriptions

---

### Chapter 1

---

### Overview of Subscribers and Subscriptions on a C-series Controller 3

---

Overview of Subscribers .....	3
Overview of Subscriptions .....	4
Enterprise Subscriber and Subscription Hierarchy .....	4
Enterprise Subscription Hierarchy .....	5
Overview of Managers .....	5
Read Privileges .....	5
Management Privileges .....	6
Managers That Control All Retailers .....	7

### Chapter 2

---

### Subscriber Logins and Service Activation 9

---

Login Events and Processes for the SRC Software .....	9
Overview of Login Events and Processes .....	9
Login Events .....	9
Summary of the Login Process .....	10
Residential Subscriber Login and Processes .....	11
PPP Subscriber Login and Service Activation .....	12
Web Login for PPP Subscribers .....	12
PPP Login Interactions .....	13
PPP Logout Interactions .....	14
DHCP Subscriber Login and Service Activation .....	15
Interface Startup .....	16
Initial Login .....	16
Initial DHCP Login Interactions .....	17

DHCP Login to Subscriber Account Interactions .....	18
Persistent DHCP Subscriber Login Interactions .....	20
DHCP Subscriber Logout Interactions .....	21
Static IP Subscribers .....	22
Single PC, IP Address Known .....	22
Subscriber IP Address Not Known .....	23
Enterprise Subscriber Login Process .....	24
Interface Startup .....	25
Subscriptions and Activations .....	25
Subscription Activation Interactions .....	27
Subscription Deactivation Interactions .....	29
Automatic Activation at Login .....	30
Enterprise-Specific Remote Session Activation .....	31

### **Chapter 3                      Configuring Subscriber-Related Properties on the SAE (SRC CLI)                      33**

Configuring the Length of Time MAC Addresses Remain in SAE Cache .....	33
Identifying a Profile for Unauthenticated Subscribers .....	34
Configuring Interim Accounting for Services and Subscribers .....	35
Avoiding Overcharges for Sessions That Time Out .....	36
Allowing Multiple Logins from the Same IP Address .....	36
Authenticating Registered Username/Password Pairs .....	37
Configuring Timers for Session Reactivation .....	38

### **Chapter 4                      Classifying Interfaces and Subscribers (SRC CLI)                      39**

Overview of Classification Scripts .....	39
How Classification Scripts Work .....	40
Interface Classification Scripts .....	40
Subscriber Classification Scripts .....	41
DHCP Classification Scripts .....	41
Overview of Configuring Classification Scripts .....	41
Subscriber Classifiers .....	41
DHCP Classifiers .....	42
Interface Classifiers .....	42
Classification Targets .....	42
Target Expressions .....	43
Classification Conditions .....	43
Glob Matching .....	44
Regular Expression Matching .....	44
Classifying Interfaces (SRC CLI) .....	45
Interface Classification Conditions .....	47
Example: Managing Interfaces for Premium and Basic PPP and DHCP	
Subscribers .....	49
Example: Managing Specific Interfaces .....	50
Example: Managing Interfaces by Using the Interface Description .....	50
Classifying Subscribers (SRC CLI) .....	51
Subscriber Classification Conditions .....	54
Sending DHCP Options to the JUNOS Router .....	57
Subscriber Classification Targets .....	58

Example: Subscriber Classification Scripts for Static IP Subscriber .....	59
Example: Subscriber Classification Scripts Using a Subscriber Group .....	60
Example: Subscriber Classification Scripts for Enterprise Subscribers .....	60
Matching on the Interface Name .....	60
Matching on the Interface Alias .....	61
Example: Creating Router Interface Subscriber Session .....	61
Example: Activating Services for a Group of Subscriber Sessions .....	61
Classifying DHCP Subscribers (SRC CLI) .....	62
DHCP Classification Conditions .....	63
Syntax for DHCP Classification Targets .....	65
Selecting DHCP Parameters .....	65
DHCP Options Supported on the SAE .....	66
Creating DHCP Profiles (SRC CLI) .....	69

## **Chapter 5                      Overview of Plug-Ins Included with the SAE                      73**

How Internal Plug-Ins Work .....	73
Plug-In Pool .....	73
Event Publishers .....	74
Types of Internal Plug-Ins .....	74
Authorization Plug-Ins .....	74
Tracking Plug-Ins .....	75
Customizing RADIUS Packets with Plug-Ins .....	75
Assigning DHCP Addresses to Subscribers .....	76
Creating and Tracking Subscriber Sessions .....	77
Activating and Tracking Service Sessions .....	79

## **Chapter 6                      Configuring Internal, External, and Synchronization Plug-Ins (SRC CLI)                      81**

Configuring Internal Plug-Ins .....	81
Configuring the SAE for External Plug-Ins .....	82
Configuring the State Synchronization Plug-In Interface .....	83

## **Chapter 7                      Configuring Accounting and Authentication Plug-Ins (SRC CLI)                      85**

Creating RADIUS Peers .....	85
Types of Tracking Plug-Ins .....	87
Configuring Tracking Plug-Ins .....	88
Configuring Flat File Accounting Plug-Ins .....	88
Configuring Headers for Flat File Accounting Plug-Ins .....	90
Configuring Basic RADIUS Accounting Plug-Ins .....	91
Configuring Flexible RADIUS Accounting Plug-Ins .....	93
Configuring Custom RADIUS Accounting-Plug-Ins .....	95
Types of Authentication Plug-Ins .....	98
Configuring Authentication Plug-Ins .....	99
Limiting Subscribers on Router Interfaces .....	99
Configuring Basic RADIUS Authentication Plug-Ins .....	100
Configuring Flexible RADIUS Authentication Plug-Ins .....	102

Configuring Custom RADIUS Authentication Plug-Ins .....	104
Configuring LDAP Authentication Plug-Ins .....	107
Configuring UDP Ports for RADIUS Plug-Ins .....	109
Defining RADIUS Packets for Flexible RADIUS Plug-Ins .....	110
Overview of Flexible RADIUS Plug-Ins .....	110
Using Default RADIUS Templates .....	110
Naming RADIUS Attribute Instances .....	111
Defining RADIUS Attributes .....	112
Standard RADIUS Attributes .....	112
Juniper Networks VSAs .....	112
Defining the Values of RADIUS Attributes .....	113
Configuring a RADIUS Packet Template .....	116
Using Flexible RADIUS Packet Definitions .....	118
Setting Values in Authentication Response Packets .....	119
Selecting IP Address Pools Using DHCP Response Packets .....	120
Configuring Event Publishers .....	121
Special Types of Event Publishers .....	121
Configuring Service-Specific Event Publishers .....	121
Configuring Retailer-Specific Event Publishers .....	121
Configuring Virtual Router-Specific Event Publishers .....	121
Configuring Global and Default Retailer Event Publishers .....	122

## Chapter 8

### Configuring Subscribers and Subscriptions (SRC CLI)

**125**

Overview of Configuring Subscribers and Subscriptions .....	125
Specifying the Activation Order for Subscriptions .....	125
Inheritance of Properties and Subscriptions .....	126
Enabling the Subscriber and Subscription Configuration on the SRC CLI .....	126
Adding Subscribers (SRC CLI) .....	126
Adding Retailers (SRC CLI) .....	127
Configuring Administrative Information for Retailers (SRC CLI) .....	128
Adding Subscriber Folders (SRC CLI) .....	129
Adding Residential Subscribers (SRC CLI) .....	130
Configuring Administrative Information for Residential Subscribers (SRC CLI) .....	133
Adding Enterprises (SRC CLI) .....	134
Configuring Administrative Information for Enterprise Subscribers (SRC CLI) .....	135
Adding Sites (SRC CLI) .....	136
Adding Devices as Subscribers (SRC CLI) .....	137
Adding Managers (SRC CLI) .....	139
Configuring Subscriptions (SRC CLI) .....	141
Configuring Accesses (SRC CLI) .....	143

<b>Part 2</b>	<b>Redirecting Subscriber Traffic Through Redirect Server</b>	
<b>Chapter 9</b>	<b>Redirecting Subscriber Traffic</b>	<b>149</b>
	Overview of Traffic Redirection .....	149
	Proxy Request Management .....	149
	HTTP Proxy and DNS .....	150
	Protection Against Denial-of-Service Attacks .....	151
	Redirect Server Redundancy .....	151
<b>Chapter 10</b>	<b>Configuring Traffic Redirection (SRC CLI)</b>	<b>153</b>
	Configuration Statements for the Redirect Server (SRC CLI) .....	153
	Before You Configure the Redirect Server on a C-Series Controller .....	154
	Configuring the Redirect Server (SRC CLI) .....	155
	Configuring General Properties for the Redirect Server (SRC CLI) .....	156
	Configuring a Connection Between the Redirect Server and the Directory (SRC CLI) .....	157
	Defining Traffic to Transmit to the Redirect Server (SRC CLI) .....	158
	Changing the Number of Requests That the Redirect Server Accepts (SRC CLI) .....	159
	Specifying Extensions for Files That the Redirect Server Accepts (SRC CLI) .....	160
	Verifying Configuration for the Redirect Server (SRC CLI) .....	161
	Enabling the Redirect Server .....	161
	Configuring the DNS Server for the Redirect Server (SRC CLI) .....	162
	Configuring the Redirect Server to Support HTTP Proxies (SRC CLI) .....	163
	Before You Configure Redundancy for a Redirect Server .....	164
	Configuring a Redundant Redirect Server (SRC CLI) .....	164
	Configuring Logging for the Redirect Server .....	166
	Changing the Configuration for the Redirect Server .....	166
	Assessing Load for Redirect Server (C-Web Interface) .....	166
<b>Part 3</b>	<b>Designing Services for Enterprise Manager Portal</b>	
<b>Chapter 11</b>	<b>Reviewing and Configuring Policies and Services for Enterprise Manager Portal</b>	<b>171</b>
	Overview of Services for Enterprise Manager Portal .....	171
	Directory Structure .....	172
	Priorities for Subscriptions .....	172
	Before You Configure Services for Enterprise Manager Portal .....	172
	Configuring Firewall Policies and Services for Enterprise Manager Portal ....	173
	Types of Firewall Services .....	173
	Overview of Basic Firewall Services and Policies .....	174
	Tasks to Configure Firewall Policies and Services .....	175
	Configuring Basic Firewall Policies .....	175

Configuring Basic Firewall Services .....	176
Reviewing the fwrule Policy Group for Exceptions to Stateful Firewalls .....	176
Reviewing the Firewall Rule Service for Exceptions to Stateful Firewalls .....	176
Reviewing Services for Exceptions to Stateless Firewalls .....	177
Parameter Values Used by Services for Exceptions to Stateless Firewalls .....	178
Planning Services for Custom Firewall Exceptions .....	179
Configuring Policies for Custom Firewall Exceptions .....	179
Configuring Services for Custom Firewall Exceptions .....	180
Configuring Priorities for Stateless or Stateful Firewall Services .....	180
Configuring Priorities to Have Enterprise Services Work Together .....	180
Configuring Priorities for Individual Scopes by Defining Them in Services .....	181
Using Stateless Firewall and BoD Applications Together .....	181
Configuring NAT Policies and Services for Enterprise Manager Portal .....	182
NAT Policies and Services in the SRC Sample Data .....	182
Configuring the dynsrcnat Policy Group .....	182
Reviewing the DynSrcNat Service .....	183
Configuring the staticdstnat Policy Group .....	183
Configuring the StaticDstNat Service .....	183
Configuring the staticsrcnat Policy Group .....	183
Configuring the StaticSrcNat Service .....	184
Configuring Bandwidth Policies and Services for Enterprise Manager Portal .....	184
Overview of Bandwidth-on-Demand Services .....	184
Parameter Values Used by BoD Services .....	185
Bandwidth Policies for Different Routing Platforms .....	186
Configuring Basic BoD Policies .....	186
Configuring Basic BoD Services .....	187
Configuring BoD Policies .....	187
Configuring BoD Services .....	188
Using BoD Services to Assign Traffic to Bandwidth Categories .....	189
Using BoD and Basic BoD Services Together to Supply Class of Service .....	189
Examples: Setting Up Forwarding Preferences .....	190
Setting Up Forwarding Preferences by Using CoS on JUNOS Routing Platforms .....	190
Setting Up Forwarding Preferences by Allocating a Percentage of a Link's Bandwidth to a Service .....	191
Enabling Schedules for Subscriptions for Enterprise Manager Portal .....	192
Configuring VPNs for Enterprise Manager Portal .....	192
Overview of VPN Management Through Enterprise Manager Portal .....	192
Before You Configure VPN Policies and Services .....	193
Configuring Policies for BoD Traffic Destined for VPNs .....	193
Configuring Services for BoD Traffic Destined for VPNs .....	194
Billing Subscribers Through SCU/DCU for JUNOS Routing Platforms .....	194

<b>Chapter 12</b>	<b>Adding VPNs from JUNOS Routing Platforms (SRC CLI)</b>	<b>197</b>
	Before You Add a JUNOS VPN to the SRC Configuration .....	197
	Configuring VPNs to Integrate into an SRC Network .....	198
	Configuration Statements for Adding VPNs and Extranet Clients .....	198
	Adding VPNs for Retailers and Enterprises .....	199
	Verifying and Updating Configuration of Extranets for VPNs .....	200
	Locating and Removing Inactive Subscriptions to a VPN .....	201
 <b>Part 4</b>	 <b>Managing Access Portals for Enterprise Subscribers</b>	
 <b>Chapter 13</b>	 <b>Overview of Enterprise Service Portals</b>	 <b>205</b>
	Function of Enterprise Service Portals .....	205
	Consistency of Data in the Directory .....	206
	Privileges of IT Managers .....	206
	Developing and Customizing Enterprise Service Portals .....	206
	Identifying the SAE .....	206
	Enterprise Service Portals Provided with the SRC Software .....	207
	Sample Enterprise Service Portal .....	207
	Enterprise Manager Portal .....	207
	NAT Address Management Portal .....	207
	Enterprise Service Portal Audit Plug-In .....	209
	Network Information Collector with Enterprise Service Portals .....	209
	Service Parameters .....	209
	Substitutions and the Parameter Acquisition Path .....	210
	Power of Substitutions .....	211
	Substituting Values for Policy Parameters .....	211
	Managing Subscriptions to Aggregate Services .....	212
	Configuring Your Web Browser to Use an Enterprise Service Portal .....	212
	Accessing Enterprise Service Portals .....	212
 <b>Chapter 14</b>	 <b>Planning Deployment for Enterprise Service Portals</b>	 <b>215</b>
	Architecture of Enterprise Service Portals .....	215
	Elements for an Enterprise Service Portal .....	215
	Communication Protocols .....	216
	Deployment Scenario for an Enterprise Service Portal .....	216
	Deciding Which Enterprise Service Portal to Use .....	217
	Planning Number of Instances of an Enterprise Service Portal .....	218
	Planning Namespace Hierarchy for an Enterprise Service Portal .....	218
 <b>Chapter 15</b>	 <b>Installing and Configuring Enterprise Service Portals</b>	 <b>221</b>
	Before You Install an Enterprise Service Portal .....	221
	Setting Up Enterprise Service Portals .....	222
	Preparing the Web Applications for Customization .....	222

Configuring Connections to the Directory .....	223
Initialization Properties for Enterprise Service Portals .....	223
Configuring Deployment Settings for Enterprise Manager Portal .....	225
Deployment Properties for Enterprise Manager Portal .....	225
Configuring the URL for an Enterprise Service Portal .....	231
Writing an Application to Allow a Machine to Provide Public IP Addresses for NAT .....	231
Configuring an Enterprise Service Portal Audit Plug-In .....	232

## Chapter 16

## Managing Services with Enterprise Manager Portal **235**

Overview of Enterprise Manager Portal .....	235
Getting Help on Enterprise Manager Portal .....	236
Setting the Configuration Level for Enterprise Manager Portal .....	236
Managing Schedules .....	237
Schedules in Enterprise Manager Portal .....	237
Enabling Scheduling for the Enterprise Manager Portal .....	238
Using Schedules in Enterprise Manager Portal .....	238
Creating a Schedule in Enterprise Manager Portal .....	238
Schedule Fields in Enterprise Manager Portal .....	240
Applying a Schedule to a Service in Enterprise Manager Portal .....	242
Disabling a Schedule for a Service in Enterprise Manager Portal .....	243
Changing Schedules in Enterprise Manager Portal .....	244
Managing Subscriptions to Bandwidth-on-Demand Services .....	244
Overview of Bandwidth-on-Demand Services .....	245
Planning Subscriptions to BoD Services .....	245
Creating a Subscription to BoD Services .....	246
Setting a Bandwidth Level .....	246
Bandwidth Level Fields in Enterprise Manager Portal .....	247
Adding Subscriptions to BoD Services .....	247
BoD Service Fields in Enterprise Manager Portal .....	250
Modifying Rules for a Subscription to a BoD Service .....	258
Modifying the Bandwidth Level .....	258
Moving the Bandwidth Level .....	258
Deleting a Subscription for a BoD Service .....	258
Deleting the Bandwidth Level .....	259
Monitoring Use of Subscriptions to BoD Services .....	259
Integrating VPNs into an SRC Network Through Enterprise Manager Portal .....	260
Overview of VPNs in an SRC Network .....	260
Modifying Subscriber VPN Configuration .....	260
VPN Fields in Enterprise Manager Portal .....	261
Creating Extranets Through Enterprise Manager Portal .....	262
Deleting Extranets Through Enterprise Manager Portal .....	263
Sending Traffic to a VPN .....	263
Modifying the VPN to Which the Router Sends Traffic .....	263
Stopping the Router from Sending Traffic to VPNs .....	264

Classifying Traffic for Stateful Firewall Exceptions and NAT Rules .....	264
Overview of Traffic Classification for Firewall Exceptions and NAT	
Rules .....	264
Classifying Traffic .....	265
Traffic Classification Fields in Enterprise Manager Portal .....	266
Modifying Values for Traffic Classifications .....	269
Deleting Traffic Classifications .....	270
Subscribing to Firewall Services Through Enterprise Manager Portal .....	270
Overview of Firewall Services in Enterprise Manager Portal .....	270
Before You Configure Firewall Exception Rules .....	271
Creating Subscriptions to Firewall Services .....	271
Firewall Service Field in Enterprise Manager Portal .....	272
Creating Firewall Exceptions for Stateless Firewalls .....	272
Fields for Exceptions to Stateless Firewalls in Enterprise Manager	
Portal .....	275
Creating Firewall Exceptions for Stateful Firewalls .....	283
Fields for Exceptions to Stateful Firewalls in Enterprise Manager	
Portal .....	283
Adding a Schedule to a Firewall Exception .....	286
.....	286
Modifying Firewall Exceptions .....	287
Deleting Firewall Exceptions .....	287
Deleting Basic Firewalls .....	287
Monitoring the Use of Subscriptions to Firewall Services .....	288
Working with IP Addressing and NAT Services .....	288
Requesting Public IP Addresses for NAT Services .....	289
Address Fields for NAT Addressing in Enterprise Manager Portal .....	290
Canceling Requests for Public IP Addresses .....	290
Returning Public IP Addresses to Service Providers .....	291
Applying NAT Rules to Traffic .....	291
Configuring Public IP Addresses for Outgoing Traffic .....	293
Outgoing Traffic Fields for NAT Addressing in Enterprise Manager	
Portal .....	293
Configuring Public IP Addresses for Incoming Traffic .....	294
Incoming Traffic Fields for NAT Addressing in Enterprise Manager	
Portal .....	294
Configuring Fixed Public Addresses for Outgoing Traffic .....	295
Modifying NAT Rules .....	296
Deleting NAT Rules .....	296
Monitoring the Status of Subscriptions .....	296
Troubleshooting Subscriptions That Are Not Functioning Correctly .....	299
Troubleshooting Subscriptions of Unknown Status .....	299

<b>Chapter 17</b>	<b>Managing Enterprise Service Portals</b>	<b>301</b>
	Displaying Information About Your Control in the Enterprise Through the Enterprise Service Portal .....	301
	Updating Data That the Enterprise Service Portal Displays .....	302
	Managing Operators Through the Enterprise Service Portal .....	302
	Creating Managers Through the Enterprise Service Portal .....	302
	Managers Fields in the Enterprise Service Portal .....	303
	Modifying Managers Through the Enterprise Service Portal .....	305
	Deleting Managers Through the Enterprise Service Portal .....	305
<b>Chapter 18</b>	<b>Using NAT Address Management Portal</b>	<b>307</b>
	Overview of NAT Address Management Portal .....	307
	Assigning IP Addresses .....	307
	Acknowledging the Release of IP Addresses .....	308
<b>Chapter 19</b>	<b>Using the Sample Enterprise Service Portal</b>	<b>311</b>
	Overview of the Sample Enterprise Service Portal .....	311
	Starting the Sample Enterprise Service Portal .....	311
	Subscribing to Services .....	312
	Activating Subscriptions .....	313
	Deactivating Subscriptions .....	314
	Suspending Subscriptions .....	314
	Canceling Suspensions of Subscriptions .....	315
	Monitoring Use of Subscriptions .....	315
	Specifying Values for Service Parameters in Subscriptions .....	315
	Restoring Default Values for Service Parameters In Subscriptions .....	316
	Deleting Subscriptions .....	316
	Monitoring Service Sessions for a Subscription .....	316
	Defining Networks for Departments in an Enterprise .....	317
	Modifying Network Definitions for Departments in an Enterprise .....	318
	Deleting Network Definitions for Departments in an Enterprise .....	319
<b>Chapter 20</b>	<b>Developing an Enterprise Service Portal</b>	<b>321</b>
	Developing a Portal Based on the Sample Enterprise Service Portal .....	321
	Preparing to Develop a Sample-Based Enterprise Service Portal .....	321
	Creating a Portal Project for a Sample-Based Enterprise Service Portal .....	322
	Building a Sample-Based Enterprise Service Portal .....	322
	Deploying a Sample-Based Enterprise Service Portal .....	323
	Testing a Sample-Based Enterprise Service Portal .....	323
	Using a Virtual Address for the Portal .....	323

**Part 5****Index**

---

Index .....	327
-------------	-----



# List of Figures

Figure 1: Enterprise Hierarchy .....	5
Figure 2: Components Involved in Subscription Activation .....	11
Figure 3: PPP Login Interactions .....	13
Figure 4: PPP Logout .....	15
Figure 5: DHCP Interface Startup .....	16
Figure 6: DHCP Subscriber Initial Login .....	17
Figure 7: DHCP Subscriber Login .....	19
Figure 8: Persistent DHCP Subscriber Login .....	20
Figure 9: DHCP Subscriber Logout .....	21
Figure 10: Static IP Subscriber Login .....	23
Figure 11: Subscriber IP Address Not Known .....	24
Figure 12: Enterprise Subscriber Session Activation .....	25
Figure 13: Service Activation Page .....	26
Figure 14: Subscription Activation Page .....	27
Figure 15: Subscription Activation .....	28
Figure 16: Subscription Deactivation .....	29
Figure 17: Remote Session Activation Sequence .....	31
Figure 18: DHCP Address Assignment .....	76
Figure 19: Creating and Tracking Subscriber Sessions .....	77
Figure 20: Activating and Tracking Service Sessions .....	79
Figure 21: Failover of a Redirect Server .....	152
Figure 22: Elements and Communication Protocols for an Enterprise Service Portal .....	215
Figure 23: Deployment for an Enterprise Service Portal .....	217
Figure 24: Bandwidth & VPNs Page .....	247
Figure 25: Bandwidth & VPNs Page with a Bandwidth Level Set .....	248
Figure 26: VPNs Page .....	261
Figure 27: Applications Page .....	265
Figure 28: Create Exception Dialog Box for Stateless Firewalls .....	273
Figure 29: Firewall Page with Firewall Service Applied and Exceptions Configured .....	274
Figure 30: Firewall Page with Firewall Service Applied .....	283
Figure 31: Addresses Page Before Requesting Addresses .....	289
Figure 32: Addresses Page After Requesting Addresses .....	290
Figure 33: NAT Page .....	292
Figure 34: Manager's Page .....	303
Figure 35: Subscriptions Page .....	314
Figure 36: Departments Page .....	318



# List of Tables

Table 1: Notice Icons .....	xxiv
Table 2: Text Conventions .....	xxiv
Table 3: Juniper Networks C-series and SRC Technical Publications .....	xxv
Table 4: Types of Subscribers .....	3
Table 5: Privilege Levels and Associated Tasks .....	6
Table 6: Login Events .....	10
Table 7: DHCP Options in UserClassificationContext Field .....	57
Table 8: DHCP Options Supported on the SAE .....	67
Table 9: Tracking Plug-Ins .....	87
Table 10: Authentication Plug-Ins .....	98
Table 11: RADIUS Attribute Instance Names .....	111
Table 12: Standard Values for RADIUS Attributes .....	113
Table 13: Services Available from Enterprise Manager Portal .....	171
Table 14: Basic Firewall Services and Policies .....	174
Table 15: Stateless Firewall Services in Sample Data .....	177
Table 16: Parameters for Stateless Firewall Services for Enterprise Manager Portal .....	178
Table 17: NAT Services and Policies	182
Table 18: Parameters for BoD Services for Enterprise Manager Portal .....	185
Table 19: Integrated BoD and Basic BoD Services in Sample Data .....	190
Table 20: Policies to Specify Forwarding Treatment for Specified Traffic Classes .....	192
Table 21: Communication Protocols for an Enterprise Service Portal .....	216
Table 22: Enterprise Service Applications .....	217
Table 23: Namespaces for Enterprise Service Portals .....	218
Table 24: Common Audit Plug-In Information .....	232
Table 25: Events Reportable to the Audit Plug-In .....	232
Table 26: Portal Configuration Support for Services on Routers .....	235
Table 27: Maximum Duration for Recurrence Patterns .....	241
Table 28: Possible Subscription Status .....	298



# About This Guide

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

## SRC Guides and Release Notes

---

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

## Audience

---

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





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

## Documentation Conventions

---

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

**Table 1: Notice Icons**

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

**Table 2: Text Conventions**

Convention	Description	Examples
<b>Bold text like this</b>	<ul style="list-style-type: none"> <li>■ Represents keywords, scripts, and tools in text.</li> <li>■ Represents a GUI element that the user selects, clicks, checks, or clears.</li> </ul>	<ul style="list-style-type: none"> <li>■ Specify the keyword <b>exp-msg</b>.</li> <li>■ Run the <b>install.sh</b> script.</li> <li>■ Use the <b>pkgadd</b> tool.</li> <li>■ To cancel the configuration, click <b>Cancel</b>.</li> </ul>
<b>Bold text like this</b>	Represents text that the user must type.	<code>user@host# set cache-entry-age cache-entry-age</code>
Fixed-width text like this	Represents information as displayed on your terminal's screen, such as CLI commands in output displays.	<pre>nic-locators {   login {     resolution {       resolver-name /realms/       login/A1;       key-type LoginName;       value-type SaeId;     }   } }</pre>
Regular sans serif typeface	<ul style="list-style-type: none"> <li>■ Represents configuration statements.</li> <li>■ Indicates SRC CLI commands and options in text.</li> <li>■ Represents examples in procedures.</li> <li>■ Represents URLs.</li> </ul>	<ul style="list-style-type: none"> <li>■ <code>system ldap server{ stand-alone;</code></li> <li>■ Use the <code>request sae modify device failover</code> command with the <code>force</code> option</li> <li>■ <code>user@host# . . .</code></li> <li>■ <code>http://www.juniper.net/techpubs/software/management/src/api-index.html</code></li> </ul>
<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>&lt; gfwif &gt;</code> .
Key name	Indicates the name of a key on the keyboard.	Press Enter.

**Table 2: Text Conventions** *(continued)*

Key names linked with a plus sign (+)	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
<i>Italic typeface</i>	<ul style="list-style-type: none"> <li>■ Emphasizes words.</li> <li>■ Identifies book names.</li> <li>■ Identifies distinguished names.</li> <li>■ Identifies files, directories, and paths in text but not in command examples.</li> </ul>	<ul style="list-style-type: none"> <li>■ There are two levels of access: <i>user</i> and <i>privileged</i>.</li> <li>■ <i>SRC-PE Getting Started Guide</i></li> <li>■ <i>o = Users, o = UMC</i></li> <li>■ The <i>/etc/default.properties</i> file.</li> </ul>
Backslash	At the end of a line, indicates that the text wraps to the next line.	Plugin.radiusAcct-1.class = \net.juniper.srmt.sae.plugin\RadiusTrackingPluginEvent
Words separated by the   symbol	Represent a choice to select one keyword or variable to the left or right of this symbol. (The keyword or variable may be either optional or required.)	diagnostic   line

## Related Juniper Networks Documentation

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

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

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

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

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

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

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

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

## Obtaining Documentation

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

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

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

## Documentation Feedback

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

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

## Requesting Technical Support

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

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <http://www.juniper.net/customers/support/downloads/710059.pdf>.

- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

### Self-Help Online Tools and Resources

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

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

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

### Opening a Case with JTAC

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

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

## **Part 1**

# **Managing Subscribers and Subscriptions**

- Overview of Subscribers and Subscriptions on a C-series Controller on page 3
- Subscriber Logins and Service Activation on page 9
- Configuring Subscriber-Related Properties on the SAE (SRC CLI) on page 33
- Classifying Interfaces and Subscribers (SRC CLI) on page 39
- Overview of Plug-Ins Included with the SAE on page 73
- Configuring Internal, External, and Synchronization Plug-Ins (SRC CLI) on page 81
- Configuring Accounting and Authentication Plug-Ins (SRC CLI) on page 85
- Configuring Subscribers and Subscriptions (SRC CLI) on page 125



## Chapter 1

# Overview of Subscribers and Subscriptions on a C-series Controller

- 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 5

## 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 on page 3.

**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	<p>Individual subscribers or households—multiple subscribers who use one or more computers and share the same connection.</p> <p>In a household, subscribers can share the same service subscription or can have their own individualized service profiles.</p>
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.

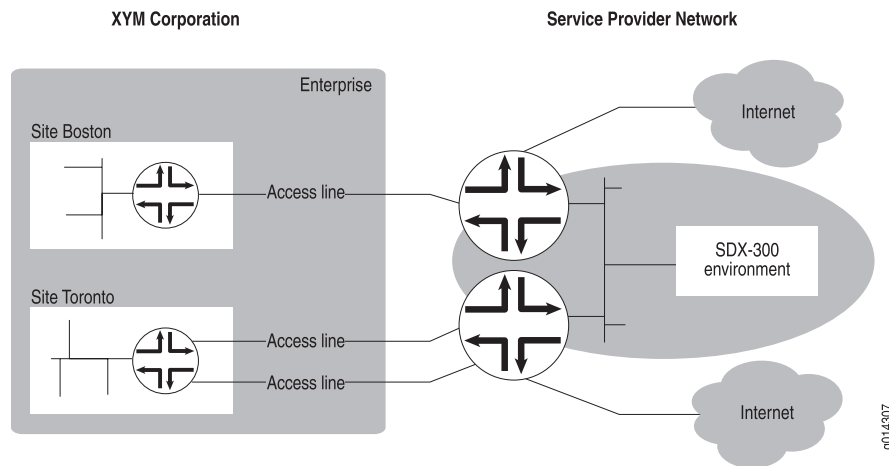
## Enterprise Subscriber and Subscription Hierarchy

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 on page 5):

- 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 on page 5 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 on page 5, 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 on page 6 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"> <li>■ Add, delete and modify managers</li> <li>■ Add, delete, and modify subscriptions</li> <li>■ Modify subscribers, including the ability to add, delete, and modify substitutions for subscribers</li> <li>■ Manually activate and deactivate subscription sessions</li> </ul>
Subscription	<ul style="list-style-type: none"> <li>■ Add, delete, and modify subscriptions</li> <li>■ Manually activate and deactivate subscription sessions</li> </ul>
Substitution	Add, delete, and modify substitutions in subscribers and subscriptions
Activation	<ul style="list-style-type: none"> <li>■ Configure automatic activation of services</li> <li>■ Manually activate and deactivate subscription sessions</li> </ul>
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

# Subscriber Logins and Service Activation

- Login Events and Processes for the SRC Software on page 9
- Residential Subscriber Login and Processes on page 11
- PPP Subscriber Login and Service Activation on page 12
- DHCP Subscriber Login and Service Activation on page 15
- Static IP Subscribers on page 22
- Enterprise Subscriber Login Process on page 24
- Subscriptions and Activations on page 25
- Automatic Activation at Login on page 30

## Login Events and Processes for the SRC Software

---

Login interactions between the components differ according to the type of subscriber. Topics include:

- Overview of Login Events and Processes on page 9
- Login Events on page 9
- Summary of the Login Process on page 10

### **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 6 on page 10.

**Table 6: 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 JUNOS 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 JUNOS routers.)	Invokes subscriber classification script, creates subscriber session.
ADDR	A subscriber obtains an unauthenticated IP address from the router through DHCP. (Supported on JUNOS routers.)	Invokes subscriber classification script, creates subscriber session.
AUTHADDR	A subscriber obtains an authenticated IP address from the router through DHCP. (Supported on JUNOS 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 JUNOS 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.

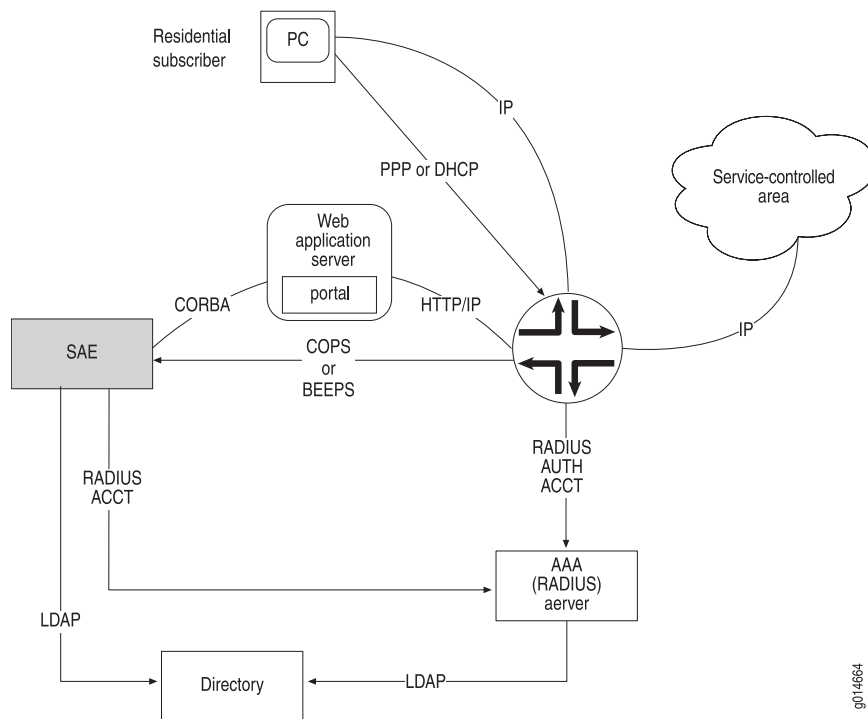
1. A login event occurs (see Table 6 on page 10) and triggers the login process.
2. In case of a portal login, the SAE invokes the authentication plug-ins to authenticate the request.
3. The SAE invokes the subscriber classification script and provides to the script details about the login event (for 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 2 on page 11 shows how residential subscribers connect to SRC components.

**Figure 2: 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.

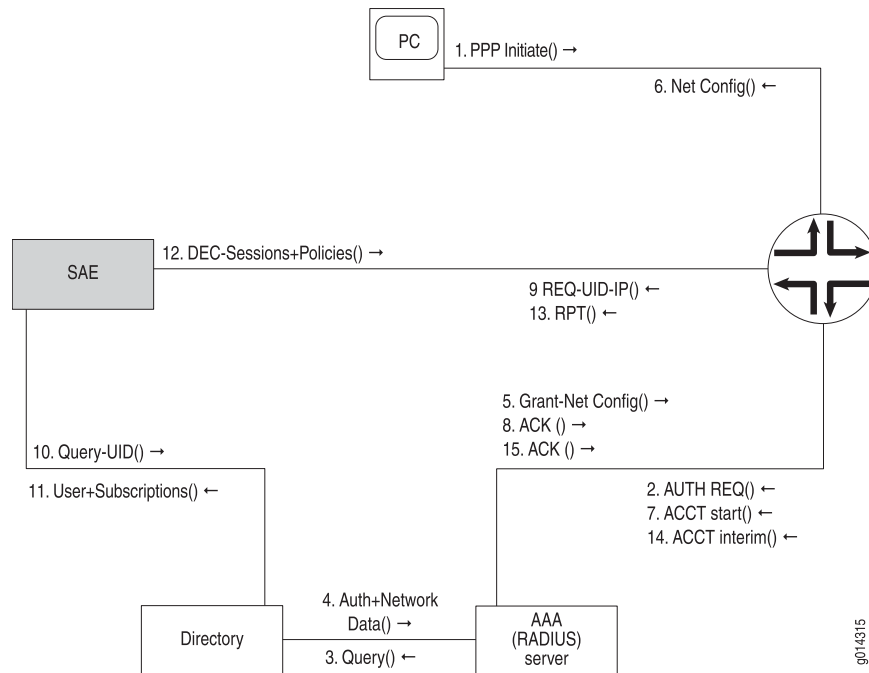
As a consequence, the Service Selection Portal (SSP) API allows creation of a Web application that:

- 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 3 on page 13 shows the interactions that take place during a PPP login.

**Figure 3: PPP Login Interactions**



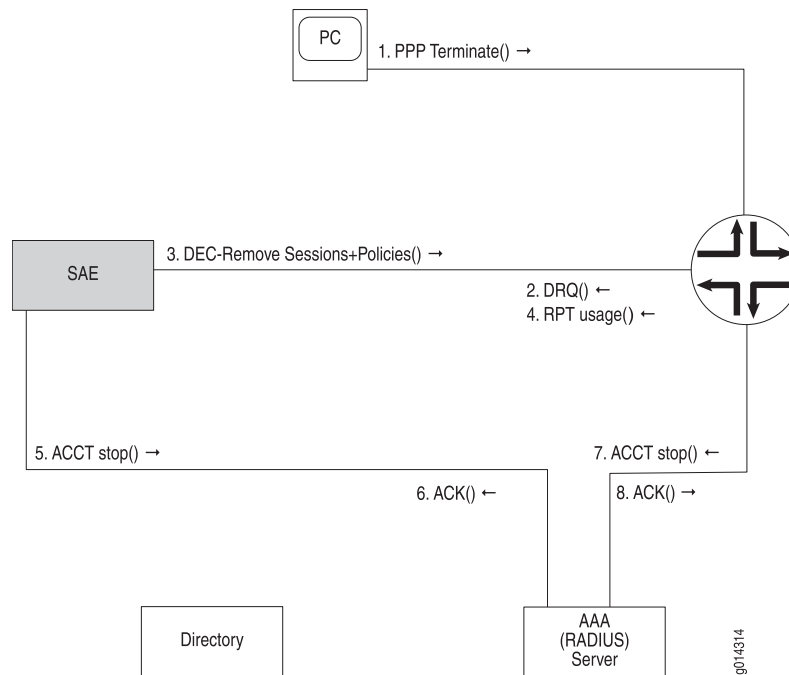
The login sequence is as follows:

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 4 on page 15 shows the interactions that take place when a subscriber logs out of a PPP session.

**Figure 4: 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 25.)
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.

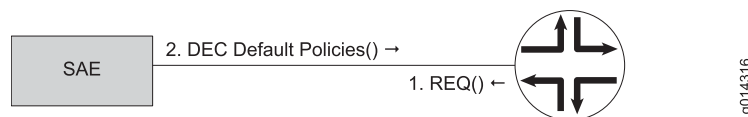
Like a subscriber with PPP access, a subscriber with DHCP access can have several accounts. The subscriber logs in to the different accounts at different times. This setup allows subscribers access to different sets of subscriptions. It supports a household in which different members share the same computer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

## 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 5 on page 16 shows this interaction.

**Figure 5: 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.

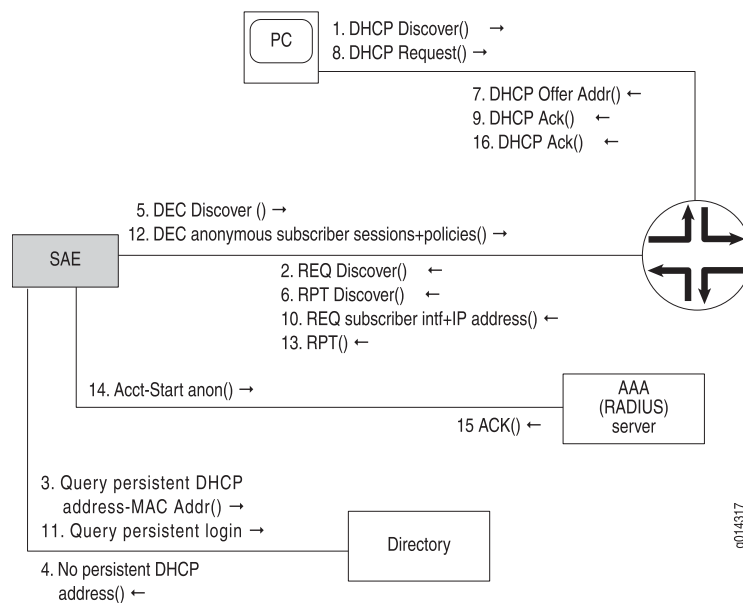
The first time a subscriber's network device starts, the router assigns an IP address to it. This address allows the subscriber access only to the SAE. The router provides this IP address for a short period of time called the lease time. After the lease time is over, the router provides a permanent IP 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 6 on page 17 shows the interactions that take place when a DHCP subscriber starts a network device.

**Figure 6: DHCP Subscriber Initial Login**



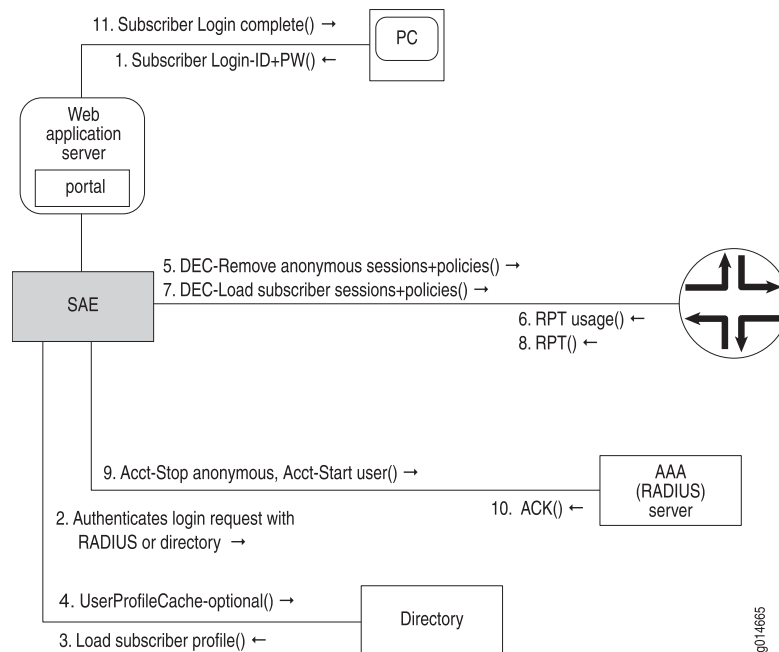
For this example, we assume that the directory responses show that there are no persistent subscriber logins. The startup sequence is as follows:

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.)
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 7 on page 19 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 7: DHCP Subscriber Login**

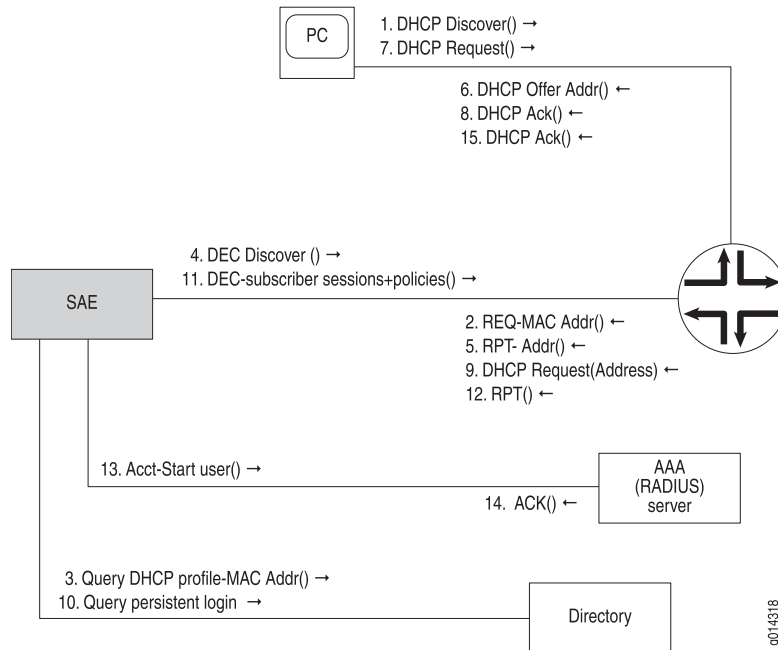
The sequence is as follows:

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 8 on page 20 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 8: Persistent DHCP Subscriber Login**



The login sequence is as follows:

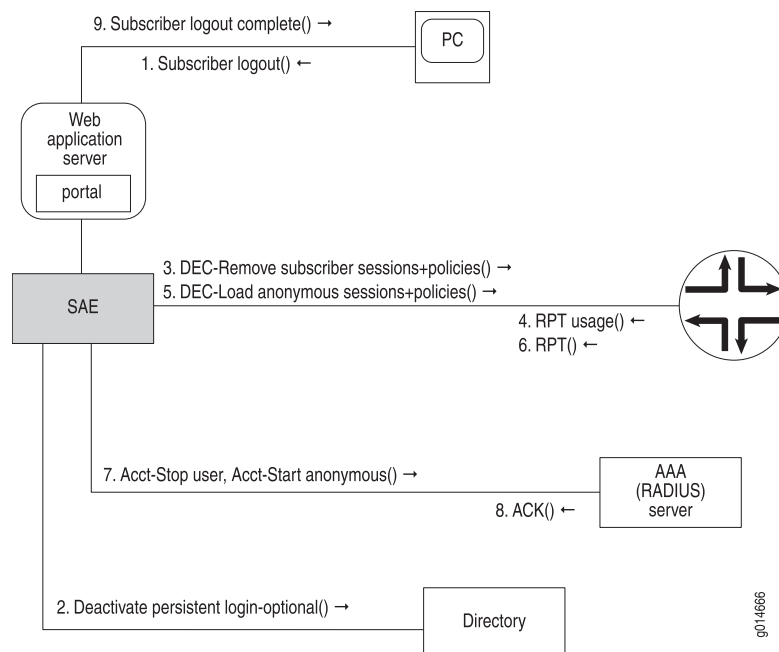
1. The DHCP client in the subscriber's network device sends a discover message to the router.
2. The router sends a COPS request (REQ) message to the SAE, informing the SAE that the router has received a DHCP discover request. The message includes the MAC address of the subscriber's network device and 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 9 on page 21 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 9: 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 10 on page 23.

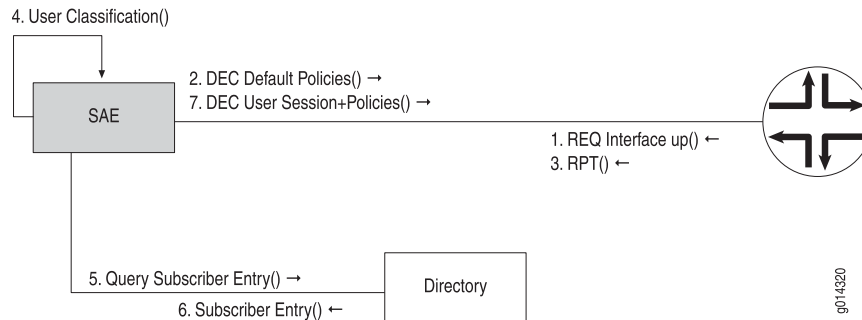
1. When the interface dedicated to the subscriber comes up, the router sends a COPS or BEEP request (REQ) message to the SAE. The SAE calls the interface classification script to determine whether the interface is being managed and which default policies are applied.
2. The SAE sends a decision (DEC) 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 10: Static IP Subscriber Login**



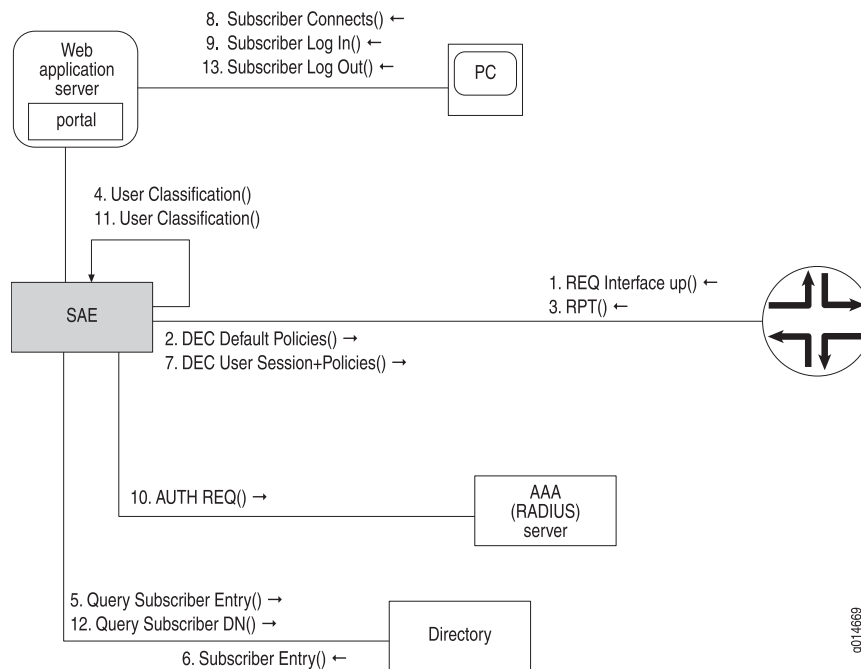
### **Subscriber IP Address Not Known**

See Figure 11 on page 24.

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 11: Subscriber IP Address Not Known**

## Enterprise Subscriber Login Process

Enterprise subscribers may connect through any access method. Any of the events described in Table 6 on page 10 can initiate an enterprise login.

## Interface Startup

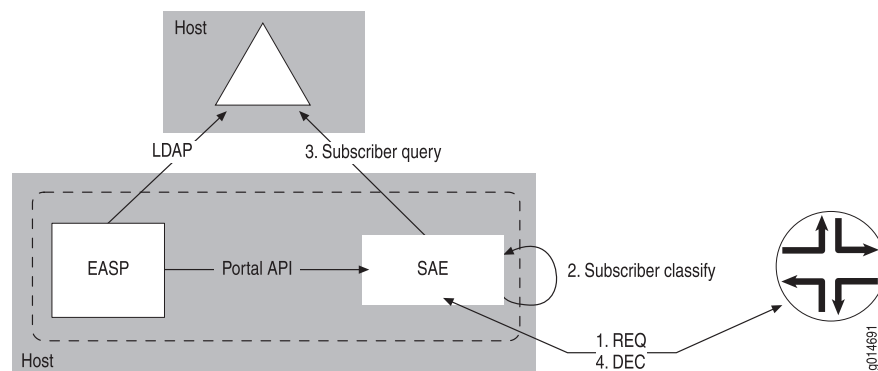
When a router interface comes up, the router sends a message to the SAE with information about that interface.

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 12 on page 25 shows the stages involved in activating an enterprise subscriber session.

**Figure 12: 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 13 on page 26 and Figure 14 on page 27). 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 13: Service 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

**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

**Virneo**

Copyright © 1999-2003 Juniper Networks

**Figure 14: 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

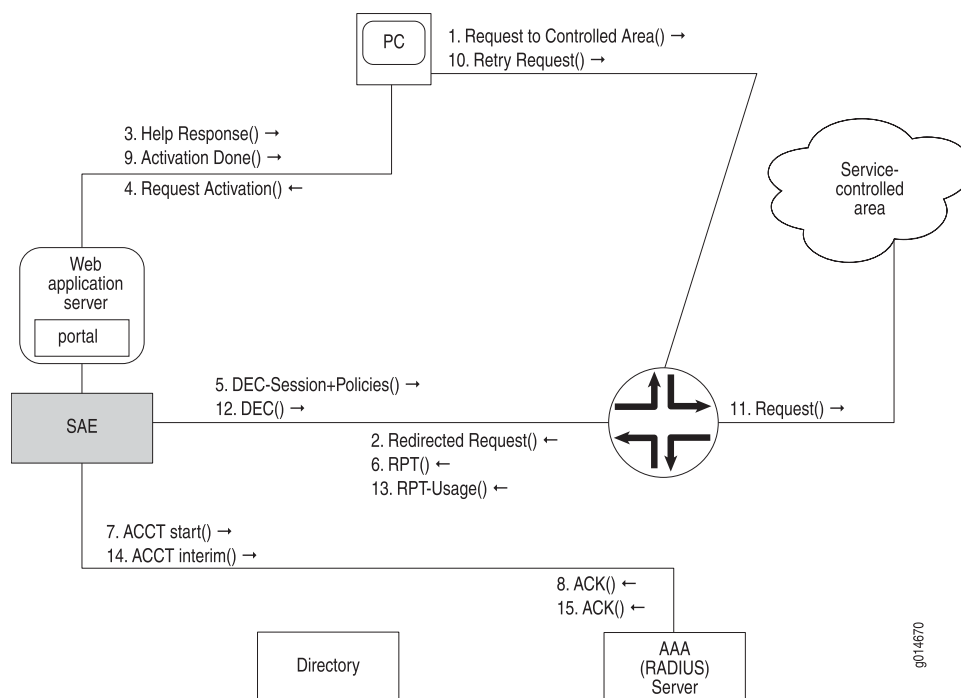
virneo

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. (

### 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 15 on page 28 shows the interactions among the components shown in Figure 2 on page 11 during the activation process. This scenario assumes that the subscriber has already logged in.

**Figure 15: 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.

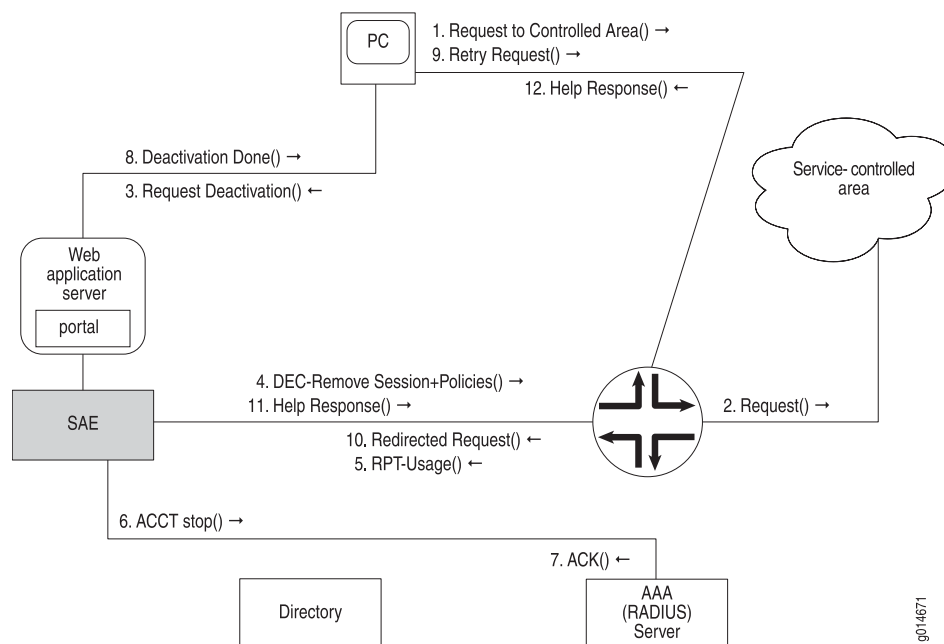
9. The SAE responds to the subscriber's activation request, indicating that the subscription is active.
10. The subscriber may now retry the request for access to the controlled resource.
11. This time, the request to the controlled resource matches the policy from the newly activated subscription, so 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 16 on page 29 shows the interactions among the components shown in Figure 2 on page 11 during the subscription deactivation process. This scenario assumes that the subscriber has already logged in.

**Figure 16: Subscription Deactivation**



g014671

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.

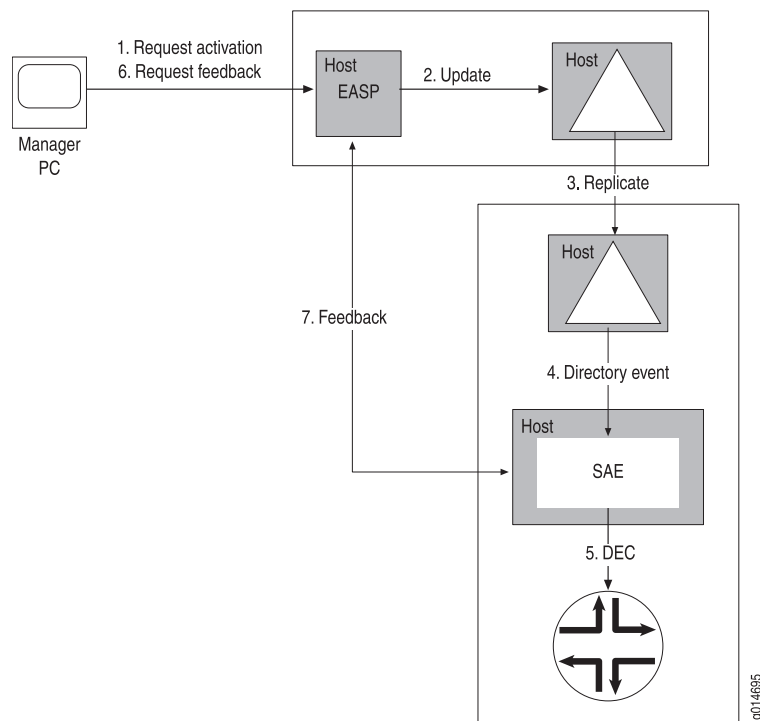
## Enterprise-Specific Remote Session Activation

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 17 on page 31 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 17: Remote Session Activation Sequence**





## Chapter 3

# Configuring Subscriber-Related Properties on the SAE (SRC CLI)

- Configuring the Length of Time MAC Addresses Remain in SAE Cache on page 33
- Identifying a Profile for Unauthenticated Subscribers on page 34
- Configuring Interim Accounting for Services and Subscribers on page 35
- Avoiding Overcharges for Sessions That Time Out on page 36
- Allowing Multiple Logins from the Same IP Address on page 36
- Authenticating Registered Username/Password Pairs on page 37
- Configuring Timers for Session Reactivation on page 38

### 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 4

# Classifying Interfaces and Subscribers (SRC CLI)

- Overview of Classification Scripts on page 39
- Overview of Configuring Classification Scripts on page 41
- Classifying Interfaces (SRC CLI) on page 45
- Example: Managing Interfaces for Premium and Basic PPP and DHCP Subscribers on page 49
- Example: Managing Specific Interfaces on page 50
- Example: Managing Interfaces by Using the Interface Description on page 50
- Classifying Subscribers (SRC CLI) on page 51
- Sending DHCP Options to the JUNOS Router on page 57
- Subscriber Classification Targets on page 58
- Example: Subscriber Classification Scripts for Static IP Subscriber on page 59
- Example: Subscriber Classification Scripts Using a Subscriber Group on page 60
- Example: Subscriber Classification Scripts for Enterprise Subscribers on page 60
- Example: Creating Router Interface Subscriber Session on page 61
- Example: Activating Services for a Group of Subscriber Sessions on page 61
- Classifying DHCP Subscribers (SRC CLI) on page 62
- Syntax for DHCP Classification Targets on page 65
- Selecting DHCP Parameters on page 65
- DHCP Options Supported on the SAE on page 66
- Creating DHCP Profiles (SRC CLI) on page 69

## 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 9 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 76 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 (SRC CLI)

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 47.

```
[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 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***

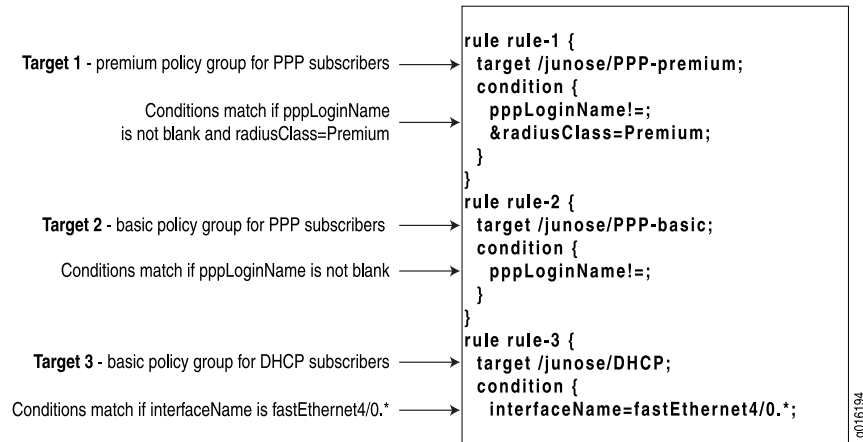
- Name of the virtual router or routing instance.
- Value—For JUNOS routers: name of the virtual router in the format  
vrname@hostname  
  
For JUNOS routing platforms: name of the routing instance
- Example—virtualRouterName = “ default@erx5”

### **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 (SRC CLI)

---

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.

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 58.

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 54.

```
[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 JUNOSe Router” on page 57.

### ***domainName***

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

### ***ifAlias***

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

### ***ifDesc***

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

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

### ***interfaceName***

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

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

For forwarding interface: interfaceName = “ FORWARDING\_INTERFACE ”

### ***loginName***

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

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

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

### ***loginType***

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

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

### ***macAddress***

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

### ***nasPortId***

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

### ***radiusClass***

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

### ***retailerDn***

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

### ***serviceBundle***

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

#### ***unauthenticatedUserDn***

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

#### ***userName***

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

#### ***virtualRouterName***

- Name of the virtual router or routing instance.
- Value—For JUNOSe routers: name of the virtual router in the format  
vrname@hostname  
  
For JUNOS routing platforms: name of the routing instance
- Example—virtualRouterName = “ default@e\_series5”

## **Sending DHCP Options to the JUNOSe Router**

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

The fields in Table 7 on page 57 are in the classification context of subscriber classification scripts.

**Table 7: DHCP Options in UserClassificationContext Field**

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

**Table 7: DHCP Options in UserClassificationContext Field** *(continued)*

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

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

```

dhcp.giAddr = " match"

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

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

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

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

## Subscriber Classification Targets

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

The syntax is:

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

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



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

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

With the exception of baseDN all the fields are optional.

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

### 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,retailername=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,retailername=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 (SRC CLI)

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 “Syntax for DHCP Classification Targets” on page 65.

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 63.

```
[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 “DHCP Options Supported on the SAE” on page 66 .

***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 JUNOS router

### ***virtualRouterName***

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

## **Syntax for DHCP Classification Targets**

---

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

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

- baseDN—DN of object where search starts.
- attributes—Comma-separated list of properties, in the format attribute = <-value->, that allow you to set specific attributes for directory objects that the script finds; see “DHCP Classification Conditions” on page 63.

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.



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

DHCP servers use DHCP options to configure DHCP clients. The DHCP local server in the JUNOSe router supports a subset of DHCP options. The SAE supports all DHCP options defined in *RFC 2132—DHCP Options and BOOTP Vendor Extensions (March 1997)* by name. It also supports other options, but you need to specify them by number and type. The DHCP options allow a flexible definition of parameters offered to DHCP subscribers. For example, they allow integration with cable modems or set-top boxes because you can configure options to control the boot sequence of these devices.

You can configure DHCP options in DHCP profiles and in DHCP classification scripts. Table 8 on page 67 lists the name, number, and type of all supported DHCP options. You can use these fields to configure DHCP options.

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

```
dhcp[12]

dhcp['host-name']
```

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

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

You can now write:

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

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

- Related Topics**
- Assigning DHCP Addresses to Subscribers on page 76
  - DHCP Subscriber Login and Service Activation on page 15

## DHCP Options Supported on the SAE

Table 8 on page 67 lists the DHCP options are available.

**Table 8: 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

**Table 8: DHCP Options Supported on the SAE** *(continued)*

Option Name	Option Number	Option Type
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
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

**Table 8: DHCP Options Supported on the SAE** *(continued)*

Option Name	Option Number	Option Type
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
nntp-server	71	ip-address
www-server	72	ip-address
finger-server	73	ip-address
irc-server	74	ip-address
streettalk-server	75	ip-address
streettalk-directory-assistance-server	76	ip-address

## Creating DHCP Profiles (SRC CLI)

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

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

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

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

- Assigning DHCP Addresses to Subscribers on page 76
- DHCP Subscriber Login and Service Activation on page 15

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 5

# Overview of Plug-Ins Included with the SAE

- How Internal Plug-Ins Work on page 73
- Types of Internal Plug-Ins on page 74
- Assigning DHCP Addresses to Subscribers on page 76
- Creating and Tracking Subscriber Sessions on page 77
- Activating and Tracking Service Sessions on page 79

## 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.



**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 Overview of 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.

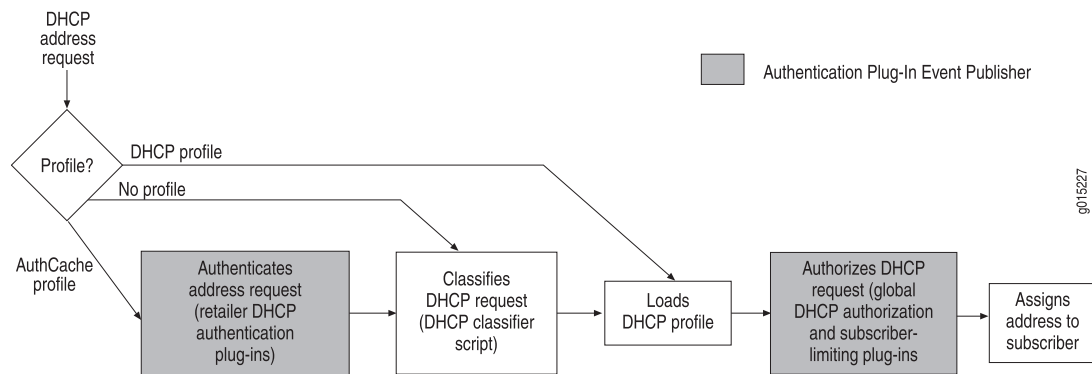
The main difference between flexible RADIUS plug-ins and custom RADIUS plug-ins is that custom plug-ins are designed to deliver better system performance than the flexible RADIUS plug-ins. To use a custom plug-in, you must provide a Java class that implements the SPI defined in the RADIUS client library. 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 “Overview of Flexible RADIUS Plug-Ins” on page 110.

## Assigning DHCP Addresses to Subscribers

Figure 18 on page 76 shows the process that the SAE uses to assign addresses to DHCP subscribers.

**Figure 18: 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 skips to authenticating the address request.
  - b. If the SAE does not find a profile, it skips to classifying the DHCP request.
  - c. If the SAE finds a DHCP profile, it skips to loading a DHCP profile.
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.

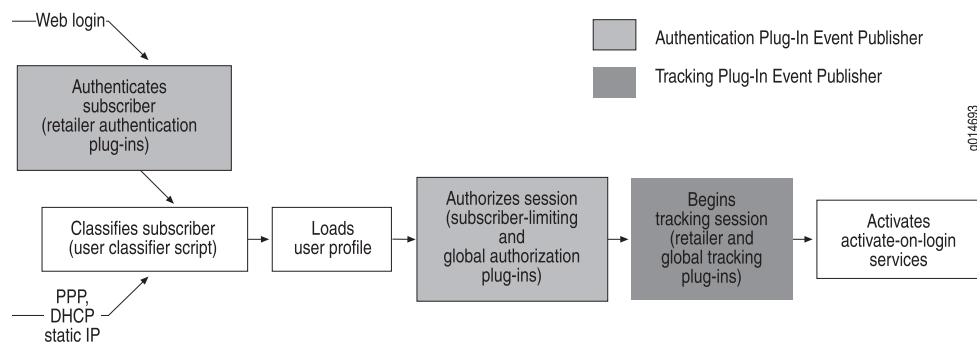
6. Assigns the address to the subscriber.

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 77.

## Creating and Tracking Subscriber Sessions

Figure 19 on page 77 shows the process that the SAE uses to create and begin tracking subscriber sessions.

**Figure 19: 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.

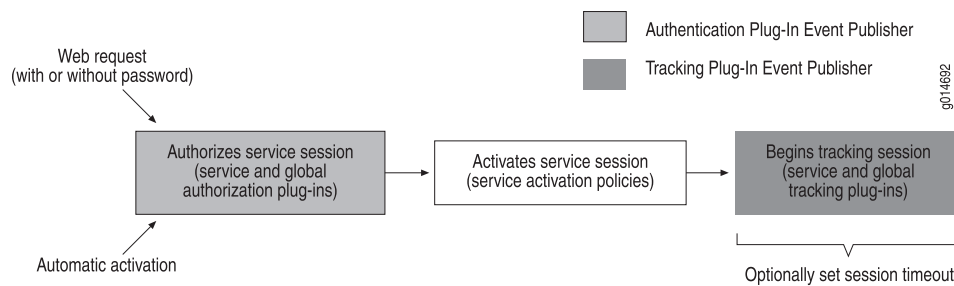
6. Activates services for the subscriber that are set up to activate on login.

## Activating and Tracking Service Sessions

Figure 20 on page 79 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 20: 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 6

# Configuring Internal, External, and Synchronization Plug-Ins (SRC CLI)

- Configuring Internal Plug-Ins on page 81
- Configuring the SAE for External Plug-Ins on page 82
- Configuring the State Synchronization Plug-In Interface on page 83

## Configuring Internal Plug-Ins

---

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

```
shared sae configuration plug-ins name name internal {  
    plug-in-class plug-in-class ;  
}  
shared sae configuration plug-ins name 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 name intnl internal
```

2. Configure the Java class name of the plug-in.

```
[edit shared sae configuration plug-ins name 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 name 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 name 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 SAE Plug-Ins .

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 name 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 name NicAgent external
```

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

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

4. (Optional) Verify your configuration.

```
[edit shared sae configuration plug-ins name 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 7

# Configuring Accounting and Authentication Plug-Ins (SRC CLI)

- Creating RADIUS Peers on page 85
- Types of Tracking Plug-Ins on page 87
- Configuring Tracking Plug-Ins on page 88
- Types of Authentication Plug-Ins on page 98
- Configuring Authentication Plug-Ins on page 99
- Configuring UDP Ports for RADIUS Plug-Ins on page 109
- Defining RADIUS Packets for Flexible RADIUS Plug-Ins on page 110
- Configuring Event Publishers on page 121

## 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 name name radius-accounting peer-group name
{
    server-address server-address ;
    server-port server-port ;
    secret secret ;
}
shared sae configuration plug-ins name name radius-authentication peer-group name
{
    server-address server-address ;
    server-port server-port ;
    secret secret ;
}
shared sae configuration plug-ins name name custom-radius-accounting peer-group
name {
    server-address server-address ;
    server-port server-port ;
}
```

```

    secret secret ;
}
shared sae configuration plug-ins name name custom-radius-authentication peer-group
name {
    server-address server-address ;
    server-port server-port ;
    secret secret ;
}
shared sae configuration plug-ins name name flex-radius-accounting peer-group
name {
    server-address server-address ;
    server-port server-port ;
    secret secret ;
}
shared sae configuration plug-ins name 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 name
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 name 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 name 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 name 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 name basicRadius
radius-accounting peer-group peer1]

```

```

user@host# show
server-address 10.10.1.1;
server-port 1812;
secret *****;

```

**Related Topics** ■ Creating Grouped Configurations for the SAE (SCR CLI)

## Types of Tracking Plug-Ins

You can configure the tracking plug-ins described in Table 9 on page 87.

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 9: Tracking Plug-Ins**

Plug-In	Description
Basic RADIUS accounting	<p>Sends accounting information to an external RADIUS accounting server or a group of redundant servers.</p> <p>Java class name—net.juniper.smgt.sae.plugin.RadiusTrackingPluginEventListener</p>
Custom RADIUS accounting	<p>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.</p> <p>Java class name—net.juniper.smgt.sae.plugin.CustomRadiusAccounting</p>
Flat file accounting	<p>Writes tracking information to a file in comma-separated format.</p> <p>Java class name—net.juniper.smgt.sae.plugin.FileTrackingPluginEventListener</p>
Flexible RADIUS accounting	<p>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.</p> <p>Java class name—net.juniper.smgt.sae.plugin.FlexibleRadiusTrackingPluginEventListener</p>

**Table 9: Tracking Plug-Ins** *(continued)*

Plug-In	Description
PCMM record-keeping server plug-in	Sends accounting information to an external PCMM record-keeping server (RKS). See <i>Configuring PCMM Record-Keeping Server Plug-Ins with SRC CLI</i> .  Java class name— <code>net.juniper.smgmt.sae.plugin.RksEventListener</code>
QoS profile tracking	Ensures that as a subscriber activates and deactivates services, the correct QoS profile is attached to the subscriber interface. See <i>Dynamically Managing QoS Profiles</i> .  Java class name— <code>net.juniper.smgmt.sae.plugin.qtp.QosProfileTrackingPluginEventListener</code>

## Configuring Tracking Plug-Ins

You can perform the following tasks to configure tracking plug-ins:

- Configuring Flat File Accounting Plug-Ins on page 88
- Configuring Headers for Flat File Accounting Plug-Ins on page 90
- Configuring Basic RADIUS Accounting Plug-Ins on page 91
- Configuring Flexible RADIUS Accounting Plug-Ins on page 93
- Configuring Custom RADIUS Accounting-Plug-Ins on page 95

## 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.

Use the following configuration statements to create flat-file accounting plug-in instances:

```
shared sae configuration plug-ins name name file-accounting {
    filename filename ;
    template template ;
    interval interval ;
    fields [(status | nas-id | host | router-name | interface-name | interface-alias |
        interface-descr | port-id | user-ip-address | login-name | accounting-id | auth-user-id
        | if-radius-class | if-session-id | service-name | radius-class | event-time | session-id
        | terminate-cause | session-time | in-octets | out-octets | in-packets | out-packets
        | nas-ip | user-mac-address | service-session-name | service-session-tag | user-type
        | user-radius-class | user-session-id | primary-user-name | subscription-name |
        login-id | if-index | event-time-millisecond | nas-port | operational | user-inet-address
        | nas-inet-address | router-type | interface-speed)...];
}
```

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 name  
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 name 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 name 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 name 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 name 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 name 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 ];
```

## Configuring Headers for Flat File Accounting Plug-Ins

When the SAE writes data to a flat file, it writes into the first line the headers that identify the attributes in the file. For example, in the following accounting file, the first line lists headers for all attribute fields in the file, and the following lines list the actual data in each field:

```
Accounting Status,NAS ID,SSP Host,Router Name,Interface Name,Interface
Alias,Interface Description,NAS port ID,User IP Address,User ID,User Accounting
ID,User Authentication ID,INTF Radius Class,INTF,SessionId, Service Name,Radius
Class,Timestamp,SessionId, Terminate Cause,Session Time,Input Octets,Output
Octets,Input Packets,Output Packets,NAS IP,User Mac address,Service Session
Name,Service Session Tag,User Session Type,User Session Radius Class,User
Session ID
start,SSP.uelmo,uelmo,default@erx7_ssp57,FastEthernet1/1.1,,IP1/1.1,default@erx7_ssp57
FastEthernet1/1:65535, 10.10.10.20,pebbles@virneo.net,,,erx fastEthernet
1/1:0001048619,Video-Gold,Video-Gold,Fri Jan 30 14:23:29 EDT 2004,
VideoGold:null:1064946209182, 0,0,0,0,0,0, 10.10.7.17,,,PPP,,
pebbles:1064946144841
```

You can assign your own names to the headers that appear in the file. To do so, define the header names in a template, and then set up file accounting plug-in instances to use the template. The default template, FileAccounting.std, defines header names for all possible attributes. You can use the default template or create your own templates.

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 (status | nas-id |
host | router-name | interface-name | interface-alias | interface-descr | port-id |
user-ip-address | login-name | accounting-id | auth-user-id | if-radius-class | if-session-id
| service-name | radius-class | event-time | session-id | terminate-cause | session-time
| in-octets | out-octets | in-packets | out-packets | nas-ip | user-mac-address |
service-session-name | service-session-tag | user-type | user-radius-class |
user-session-id | primary-user-name | subscription-name | login-id | if-index |
event-time-millisecond | nas-port | operational | user-inet-address | nas-inet-address
| router-type | interface-speed | service-bundle | user-dn | uid | domain | retailer-dn |
password | service-scope | session-timeout | downstream-bandwidth |
upstream-bandwidth | dhcp-packet | aggr-session-id | aggr-login-name | aggr-user-dn
| aggr-user-inet-address | aggr-accounting-id | aggr-auth-user-id) {
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.

```
[edit shared sae group west-region configuration file-accounting-template std]  
user@host# set attributes attribute 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 name name radius-accounting {  
    load-balancing-mode (failover | roundRobin);  
    fallback-timer fallback-timer ;  
    nas-ip (Ssplp | Erxp);  
    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 name  
basicRadius radius-accounting
```

2. Configure the mode for load-balancing RADIUS servers.

```
[edit shared sae group west-region configuration plug-ins name 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 name basicRadius
radius-accounting]
user@host# set fallback-timer fallback-timer
```

4. (Optional) Configure the value of the NAS-IP attribute.

```
[edit shared sae group west-region configuration plug-ins name 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 name 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 name 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 name 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 name 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 name 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 name 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 name basicRadius
 radius-accounting]
user@host# set default-peer default-peer
```

12. (Optional) Verify your configuration.

```
[edit shared sae group west-region configuration plug-ins name 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;
```

## 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 name name flex-radius-accounting {
  load-balancing-mode (failover | roundRobin);
  failback-timer failback-timer ;
  timeout timeout ;
  retry-interval retry-interval ;
  maximum-queue-length maximum-queue-length ;
  bind-address bind-address ;
  udp-port udp-port ;
  error-handling (0 | 1);
  default-peer default-peer ;
  template template ;
}
```

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 name  
flexRadiusAct flex-radius-accounting
```

2. Configure the mode for load-balancing RADIUS servers.

```
[edit shared sae group west-region configuration plug-ins name 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 name 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 name 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 name 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 name 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 name 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 name 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 name 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 name 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 name flexRadiusAct
flex-radius-accounting]
user@host# set template template
```

12. (Optional) Verify your configuration.

```
[edit shared sae group west-region configuration plug-ins name
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 *****;
}
```

## Configuring Custom RADIUS Accounting-Plug-Ins

The custom RADIUS accounting plug-ins provide the same functions as the flexible RADIUS accounting plug-ins, but are designed to deliver better system performance. To use a custom plug-in, you must provide a Java class that implements the service provider interface (SPI) defined in the RADIUS client library. Use this SPI to specify which fields and field values to include in RADIUS accounting packets. The RADIUS client library is part of the SAE core application programming interface (API).

See the documentation for the RADIUS client library in the SAE core API documentation on the Juniper Networks Web site at

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

For a sample implementation, see the `SDK+AppSupport+Demos+Samples.tar.gz` file on the Juniper Networks Web site at: <https://www.juniper.net/support/csc/swdist-erx/src.html>. The application is located the following directory:

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

Use the following configuration statements to set up custom RADIUS accounting plug-ins:

```
shared sae configuration plug-ins name name custom-radius-accounting {
  java-class-radius-packet-handler java-class-radius-packet-handler ;
  class-path-radius-packet-handler class-path-radius-packet-handler ;
  append-acct-status-type-attribute;
  require-mandatory-attributes;
  load-balancing-mode (failover | roundRobin);
  fallback-timer fallback-timer ;
  timeout timeout ;
  retry-interval retry-interval ;
  maximum-queue-length maximum-queue-length ;
  bind-address bind-address ;
  udp-port udp-port ;
  default-peer default-peer ;
}
```

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 name  
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 name 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 name 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 name 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 name 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 name 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 name 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 name 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 name 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 name 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 name 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 name 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 name 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 name
 customRadiusAct custom-radius-accounting]
user@host# show
java-class-radius-packet-handler
net.juniper.smgmt.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;
```

## Types of Authentication Plug-Ins

This section shows how to configure the authentication plug-ins described in Table 10 on page 98. 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 10: 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.smgmt.sae.plugin.RadiusAuthPluginEventListener

**Table 10: Authentication Plug-Ins** *(continued)*

Plug-In	Description
Custom RADIUS authentication	<p>Provides customized functions that can also be found in the flexible RADIUS authentication plug-ins. Custom plug-ins are internal plug-ins that are designed to deliver better system performance than the flexible RADIUS plug-ins. You can extend this plug-in by using the RADIUS client library.</p> <p>Java class name—<code>net.juniper.smgt.sae.plugin.CustomRadiusAuth</code></p>
Flexible RADIUS authentication	<p>Performs the same functions as the basic RADIUS authentication plug-in, but also lets you customize RADIUS authentication packets that the SAE sends to RADIUS servers. You can specify which fields are included in RADIUS authentication packets and what information is contained in the fields.</p> <p>Java class name—<code>net.juniper.smgt.sae.plugin.FlexibleRadiusAuthPluginEventListener</code></p>
LDAP authentication	<p>Performs authentication against different directories using different authentication methods. There are two LDAP authentication plug-ins: one authenticates subscribers, and the second authenticates SRC administrators so that they can access the SAE Web Admin application.</p> <p>Java class name of the subscriber authentication plug-in—<code>net.juniper.smgt.sae.plugin.LdapAuthenticator</code></p> <p>Java class name of the administrator authentication plug-in—<code>net.juniper.smgt.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.smgt.sae.plugin.LimitNumSubscriberPerIntfAuthPluginListener</code></p>

## Configuring Authentication Plug-Ins

You can perform the following tasks to configure authentication plug-ins:

1. Limiting Subscribers on Router Interfaces on page 99
2. Configuring Basic RADIUS Authentication Plug-Ins on page 100
3. Configuring Flexible RADIUS Authentication Plug-Ins on page 102
4. Configuring Custom RADIUS Authentication Plug-Ins on page 104
5. Configuring LDAP Authentication Plug-Ins on page 107

### 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 name 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 name  
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 name 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 name 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 name name radius-authentication {
    load-balancing-mode (failover | roundRobin);
    fallback-timer fallback-timer ;
    nas-ip (Ssfp | Exlp);
    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 name RadiusAuth radius-authentication
```

2. Configure the mode for load-balancing RADIUS servers.

```
[edit shared sae group west-region configuration plug-ins name 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 name 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 name 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 name 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 name 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 name 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 name 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 name RadiusAuth
 radius-authentication]
user@host# set default-peer default-peer
```

10. (Optional) Verify your configuration.

```
[edit shared sae group west-region configuration plug-ins name RadiusAuth
 radius-authentication]
user@host# show
load-balancing-mode failover;
failback-timer -1;
retry-interval 3000;
maximum-queue-length 10000;
default-peer peer1;
```

## 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 name name flex-radius-authentication {
  load-balancing-mode (failover | roundRobin);
  failback-timer failback-timer ;
  timeout timeout ;
  retry-interval retry-interval ;
  maximum-queue-length maximum-queue-length ;
  bind-address bind-address ;
  udp-port udp-port ;
  error-handling (0 | 1);
  default-peer default-peer;
  template template ;
}
```

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 name
flexRadiusAuth flex-radius-authentication
```

2. Configure the mode for load-balancing RADIUS servers.

```
[edit shared sae group west-region configuration plug-ins name 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 name 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 name 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 name 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 name 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 name 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 name 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 name 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 name 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 name flexRadiusAct
flex-radius-accounting]
user@host# set template template
```

12. (Optional) Verify your configuration.

```
[edit shared sae group west-region configuration plug-ins name
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 *****;
}
```

## 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 SAE core API documentation on the Juniper Networks Web site at

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

For a sample implementation, see in the `SDK+AppSupport+Demos+Samples.tar.gz` file on the Juniper Networks Web site at:

<https://www.juniper.net/support/csc/swdist-erx/src.html> The application is located the following directory:

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

Use the following configuration statements to set up custom RADIUS authentication plug-ins:

```
shared sae configuration plug-ins name name custom-radius-authentication {
  java-class-radius-packet-handler java-class-radius-packet-handler ;
  class-path-radius-packet-handler class-path-radius-packet-handler ;
  require-mandatory-attributes;
  load-balancing-mode (failover | roundRobin);
  fallback-timer fallback-timer ;
  timeout timeout ;
  retry-interval retry-interval ;
  maximum-queue-length maximum-queue-length ;
  bind-address bind-address ;
  udp-port udp-port ;
  default-peer default-peer;
}
```

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 name  
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 name 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 name 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 name 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 name 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 name 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 name 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 name 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 name 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 name 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 name 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 name 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 name customRadiusAuth
custom-radius-authorization]
```

```
user@host# show
```

```

java-class-radius-packet-handler
net.juniper.smgmt.radius.RadiusPacketHandlerImpl;
require-mandatory-attributes;
load-balancing-mode failover;
failback-timer -1;
timeout 15000;
retry-interval 3000;
maximum-queue-length 10000;
default-peer peer4;

```

## Configuring LDAP Authentication Plug-Ins

Use the following configuration statements to configure LDAP authentication plug-ins:

```

shared sae configuration plug-ins name name ldap-authentication {
  method (search | bind);
  server server ;
  bind-dn bind-dn ;
  bind-password bind-password ;
  search-filter search-filter ;
  (ldaps);
  search-base-dn search-base-dn ;
  name-attribute name-attribute ;
  password-attribute password-attribute ;
  service-bundle-attribute service-bundle-attribute ;
  session-volume-quota session-volume-quota ;
  timeout timeout ;
}

```

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 name
ldapAuth ldap-authentication

```

2. Configure the LDAP authentication method that the SAE uses.

```

[edit shared sae group west-region configuration plug-ins name 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 name 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 name 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 name 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 name 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 name 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 name 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 name 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 name 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 name 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 name 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 name 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 name ldapAuth
  ldap-authentication]
user@host# show
method search;
search-filter (objectClass=umcSubscriber);
name-attribute uniqueId;
timeout 5000;
```

## 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.

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

---

1. Overview of Flexible RADIUS Plug-Ins on page 110
2. Defining the Values of RADIUS Attributes on page 113
3. Configuring a RADIUS Packet Template on page 116
4. Using Flexible RADIUS Packet Definitions on page 118

### Overview of Flexible RADIUS Plug-Ins

Flexible RADIUS accounting and authentication plug-ins allow you to define the content of RADIUS packets that the SAE sends to RADIUS servers. You can specify which attributes are included in different types of RADIUS packets (for example, session start or stop requests, or accounting on or off requests). You can also specify what information is contained in the attribute fields.

A RADIUS attribute configuration consists of RADIUS attribute instances. Each instance defines attributes for a specific type of packet—For example, start requests or accounting off requests.

Within each attribute instance, you define individual RADIUS attributes. The following is a RADIUS attribute instance for authentication requests:

```
radius-attributes auth {
  attributes {
    User-Name loginId;
    User-Password password;
    NAS-Identifier localNasId;
    NAS-IP-Address localNasIp;
    NAS-Port nasPort;
  }
}
```

Each RADIUS packet template can consist of multiple RADIUS attribute instances.

### Using Default RADIUS Templates

The SRC software comes with two default templates:

- **stdAcct**—Defines RADIUS accounting packets and is used in the default RADIUS flexible accounting plug-in instance `flexRadiusAcct`.

- **stdAuth**—Defines RADIUS authentication packets and is used in the default RADIUS flexible authentication plug-in instance `flexRadiusAuth`.

## Naming RADIUS Attribute Instances

Attribute instances define attributes for a specific type of RADIUS packet. The name that you assign to an attribute instance specifies the type of packet to which the attribute definition is applied. Table 11 on page 111 lists the available packet types.

**Table 11: 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
dhcpresp	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
svcresp	Any service authorization response
svcstart	Service Session Start requests
svcstop	Service Session Stop or Interim requests
useracct	Subscriber Session Start, Stop, or Interim requests
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](http://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 dhcresp {
  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 12 on page 113) 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 12: 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 7 on page 57 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

**Table 12: Standard Values for RADIUS Attributes** *(continued)*

Value	Type of Plug-In	Comments
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 JUNOS 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.

**Table 12: Standard Values for RADIUS Attributes** (continued)

Value	Type of Plug-In	Comments
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"> <li>1. Service definition (lowest)</li> <li>2. Authorization</li> <li>3. API call (highest)</li> </ol> <p><b>NOTE:</b> 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

**Table 12: Standard Values for RADIUS Attributes** *(continued)*

Value	Type of Plug-In	Comments
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 name name flex-radius-accounting
  radius-packet-definition name ...
shared sae configuration plug-ins name name flex-radius-accounting
  radius-packet-definition name attributes name {
    value ;
  }
shared sae configuration plug-ins name name flex-radius-authentication
  radius-packet-definition name ...
shared sae configuration plug-ins name 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 11 on page 111, 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";
    }
}
}

```

## Using Flexible RADIUS Packet Definitions

This topic shows some of the ways you can use flexible RADIUS packet definitions. Remember that the name of the attribute instance determines the type of RADIUS packet in which the packet definition is used.

- To use the Challenge Handshake Authentication Protocol (CHAP) to authenticate subscribers, include the Chap-Password and optionally the Chap-Challenge attributes in authentication requests. (We recommend that you use Chap-Password only. Use Chap-Challenge only if required.) To use a CHAP password, include the following in attribute instance auth:

Chap-Password = password

- To cause the Calling-Station-Id attribute to use the subscriber's MAC address:

Calling-Station-Id = userMacAddress

- To set the value to prefix N followed by the service name and the prefix S followed by the service session name:

'N'+serviceName, 'S'+serviceSessionName

- To construct a value for the Nas-Port-Id attribute by concatenating the value of routerName, a space, and the Nas-Port-ID on the router:

Nas-Port-Id=routerName + " " + portId

For example, the constructed value might be:

default@phoenix FastEthernet 4/2

- The following example sets the User-Name attribute as follows:
- Sets the value to accountingId, or
- If accountingId is empty, sets the value to loginName, or
- If loginName is also empty, sets the value to NN

User-Name = accountingId or loginName or " NN"

- To extract the lower 32 bits of the 64-bit inOctet counter:

Acct-Input-Octets = lowWord(inOctets)

- To set the counter fields in the RADIUS packet to the appropriate 32-bit values:

Acct-Input-Octets = lowWord(inOctets)  
Acct-Output-Octets = lowWord(outOctets)  
Acct-Input-Packets = inPackets  
Acct-Output-Packets = outPackets

Acct-Input-Gigawords = highWord(inOctets)  
Acct-Output-Gigawords = highWord(outOctets)

- The inOctets and outOctets are 64-bit values and must be split into lower 32-bit (Acct-\*-Octets) and upper 32-bit (Acct-\*-Gigawords) values.
- The inPacket and outPacket counters are 32-bit values and can be assigned directly.

## Setting Values in Authentication Response Packets

You can use some special attribute values to set values in authentication response packets. For example:

- setRadiusClass(ATTR)
- setSessionTimeout(ATTR)
- setSessionVolumeQuota(ATTR)

Table 12 on page 113 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

---

- Special Types of Event Publishers on page 121
- Configuring Global and Default Retailer Event Publishers on page 122

### Special Types of Event Publishers

The SCR CLI lets you configure global and default retailer event publishers. You can also configure service-specific event publishers, retailer-specific event publishers, and virtual router-specific event publishers.

#### 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.

#### 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.

#### 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.

#### Related Topics

- Adding Retailers (SRC CLI) on page 127
- Adding JUNOSe Routers and Virtual Routers with the CLI

■ *SRC-PE Network Guide*

## 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 Topics** ■ Configuring an SAE Group



## Chapter 8

# Configuring Subscribers and Subscriptions (SRC CLI)

- Overview of Configuring Subscribers and Subscriptions on page 125
- Enabling the Subscriber and Subscription Configuration on the SRC CLI on page 126
- Adding Subscribers (SRC CLI) on page 126
- Adding Retailers (SRC CLI) on page 127
- Configuring Administrative Information for Retailers (SRC CLI) on page 128
- Adding Subscriber Folders (SRC CLI) on page 129
- Adding Residential Subscribers (SRC CLI) on page 130
- Configuring Administrative Information for Residential Subscribers (SRC CLI) on page 133
- Adding Enterprises (SRC CLI) on page 134
- Configuring Administrative Information for Enterprise Subscribers (SRC CLI) on page 135
- Adding Sites (SRC CLI) on page 136
- Adding Devices as Subscribers (SRC CLI) on page 137
- Adding Managers (SRC CLI) on page 139
- Configuring Subscriptions (SRC CLI) on page 141
- Configuring Accesses (SRC CLI) on page 143

### Overview of Configuring Subscribers and Subscriptions

---

- Specifying the Activation Order for Subscriptions on page 125
- Inheritance of Properties and Subscriptions on page 126

### *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 editor
```

If you are using multiple C-series Controllers, we recommend that you enable the policy, service, and subscriber editor on only one C-series Controller on your network. 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 (SRC CLI)**

---

The tasks to configure subscribers are:

- Adding Retailers (SRC CLI) on page 127
- Configuring Administrative Information for Retailers (SRC CLI) on page 128
- Adding Subscriber Folders (SRC CLI) on page 129

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 (SRC CLI) on page 130
- Adding Enterprises (SRC CLI) on page 134
- Configuring Administrative Information for Enterprise Subscribers (SRC CLI) on page 135

- Adding Sites (SRC CLI) on page 136
- Adding Devices as Subscribers (SRC CLI) on page 137

After you add subscribers, you can add managers and configure subscriptions.

- Related Topics**
- Adding Managers (SRC CLI) on page 139
  - Configuring Subscriptions (SRC CLI) on page 141

## Adding Retailers (SRC CLI)

---

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 (SRC CLI)

---

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 (SRC CLI)

---

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 (SRC CLI)

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 (SRC CLI)

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 (SRC CLI)

---

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 JUNOS.
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 (SRC CLI)” on page 143.)

## Configuring Administrative Information for Enterprise Subscribers (SRC CLI)

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 (SRC CLI)

---

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 (SRC CLI)” on page 143.)

## Adding Devices as Subscribers (SRC CLI)

---

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 (SRC CLI)

---

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 (SRC CLI)

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 Overview of Services for the SRC Software.

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 Overview of Service Schedules.

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.

```
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;
```

## Configuring Accesses (SRC CLI)

---

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**

# **Redirecting Subscriber Traffic Through Redirect Server**

- Redirecting Subscriber Traffic on page 149
- Configuring Traffic Redirection (SRC CLI) on page 153



## Chapter 9

# Redirecting Subscriber Traffic

- Overview of Traffic Redirection on page 149
- Redirect Server Redundancy on page 151

### 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.

### 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.

## ***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.

### **Related Topics**

- Redirect Server Redundancy on page 151
- Configuration Statements for the Redirect Server (SRC CLI) on page 153
- Configuring the Redirect Server (SRC CLI) on page 155
- Configuring the Redirect Server (C-Web Interface)

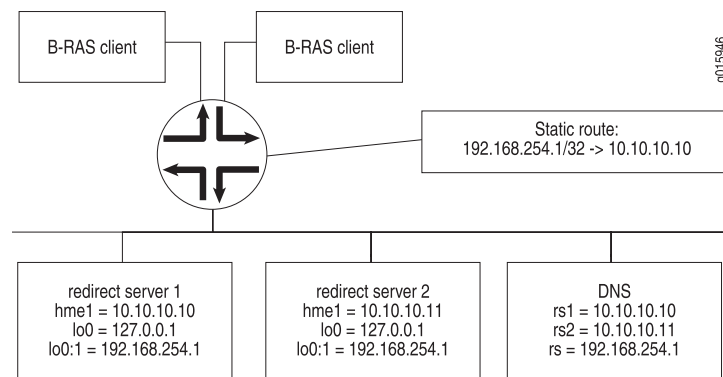
## **Redirect Server Redundancy**

---

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 21 on page 152 shows a configuration in which two redirect servers use the same virtual IP address, 192.168.254.1.

**Figure 21: Failover of a Redirect Server**

- Related Topics**
- Overview of Traffic Redirection on page 149
  - Before You Configure Redundancy for a Redirect Server on page 164
  - Configuring a Redundant Redirect Server (SRC CLI) on page 164
  - Configuring a Redundant Redirect Server (C-Web Interface)

## Chapter 10

# Configuring Traffic Redirection (SRC CLI)

- Configuration Statements for the Redirect Server (SRC CLI) on page 153
- Before You Configure the Redirect Server on a C-Series Controller on page 154
- Configuring the Redirect Server (SRC CLI) on page 155
- Configuring General Properties for the Redirect Server (SRC CLI) on page 156
- Configuring a Connection Between the Redirect Server and the Directory (SRC CLI) on page 157
- Defining Traffic to Transmit to the Redirect Server (SRC CLI) on page 158
- Changing the Number of Requests That the Redirect Server Accepts (SRC CLI) on page 159
- Specifying Extensions for Files That the Redirect Server Accepts (SRC CLI) on page 160
- Verifying Configuration for the Redirect Server (SRC CLI) on page 161
- Enabling the Redirect Server on page 161
- Configuring the DNS Server for the Redirect Server (SRC CLI) on page 162
- Configuring the Redirect Server to Support HTTP Proxies (SRC CLI) on page 163
- Before You Configure Redundancy for a Redirect Server on page 164
- Configuring a Redundant Redirect Server (SRC CLI) on page 164
- Configuring Logging for the Redirect Server on page 166
- Changing the Configuration for the Redirect Server on page 166
- Assessing Load for Redirect Server (C-Web Interface) on page 166

## Configuration Statements for the Redirect Server (SRC CLI)

---

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;
}

```

- Related Topics**
- Overview of Traffic Redirection on page 149
  - Configuring the Redirect Server (SRC CLI) on page 155
  - For detailed information about each configuration statement, see the *SRC-PE CLI Command Reference*.

## Before You Configure the Redirect Server on a C-Series Controller

---

Before you configure the redirect server on a C-series Controller:

- Configure the connection between the redirect server and the JUNOSe router by configuring policies on the C-series controller:
  - Configure and enable the HTTP local server on the JUNOSe router
  - On the C-series Controller, configure a policy that includes the following policy actions to define which traffic to send to the redirect server:
    - An exception action to specify that an HTTP application receive traffic.
    - An http redirect policy action to specify the URL to receive packets identified in the exception application action.



**NOTE:** Alternatively, if the distance between the JUNOSe routers and the C-series Controller is one hop away, you can configure a next-hop policy on the JUNOSe router that specifies a destination address that is the virtual IP address of the active redirect server rather than configuring an SRC policy.

- If you plan to configure a redundant redirect server, make sure that you are familiar with the network configuration required.

#### Related Topics

- Before You Configure Redundancy for a Redirect Server on page 164
- Redirect Server Redundancy on page 151
- Overview of Traffic Redirection on page 149
- Configuring the Redirect Server (SRC CLI) on page 155
- Configuring the Redirect Server (C-Web Interface)

## Configuring the Redirect Server (SRC CLI)

The redirect server on a C-series Controller 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 (SRC CLI)” on page 156 .

2. Configure a connection from the redirect server to the directory.

See “Configuring a Connection Between the Redirect Server and the Directory (SRC CLI)” on page 157 .

3. (Optional) Define traffic to be forwarded to the redirect server. In most cases you can accept the default values—traffic destined for port 80 (Web requests) and forwarded from all interface on a C-series Controller.

See “Defining Traffic to Transmit to the Redirect Server (SRC CLI)” on page 158 .

4. (Optional) Configure the number of requests that the redirect server accepts.

See “Changing the Number of Requests That the Redirect Server Accepts (SRC CLI)” on page 159 .

5. (Optional) Configure the types of files for which the redirect server accepts requests.

See “Specifying Extensions for Files That the Redirect Server Accepts (SRC CLI)” on page 160 .

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 (SRC CLI)” on page 162.

7. (Optional) Configure support for HTTP proxies.

See Verifying Configuration for the Redirect Server (SRC CLI) on page 161.

8. (Optional) Configure a redundant redirect server.

See “Configuring a Redundant Redirect Server (SRC CLI)” on page 164.

9. Enable the redirect server.

See “Enabling the Redirect Server” on page 161.

- Related Topics**
- Overview of Traffic Redirection on page 149
  - Redirect Server Redundancy on page 151
  - Configuration Statements for the Redirect Server (SRC CLI) on page 153

## Configuring General Properties for the Redirect Server (SRC CLI)

---

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.

- Related Topics**
- Overview of Traffic Redirection on page 149
  - Configuring the Redirect Server (SRC CLI) on page 155
  - Verifying Configuration for the Redirect Server (SRC CLI) on page 161

## Configuring a Connection Between the Redirect Server and the Directory (SRC CLI)

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
```

- Related Topics**
- Overview of Traffic Redirection on page 149
  - Configuring the Redirect Server (SRC CLI) on page 155
  - Verifying Configuration for the Redirect Server (SRC CLI) on page 161

## Defining Traffic to Transmit to the Redirect Server (SRC CLI)

---

You can define traffic to be forwarded to the redirect server by identifying the destination port number (typically, port 80 for Web requests) for packets and the physical interface on a C-series Controller from which subscriber traffic is forwarded to the redirect server. In most cases you can accept the default values for configuration for IP redirection. If you do not specify an interface, traffic is accepted on all interfaces.

Use the following configuration statements to define traffic to transmit to the 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 Controller.

```
[edit redirect-server ip-redirect]
user@host# set interface interface
```

If you do not specify an interface, the C-series Controller 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# set port port
```

- Related Topics**
- Overview of Traffic Redirection on page 149
  - Configuring the Redirect Server (SRC CLI) on page 155
  - Verifying Configuration for the Redirect Server (SRC CLI) on page 161

## Changing the Number of Requests That the Redirect Server Accepts (SRC CLI)

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.

- Related Topics**
- Overview of Traffic Redirection on page 149
  - Configuring the Redirect Server (SRC CLI) on page 155
  - Verifying Configuration for the Redirect Server (SRC CLI) on page 161

## Specifying Extensions for Files That the Redirect Server Accepts (SRC CLI)

---

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, .shtm, .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 you configured . 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
```

- Related Topics**
- Overview of Traffic Redirection on page 149
  - Configuring the Redirect Server (SRC CLI) on page 155
  - Verifying Configuration for the Redirect Server (SRC CLI) on page 161

## Verifying Configuration for the Redirect Server (SRC CLI)

---

**Purpose** Verify the configuration for the redirect server.

**Action** 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;
```

- Related Topics**
- Overview of Traffic Redirection on page 149
  - Configuring the Redirect Server (SRC CLI) on page 155
  - Viewing Statistics for the Redirect Server (SRC CLI)
  - Viewing Statistics for Filtered Traffic

## Enabling the Redirect Server

---

To enable the redirect server:

```
user@host> enable component redir
```

- Related Topics**
- Overview of Traffic Redirection on page 149
  - Configuring the Redirect Server (SRC CLI) on page 155

## Configuring the DNS Server for the Redirect Server (SRC CLI)

---

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.

- 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
```

- Related Topics**
- Overview of Traffic Redirection on page 149
  - Configuring the Redirect Server (SRC CLI) on page 155

## Configuring the Redirect Server to Support HTTP Proxies (SRC CLI)

---

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.

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:

- From configuration mode, access the configuration statement that configures the redirect server.

```
user@host# edit redirect-server
```

- Enable HTTP proxy support.

```
[edit redirect-server]
user@host# set proxy-support
```

- 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.

- Related Topics**
- Overview of Traffic Redirection on page 149

- Configuring the Redirect Server (SRC CLI) on page 155
- For information about configuring the DNS server included with the SRC software, see Configuring the DNS Server for the Redirect Server (SRC CLI) on page 162.

## Before You Configure Redundancy for a Redirect Server

---

If you plan to use a redundant configuration for the redirect server, ensure that:

- If you use a next-hop address for policies that capture web traffic and send it to the redirect server, that the virtual IP address to be used is also the next-hop address.
- 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 JUNOSe router, the hosts on which the redirect server runs must be included.

### Related Topics

- Overview of Traffic Redirection on page 149
- Redirect Server Redundancy on page 151
- Configuring a Redundant Redirect Server (SRC CLI) on page 164
- Configuring a Redundant Redirect Server (C-Web Interface)

## Configuring a Redundant Redirect Server (SRC CLI)

---

Although configuration of a redundant redirect server is optional, we recommend that you configure redundancy to maintain high availability for the server.

Before you configure the redirect server, review configuration prerequisites. See “Before You Configure Redundancy for a Redirect Server” on page 164.

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 ...
```

- Related Topics**
- Overview of Traffic Redirection on page 149
  - Redirect Server Redundancy on page 151
  - Configuring the Redirect Server (SRC CLI) on page 155
  - Configuring the Virtual IP Address (SCR CLI)
  - Configuring a Redundant Redirect Server (C-Web Interface)

## Configuring Logging for the Redirect Server

---

The redirect server logs incoming HTTP requests through syslog with a priority of INFO and log facility of LOCAL7.

- Related Topics**
- Configuring a Component to Store Log Messages in a File with SRC CLI
  - Configuring System Logging with SRC CLI

## Changing the Configuration for the Redirect Server

---

When you change the configuration for the redirect server and commit that configuration, the redirect server is automatically restarted.

- Related Topics**
- Configuring the Redirect Server (SRC CLI) on page 155

## Assessing Load for Redirect Server (C-Web Interface)

---

**Purpose** View the number of requests sent to the redirect server, and whether the requests reach the configured limit for the server and for server users. You can then use this information to fine-tune the properties for redirect server.

- Action**
1. Click **Monitor > Redirect Server > Statistics**.
- The Redirect Server Statistics pane appears.
2. From the Output Style list, select an output style as described in the Help text in the main pane.
  3. Click **OK**. The Redirect Server pane displays the following statistics:
    - Uptime
    - Accepted requests
    - Rejected requests
    - Number of user-limit leaky buckets

- Number of user limits reached
- Number of global limits reached

You can also obtain statistics for redirect server through SNMP. The name of the MIB for redirect server is Juniper-SDX-REDIRECTOR-MIB.

- Related Topics**
- Overview of Traffic Redirection on page 149
  - Configuring General Properties for the Redirect Server (SRC CLI) on page 156
  - Viewing Statistics for the Redirect Server (C-Web Interface)
  - Viewing Information About Filtered Traffic (C-Web Interface)



### **Part 3**

# **Designing Services for Enterprise Manager Portal**

- Reviewing and Configuring Policies and Services for Enterprise Manager Portal on page 171
- Adding VPNs from JUNOS Routing Platforms (SRC CLI) on page 197



## Chapter 11

# Reviewing and Configuring Policies and Services for Enterprise Manager Portal

- Overview of Services for Enterprise Manager Portal on page 171
- Before You Configure Services for Enterprise Manager Portal on page 172
- Configuring Firewall Policies and Services for Enterprise Manager Portal on page 173
- Configuring NAT Policies and Services for Enterprise Manager Portal on page 182
- Configuring Bandwidth Policies and Services for Enterprise Manager Portal on page 184
- Enabling Schedules for Subscriptions for Enterprise Manager Portal on page 192
- Configuring VPNs for Enterprise Manager Portal on page 192
- Billing Subscribers Through SCU/DCU for JUNOS Routing Platforms on page 194

## Overview of Services for Enterprise Manager Portal

Enterprise Manager Portal is an application that lets service providers provision services for enterprise subscribers.

Enterprise Manager Portal can apply the types of services listed in Table 13 on page 171 to enterprise traffic as specified on JUNOS routing platforms or JUNOSe routers.

**Table 13: 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. Configure the SAE.
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 and Locating Subscriber Management Information.

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 and Adding JUNOSe Routers and Virtual Routers with the CLI.

4. For prerequisites to using policy rules on JUNOS routing platforms and JUNOSe routers, see Before You Configure SRC Policies.
5. For general information about configuring services, see Policy Management Overview.

## Configuring Firewall Policies and Services for Enterprise Manager Portal

---

Before you configure firewall policies and services in Enterprise Manager Portal, you review and update the configuration from the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface. Topics in this section include:

- Types of Firewall Services on page 173
- Overview of Basic Firewall Services and Policies on page 174
- Tasks to Configure Firewall Policies and Services on page 175
- Configuring Basic Firewall Policies on page 175
- Configuring Basic Firewall Services on page 176
- Reviewing the fwrule Policy Group for Exceptions to Stateful Firewalls on page 176
- Reviewing the Firewall Rule Service for Exceptions to Stateful Firewalls on page 176
- Reviewing Services for Exceptions to Stateless Firewalls on page 177
- Parameter Values Used by Services for Exceptions to Stateless Firewalls on page 178
- Planning Services for Custom Firewall Exceptions on page 179
- Configuring Policies for Custom Firewall Exceptions on page 179
- Configuring Services for Custom Firewall Exceptions on page 180
- Configuring Priorities for Stateless or Stateful Firewall Services on page 180

### Types of Firewall Services

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 14 on page 174 shows the names of the services and policies associated with the basic firewall services in the sample data.

**Table 14: 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 175
2. “Configuring Basic Firewall Services” on page 176
3. For stateful firewalls:
  - a. “Reviewing the fwrule Policy Group for Exceptions to Stateful Firewalls” on page 176
  - b. “Reviewing Services for Exceptions to Stateless Firewalls” on page 177
4. For stateless firewalls:
  - a. “Reviewing Services for Exceptions to Stateless Firewalls” on page 177
  - b. “Parameter Values Used by Services for Exceptions to Stateless Firewalls” on page 178
  - c. “Planning Services for Custom Firewall Exceptions” on page 179
  - d. “Configuring Policies for Custom Firewall Exceptions” on page 179
  - e. “Configuring Services for Custom Firewall Exceptions” on page 180

## **Configuring Basic Firewall Policies**

You can create policies with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.

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 180.

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 with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.

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 Firewall Rule 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 180.

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 15 on page 177 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 15: 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 15 on page 177, 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 16 on page 178 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 172 use these parameters.

**Table 16: 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 with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.

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 with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface. You can create services that take actions such as those listed in Table 15 on page 177.

To configure a service for a custom firewall exception:

1. Create a service for each traffic action listed in Table 15 on page 177. 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 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 15 on page 177 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

Before you configure NAT addressing in Enterprise Manager Portal, review and update the configuration from the SRC CLI or the C-Web interface. Topics in this section include:

- NAT Policies and Services in the SRC Sample Data on page 182
- Configuring the dynsrcnat Policy Group on page 182
- Reviewing the DynSrcNat Service on page 183
- Configuring the staticdstnat Policy Group on page 183
- Configuring the StaticDstNat Service on page 183
- Configuring the staticsrcnat Policy Group on page 183
- Configuring the StaticSrcNat Service on page 184

### NAT Policies and Services in the SRC Sample Data

The NAT policy groups and services provided in the sample data are designed to work with Enterprise Manager Portal and require little configuration. Table 17 on page 182 shows the names of the policy groups and services associated with each type of NAT that the SRC software supports.

**Table 17: 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 the *SRC-PE Services and Policies Guide*.

### 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 configure bandwidth-on-demand services to make them available through the Enterprise Manager Portal. Topics in this section include:

- Overview of Bandwidth-on-Demand Services on page 184
- Parameter Values Used by BoD Services on page 185
- Bandwidth Policies for Different Routing Platforms on page 186
- Configuring Basic BoD Policies on page 186
- Configuring Basic BoD Services on page 187
- Configuring BoD Policies on page 187
- Configuring BoD Services on page 188
- Using BoD Services to Assign Traffic to Bandwidth Categories on page 189
- Using BoD and Basic BoD Services Together to Supply Class of Service on page 189
- Examples: Setting Up Forwarding Preferences on page 190

## Overview of Bandwidth-on-Demand Services

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 JUNOS 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. .

### **Parameter Values Used by BoD Services**

Table 18 on page 185 lists the parameters for which Enterprise Manager Portal provides values. The parameter names start with “ bod” (service’s LDAP attribute parameterSubstitution).

**Table 18: 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 Policy Management Overview.

## **Configuring Basic BoD Policies**

You can create policies with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.

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 18 on page 185.
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 with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.

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 Policy Components.

You can create policies with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.

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 JUNOS 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 Policy Information Model.

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 with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.



**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. 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.

## Examples: Setting Up Forwarding Preferences

We provide two examples for setting up forwarding preferences.

### Setting Up Forwarding Preferences by Using CoS on JUNOS Routing Platforms

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 19 on page 190 lists the services and policies in the sample data. You can locate the services in *l = ent/junos*, *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 186 and “Configuring BoD Policies” on page 187 .

**Table 19: 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.

**Table 19: Integrated BoD and Basic BoD Services in Sample Data** *(continued)*

Name of Service	Category of Service	Name of Policy Group	Description of Service
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 by Allocating a Percentage of a Link's Bandwidth to a Service

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 20 on page 192.

**Table 20: 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 the SRC CLI or the C-Web interface, navigate to the service to be scheduling-enabled.
2. For service parameters, add the Substitution **isSchedulable = 1**.

This substitution lets enterprise subscribers configure schedules for subscribers to this service.

## Configuring VPNs for Enterprise Manager Portal

You configure VPNs, then manage them through the Enterprise Manager Portal. Topics in this section include:

- Overview of VPN Management Through Enterprise Manager Portal on page 192
- Before You Configure VPN Policies and Services on page 193
- Configuring Policies for BoD Traffic Destined for VPNs on page 193
- Configuring Services for BoD Traffic Destined for VPNs on page 194

## Overview of VPN Management Through 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, complete the following tasks specific to the VPN configuration:

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.

The identifier for a VPN in the directory must match the name of the routing instance configured on the JUNOS routing platform.

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 193 and “Configuring Services for BoD Traffic Destined for VPNs” on page 194.

4. Implement an addressing scheme for VPNs that allows extranet clients to access the VPNs.

- Related Topics**
- Before You Configure Services for Enterprise Manager Portal on page 172
  - Before You Add a JUNOS VPN to the SRC Configuration on page 197
  - Adding VPNs for Retailers and Enterprises on page 199

## **Configuring Policies for BoD Traffic Destined for VPNs**

You can manage policies with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.

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 with the Policies, Services, and Subscribers CLI or the Policies, Services, and Subscribers subtasks in the C-Web interface.

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 “Configuring Policies for BoD Traffic Destined for VPNs” on page 193.

```
!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 12

# Adding VPNs from JUNOS Routing Platforms (SRC CLI)

- Before You Add a JUNOS VPN to the SRC Configuration on page 197
- Configuring VPNs to Integrate into an SRC Network on page 198
- Configuration Statements for Adding VPNs and Extranet Clients on page 198
- Adding VPNs for Retailers and Enterprises on page 199
- Verifying and Updating Configuration of Extranets for VPNs on page 200
- Locating and Removing Inactive Subscriptions to a VPN on page 201

### 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.

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.

- Related Topics**
- Overview of NAT Address Management Portal on page 307
  - Assigning IP Addresses on page 307

## 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 Controllers, you add VPNs through the CLI and can manage the VPNs through an enterprise portal that runs on another system.

- Related Topics**
- Adding VPNs for Retailers and Enterprises on page 199

## 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-extrane t...];
}
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-extrane t...];
}

```

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 "];
```

## 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.



## **Part 4**

# **Managing Access Portals for Enterprise Subscribers**

- Overview of Enterprise Service Portals on page 205
- Planning Deployment for Enterprise Service Portals on page 215
- Installing and Configuring Enterprise Service Portals on page 221
- Managing Services with Enterprise Manager Portal on page 235
- Managing Enterprise Service Portals on page 301
- Using NAT Address Management Portal on page 307
- Using the Sample Enterprise Service Portal on page 311
- Developing an Enterprise Service Portal on page 321



## Chapter 13

# Overview of Enterprise Service Portals

- Function of Enterprise Service Portals on page 205
- Enterprise Service Portals Provided with the SRC Software on page 207
- Enterprise Service Portal Audit Plug-In on page 209
- Network Information Collector with Enterprise Service Portals on page 209
- Service Parameters on page 209
- Substitutions and the Parameter Acquisition Path on page 210
- Managing Subscriptions to Aggregate Services on page 212
- Configuring Your Web Browser to Use an Enterprise Service Portal on page 212
- Accessing Enterprise Service Portals on page 212

### 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 on the Juniper Networks Web site at <http://www.juniper.net/techpubs/software/management/src/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 in the SDK+AppSupport+Demos+Samples.tar.gz file on the Juniper Networks Web site at: <https://www.juniper.net/support/csc/swdist-erx/src.html> 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 on the Juniper Networks Web site at <http://www.juniper.net/techpubs/software/management/src/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 in the **SDK+AppSupport+Demos+Samples.tar.gz** file on the Juniper Networks Web site at: <https://www.juniper.net/support/csc/swdist-erx/src.html>. The file is located in the folder **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.

**Related Topics** ■ Locating Subscriber Management Information

## 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.

## 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 *Parameters and Substitutions* and *Value Acquisition for Single Subscriptions*.

## **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.

- Related Topics**
- Parameters and Substitutions
  - Value Acquisition for Multiple Subscriptions

## 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.

- Related Topics** *SRC-PE Services and Policies Guide.*

## 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 14

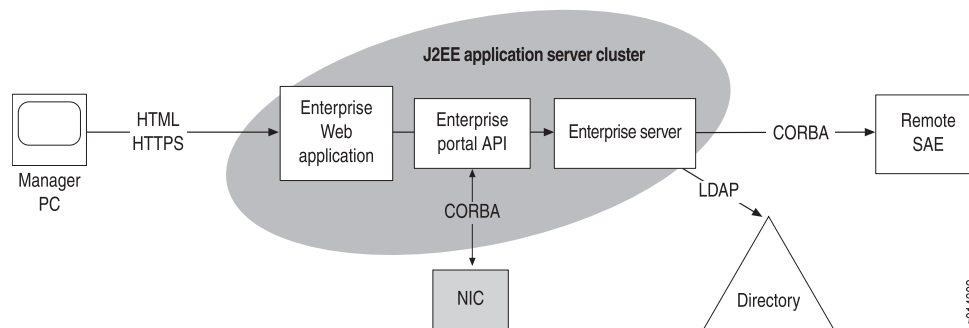
# Planning Deployment for Enterprise Service Portals

- Architecture of Enterprise Service Portals on page 215
- Deployment Scenario for an Enterprise Service Portal on page 216
- Deciding Which Enterprise Service Portal to Use on page 217
- Planning Number of Instances of an Enterprise Service Portal on page 218
- Planning Namespace Hierarchy for an Enterprise Service Portal on page 218

## Architecture of Enterprise Service Portals

Figure 22 on page 215 shows the basic elements and communication protocols of an enterprise service portal.

**Figure 22: 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

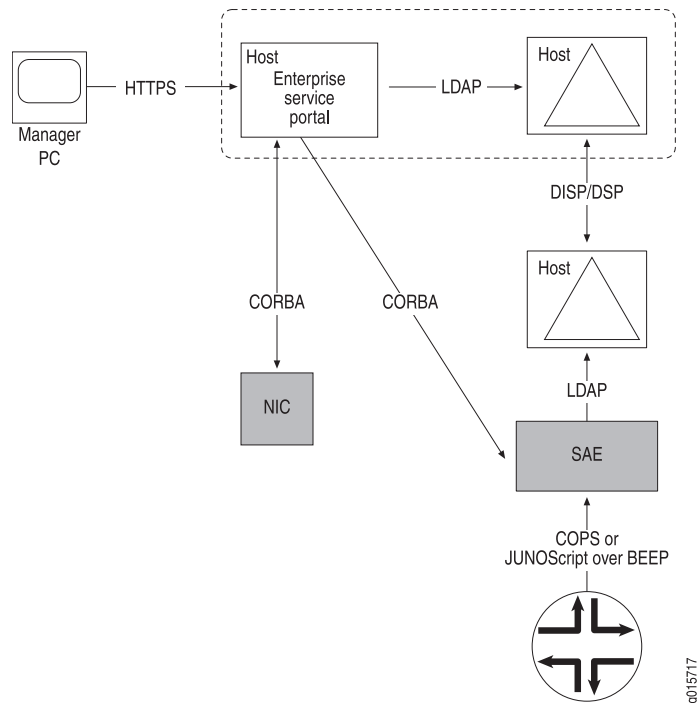
Table 21 on page 216 describes the communication protocols that are used between elements in the enterprise service portal network.

**Table 21: 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 23 on page 217 shows component interactions for a sample deployment of an enterprise service portal.

**Figure 23: 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 22 on page 217 describes which application to use in your organization.

**Table 22: 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

**Table 22: Enterprise Service Applications** *(continued)*

To Perform This Task	Use This Application
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 23 on page 218). 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 23: 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 15

# Installing and Configuring Enterprise Service Portals

- Before You Install an Enterprise Service Portal on page 221
- Setting Up Enterprise Service Portals on page 222
- Preparing the Web Applications for Customization on page 222
- Configuring Connections to the Directory on page 223
- Configuring Deployment Settings for Enterprise Manager Portal on page 225
- Configuring the URL for an Enterprise Service Portal on page 231
- Writing an Application to Allow a Machine to Provide Public IP Addresses for NAT on page 231
- Configuring an Enterprise Service Portal Audit Plug-In on page 232

### 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.
- 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. . 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 NIC, see Locating Subscriber Management Information).
- In the directory, create any new namespaces for the enterprise service portals you will install. . 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.

## Setting Up Enterprise Service Portals

---

Tasks to install an enterprise service portal are:

1. “Preparing the Web Applications for Customization” on page 222
2. “Configuring Connections to the Directory” on page 223
3. (Enterprise Manager Portal only) “Configuring Deployment Settings for Enterprise Manager Portal” on page 225
4. “Configuring the URL for an Enterprise Service Portal” on page 231

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 231.
- 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 Audit Plug-In” on page 232.

## 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.

See “Initialization Properties for Enterprise Service Portals” on page 223.

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).
- 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.

See *SRC 2.0.x Getting Started Guide*.

See *SRC 2.0.x Getting Started Guide*.

#### ***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.

See “Deployment Properties for Enterprise Manager Portal” on page 225.

4. Replace the *web.xml* file in the WAR files.

```
jar uvf entmgr.war WEB-INF/web.xml
```

## Deployment Properties for Enterprise Manager Portal

The *web.xml* file contains deployment properties for Enterprise Manager Portal. 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. 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

## **Configuring the URL for an Enterprise Service Portal**

---

The way you deploy the enterprise service portals depends on your Web application server. See the documentation for your Web application server for information about the deployment.

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
2. Install the application that you created in the preceding step on a machine that contains the software for managing IP addresses.

## 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 and its documentation is in the `SDK+AppSupport+Demos+Samples.tar.gz` file on the Juniper Networks Web site at: <https://www.juniper.net/support/csc/swdist-erx/src.html>. You can locate the application in the directory `/SDX/doc/ent/plugin/doc/net/juniper/smg/ent/plugin`. The sample listener sends output to a log file. The documentation for the plug-in is also in the `SDK+AppSupport+Demos+Samples.tar.gz` file in the folder `/SDX/doc/ent/plugin/doc`. You can also find the documentation on the Juniper Networks Web site at <http://www.juniper.net/techpubs/software/management/src/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 24 on page 232 shows the common information that is provided by every enterprise service portal audit plug-in event.

**Table 24: 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 25 on page 232 describes the events that an audit plug-in listener can listen for and the information reported in those events.

**Table 25: 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.

**Table 25: Events Reportable to the Audit Plug-In** (continued)

Event	IT Manager Action That Initiates Event	Information Reported
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"> <li>■ DN of the new subscription object in the directory.</li> <li>■ Attributes of the new subscription, including sspState, sspAction, and parameterSubstitution.</li> </ul>
UnsubscribeAuditEvent	Unsubscribes from a service.	Common information plus: <ul style="list-style-type: none"> <li>■ DN of the subscription object removed from the directory.</li> <li>■ Attributes of the removed subscription, including sspState, sspAction, and parameterSubstitution.</li> </ul>
SubscriberUpdateAuditEvent	Changes the parameterSubstitution 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"> <li>■ DN of the subscriber object that is changed.</li> <li>■ Attributes changed in the operation, including the old values and new values of the attributes.</li> </ul>
SubscriptionUpdateAuditEvent	Changes the parameterSubstitution attribute of a subscription object; suspends, resumes, activates, or deactivates a subscription.	Common information plus: <ul style="list-style-type: none"> <li>■ DN of the subscription object that is changed.</li> <li>■ Old and new values of the changed attributes:</li> <li>■ parameterSubstitution attribute when subscriber object is changed.</li> <li>■ sspState attribute when subscription is suspended or resumed.</li> <li>■ sspAction attribute when subscription is activated or deactivated.</li> </ul>

**Table 25: Events Reportable to the Audit Plug-In** (continued)

Event	IT Manager Action That Initiates Event	Information Reported
ServiceOpStateAuditEvent	<p>Changes the operational state of a session.</p> <p><b>NOTE:</b> 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.</p>	<p>Common information plus:</p> <ul style="list-style-type: none"> <li>■ DN of the subscriber that owns the subscription session. The subscriber must be a leaf in the subscriber tree in the enterprise scenario.</li> <li>■ DN of the subscription object where the subscription session comes from.</li> <li>■ Operational state of the session after the IT manager's action.</li> </ul>
ExportAuditEvent	Exports a VPN.	<p>Common information plus:</p> <ul style="list-style-type: none"> <li>■ DN of VPN that is exported.</li> <li>■ DN of the subscriber to which the VPN is exported.</li> </ul>
UnexportAuditEvent	Cancels the export of a VPN.	<p>Common information plus:</p> <ul style="list-style-type: none"> <li>■ DN of VPN for which export is canceled.</li> <li>■ DN of the subscriber for which export of the VPN was canceled.</li> </ul>

## Chapter 16

# Managing Services with Enterprise Manager Portal

- Overview of Enterprise Manager Portal on page 235
- Getting Help on Enterprise Manager Portal on page 236
- Setting the Configuration Level for Enterprise Manager Portal on page 236
- Managing Schedules on page 237
- Managing Subscriptions to Bandwidth-on-Demand Services on page 244
- Integrating VPNs into an SRC Network Through Enterprise Manager Portal on page 260
- Classifying Traffic for Stateful Firewall Exceptions and NAT Rules on page 264
- Subscribing to Firewall Services Through Enterprise Manager Portal on page 270
- Working with IP Addressing and NAT Services on page 288
- Monitoring the Status of Subscriptions on page 296
- Troubleshooting Subscriptions That Are Not Functioning Correctly on page 299
- Troubleshooting Subscriptions of Unknown Status on page 299

## 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. 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 26 on page 235 lists the types of services that can be configured from Enterprise Manager Portal for JUNOSe routers and JUNOS routing platforms.

**Table 26: Portal Configuration Support for Services on Routers**

Type of Service	JUNOSe Router	JUNOS Routing Platform
BoD services	Yes	Yes
VPNs	No	Yes

**Table 26: Portal Configuration Support for Services on Routers** *(continued)*

Type of Service	JUNOSe Router	JUNOS Routing Platform
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.

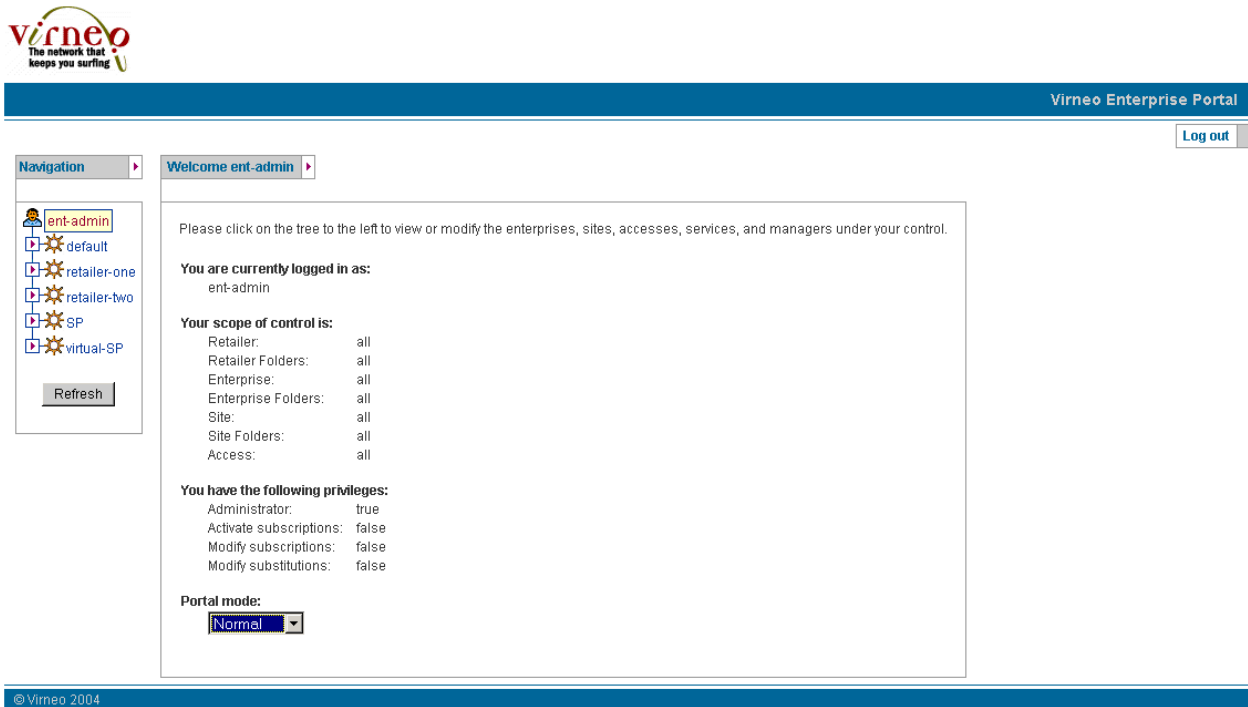
Some fields and pages in the portal offer more extensive online help. To view this help, click the help icon .

## 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

You can establish schedules for specified services through the Enterprise Manager Portal. Topics include:

- Schedules in Enterprise Manager Portal on page 237
- Enabling Scheduling for the Enterprise Manager Portal on page 238
- Using Schedules in Enterprise Manager Portal on page 238
- Disabling a Schedule for a Service in Enterprise Manager Portal on page 243
- Changing Schedules in Enterprise Manager Portal on page 244

### Schedules in Enterprise Manager Portal

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.

## Enabling Scheduling for the Enterprise Manager Portal

To enable scheduling:

1. Edit the *web.xml* file for the portal to enable scheduling.

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.

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.

## Using Schedules in Enterprise Manager Portal

Tasks to use a schedule are:

1. Creating a Schedule in Enterprise Manager Portal on page 238
2. Applying a Schedule to a Service in Enterprise Manager Portal on page 242

## Creating a Schedule in Enterprise Manager Portal

To create a schedule:

1. Click the **Schedules** tab.

The Schedules page appears.

default ▶ local ▶ Acme ▶ Boca ▶ Primary ▶

Bandwidth & VPNs	Applications	Firewall	Addresses	NAT	<b>Schedules</b>	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.

**Schedule Definition Page - Microsoft Internet Explorer**

<b>Schedule Name</b>		<b>Subscription is:</b>	
<input type="text"/>		<input type="radio"/> enabled during schedule <input type="radio"/> enabled outside schedule	

<b>Schedule Time</b>		
<b>Start Time</b>	<b>Time Zone</b>	<b>Duration</b>
<input type="text"/> <i>e.g. 10:45</i>	<input type="text" value="Canada/Eastern"/> <i>e.g. America/Los_Angeles</i>	<input type="text"/> <input type="text"/> <i>e.g. 8 hour(s)</i>

<b>Recurrence Pattern</b>				
<input checked="" type="radio"/> <b>Once</b>	<input type="radio"/> <b>Daily</b>	<input type="radio"/> <b>Weekly</b>	<input type="radio"/> <b>Monthly</b>	<input type="radio"/> <b>Yearly</b>
<input type="text"/> <i>e.g. 12/31/2004</i>	Every: <input type="radio"/> day <input type="radio"/> weekday	Every week on: <input type="checkbox"/> Sunday <input type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday <input type="checkbox"/> Friday <input type="checkbox"/> Saturday	Day <input type="text"/> of every month.	Every <input type="text"/> <input type="text"/>
Range of recurrence Start: <input type="text"/> <i>e.g. 12/31/2004</i> End by: <input type="text"/> <i>e.g. 01/31/2005</i>				

3. Enter field values to define a schedule, and click **Save**.

See “Schedule Fields in Enterprise Manager Portal” on page 240.

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 Fields in Enterprise Manager Portal**

Use the fields in this topic to define a service schedule.

**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 27 on page 241 shows the maximum duration for specified recurrence patterns.

**Table 27: 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 in Enterprise Manager Portal**

Before you can schedule a subscription, you must define a schedule..

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 ▼ Apply

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 Edit	Gold ▼	None ▼	GoldVideo ▼	<input type="checkbox"/>	Delete
				Apply	Status... Usage data...	
Rule2	Source IPs: 10.10.10.168/24 Destination IPs: 10.10.10.100/24 Edit	Silver ▼	None ▼	No schedule ▼	<input type="checkbox"/>	Delete
				Apply	Status... Usage data...	
Create Subscription						

### Disabling a Schedule for a Service in Enterprise Manager Portal

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 296 .

## Changing Schedules in Enterprise Manager Portal

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. , 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

---

You can configure and manage bandwidth-on-demand services in Enterprise Manager Portal. Topics include:

- Overview of Bandwidth-on-Demand Services on page 245
- Planning Subscriptions to BoD Services on page 245
- Creating a Subscription to BoD Services on page 246
- Modifying Rules for a Subscription to a BoD Service on page 258

- Modifying the Bandwidth Level on page 258
- Moving the Bandwidth Level on page 258
- Deleting a Subscription for a BoD Service on page 258
- Deleting the Bandwidth Level on page 259
- Monitoring Use of Subscriptions to BoD Services on page 259

## Overview of 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.

## 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. Tasks to create a subscription are:

1. Setting a Bandwidth Level on page 246
2. Adding Subscriptions to BoD Services on page 247

### Setting a Bandwidth Level

To create a subscription to a bandwidth level:

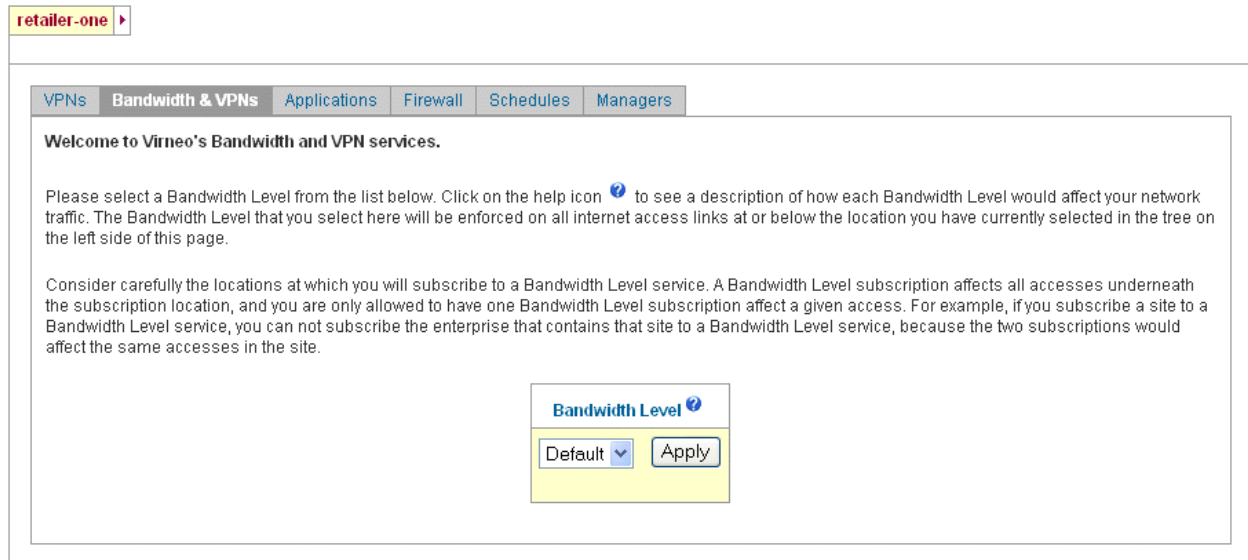
1. In the navigation pane of Enterprise Manager Portal, click the subscriber for whom you want to provision bandwidth.
2. Click the **Bandwidth & VPNs** tab.



**NOTE:** If VPN features are not configured, the tab is named Bandwidth.

---

The Bandwidth & VPNs page appears.

**Figure 24: Bandwidth & VPNs Page**

- 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 Fields in Enterprise Manager Portal***

Use the field in this topic to define the bandwidth level.

#### ***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 25: 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 Destination Address 192.0.2.0/24	Gold ▼	None ▼	No schedule ▼	<input type="checkbox"/>	Delete Status... Usage data...
<div>Create Bandwidth Rule</div>						

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"/>	

5. Using field values to configure subscriptions for BoD services.

See “BoD Service Fields in Enterprise Manager Portal” on page 250

You can configure any number of subscriptions by assigning different traffic flows, identified by rules under Affected Traffic on the Bandwidth & VPNs page, to different BoD services.

6. Click Create.

The subscription appears in the Bandwidth & VPNs page.

### ***BoD Service Fields in Enterprise Manager Portal***

Use the fields in this topic to configure subscriptions for BoD services.

#### ***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 236).

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 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 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.
- 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 260.
- 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.
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.
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 259.
2. Set a bandwidth level for another subscriber. See "Creating a Subscription to BoD Services" on page 246.
3. Create BoD services. See "Creating a Subscription to BoD Services" on page 246.

### ***Deleting a Subscription for a BoD Service***

To delete a subscription to a BoD service:

1. Start at the subscriber's Bandwidth page.
2. Click **Delete** for the subscription.

## Deleting the Bandwidth Level

To delete the bandwidth level:

1. Start at the subscriber's Bandwidth page.
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

**Purpose** Monitor the use of a bandwidth subscription.

- Action**
1. Start at the subscriber's Bandwidth page.
  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
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.

## Integrating VPNs into an SRC Network Through Enterprise Manager Portal

---

You can integrate VPNs into your SRC network through the Enterprise manager portal. Topics include:

- Overview of VPNs in an SRC Network on page 260
- Modifying Subscriber VPN Configuration on page 260
- Creating Extranets Through Enterprise Manager Portal on page 262
- Deleting Extranets Through Enterprise Manager Portal on page 263
- Sending Traffic to a VPN on page 263
- Modifying the VPN to Which the Router Sends Traffic on page 263
- Stopping the Router from Sending Traffic to VPNs on page 264

### Overview of VPNs in 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 can make modifications to VPNs that a subscriber owns.

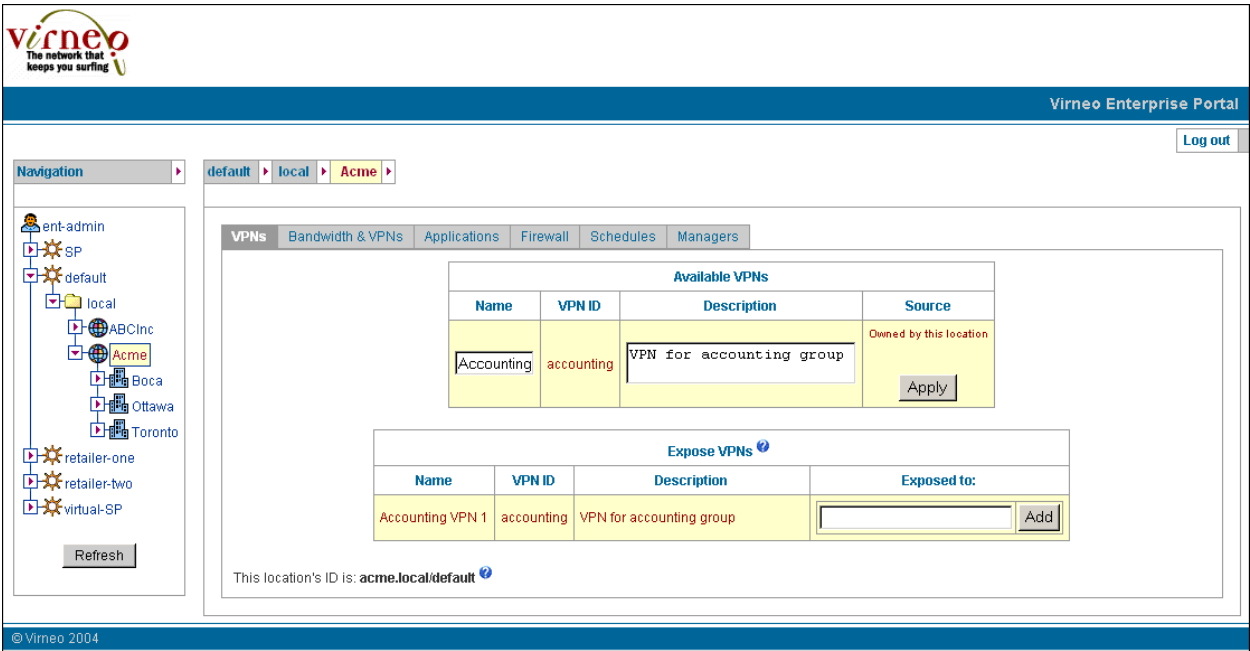
### Modifying Subscriber VPN Configuration

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 26: VPNs Page



3. Using the field descriptions below, modify the VPN.
4. Click **Apply**.

### VPN Fields in Enterprise Manager Portal

Use the fields in this topic to modify a VPN configuration through Enterprise manager Portal.

#### 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 Through Enterprise Manager Portal**

If the service provider configures the portal to display extranet features, IT managers with privileges to configure VPNs in their scope of control 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). 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 Through Enterprise Manager Portal***

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. Configure a 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.
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.
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 classify traffic affected by a firewall exception to a stateful firewall or by a NAT rule. Topics include:

- Overview of Traffic Classification for Firewall Exceptions and NAT Rules on page 264
- Classifying Traffic on page 265
- Modifying Values for Traffic Classifications on page 269
- Deleting Traffic Classifications on page 270

### Overview of Traffic Classification for 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 27: 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**

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:

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**.

### Traffic Classification Fields in Enterprise Manager Portal

Use the fields in this topic to classify traffic for firewall exceptions and NAT rules.

#### ***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.
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.
2. Click **Delete** for the application protocol.

## **Subscribing to Firewall Services Through Enterprise Manager Portal**

---

You can configure subscriptions to firewall services through Enterprise manager Portal. Topics include:

- Overview of Firewall Services in Enterprise Manager Portal on page 270
- Before You Configure Firewall Exception Rules on page 271
- Creating Subscriptions to Firewall Services on page 271
- Creating Firewall Exceptions for Stateless Firewalls on page 272
- Creating Firewall Exceptions for Stateful Firewalls on page 283
- Adding a Schedule to a Firewall Exception on page 286
- Modifying Firewall Exceptions on page 287
- Deleting Firewall Exceptions on page 287
- Deleting Basic Firewalls on page 287
- Monitoring the Use of Subscriptions to Firewall Services on page 288

## ***Overview of Firewall Services in Enterprise Manager Portal***

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.

### ***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 236.

### ***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.

See “Firewall Service Field in Enterprise Manager Portal” on page 272.

4. Select a firewall service from the menu, and click **Apply**.

The Firewall page changes to allow you to create firewall exceptions.

### Firewall Service Field in Enterprise Manager Portal

Use the field in this topic to specify a firewall service in Enterprise manager Portal.

#### 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.
2. In the Firewall page, click **Create Firewall Exception**.

The Create Exception dialog box appears. Figure 28 on page 273 shows the appearance of the dialog box when Enterprise Manager Portal is set to Advanced mode.

**Figure 28: Create Exception Dialog Box for Stateless Firewalls**

The screenshot shows a web browser window titled "Create Exception - Microsoft Internet Explorer". Inside the browser is a form titled "Create Exception". The form has the following fields and controls:

- Rule Name:** A text input field.
- IP Protocols:** A text input field.
- ToS Byte:** A section containing three radio buttons: "DiffServ" (selected), "Precedence", and "Free Format (e.g. 110101xx)". The "DiffServ" option has a dropdown menu next to it. The "Free Format" option has a text input field below it.
- Source IP Addresses:** A list box with up and down arrows.
- Source Ports:** A text input field.
- Destination IP Addresses:** A list box with up and down arrows.
- Destination Ports:** A text input field.
- TCP Flags:** A text input field.
- Fragmentation Flags:** A text input field.
- Fragment Offset:** A text input field.
- Packet Length:** A text input field.
- ICMP Type:** A text input field.
- ICMP Code:** A text input field.
- Priority:** A text input field with the value "0".
- Direction:** A dropdown menu with "Incoming" selected.
- Action:** A dropdown menu with "Allow" selected.
- Enabled:** A checkbox that is currently unchecked.

At the bottom of the form are three buttons: "Create", "Cancel", and "Reset".

- Enter field values to configure the values for the firewall exception.

See “Fields for Exceptions to Stateless Firewalls in Enterprise Manager Portal” on page 275.

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.

- Click **Create**.

The Firewall page shows the exception configured. Figure 29 on page 274 shows three exceptions configured for a brickwall firewall service. The exceptions appear in priority order.

**Figure 29: Firewall Page with Firewall Service Applied and Exceptions Configured**

The screenshot shows the 'Firewall Service' configuration page. At the top, there are tabs for 'Bandwidth & VPNs', 'Firewall', 'Addresses', 'NAT', 'Schedules', and 'Managers'. The 'Firewall' tab is active, showing a 'Firewall Service' section with a dropdown menu set to 'BrickWall' and an 'Apply' button. Below this is a table titled 'Exceptions to Firewall Service' with columns: Name, Affected Traffic, Priority, Direction, Firewall Action, Schedule, Enabled, and a 'Delete' button. The table contains four rows of exceptions:

Name	Affected Traffic	Priority	Direction	Firewall Action	Schedule	Enabled	Delete
tcpProto1	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	4	Incoming	Allow	No schedule	<input checked="" type="checkbox"/>	Delete Status... Usage data...
tcpRule2	All Traffic	7	Incoming	Allow	No schedule	<input type="checkbox"/>	Delete Status... Usage data...
icmpRule	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	10	Outgoing	Discard	No schedule	<input type="checkbox"/>	Delete Status... Usage data...
tcpProtocol	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 & !syn & rst & !push & ack & urgent Fragmentation Flags: dont-fragment Fragment Offset: 100..170 Packet Length: 60..70	45	Incoming	Allow	No schedule	<input checked="" type="checkbox"/>	Delete Status... Usage data...

At the bottom of the table is a 'Create Firewall Exception' button.

## Fields for Exceptions to Stateless Firewalls in Enterprise Manager Portal

Use the fields in this topic to configure rules for exceptions to stateless firewalls.

### ***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.
2. Access the subscriber’s Firewall page.

Figure 30: Firewall Page with Firewall Service Applied

default ▸ local ▸ Acme ▸ Boca ▸ Primary ▸

Bandwidth & VPNsApplicationsFirewallAddressesNATSchedulesManagers

Firewall Service ⓘ

EmailAndWeb ▾Apply

Status...

Exceptions to Firewall Service

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. Enter field values to configure the values for the firewall exception.  
  
See “Fields for Exceptions to Stateful Firewalls in Enterprise Manager Portal” on page 283.
4. Click **Create**.

Fields for Exceptions to Stateful Firewalls in Enterprise Manager Portal

Use the fields in this topic to specify exceptions to stateful firewalls.

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 236), 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 236), 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.
- 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. .
- 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.

To add a schedule to a firewall exception:

1. Access the subscriber's Firewall page.
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.
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.
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 283 and “Applying NAT Rules to Traffic” on page 291.

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.
5. Select **No Firewall** from the Firewall Service menu.
6. Click **Apply**.

## Monitoring the Use of Subscriptions to Firewall Services

**Purpose** Monitor the use of firewall subscriptions.

- Action**
1. Access the subscriber's Firewall page.
  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.

**Service Usage**

**Service Usage Data**

This data is for the subscription **tcpProtocol** to service **Firewall Exception**.

Access Link	Usage Data					
	For Period From	For Period To	Incoming Bytes	Outgoing Bytes	Incoming Packets	Outgoing Packets
primary.toronto.acme.local/default	Wednesday, October 26, 2005 1:46:56 PM	Wednesday, October 26, 2005 1:56:28 PM	0	0	0	0

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.

Copyright © 1998-2005, Juniper Networks, Inc. ENT.B.6.2.1.002

## Working with IP Addressing and NAT Services

You can configure NAT addressing and services from Enterprise Manager Portal. Topics include:

- Requesting Public IP Addresses for NAT Services on page 289
- Canceling Requests for Public IP Addresses on page 290
- Returning Public IP Addresses to Service Providers on page 291
- Applying NAT Rules to Traffic on page 291
- Configuring Public IP Addresses for Outgoing Traffic on page 293
- Configuring Public IP Addresses for Incoming Traffic on page 294

- Configuring Fixed Public Addresses for Outgoing Traffic on page 295
- Modifying NAT Rules on page 296
- Deleting NAT Rules on page 296

### 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 31: Addresses Page Before Requesting Addresses**

default > local > Acme > Boca > Primary

Bandwidth & VPNs Applications Firewall **Addresses** NAT Schedules Managers

**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.
- See “Address Fields for NAT Addressing in Enterprise Manager Portal” on page 290.
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 32 on page 290. 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 32: Addresses Page After Requesting Addresses**

Acme ▸ Boca ▸ Primary ▸

Bandwidth & VPNs Applications Firewall **Addresses** NAT Schedules Managers

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:		<input type="button" value="Release"/>

Request More Public IP Addresses		
Number of Addresses	Contiguous	
<input type="text" value="1"/>	<input type="checkbox"/>	<input type="button" value="Request"/>

**Outstanding Requests for Public IP Addresses**

No outstanding requests for public IP addresses exist.

### Address Fields for NAT Addressing in Enterprise Manager Portal

Use the fields in this topic to specify address range(s).

#### 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.

default ▶ local ▶ Acme ▶ Boca ▶ **Primary** ▶

**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"/>	<b>Request</b>

**Outstanding Requests for Public IP Addresses**

Request Time	Number of Addresses	Contiguous	
Tue Jul 19 09:47:51 EDT 2005	1	No	<b>Cancel</b>

## 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.
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 236).

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 33: NAT Page**

The screenshot shows the Virneo Enterprise Portal interface. The top navigation bar includes the Virneo logo and a 'Log out' button. The left sidebar shows a tree view of the network configuration, with 'Backup' selected under the 'local' section. The main content area has a tabbed interface with 'NAT' selected. The NAT page displays three configuration sections:

- Public Addresses for Outgoing Traffic:** A table with columns 'Address Range', 'Port Range', and 'Enabled'. It shows a single entry with 'From' and 'To' IP addresses set to 192.0.2.22. A 'Create' button is present.
- Public Addresses for Incoming Traffic:** A table with columns 'Priority', 'Name', 'Public IP', 'Private IP', 'Application', and 'Enabled'. It shows a single entry with 'Public IP' set to 192.0.2.22. A 'Create' button is present.
- Fixed Public Addresses for Outgoing Traffic:** A table with columns 'Priority', 'Name', 'Private IP', 'Public IP', 'Application', and 'Enabled'. It shows a single entry with 'Public IP' set to 192.0.2.22. A 'Create' button is present.

3. Configure NAT for incoming and outgoing interfaces on the router.

**Related Topics**

- Configuring Public IP Addresses for Outgoing Traffic on page 293
- Configuring Public IP Addresses for Incoming Traffic on page 294

## 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. Enter field values to specify how the router will apply the NAT rule to outgoing traffic.

See “Outgoing Traffic Fields for NAT Addressing in Enterprise Manager Portal” on page 293.

3. Select **Enabled**.
4. Click **Create**.

### Outgoing Traffic Fields for NAT Addressing in Enterprise Manager Portal

Use fields in this topic to configure NAT addressing for outgoing traffic.

#### 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.

### **Incoming Traffic Fields for NAT Addressing in Enterprise Manager Portal**

Use fields in this topic to configure NAT addressing for incoming traffic.

#### ***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.
  - 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 236).
2. Locate the area called Fixed Public Addresses for Outgoing Traffic in the NAT page (see Figure 33 on page 292).

- 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**

---

**Purpose** Monitor the status of a subscription.

- Action**
- 1. Start at the page that lists information about the subscription.  
  
For an example, a page that 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 - Microsoft Internet Explorer**

**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](#)

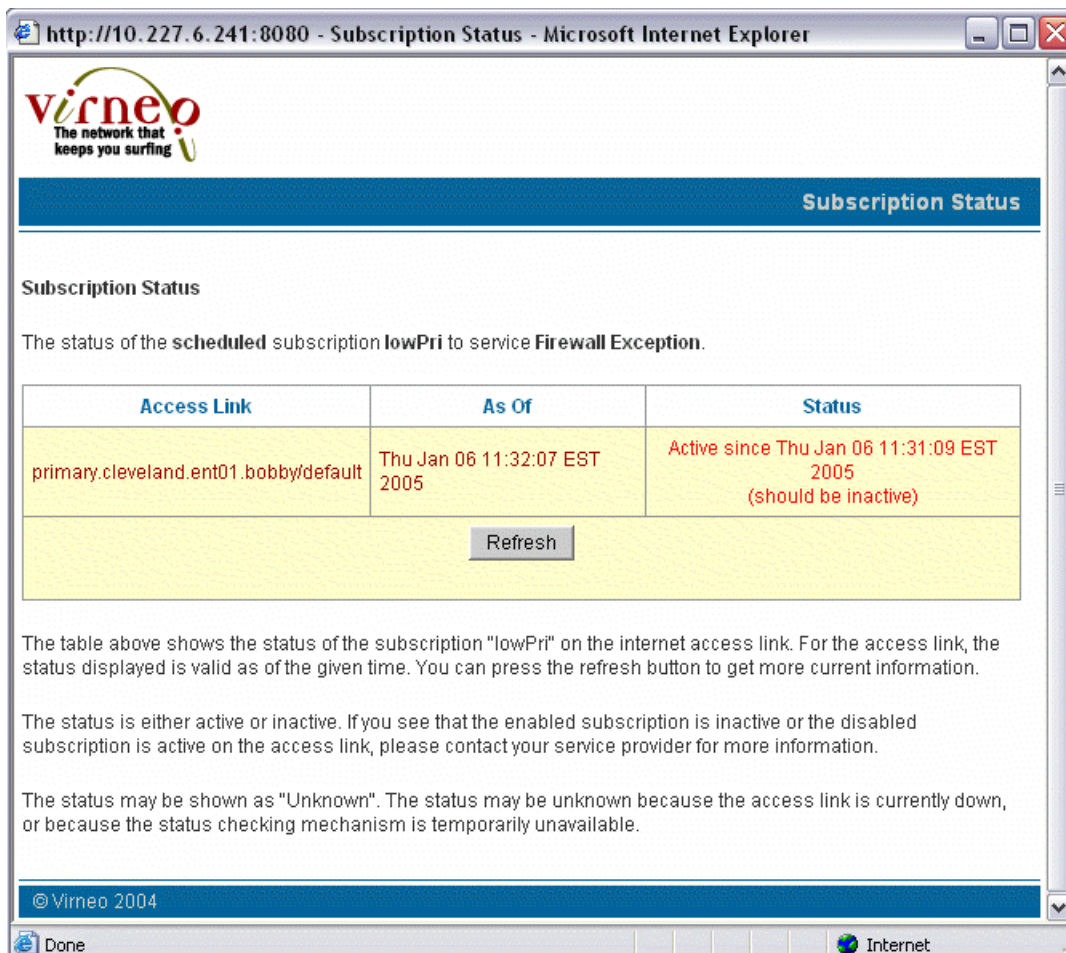
Each row in the table above shows the status of the subscription on one internet access link. For each access link, the status displayed is valid as of the given time. You can press the refresh button to get more current information.

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.



**Meaning** Table 28 on page 298 shows the possible status for subscriptions.

**Table 28: Possible Subscription Status**

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

---

**Problem** One or more subscriptions are not functioning correctly.

**Solution** 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

---

**Problem** Subscriptions of unknown status and subscriptions 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.

**Solution** 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 17

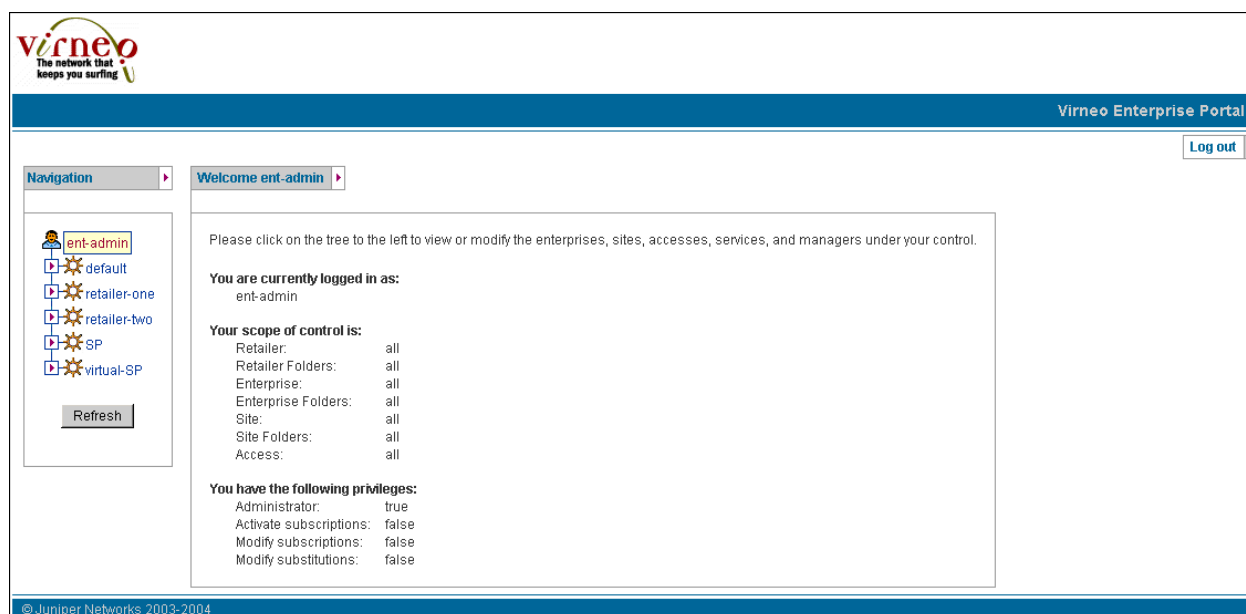
# Managing Enterprise Service Portals

- Displaying Information About Your Control in the Enterprise Through the Enterprise Service Portal on page 301
- Updating Data That the Enterprise Service Portal Displays on page 302
- Managing Operators Through the Enterprise Service Portal on page 302
- Creating Managers Through the Enterprise Service Portal on page 302
- Modifying Managers Through the Enterprise Service Portal on page 305
- Deleting Managers Through the Enterprise Service Portal on page 305

## Displaying Information About Your Control in the Enterprise Through the Enterprise Service Portal

**Purpose** Display information about your scope of control and permissions in the enterprise.

**Action** 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 Through the Enterprise Service Portal

---

Typically, a service provider uses the SRC CLI, the C-Web interface, or an LDAP client to create one operator for each enterprise. This operator, or manager, represents the primary IT manager for the enterprise.

The primary IT manager uses the enterprise service portal to create and manage other managers in the directory and gives those managers privileges to manage specific sites and accesses.

- Related Topics**
- Creating Managers Through the Enterprise Service Portal on page 302
  - Modifying Managers Through the Enterprise Service Portal on page 305
  - Deleting Managers Through the Enterprise Service Portal on page 305

## Creating Managers Through the Enterprise Service Portal

---

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 34: Manager's Page**

Virneo Enterprise Portal

Log out

Navigation

ent-admin

- SP
- default
- retailer-one
- retailer-two
- virtual-SP

Refresh

default

Managers

Login ID	Admin.	Modify sub.	Modify params.	Activate sub.	Modify VPNs	Password	
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	Create

© Virneo 2004

3. Complete the fields in a new line of the table.

See “Managers Fields in the Enterprise Service Portal” on page 303.

4. Click **Create**.

The portal adds the new manager to the table.

## Managers Fields in the Enterprise Service Portal

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 Through the Enterprise Service Portal**

---

To modify a manager's privileges:

1. Start at the Manager's page.
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 Through the Enterprise Service Portal**

---

To delete a manager:

1. Start at the Manager's page.
2. Click **Delete** for the manager.



## Chapter 18

# Using NAT Address Management Portal

- Overview of NAT Address Management Portal on page 307
- Assigning IP Addresses on page 307
- Acknowledging the Release of IP Addresses on page 308

### 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.

### 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.

**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**

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	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"/>

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 acknowledge release of IP addresses:

- 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 19

# Using the Sample Enterprise Service Portal

- Overview of the Sample Enterprise Service Portal on page 311
- Starting the Sample Enterprise Service Portal on page 311
- Subscribing to Services on page 312
- Activating Subscriptions on page 313
- Deactivating Subscriptions on page 314
- Suspending Subscriptions on page 314
- Canceling Suspensions of Subscriptions on page 315
- Monitoring Use of Subscriptions on page 315
- Specifying Values for Service Parameters in Subscriptions on page 315
- Restoring Default Values for Service Parameters In Subscriptions on page 316
- Deleting Subscriptions on page 316
- Monitoring Service Sessions for a Subscription on page 316
- Defining Networks for Departments in an Enterprise on page 317
- Modifying Network Definitions for Departments in an Enterprise on page 318
- Deleting Network Definitions for Departments in an Enterprise on page 319

### 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 is *tagsEntDemo.war*. You can locate the WAR file in the `SDK+AppSupport+Demos+Samples.tar.gz` file on the Juniper Networks Web site at: <https://www.juniper.net/support/csc/swdist-erx/src.html>. 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/tageEntDemo**

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: ent-admin, default, local, Acme, Boca, Backup, Primary, Ottawa, Toronto, retailer-one, retailer-two, SP, and virtual-SP. The 'Primary' node is selected. Below the tree is a 'Refresh' button. The main content area has a breadcrumb trail: default > local > Acme > Boca > Primary. Below this is a tabbed interface with 'Subscriptions' selected. The table below shows a list of services and their current local subscriptions.

Service	Current local subscriptions	New local subscription name	
Internet-Gold	[unnamed]	<input type="text"/>	<input type="button" value="Subscribe"/>
News		<input type="text"/>	<input type="button" value="Subscribe"/>
Video-Bronze	video-bronze-boca-primary1	<input type="text"/>	<input type="button" value="Subscribe"/>
Audio-Bronze		<input type="text"/>	<input type="button" value="Subscribe"/>
PingDoSProtect		<input type="text"/>	<input type="button" value="Subscribe"/>
StaticDestNat		<input type="text"/>	<input type="button" value="Subscribe"/>
MultiService		<input type="text"/>	<input type="button" value="Subscribe"/>
DynSrcNat		<input type="text"/>	<input type="button" value="Subscribe"/>
GoldSecured		<input type="text"/>	<input type="button" value="Subscribe"/>
Internet-Silver		<input type="text"/>	<input type="button" value="Subscribe"/>
ISP-SP		<input type="text"/>	<input type="button" value="Subscribe"/>
Video-Silver		<input type="text"/>	<input type="button" value="Subscribe"/>
Audio-Silver		<input type="text"/>	<input type="button" value="Subscribe"/>
Video-Gold		<input type="text"/>	<input type="button" value="Subscribe"/>
Silver		<input type="text"/>	<input type="button" value="Subscribe"/>
BrickWall		<input type="text"/>	<input type="button" value="Subscribe"/>
GoldMetered		gold-metered-eng	<input type="button" value="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.

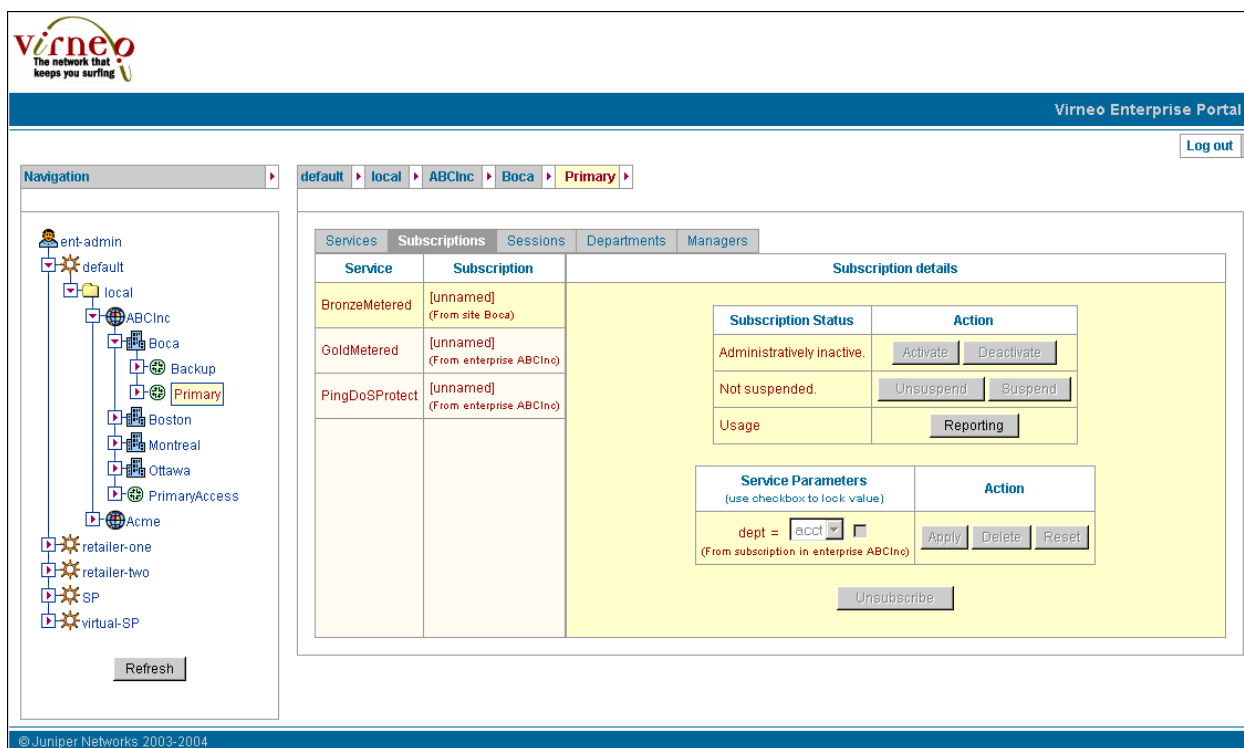
4. Click **Subscribe**.

## 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 35: Subscriptions Page**

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.
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.
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 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

**Purpose** Monitor the use of a subscription.

- Action**
1. Start at the subscriber's Subscriptions page.
  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.
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.
- 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

---

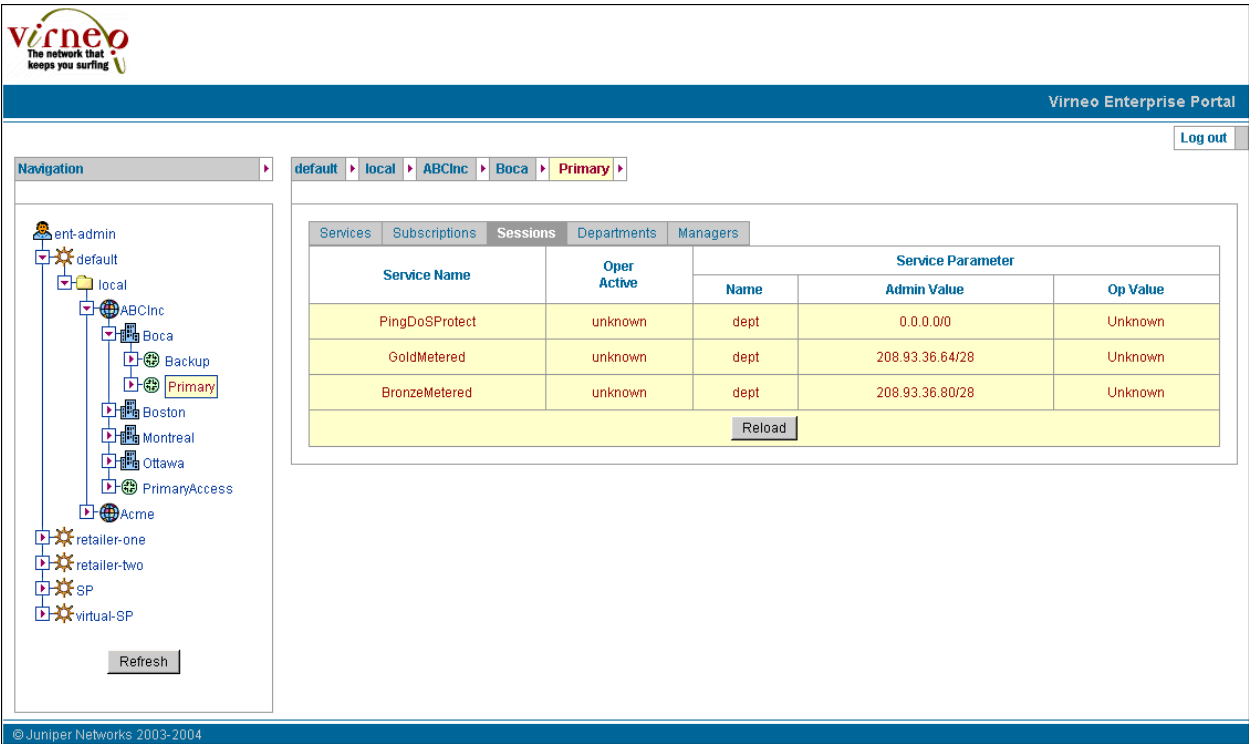
To delete a subscription:

- 1. Start at the subscriber's Subscriptions page.
- 2. Click the subscription you want to delete.
- 3. Click **Unsubscribe**.

## Monitoring Service Sessions for a Subscription

---

<b>Purpose</b>	Monitor the service sessions for a subscription.
<b>Action</b>	<ul style="list-style-type: none"><li>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.</li><li>2. Click the <b>Sessions</b> tab.  The portal displays the status of each subscription and the parameters associated with each subscription.</li></ul>



To update the data on this page, click **Reload**.

## Defining Networks for Departments in an Enterprise

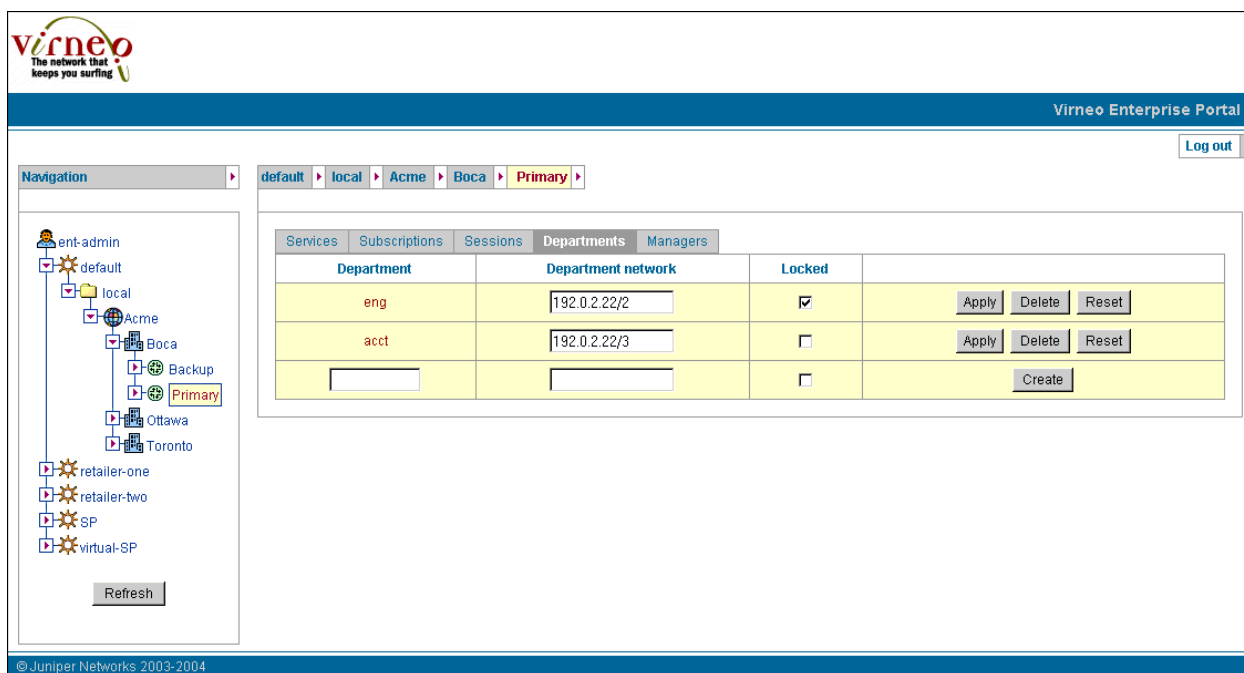
To define the networks for departments in an enterprise:

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 36: Departments Page**

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. For more information about parameters and substitutions, see [Parameters and Substitutions](#).

## Modifying Network Definitions for Departments in an Enterprise

To modify a network definition for a department:

1. Start at the subscriber's Departments page.
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.
2. Click **Delete** for the department.



## Chapter 20

# Developing an Enterprise Service Portal

- Developing a Portal Based on the Sample Enterprise Service Portal on page 321
- Preparing to Develop a Sample-Based Enterprise Service Portal on page 321
- Creating a Portal Project for a Sample-Based Enterprise Service Portal on page 322
- Building a Sample-Based Enterprise Service Portal on page 322
- Deploying a Sample-Based Enterprise Service Portal on page 323
- Testing a Sample-Based Enterprise Service Portal on page 323
- Using a Virtual Address for the Portal on page 323

### 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 click **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

---

**Purpose** Test a sample-based Enterprise Service Portal.

- Action**
1. Use a virtual address for the portal See “Using a Virtual Address for the Portal” on page 323.
  2. Test the portal. See Configuring Simulated Router Drivers (SRC CLI).

**Related Topics** ■ Building a Sample-Based Enterprise Service Portal on page 322

## 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.



## **Part 5**

# **Index**

- Index on page 327



# Index

## A

access lines.....	5
description.....	4, 5
accesses	
configuring subscriptions	
SRC CLI.....	143
accounting	
basic RADIUS accounting plug-in.....	87
custom RADIUS accounting plug-ins.....	87
flat file accounting plug-ins.....	87
flexible RADIUS accounting plug-ins.....	87
anonymous subscriber.....	18
application protocols, managing.....	264
architecture	
enterprise service portal.....	215
authenticated subscriber.....	18
authentication plug-ins	
configuring	
SRC CLI.....	98
types.....	74
authorization plug-ins	
configuring	
SRC CLI.....	98
types.....	74

## B

bandwidth on demand. <i>See</i> BoD	
basic RADIUS accounting plug-in.....	87
configuring	
SRC CLI.....	91
basic RADIUS authentication plug-in.....	98
configuring	
SRC CLI.....	100
BoD (bandwidth on demand)	
services.....	171, 184
subscriptions.....	245

## C

callback interface.....	209
captive portal	
preventing access to resources.....	149

classification scripts	
conditions.....	39
glob matching.....	41
joining.....	41
regular expression matching.....	44
configuring	
SRC CLI.....	41
descriptions.....	39
DHCP classification, C-series controller	
configuring, SRC CLI.....	62
description.....	39
targets.....	65
DHCP classification, C-series Controller	
conditions.....	63
interface classification, C-series controller	
conditions.....	47
configuring, SRC CLI.....	45
description.....	39
examples.....	47
how it works.....	39
targets.....	47
structure	
SRC CLI.....	41
subscriber classification, C-series controller	
condition.....	54
configuring, SRC CLI.....	51
description.....	39
DHCP options.....	57
enterprise subscriber example.....	59
how it works.....	39
static IP subscriber example.....	59
subscriber group example.....	59
targets.....	58
target, C-series controller	
definition.....	39
expressions.....	41
types.....	41
component interactions	
DHCP	
initial login.....	17
persistent login.....	20
subscriber account login.....	18
subscriber logout.....	21
enterprise subscribers	
login.....	24
remote session activation.....	31

PPP	
login.....	12
logout.....	14
static IP subscribers.....	22
subscription activation.....	27
subscription deactivation.....	29
configuration level in Enterprise Manager Portal.....	236
conventions	
notice icons.....	xxiii
text.....	xxiii
COPS (Common Open Policy Service)	
DHCP interactions	
initial login.....	17
logout.....	21
persistent login .....	20
subscriber account login .....	19
interface startup interactions.....	16
PPP interactions	
login.....	13
logout.....	15
static IP subscriber interactions.....	22
subscription activation interactions.....	28
subscription deactivation interactions.....	29
CORBA (Common Object Request Broker Architecture)	
plug-in interface	
enterprise service portal.....	216
custom RADIUS accounting plug-ins.....	87
configuring	
SRC CLI.....	95
custom RADIUS authentication plug-ins.....	99
configuring	
SRC CLI.....	104
customer support.....	xxvii
contacting JTAC.....	xxvii

## D

DCU (destination class usage).....	194
default retailer authentication plug-ins	
configuring	
SRC CLI.....	122
default retailer DHCP authentication plug-ins	
configuring	
SRC CLI.....	122
denial-of-service attacks.....	151
deployment scenarios	
enterprise service portal.....	216
destination class usage.....	194
DHCP (Dynamic Host Configuration Protocol)	
address assignment.....	76
classification scripts. <i>See</i> classification scripts	
options.....	66

profiles	
SRC CLI.....	69
subscribers	
login process.....	15
logout process.....	21
directory server	
deployment with remote SAE.....	217
DirX directory server	
deployment with remote SAE.....	217
documentation set	
comments on.....	xxvii

## E

enterprise	
description.....	4
service parameters.....	209
Enterprise Manager Portal	
application protocols, managing.....	265
BoD subscriptions.....	245
configuration level.....	236
deployment settings.....	225
firewall exception rules	
stateful firewalls.....	283
stateless firewalls.....	272
firewall subscriptions.....	270
fixed addresses for outgoing traffic.....	295
help.....	235
NAT	
IP address.....	289, 290, 291
rules for traffic.....	291
NAT Address Management Portal.....	231
NAT rules.....	291, 296
overview.....	207, 235
policies.....	171
public IP addresses, configuring	
incoming traffic.....	294
outgoing traffic.....	293
schedules.....	237, 244
services.....	171
Enterprise Service Portal audit plug-in.....	232
enterprise service portals.....	205
accessing.....	212
architecture.....	215
configuring directory connections.....	223
data, displaying.....	301
deploying.....	231
improving performance.....	209
installing.....	222
managers.....	302, 305
operators, managing.....	305
overview.....	205
performance.....	209
planning.....	218
prerequisites.....	212, 221
server description.....	215

- value substitution.....211
- value substitution for policy parameters.....211
- See also* Enterprise Manager Portal
- enterprise subscribers.....3
  - adding
    - SRC CLI.....134
- enterprise subscribers, login process .....24
- enterprise tag library.....205, 207
- event publishers
  - configuring
    - SRC CLI.....121
  - default retailer authentication, configuring
    - SRC CLI.....122
  - default retailer DHCP authentication, configuring
    - SRC CLI.....122
  - description.....73
  - retailer-specific.....121
  - service-specific.....121
  - virtual router-specific.....121
- events, IT manager audit.....232
- example-simple.....49, 50, 59, 60, 61, 190
- external plug-ins
  - configuring
    - SRC CLI.....82

**F**

- firewall services
  - configuring.....173, 176
  - description.....270
  - managing in Enterprise Manager Portal.....270
  - policies for.....175
  - router support.....171
- flat file accounting plug-ins.....87
  - configuring
    - SRC CLI.....88
  - configuring headers
    - SRC CLI.....90
- flexible RADIUS accounting plug-ins.....87
  - attributes, defining
    - SRC CLI.....110
  - configuring.....93
  - RADIUS packets, defining.....109
- flexible RADIUS authentication plug-ins.....99
  - attributes, defining
    - examples.....118
    - SRC CLI.....110
  - configuring
    - SRC CLI.....102
  - RADIUS packets, defining
    - SRC CLI.....109
  - setting responses
    - SRC CLI.....118
- forwarding preferences.....189, 191

**G**

- general properties
  - configuring
    - SRC CLI.....156

**H**

- HTTP proxy.....149

**I**

- installing software
  - enterprise service portals.....222
- interface classification scripts. *See* classification scripts
- interfaces
  - callback.....209
- interim accounting, configuring on SAE.....35
- internal plug-ins
  - configuring
    - SRC CLI.....81
- IP addresses
  - acknowledging release.....308
  - assigning in NAT Address Management
    - Portal.....307
  - NAT services.....289, 290, 291
- IT manager
  - audit plug-in
    - events.....232
  - operators, managing.....302, 305

**J**

- Java development environment, Tomcat.....321
- JSP tag library. *See* enterprise tag library
- JUNOS routing platforms
  - CoS (Class of Service).....184
  - forwarding preferences.....191
  - managing traffic.....171
  - policies
    - basic BoD.....186
    - BOD.....187
    - BoD and VPNs.....193
    - firewall.....173
    - NAT.....182
  - provisioning services
    - prerequisites .....172
  - routing preferences.....189
  - services.....194
    - basic BoD.....187
    - BoD.....188
    - BoD and VPNs.....194
    - firewall.....173
    - NAT.....182

JUNOS routers	
policies	
basic BoD.....	186
BOD.....	187
quality of service (QoS).....	184
services	
basic BoD.....	187
BoD.....	188

**L**

LDAP authentication plug-in.....	99
configuring	
SRC CLI.....	107
limiting subscribers plug-in.....	99
configuring	
SRC CLI.....	99
listeners, defining.....	209
logging	
redirect server.....	166
login events, description.....	9
login process	
enterprise.....	24
residential.....	9, 11
DHCP.....	15
PPP.....	12
<i>See also</i> logout process, residential	
summary.....	10
login registration	
configuring	
SRC CLI.....	37
logout process, residential	
DHCP.....	21

**M**

managers	
configuring	
SRC CLI.....	139
control over all retailers.....	7
management privileges.....	5
subscribers and subscriptions.....	5
manuals	
comments on.....	xxvii

**N**

NAT (Network Address Translation).....	307
rules.....	296
services for Enterprise Manager Portal.....	182
services, IP address.....	289, 291, 307
types.....	291
VPNs.....	197
<i>See also</i> NAT Address Management Portal	

NAT Address Management Portal	
acknowledging IP address release.....	308
assigning IP addresses.....	307
deployment settings.....	225
Enterprise Manager Portal.....	231
overview.....	307
Network Address Translation. <i>See</i> NAT	
NIC (network information collector)	
enterprise service portals. with.....	209
notice icons.....	xxiii

**P**

parameters	
acquisition path and substitutions.....	210
sample enterprise service portal.....	318
performance	
enterprise service portals.....	209
plug-ins.....	232
activating service sessions.....	79
authentication	
configuring, SRC CLI.....	98
authorization	
configuring, SRC CLI.....	98
basic RADIUS accounting.....	87
configuring, SRC CLI.....	91
basic RADIUS authentication.....	98
configuring, SRC CLI.....	100
creating subscriber sessions.....	77
custom RADIUS accounting.....	87
configuring, SRC CLI.....	95
custom RADIUS authentication.....	99
configuring, SRC CLI.....	104
defining RADIUS packets	
SRC CLI.....	109
DHCP address assignment.....	76
event publishers. <i>See</i> event publishers	
external	
configuring, SRC CLI.....	82
flat file accounting.....	87
configuring, SRC CLI.....	88
flexible RADIUS accounting.....	87
configuring.....	93
flexible RADIUS authentication.....	99
configuring, SRC CLI.....	102
internal.....	74
authorization.....	74
configuring RADIUS peers, SRC CLI.....	85
configuring, SRC CLI.....	81
customizing RADIUS packets.....	74
how they work.....	73
pool.....	73
RADIUS attributes, SRC CLI.....	110
tracking.....	74
LDAP authentication.....	99
configuring, SRC CLI.....	107

limiting subscribers.....	99
configuring, SRC CLI.....	99
listeners.....	209
state synchronization	
configuring, SRC CLI.....	83
tracking	
configuring, SRC CLI.....	87
service sessions.....	79
subscriber sessions.....	77
<i>See also</i> Enterprise Service Portal audit plug-in	
policies	
basic BoD.....	186
BoD.....	187
BoD and VPNs.....	193
NAT.....	182
parameters.....	211
PPP subscribers	
login process.....	12
Web login.....	12
precedence	
subscriptions.....	171
prevention, use of unauthorized resources.....	149
privileges	
IT managers.....	205
protocols	
routing.....	197
proxy HTTP.....	149
proxy request management.....	149
public addresses, VPNs.....	197

## Q

QoS tracking plug-in.....	88
---------------------------	----

## R

RADIUS attributes	
defining in RADIUS plug-ins	
SRC CLI.....	110
examples, defining in RADIUS plug-ins	
SRC CLI.....	118
RADIUS client library, custom RADIUS plug-ins.....	74
RADIUS packets, customizing in plug-ins.....	74
RADIUS peers	
configuring in plug-ins	
SRC CLI.....	85
RADIUS plug-ins.....	87
authentication.....	98
UDP port.....	109
<i>See also</i> plug-ins	
redirect server	
assessing load	
C-Web interface.....	166
configuration statements	
SRC CLI.....	153

configuring	
SRC CLI.....	155
configuring DNS server for	
SRC CLI.....	162
configuring HTTP proxy support	
SRC CLI.....	163
configuring redundant	
SRC CLI.....	164
directory connection	
SRC CLI.....	157
failover.....	151
file extensions	
SRC CLI.....	160
logging	
SRC CLI.....	166
number of requests	
SRC CLI.....	159
protection against denial-of-service attacks.....	151
redundancy.....	151, 164
static route to router.....	151
traffic definition	
SRC CLI.....	158
verifying	
SRC CLI.....	161
redundancy	
redirect server.....	151
residential subscribers.....	3
adding	
SRC CLI.....	130
login process. <i>See</i> login process	
retailers	
subscribers.....	3
adding, SRC CLI.....	127
router subscribers.....	4
adding	
SRC CLI.....	137
routing instances.....	193
VPNs.....	197
routing scheme.....	197
rules, NAT.....	296

## S

SAE (service activation engine)	
classification scripts. <i>See</i> classification scripts	
identifying.....	206
login events.....	9
login process. <i>See</i> login process	
SAE (service activation engine), configuring	
interim accounting	
SRC CLI.....	35
login registration	
SRC CLI.....	37
multiple logins from same IP address	
SRC CLI.....	36

reduce reported session time	
SRC CLI.....	36
session reactivation timers	
SRC CLI.....	38
time for MAC address in cache	
SRC CLI.....	33
unauthenticated user DN	
SRC CLI.....	34
sample enterprise service portal	
configuring connection to directory .....	223
customizing.....	222
privileges.....	205
data, displaying.....	302
managing services.....	312
monitoring	
service sessions.....	316
subscriptions.....	315
networks for departments.....	317, 318, 319
overview.....	207
service parameters.....	315, 316
sample residential portal	
developing portal based on the sample.....	321
sending traffic to VPNs.....	263
service activation.....	209
service activation engine. <i>See</i> SAE	
service parameters, enterprise.....	209
service schedules	
Enterprise Manager Portal, in.....	237
service sessions	
activate-on-login.....	30, 79
activating and tracking.....	79
activating with Web application.....	26
enterprise, remote activation.....	31
services.....	270
basic BoD.....	184, 187
BoD.....	188, 189, 245
JUNOS routing platforms.....	194
BoD and VPNs.....	194
NAT.....	182
sample enterprise service portal, managing.....	312
<i>See also</i> firewall services	
sites.....	4, 5
subscriber.....	3
adding, SRC CLI.....	136
source class usage (SCU).....	194
state synchronization plug-in interface	
configuring	
SRC CLI.....	83
static IP subscribers, login process.....	22
static routing.....	197
subscriber classification scripts. <i>See</i> classification scripts	
subscriber folders.....	4
adding	
SRC CLI.....	129
subscriber sessions	
activating with Web application.....	27
creating and tracking.....	77
enterprise, creating and activating.....	24
subscribers	
adding	
SRC CLI.....	126
billing.....	194
enterprise.....	3
adding, SRC CLI.....	134
inheriting properties.....	126
inheriting subscriptions.....	126
residential.....	3
adding, SRC CLI.....	130
retailer.....	3
adding, SRC CLI.....	127
router.....	4
adding, SRC CLI.....	137
sites.....	3
adding, SRC CLI.....	136
types.....	3
subscriptions.....	4
access, configuring	
SRC CLI.....	143
activation order, specifying	
SRC CLI.....	125
enterprise hierarchy.....	212
multiple per subscriber.....	141
priority.....	171
sample enterprise service portal, creating.....	312
substitutions	
parameter acquisition path.....	210
use.....	211
support, technical <i>See</i> technical support	
<b>T</b>	
targets. <i>See</i> classification scripts	
technical support	
contacting JTAC.....	xxvii
text conventions defined.....	xxiii
Tomcat, as Java development environment.....	321
tracking plug-ins.....	74
configuring	
SRC CLI.....	87
<b>U</b>	
UDP ports	
RADIUS plug-ins.....	109
User Datagram Protocol. <i>See</i> UDP	
<b>V</b>	
validating	
VPNs.....	201

value substitution.....	211
virtual private networks. <i>See</i> VPNs <i>See</i> VPNs	
VPNs (virtual private networks)	
adding	
SRC CLI.....	199
configuration requirements.....	197
configuration statements.....	198
definition.....	198
directory.....	260
extranet clients, modifying	
SRC CLI.....	200
identifiers.....	193
invalid subscriptions.....	201
modifying.....	200, 260
VPN to which router sends traffic.....	263
routing schemes.....	197
sending traffic.....	263
stopping router from sending traffic.....	264
using NAT.....	197
validating.....	201

