**SRC-PE Software**

# Getting Started Guide

*Release 2.0.x*

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA
408-745-2000
**www.juniper.net**

## Software License

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

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

For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.

## END USER LICENSE AGREEMENT

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

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

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

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

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

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

    c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface,

processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# Table of Contents

## Part 2        Managing Your C-series Controller

**Chapter 7**    **Configuring Remote Access to a C-series Controller with the SRC CLI**    **71**

**Part 3**    **Managing SRC Licenses**

**Chapter 8**    **Overview of SRC Licenses**    **83**

**Chapter 9**    **Overview of the SRC License Server**    **85**

**Chapter 10**    **Installing Licenses for C-series Controllers**    **89**

# About This Guide

This preface provides the following guidelines for using the *SRC-PE Software Getting Started Guide.*

- Objectives on page xix

- Audience on page xix

- Documentation Conventions on page xx

- Related Juniper Networks Documentation on page xxi

- Obtaining Documentation on page xxiii

- Documentation Feedback on page xxiv

- Requesting Support on page xxiv

## Objectives

This guide provides the information that you need to install and perform basic configuration of the Session and Resource Control (SRC) software. It also provides information about how to configure the SRC software in a number specific use scenarios.

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

## Audience

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

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

## Documentation Conventions

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

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

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

**Table 1:  Notice Icons**

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

**Table 2:  Text Conventions**

| Convention | Description | Examples |
|---|---|---|
| Bold typeface | ■ Represents keywords, scripts, and tools in text.<br>■ Represents a GUI element that the user selects, clicks, checks, or clears. | ■ Specify the keyword **exp-msg**.<br>■ Run the **install.sh** script.<br>■ Use the **pkgadd** tool.<br>■ To cancel the configuration, click **Cancel**. |
| **Bold sans serif typeface** | Represents text that the user must type. | user@host# **set cache-entry-age** *cache-entry-age* |
| Monospace sans serif typeface | Represents information as displayed on your terminal's screen, such as CLI commands in output displays. | ```nic-locators {
  login {
    resolution {
      resolver-name /realms/login/A1;
      key-type LoginName;
      value-type SaeId;
    }``` |

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

| Convention | Description | Examples |
|---|---|---|
| Regular sans serif typeface | ▪ Represents configuration statements.<br>▪ Indicates SRC CLI commands and options in text.<br>▪ Represents examples in procedures.<br>▪ Represents URLs. | ▪ system ldap server {<br>    stand-alone;<br>▪ Use the **request sae modify device failover** command with the **force** option.<br>▪ user@host# . . .<br>▪ http://www.juniper.net/techpubs/software/ management/sdx/api-index.html |
| *Italic sans serif typeface* | Represents variables in SRC CLI commands. | user@host# **set local-address** *local-address* |
| Angle brackets | In text descriptions, indicate optional keywords or variables. | Another runtime variable is < gfwif > . |
| Key name | Indicates the name of a key on the keyboard. | Press Enter. |
| Key names linked with a plus sign ( + ) . | Indicates that you must press two or more keys simultaneously. | Press Ctrl + b. |
| *Italic typeface* | ▪ Emphasizes words.<br>▪ Identifies chapter, appendix, and book names.<br>▪ Identifies distinguished names.<br>▪ Identifies files, directories, and paths in text but not in command examples. | ▪ There are two levels of access: *user* and *privileged*.<br>▪ *Chapter 2, Services.*<br>▪ *o = Users, o = UMC*<br>▪ The */etc/default.properties* file. |
| Backslash | At the end of a line, indicates that the text wraps to the next line. | Plugin.radiusAcct-1.class = \<br>net.juniper.smgt.sae.plugin\<br>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.

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

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

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

| Document | Description |
| --- | --- |
| **Core Documentation Set** | |
| *C2000 and C4000 Hardware Guide* | Describes the hardware platforms and how to install, maintain, replace, and troubleshoot them. The guide also includes specifications. |
| *C2000 and C4000 Quick Start Guide* | Describes how to get the C-series Controller up and running quickly. Intended for experienced installers who want to expedite the installation process. |
| *SRC-PE Getting Started Guide* | Describes the SRC software, how to set up an initial software configuration, 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. |
| *SRC-PE CLI User Guide* | 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. |
| *SRC-PE Network Guide: SAE, Juniper Networks Routers, NIC, and SRC-ACP* | 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 for using JUNOSe routers and JUNOS routing platforms in the SRC network. |
| *SRC-PE Integration Guide: Network Devices, Directories, and RADIUS Servers* | Describes how to integrate external components—network devices, directories, and RADIUS servers—into the SRC network. The guide provides detailed information about integrating specific models of the external components. |
| *SRC-PE Services and Policies Guide* | 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. |
| *SRC-PE Subscribers and Subscriptions Guide* | 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. |
| *SRC-PE Monitoring and Troubleshooting Guide* | 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. |
| *SRC-PE Solutions Guide* | 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. |
| *SRC-PE CLI Command Reference, Volume 1* *SRC-PE CLI Command Reference, Volume 2* | 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. |
| *SRC-PE NETCONF API Guide* | 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. |
| *SRC-PE XML API Configuration Reference* | 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). |
| *SRC-PE XML API Operational Reference* | 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). |

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

| Document | Description |
|---|---|
| *SRC-PE Comprehensive Index* | Provides a complete index of the SRC guides, excluding the *C-series Hardware Guide*, the *SRC CLI Command Reference*, the *SRC-PE NETCONF API Guide*, the *SRC-PE XML API Configuration Reference*, and the *SRC-PE XML API Operational Reference*. |
| **Application Library** | |
| *SRC Application Library Guide* | Describes how to install and work with applications that you can use to extend the capabilities of the SRC software. The guide documents the following applications: SRC-SG (SOAP Gateway) Web applications, an application to provide threat mitigation, an application to provide tracking and QoS control at the application level by integrating the SRC software with the Ellacoya deep packet inspection (DPI) platform, and an application to control volume usage. |
| **Release Notes** | |
| *SRC-PE Release Notes* <br><br> *SRC Application Library Release Notes* | In the *Release Notes*, 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 *Release Notes* differs from the information found in the documentation set, follow the *Release Notes*. <br><br> Release notes are included in the corresponding software distribution and are available on the Web. |

## Obtaining Documentation

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

http://www.juniper.net/

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

## Documentation Feedback

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

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

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

- Document name

- Document part number

- Page number

- Software release version

## Requesting Support

For technical support, open a support case using the Case Manager link at

http://www.juniper.net/support/

or call 1-888-314-JTAC (from the United States, Canada, or Mexico) or 1-408-745-9500 (from elsewhere).

**Part 1**
# SRC Overview

## Chapter 1
# SRC Product Overview

This chapter provides a general overview of the Session and Resource Control (SRC) software, formerly the Service Deployment System (SDX) software, and of the C-series Controllers. Topics include:

- SRC Product Description on page 3

- SRC Product Features and Benefits on page 6

## SRC Product Description

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

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

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

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

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

When integrated with the Juniper Networks Intrusion Detection and Prevention (IDP) system by using the SRC application library, an SRC-managed network can protect against malicious traffic that can affect overall network performance. When integrated with Juniper Networks Instant Virtual Extranet (IVE) Host Checker integration application, an SRC-managed network can verify that the subscriber systems used to connect to a service provider comply with a service provider's policies.

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

1. Creating innovative, revenue-generating services

2. Delivering numerous on-demand services to subscribers

3. Tracking services with intelligent accounting applications

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

**Figure 1: SRC Network with C-series Controllers**
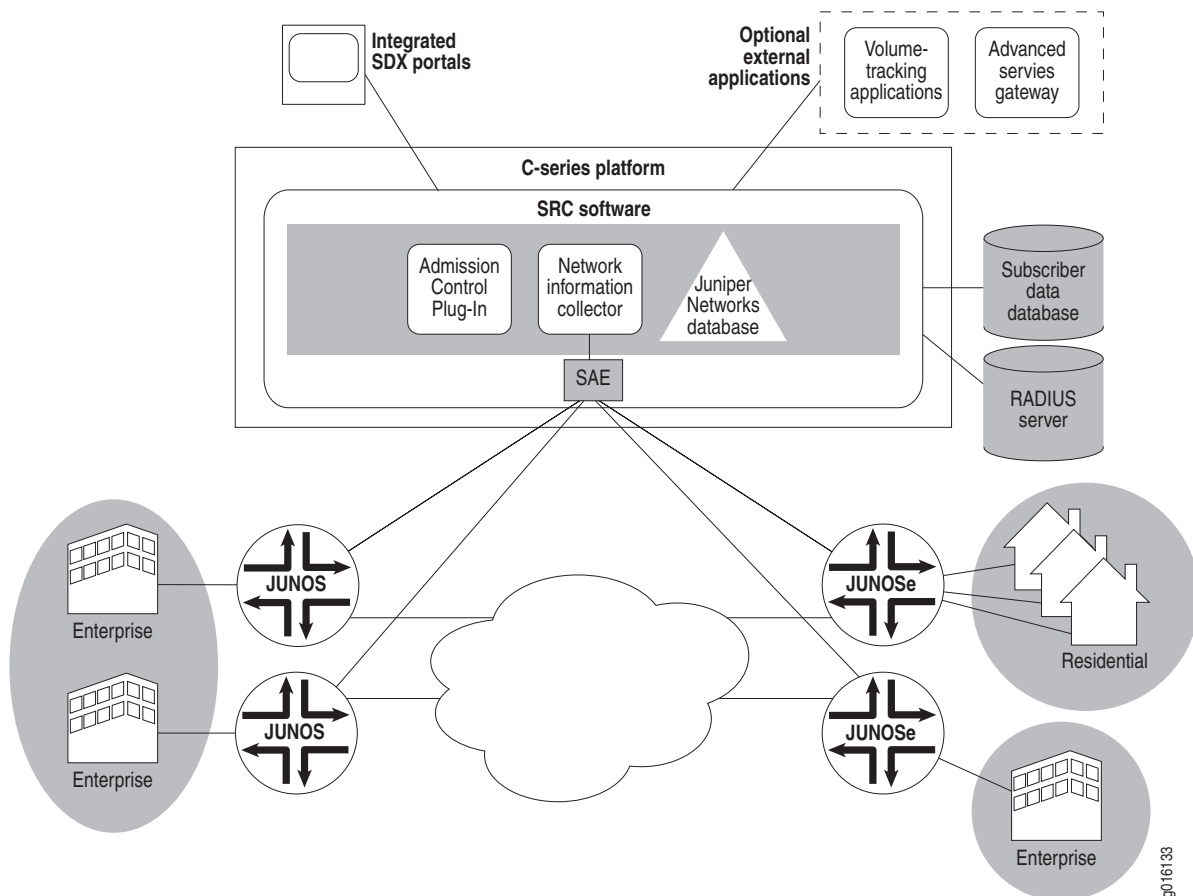
In addition, the SRC software can be used in a PacketCable MultiMedia (PCMM) environment to simplify other management tasks, such as:

1. Creating end-to-end service quality for subscribers in a PCMM environment

2. Marking traffic forwarded from specified systems, such as video servers

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

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

**Figure 2: SRC-Managed PCMM Network**
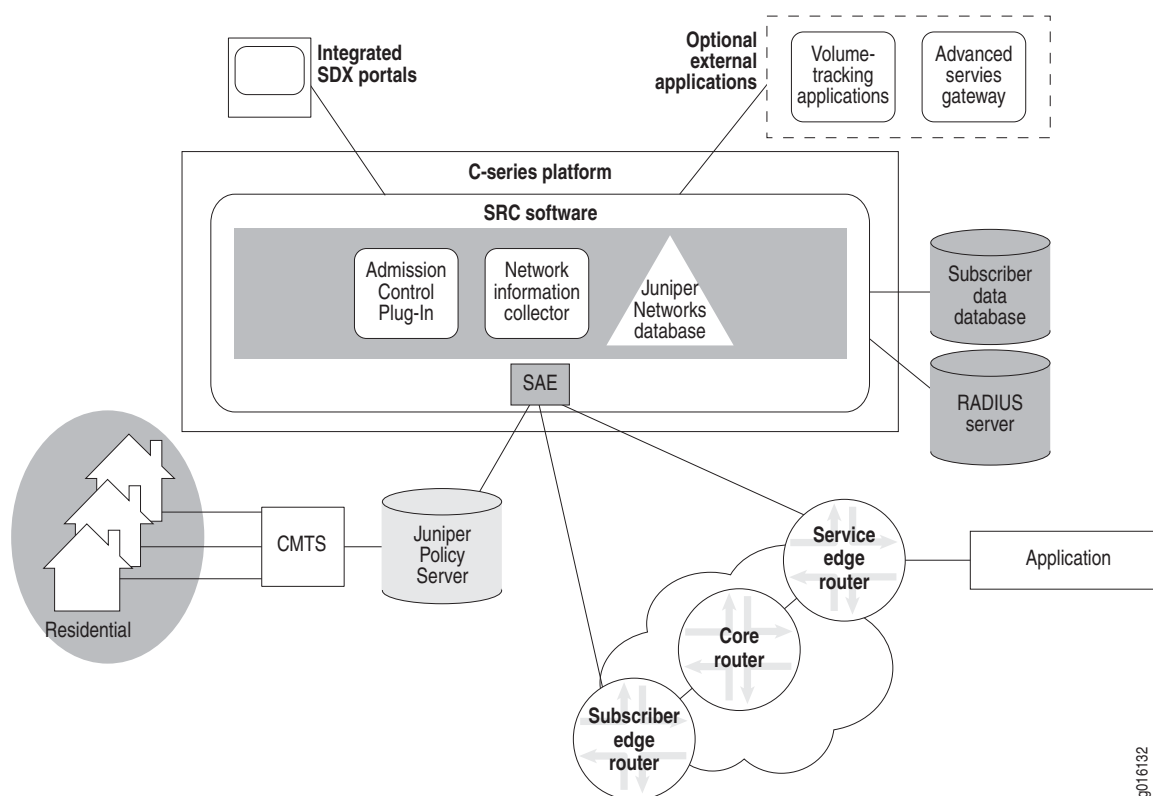
# SRC Product Features and Benefits

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

**Table 4: SRC Software Features and Benefits**

| Feature | Benefit |
| --- | --- |
| Carrier-class architecture | ■ Provides a distributed architecture for flexibility.<br>■ Integrates with provider subscriber databases and supports customer profiles to define subscriber groups.<br>■ Instantiates each key server multiple times for either load distribution or failover.<br>■ Facilitates a variety of wholesale and retail models.<br>■ Uses CLI and GUI management and monitoring. |
| Seamless integration with operations support systems (OSS) | ■ Uses modular design and standards-based interfaces such as HTML/XML, RADIUS, LDAP, Common Object Request Broker Architecture (CORBA), and Simple Object Access Protocol (SOAP).<br>■ Supports open interfaces and mediation mechanisms to facilitate system integration with diverse OSS applications, including systems for subscriber management, customer care, order entry, provisioning, billing, security, and sales support.<br>■ Ensures smooth integration with back office solutions. (We partner with leading providers of telecommunications, RADIUS/authentication, authorization, and accounting (AAA), and billing systems to offer these services.) |
| Financial advantages | ■ Avoids the misconception of a one-size-fits-all Internet access model by offering compelling content options with the appropriate level of bandwidth, quality of service (QoS), and network functions (for example, security, traffic prioritization, and filtering).<br>■ Allows providers to hold down on capital expenditures and operating expenses by offering a wide range of flexible services, tools, billing models, and revenue streams, and by using the same network infrastructure. |
| Optimal scalability | ■ Scales for rapidly growing networks and subscriber bases.<br>■ Works with JUNOSe routers, JUNOS routing platforms, and PCMM-compliant CMTS devices to automatically provision and support thousands to millions of subscribers in a distributed environment.<br>■ Uses zero-touch subscriber provisioning, which removes the roadblocks that can slow large-scale broadband subscriber acquisition. |
| Easy-to-build wholesale-retail model | ■ Provides a transparent infrastructure to Internet service provider (ISP), application service provider (ASP), and content partners, which lets partners retain ownership and management of their subscriber bases.<br>■ Frees partners from the responsibility of handling network operations so that they can focus solely on service delivery. |
| Intelligent accounting | ■ Tracks service usage to enable rich and creative tariff models.<br>■ Supports customer care, rating and billing, security, and sales support systems.<br>■ Simplifies the task of collecting and managing retailer and subscriber accounting data.<br>■ Uses a configuration interface to choose the policy rules to be used for accounting per interface direction (ingress and egress).<br>■ Activates multiple service sessions simultaneously for a given subscriber; each session can be tracked separately.<br>■ Supports plug-in software that gives service providers the ability to extend system capabilities.<br>■ Allows for flexible accounting rules. |

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

| Feature | Benefit |
| --- | --- |
| Easy subscriber management | ■ Uses configuration interfaces for service definition and subscriber management.<br><br>■ Uses a directory that acts as a central repository of customer information and service portal configurations. The directory stores router information.<br><br>■ Works with JUNOSe routers, JUNOS routing platforms, and PCMM-compliant CMTS to collect subscribers' credentials and queries the RADIUS server for authentication and authorization.<br><br>■ Accommodates and manages a very large number of subscribers (for example, a typical subscriber base may be in the millions). |
| Dynamic policy management | ■ Gives subscribers consistent service experience across the network, regardless of the actual network deployment and the mode of connection to the network.<br><br>■ Enables real-time provisioning and collection of subscriber usage data.<br><br>■ Offers high availability based on seamless failover.<br><br>■ Uses configuration interfaces to define policies and store them in a central repository.<br><br>■ Provides robust support for access, QoS, and activation of new services on demand with configurable policies.<br><br>■ Performs dynamic policy decisions while services are activated, leveraging on the directory content to make policy decisions.<br><br>■ Provides end-to-end service levels across the network. |
| Web-based portal | ■ Creates dynamic Web pages, giving subscribers personalized displays to select services on demand.<br><br>■ Offers branding opportunities for network provider/service provider partners.<br><br>■ Identifies subscribers, grants them access to defined services, and maps their selected service(s) to the network by means of dynamically provisioned policies.<br><br>■ Allows portals to be deployed in any application server with support for CORBA or SOAP.<br><br>■ Provides a starting point for rapid portal development through documented sample portals supplied for Java 2 Enterprise Edition (J2EE) application servers. |
| Easy service creation | ■ Uses a policy editor to enable the definition of various policy objects.<br><br>■ Uses configuration interfaces to define new services and to create service templates for future use. Service templates provide the service-provisioning information that configures the router for efficient, real-time delivery of that service.<br><br>■ Provides flexible service creation, a reusable service library, and automated service implementation.<br><br>■ Allows providers to define policies once and apply them network-wide. |
| Service activation engine (SAE) | ■ Translates services into lists of policies to be enforced on the router.<br><br>■ Initiates the service-usage data-collection process.<br><br>■ Customizes services with differentiated QoS and policies.<br><br>■ Collects usage data (time and volume) by subscriber and service to enable differentiated rating and billing. |

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

| Feature | Benefit |
| --- | --- |
| Flexible open interface support | ■ Allows an external entity or system to control the SRC software's behavior. |
| | ■ Uses application programming interfaces (APIs) to authenticate managers; to navigate among retailers, enterprises, and sites; and to create, delete, activate, and deactivate service sessions. |
| | ■ Provides a Common Open Policy Service for policy provisioning (COPS-PR) interface. |
| | ■ Integrates into a PCMM environment with support for CableLabs PCMM specification. |
| | ■ Extends policies to systems that do not have a supported router driver. |
| | ■ Integrates with IDP to protect network traffic. |
| | ■ Integrates with IVE to verify that the subscriber systems used to connect to a service provider comply with the service provider's policies. |
| | ■ Integrates with the Ellacoya Networks Deep Packet Inspection (DPI) platform to provide a traffic management solution that combines the advanced traffic identification and reporting features of the Ellacoya DPI with the SRC software's intelligent service policy enforcement. With this solution, providers can identify, monitor, and control traffic on a per-application or per-subscriber basis. |
| | ■ Integrates into an IP multimedia system (IMS) environment. The SRC software provides a Diameter protocol-based interface that allows the SRC software to integrate with services found on the application layer of IMS. |

**Chapter 2**

# SRC Components

This chapter provides a general overview of the components provided in the SRC software. Topics include:

- SRC Component Overview on page 9

- SRC Server Components on page 13

- SRC Repository for Data on page 15

- SRC Configuration and Management Tools on page 17

- SRC Service Management Applications on page 22

- SRC Programming Interfaces on page 25

- SRC Authentication and Accounting Applications on page 27

- SRC Demonstration Applications on page 30

- SRC Auxiliary Applications on page 35

## SRC Component Overview

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

Table 5 gives a brief description of the components that make up the SRC software and shows which components run on C-series Controllers and Solaris platforms. For more information, see the following sections.

**Table 5: Descriptions of SRC Components**

| Component | Description | SRC Software on C-series Controllers | SRC Software on Solaris Platforms |
|---|---|---|---|
| **Server Components** | | | |
| Service activation engine (SAE) | ■ Authorizes, activates, and deactivates subscriber and service sessions by interacting with systems such as Juniper Networks routers, cable modem termination system (CMTS) devices, RADIUS servers, and directories.<br><br>■ Collects accounting information about subscribers and services from routers, and stores the information in RADIUS accounting servers, flat files, and other accounting databases.<br><br>■ Provides plug-ins and application programming interfaces (APIs) for starting and stopping subscriber and service sessions and for integrating with systems that authorize subscriber actions and track resource usage. | X | X |
| Juniper Policy Server (JPS) | Acts as a policy decision point (PDP) and policy enforcement point (PEP) that manages the relationships between application managers and CMTS devices in a PCMM environment. | X | X |
| Network information collector (NIC) | Collects information about the state of the network and can provide a mapping from a given type of network data to another type of network data. | X | X |
| Redirect Server | Redirects HTTP requests received from IP Filter to a captive portal page. | X | X |
| **Repository** | | | |
| Directory | Provides a repository of subscriber information, services, policies, and service portal configurations. The SRC software uses the Lightweight Directory Access Protocol (LDAP) for interactions with the directory. | For subscriber data | X |
| Juniper Networks Database | Repository for SRC data on a C-series Controller. | X | X |
| **SRC Configuration and Management Tools** | | | |
| SRC command line interface (CLI) | Provides a way to configure the SRC software on a C-series Controller and SRC components on a Solaris platform from a JUNOS-like CLI. The SRC CLI includes the policies, services, and subscribers CLI, which has separate access privileges. | X | X |
| C-Web interface | Provides a way to configure, monitor, and manage the SRC software on a C-series Controller through a Web browser. The C-Web interface includes a policies, services, and subscribers component, which has separate access privileges. | X | X |
| Local configuration tools | Generates start scripts and initial local configuration for newly installed SAEs and SNMP agents. | | X |
| Policy Editor and management | Defines how the router or CMTS device treats subscriber traffic. Gives service providers the ability to define and modify policies and to store these policies in the directory. | CLI and C-Web format | CLI and GUI formats |

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

| Component | Description | SRC Software on C-series Controllers | SRC Software on Solaris Platforms |
|---|---|---|---|
| SDX Admin | Allows service providers to add, modify, and delete services, network definitions, and advanced configurations within the SRC software. | | X |
| Simple Network Management Protocol (SNMP) agent | Monitors system performance and availability. It runs on all the SRC hosts and makes management information available through SNMP tables and sends notifications by means of SNMP traps. | X | X |
| **Service Management Applications** | | | |
| SRC SOAP Gateway (SRC-SG) | Allows a gateway client—an application that is not part of the SRC network—to interact with SRC components through a Simple Object Access Protocol (SOAP) interface. (Available in the application library.) | | X |
| Deep Packet Inspection Integration application | Integrates Ellacoya Networks Deep Packet Inspection (DPI) platform to provide a traffic management solution that combines the advanced traffic identification and reporting features of the Ellacoya DPI with the SRC software's intelligent service policy enforcement. (Available in the application library.) | | X |
| Enterprise Audit Plug-In | Defines a callback interface, which receives events when IT managers complete specified operations. | | X |
| Enterprise Manager Portal | Allows service providers to provision services for enterprise subscribers on JUNOSe routers and JUNOS routing platforms and that allows IT managers to manage services. Enterprise Manager Portal can be used with NAT Address Management Portal to allows service providers to manage public IP addresses for use with NAT services on JUNOS routing platforms and to all IT managers to make requests about public IP addresses through the Enterprise Manager Portal. | | X |
| Sample enterprise service portal | Lets service providers supply an interface to their business customers for managing and provisioning services. | | X |
| Threat Mitigation Portal (SRC-TMP) | Manages threats on the SRC-managed network using information provided by Juniper Networks IDP Sensors and Juniper Networks NetScreen-Security Manager. Provides the SRC Threat Mitigation Portal (SRC-TMP) and application to manage the response to attacks. (Available in the application library.) | | X |
| **SRC Programming Interfaces** | | | |
| NETCONF API | Allows you to configure or request information from the NETCONF server on a C-series Controller that runs the SRC software. | Applications developed with the NETCONF API run on a system other than a C-series Controller | |
| CORBA plug-in service provider interface (SPI) | Tracks sessions and enables linking the rest of the service provider's operations support system (OSS) with the SRC software so that the OSS can be notified of events in the life cycle of SAE sessions. | Hosted plug-ins only | X |
| CORBA remote API | Provides remote access to the SAE core API. | Applications that use these extensions to the SRC software run on a system other than a C-series Controller | |
| NIC access API | Performs NIC resolutions. | | |
| SAE core API | Controls the behavior of the SRC software. | X | X |

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

| Component | Description | SRC Software on C-series Controllers | SRC Software on Solaris Platforms |
|---|---|---|---|
| Script services | Provides an interface to call scripts that supply custom services such as provisioning policies on a number of systems across a network. | X | X |
| **Authorization and Accounting Applications** | | | |
| AAA RADIUS servers | Authenticates subscribers and authorizes their access to the requested system or service. Accepts accounting data—time active and volume of data sent—about subscriber and service sessions. | | X |
| SRC Admission Control Plug-In (SRC-ACP) | Authorizes and tracks subscribers' use of network resources associated with services that the SRC application manages. (Available in the application library.) | X | X |
| Flat file accounting | Stores tracking data to accounting flat files that can be made available to external systems that send the data to a rating and billing system. | X | X |
| SRC Volume Tracking Application (SRC-VTA) | Monitors subscriber resource usage to allow service providers to offer flexible usage quotas, limit bandwidth to subscribers that overuse network resources, and to notify subscribers who may have been compromised by viruses or worms that overuse network resources. (Available in the application library.) | | X |
| **Demonstration Applications (available in the SRC application library)** | | | |
| Intrusion detection and protection (IDP) integration applications | Integrates IDP into an SRC-managed environment to manage malicious traffic sent to or received by subscribers. | | X |
| IP television (IPTV) application | Demonstrates how the SRC software might be used to manage network resources for IPTV services. | X | X |
| Instant Virtual Extranet (IVE) Host Checker integration application | Integrates the IVE Host Checker into an SRC-managed environment to verify that the subscriber systems used to connect to a service provider comply with the service provider's policies. | | X |
| Monitoring Agent application | Integrates IP address managers, such as a DHCP server or a RADIUS server, into an SRC-managed network so that the SAE is notified about subscriber events. | | X |
| Prepaid Account Administration application | Manages prepaid accounts for the prepaid services demonstration application. | | X |
| Prepaid service application | Demonstrates how the SRC software might be used to manage prepaid accounts. | | X |
| Residential service selection portals | Provides a framework for building Web applications that allow residential and enterprise subscribers to manage their own network services. It comes with several full-featured sample Web applications that are easy to customize and suitable for deployment. | | X |
| Traffic-Mirroring Administration application | Manages and monitors mirroring tasks. | | X |
| Traffic-Mirroring Application | Mirrors subscriber traffic on any subscriber access platform supported by the SRC software. Provides the Traffic-Mirroring Administration portal to manage the mirroring of subscriber traffic. | | X |

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

| Component | Description | SRC Software on C-series Controllers | SRC Software on Solaris Platforms |
|---|---|---|---|
| **Auxiliary Applications** | | | |
| Application server | Enables J2EE applications, including Web applications, to be used with the SRC software. | These third-party applications run on a system other than a C-series Controller | |
| IP Filter | On Solaris platforms, filters traffic as specified by configured rules. | | |
| Other applications | Third-party applications created to run in an SRC environment. | | |

## SRC Server Components

The SRC server components are;

■ Service Activation Engine on page 13

■ Juniper Policy Server on page 14

■ Network Information Collector on page 14

■ Redirect Server on page 15

### *Service Activation Engine*

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

#### Policy and Service Management

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

### Accounting Support

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

### SAE Extensions

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

## Juniper Policy Server

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

## Network Information Collector

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

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

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

**Table 6: Available NIC Resolutions**

| Key | Value |
| --- | --- |
| Accounting ID of a subscriber | SAE reference |
| Enterprise's distinguished name (DN | SAE reference |
| Subscriber's IP address | Subscriber's login name |
| Subscriber's IP address | Accounting ID |

**Table 6: Available NIC Resolutions   (continued)**

| Key | Value |
| --- | --- |
| Subscriber's IP address for situations in which the SAE manages the subscriber | SAE reference |
| Subscriber's IP address for situations in which the SAE manages the interface that the subscriber uses, but not the subscriber | SAE reference |
| Subscriber's login name | SAE reference |
| Subscriber's primary username | SAE reference |

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

### *Redirect Server*

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

## SRC Repository for Data

The Juniper Networks database on a C-series Controller or a Solaris platform contains most SRC configuration data, including license information, service definitions, policies, and SAE configurations, as well as user profile data. You use user profiles to categorize groups of users, allowing you to keep your user data separate in your own directory. If you run the SRC software on a Solaris platform, you can configure it to use a third-party directory rather than the Juniper Networks database.

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

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

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

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

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

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

### *Directory as Repository for SRC Data*

For the SRC software running on a Solaris platform to work with a third-party directory, all the information must be provisioned in the directory. We provide tools, such as the SRC CLI, SDX Admin, and Policy Editor, to help provision the information into the directory. An external OSS can also provision all or part of the information directly through the LDAP interface.

#### LDAP Version 3

The SRC software on Solaris platforms employs LDAP version 3 to interact with third-party directories. The SRC software is compatible with any LDAP version 3–compliant directory, but some integration work might be necessary, such as for the following requirements:

- Schema extension—This mandatory requirement must be completed as outlined in *Integrating Directories* in the *SRC Integration Guide: Network Devices, Directories, and RADIUS Servers*.

- Access control—This is an important function for wholesale/retail applications and for enterprise scenarios.

- Virtual list view control—Requirements are described in LDAP Extensions for Scrolling View Browsing of Search Results—draft-ietf-ldapext-ldapv3-vlv-09.txt (June 2003 expiration). This requirement is important when you run the eventing system.

#### Prepackaged Integration

For SRC software installed on Solaris platforms, we provide prepackaged integration for:

- DirX directory server—Optional add-on package offered with the SRC software. This directory is based on the Siemens DirX Solutions product.

- eTrust Directory—Optional add-on package offered with the SRC software. The directory server is a product of Computer Associates International, Inc.

- Oracle Internet Directory—Optional add-on package offered with the SRC software. This directory is a software component in the Oracle Application Server 10g.

■ Sun ONE Directory Server—Sun Microsystems product included with Solaris 9. The SRC software's Sun ONE Directory Server add-on package also contains the UMC schema for Sun ONE Directory Server.

### Third-Party Directory Servers

For information about the directory servers that you can integrate with the SRC software running on a Solaris platform, see the *SRC-PE Release Notes.* The SRC software is designed to work with directory servers that are robust, scalable, and suitable for the carrier market.

## SRC Configuration and Management Tools

The SRC software provides the following configuration and management tools:

■ SRC CLI—C-series Controller and SRC software on a Solaris platform

■ C-Web Interface—C-series Controller and SRC software on a Solaris platform

■ Local Configuration Tools—Solaris platform only

■ Policy Editor and Management—Solaris platform only

■ SDX Admin—Solaris platform only

■

### SRC CLI

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

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

### C-Web Interface

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

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

**Figure 3:  C-Web Page for SAE Configuration**



## Local Configuration Tools

The local configuration tool allows administrators to configure local files on the hosts that support SRC components such as the SAE and NIC. For some SRC components, the local configuration tool also reads data from and writes information to the directory.

Figure 4 shows an example of the configuration tool.

**Figure 4:  Sample Configuration Tool Window**
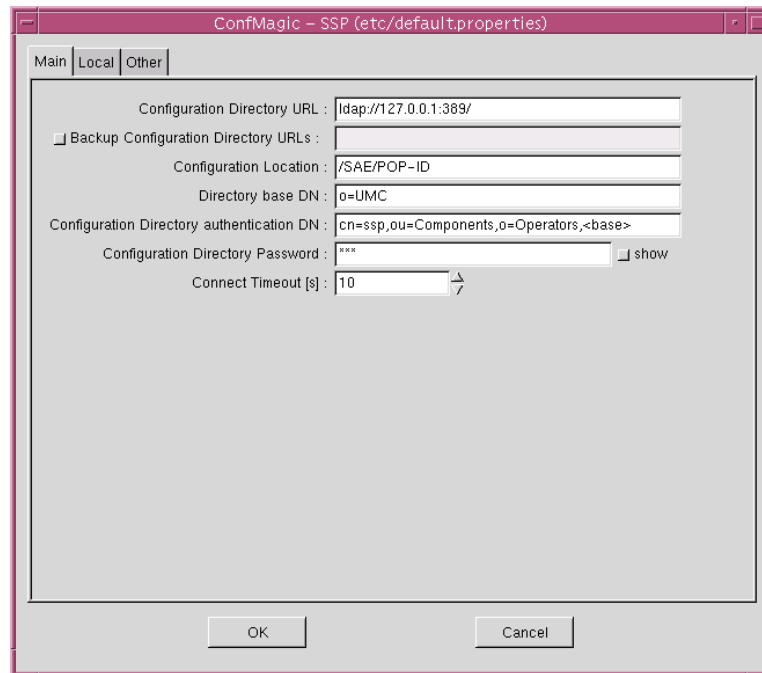


## Policy Editor and Management

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

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

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

The Policy Editor application allows easy specification and validation of policies. Policy Editor stores policies in a central repository, or directory. It works closely with a policy engine, which performs dynamic policy decisions while activating services, leveraging on the directory content to decide which policies to use in a given context.

Figure 5 provides an example of Policy Editor. You can also configure policies with the SRC CLI.

**Figure 5:  Sample Policy Editor Window**
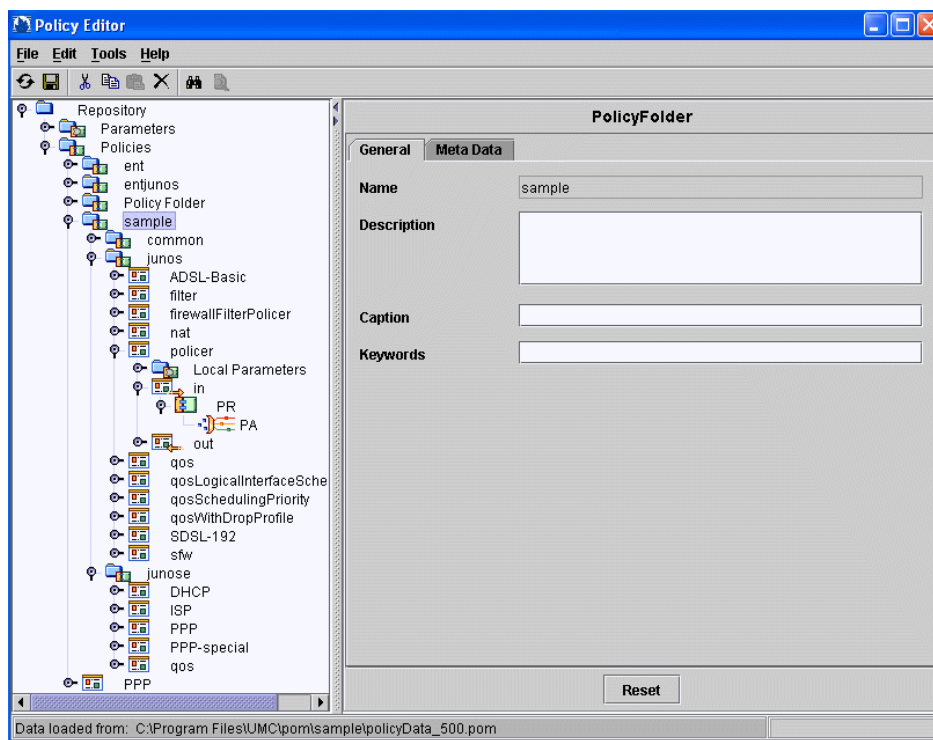


## SDX Admin

SDX Admin allows service providers to add, modify, and delete services, network definitions, and advanced configurations within the SRC software. For small installations and demonstrations, you can use SDX Admin to create and modify retailers, subscribers, and subscriptions to services.

Figure 6 shows the two panes that make up the SDX Admin interface:

■ Navigation pane—Displays objects in a hierarchical tree. This pane is used to select and navigate through objects or the directory.

■ Content pane—Displays details of objects that appear in the navigation pane. This pane is used to display and modify information about objects.

**Figure 6: SDX Admin Panes**
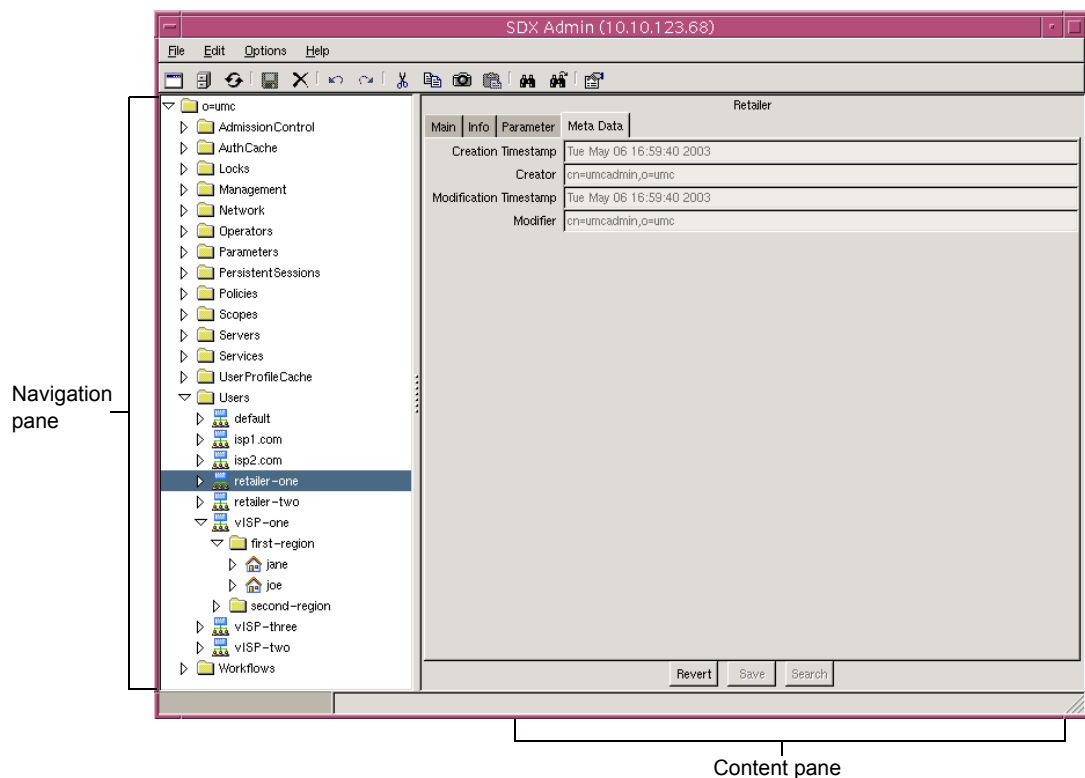


From SDX Admin, for example, you can create and define a new service, define a grouping of virtual routers, or define a new retailer.

Also, using SDX Admin, administrators can set the language for SRC interfaces so that information can be displayed in the language of choice. The language environment is set globally on the host that is running the SDX Admin software.

## SDX SNMP Agent

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

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

## SRC Service Management Applications

The SRC software and SRC application library provide the following service management applications:

- SRC SOAP Gateway on page 22

- Deep Packet Inspection Integration Application on page 22

- Enterprise Audit Plug-In on page 23

- Enterprise Manager Portal on page 24

- Sample Enterprise Service Portal on page 24

- Threat Mitigation Portal on page 24

### SRC SOAP Gateway

The SRC SOAP Gateway (SRC-SG) allows a gateway client—an application that is not part of the SRC network—to interact with SRC components through a SOAP interface. This feature is useful for business-to-business situations, such as a wholesaler-retailer environment. Typically, the wholesaler owns and administers the SRC components, and the retailer maintains a database of subscribers. Retailers purchase services from one or more wholesalers and sell the services to their subscribers. Using information provided by the wholesaler, the retailer creates a gateway client to communicate with the components in the SRC software.

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

### Deep Packet Inspection Integration Application

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

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

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

### Benefits of the DPI Integration

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

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

  Once subscribers have used their quota, you can apply a policy that throttles back on or blocks a subscriber's peer-to-peer traffic, bill the subscriber for additional usage, or allow the subscriber to purchase additional quota.

- Limit the total percentage of network resources that a specific type of traffic is allowed to consume.

- Provide higher or guaranteed levels of performance for premium services by applying QoS control to application sessions. For example, two subscribers start an Xbox Live session. The Ellacoya DPI platform detects activity for this application, and sends application usage counters to the SRC software. The SRC software pushes policies that deliver a specific level of QoS for this application session to a router or other network device.

- Charge subscribers based on their usage of premium content-based services.

- Offer and charge for tiered Internet services based on both speed and application.

- Better support network planning functions by gaining an in depth understanding of traffic flows and patterns on a per subscriber and per application basis.

## *Enterprise Audit Plug-In*

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

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

### Enterprise Manager Portal

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

Figure 7 shows a sample page in the Enterprise Manager Portal.

**Figure 7: Sample Page in Enterprise Manager Portal**
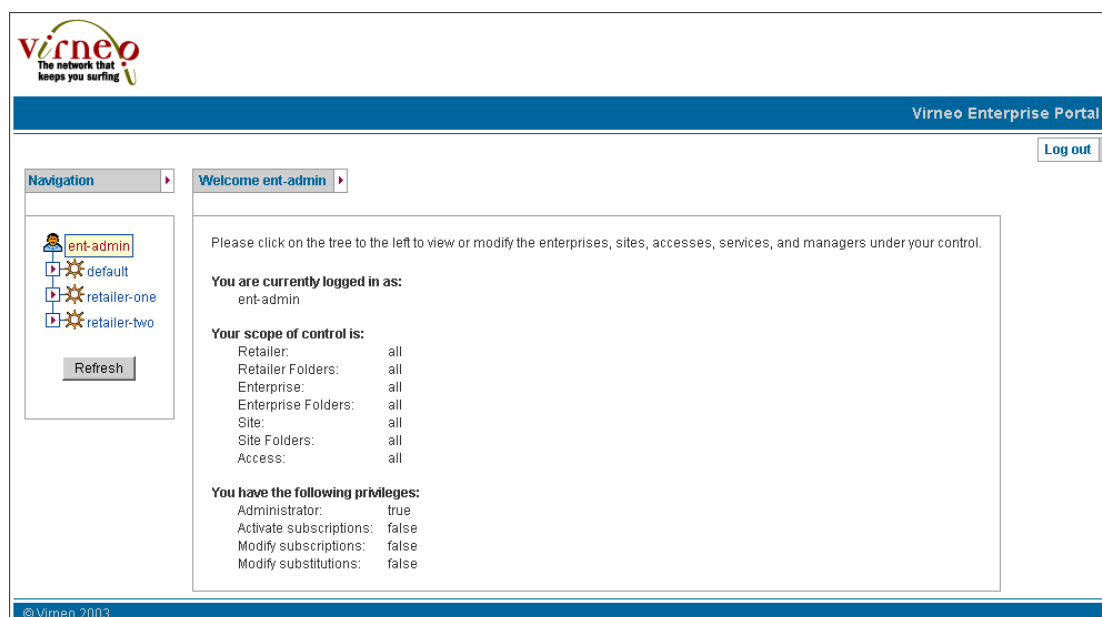


You can use the Enterprise Manager Portal with the NAT Address Management Portal to allow service providers to manage public IP addresses for use with NAT services on JUNOS routing platforms and to allow IT managers to make requests about public IP addresses through the Enterprise Manager Portal. The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

### Sample Enterprise Service Portal

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

### Threat Mitigation Portal

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

The application uses these components to respond to threats:

■ Juniper Networks Intrusion Detection and Prevention (IDP) Sensors to detect the threats.

■ Juniper Networks NetScreen-Security Manager to manage the IDP Sensors and to signal the SRC-TMP when a threat is detected.

■ The SRC-TMP, which is the user interface for the application, to manage threats and act upon them.

## SRC Programming Interfaces

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

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

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

### NETCONF API

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

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

### CORBA Plug-In SPI

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

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

### CORBA Remote API

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

- SAE access interface module—Provides remote access to the SAE core API

- Java script interface module—Allows you to control the SAE with a Java script

- Python script interface module—Allows you to control the SAE with a Python script

- Event notification interface module—Allows you to integrate the SAE with external IP address managers

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

### NIC Access API

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

Chapter 2: SRC Components

### SAE Core API

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

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

### Script Services

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

- Provisioning of layer 2 devices, such as digital subscriber line access multiplexers (DSLAMs).

- Setting up of network connections such as MPLS tunnels.

- Provisioning of policies for network devices that do not have a supported SAE router driver.

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

## SRC Authentication and Accounting Applications

The following components help to provide accounting or authentication:

- AAA RADIUS Servers on page 27

- SRC Admission Control Plug-In on page 28

- Flat-File Accounting on page 29

- SRC Volume Tracking Application on page 29

### AAA RADIUS Servers

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

SRC Authentication and Accounting Applications ■ 27

We recommend that service providers move to a more sophisticated RADIUS server, such as the Interlink RAD-Series RADIUS or the Juniper Networks Steel-Belted Radius/SPE server, or integrate the SRC software with some other currently used RADIUS server. The SRC software works with other AAA RADIUS systems; however, we test and support system integration only with RAD-Series RADIUS Server and Steel-Belted Radius/SPE server software.

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

- RFC 2882—Network Access Servers Requirements: Extended RADIUS Practices (July 2000)

- RFC 2869—RADIUS Extensions (June 2000)

- RFC 2865—Remote Authentication Dial In User Service (RADIUS) (June 2000)

When a provider uses the SDX schema to integrate the RADIUS server with the directory, the SRC software provides the highest level of subscriber control. For example, when subscriber information is stored in the directory, the SRC software can provide a list of services for each individual subscriber.

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

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

### SRC Admission Control Plug-In

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

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

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

Figure 8 shows a typical network topology.

**Figure 8: Position of SRC-ACP in the Network**
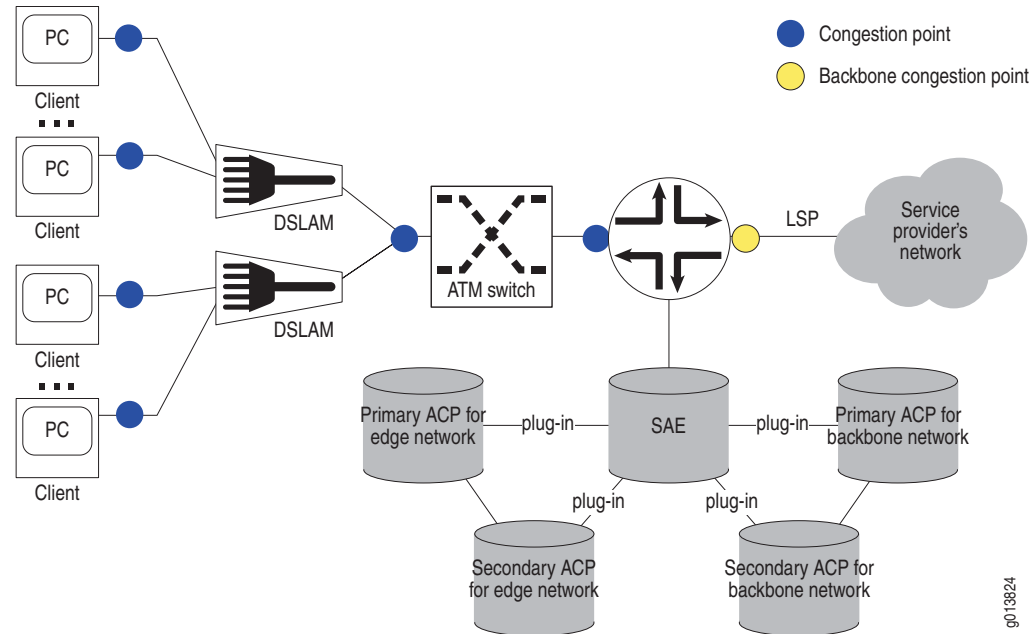


## Flat-File Accounting

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

## SRC Volume Tracking Application

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

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

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

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

**Managing Subscriber Accounts with Web Portals**

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

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

## SRC Demonstration Applications

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

- IDP Integration Applications on page 30

- IPTV Application on page 31

- IVE Host Checker Integration Application on page 31

- Monitoring Agent Application on page 31

- Prepaid Account Administration Application on page 31

- Prepaid Service Application on page 31

- Residential Service Selection Portals on page 32

- Traffic-Mirroring Administration Application on page 34

- Traffic-Mirroring Application on page 34

### IDP Integration Applications

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

- Applying policies, such as policies that limit subscriber bandwidth, to subscriber interfaces

- Sending e-mail messages that describe the nature of an incident

- Redirecting Web requests to an IDP captive portal where a page provides the source or destination of the problem traffic and a description of the incident

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

### IPTV Application

The IPTV application is a sample application that demonstrates how to use extended features of SRC-ACP and the SAE to manage network resources. You can use SRC-ACP to perform call admission control, allocate bandwidth, and initialize and execute applications. You can use the SAE to set up and manage LSP tunnels with router drivers and script service.

### IVE Host Checker Integration Application

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

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

### Monitoring Agent Application

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

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

- A subscriber logs in

- An address assignment is terminated

### Prepaid Account Administration Application

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

- View or update information about current accounts

- Create new accounts

- Clear expired accounts

The SRC application library includes Prepaid Account Administration application.

### Prepaid Service Application

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

The demonstration application consists of two components:

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

- Prepaid Account Administration application—Allows you to manage prepaid accounts.

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

### Residential Service Selection Portals

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

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

The SRC software provides examples of residential portals.

Figure 9 shows a residential Web portal that could be created with the SRC software.

**Figure 9: Sample Residential Web Portal**
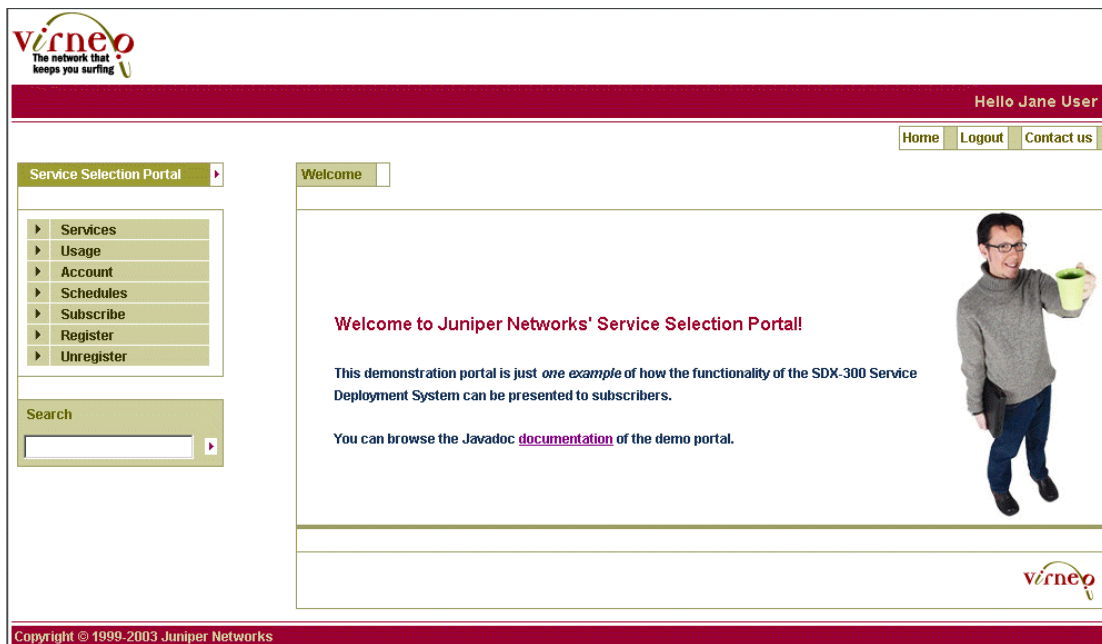


Web-based residential portals that you develop for the SRC software are compatible with PDAs. Figure 10 shows a login page for a sample residential portal that is being accessed from a PDA.

**Figure 10: Sample Login Page for a Residential Portal on a PDA**

### Traffic-Mirroring Administration Application

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

■ Specify the subscriber whose traffic is be mirrored and the IP addresses of the traffic to be mirrored

■ Manage currently active mirroring tasks

■ Manage pending actions

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

### Traffic-Mirroring Application

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

■ Monitor subscriber traffic and intercept traffic from a particular source or to a particular destination.

■ Take actions for subscribers with intercepted traffic by applying policies to the subscriber traffic.

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

## SRC Auxiliary Applications

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

- Application Server on page 35

- IP FIlter on page 35

- Other Applications on page 35

### *Application Server*

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

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

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

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

### *IP FIlter*

For SRC installations on a Solaris platform, IP Filter filters traffic as specified by Network Address Translation (NAT) rules and redirects incoming HTTP requests that meets criteria for the filter to the redirect server. The redirect server can then direct this traffic to a captive portal page.

### *Other Applications*

Other companies have created applications for use with the SRC software. For information about applications created by Juniper Networks partners, see

http://www.juniper.net/partners/content_partners.html

**Part 2**

# Managing Your C-series Controller

## Chapter 3

# Planning a Deployment of C-series Controllers

This chapter describes points to consider when you plan a deployment of C-series Controllers. Topics include:

-

-

-

## Components in an SRC Deployment

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

- Admission Control Plug-in

- Juniper Policy Server

- Network information collector

- Redirect server

- SAE

- SNMP agent

- Policies, services, subscribers, and subscriptions management

Applications that you develop and Web-based applications such as the Enterprise Manager Portal, SRC SOAP Gateway (SRC-SG) applications, and residential portals run on other systems. You configure these applications to communicate with the SRC software. Although the software on C-series Controllers provides a small Web application server, this server is for testing or demonstration purposes only; it is not designed to be used in a production environment.

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

Figure 11 illustrates the interaction of the various components in an SRC environment that includes a C-series Controller.

**Figure 11:  C-series Controller and Related Components**
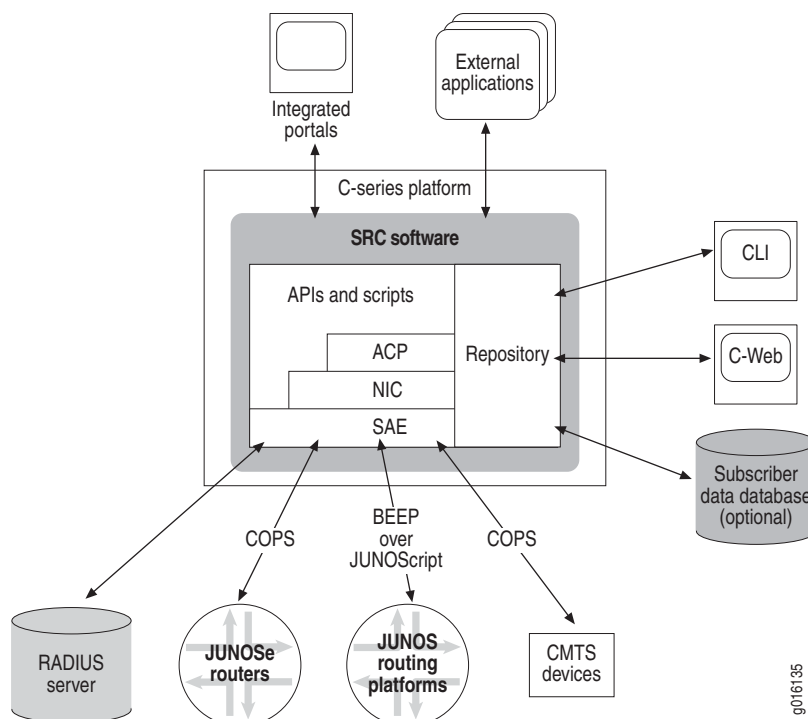


## Considerations When Planning a Deployment of C-series Controllers

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

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

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

■ High availability for the Juniper Networks database—The database provides a robust redundancy scheme that you can customize for your deployment. The configuration lets you specify which databases are primary and which are secondary, and how data is propagated among a number of databases.

■ High availability for SRC components —Components such as SAE and NIC let you configure high availability separately for each software component, which means that software redundancy can be configured as a mesh over a number of C-series Controllers.

■ Secure remote access—Remote access to the SRC CLI can be set up through Telnet or SSH and to the C-Web interface through http or https.

■ Directory connections—You can secure connections between the directory and other applications through secure LDAP.

■ Web applications—Applications can leverage the security configured for your Web application server.

■ RADIUS server—Because RADIUS is stateless, you can configure a sufficient number of RADIUS servers for the load, and you can configure both the routers and the SAE to load balance across them.

■ Common Open Policy Service (COPS) connections— The JUNOSe routers can be configured with primary, secondary, and tertiary COPS servers, so it is possible to configure many failover schemes. This flexibility lets you locate backup SAEs remotely to provide geographical redundancy or close to the routers they manage to improve network performance.

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

■ Load balancing for the network information collector (NIC)—You can provide load balancing for the NIC in the following ways:

■ Deploy two or more NIC hosts that each have the same configuration, and then configure NIC proxies to load balance across the NIC hosts.

■ Run the NIC hosts locally in the Dynamic Service Activator (DSA).

■ For NIC scenarios that require an SAE plug-in to track data about individual subscribers for a deployment in a large network, deploy NIC hosts to handle parts of the network with a different set of NIC hosts to aggregate requests.

## Deployment Scenario

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

Figure 12 shows how C-series Controllers can be deployed. The example shows two platforms in a network operations center. Any number of C-series Controllers can be deployed at one or more sites.

**Figure 12:  Deployment Scenario for C-series Controllers**
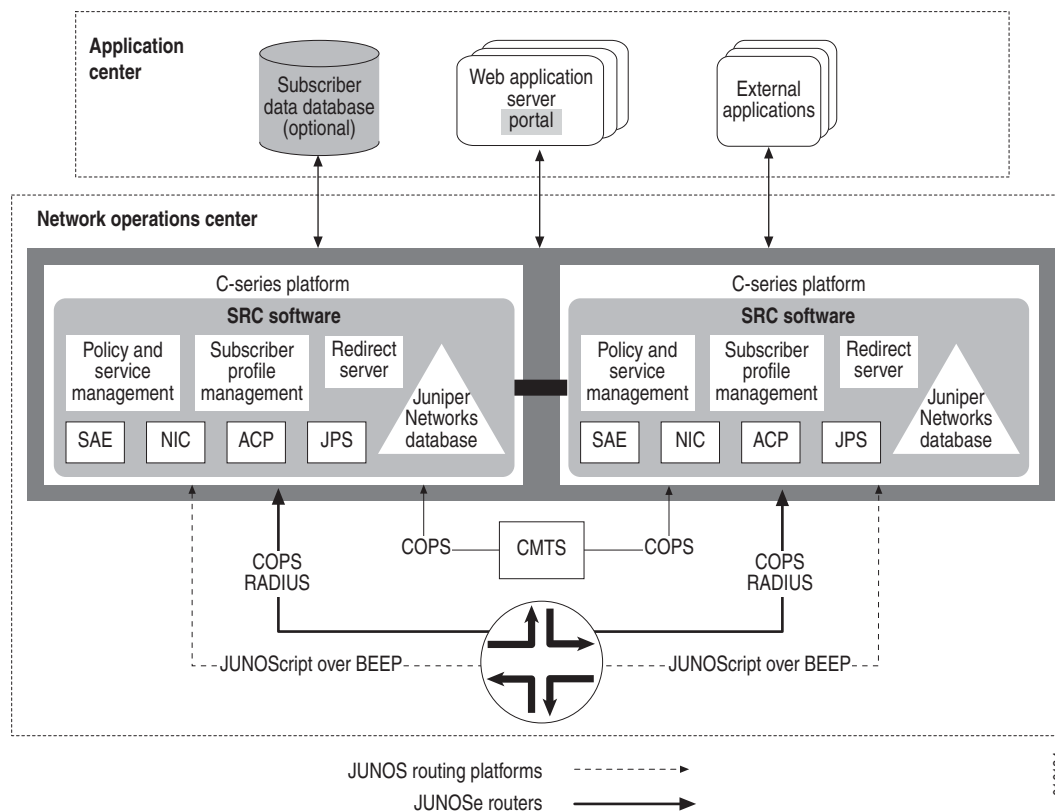


Juniper Networks Professional Services can assist you in determining the best deployment scenario for your environment.

## Chapter 4

# Configuring a C-series Controller

This chapter describes how to configure a C-series Controller. Topics include:

- Before You Begin Configuring the SRC Software on a C-series Controller on page 43

- Configuring the SRC Software on page 44

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

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

- You are familiar with how to use the SRC CLI.

  - Initial system setup and configuration have been completed, including configuration for:

  - C-series Controller hostname

  - Initial configuration for the Juniper Networks database and the database enabled on the system

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

  - Domain name system

  - Eth0 interface

  - An administrative account that has superuser privileges

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

  - Telnet and or SSH access

### *Related Topics*

- *C-series Hardware Guide*

- *SRC-PE CLI User Guide*

## Configuring the SRC Software

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

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

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

   Make any updates needed to the initial configuration.

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

   root@host> **set cli password**

   Do not use the `root` account for normal operation.

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

   See *Chapter 14, Configuring System Time on C-Series Controllers with the SRC CLI*.

4. Configure NTP.

   See *Chapter 14, Configuring System Time on C-Series Controllers with the SRC CLI*.

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

   See *Chapter 20, Managing the Juniper Networks Database with the SRC CLI*.

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

6. Configure remote access to other interfaces.

   See *Chapter 7, Configuring Remote Access to a C-series Controller with the SRC CLI*.

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

   See *Chapter 7, Configuring Remote Access to a C-series Controller with the SRC CLI*.

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

   See *Chapter 7, Configuring Remote Access to a C-series Controller with the SRC CLI*.

9. (Optional) Configure the system log server.

   See *Chapter 17, Configuring System Logging for a C-series Controller with the SRC CLI*.

10. (Optional) Configure user accounts.

    See *Chapter 24, Configuring User Access with the SRC CLI*.

11. Configure SRC components.

    See *Configuring SRC Components* on page 45.

## *Configuring SRC Components*

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

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

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

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

2. Configure SAE local properties.

   See *Chapter 21, Setting Up an SAE with the SRC CLI*.

3. Obtain your SRC software license.

   See *Chapter 8, Overview of SRC Licenses*.

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

   See *Chapter 10, Installing Licenses for C-series Controllers*.

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

    See *Chapter 28, Configuring and Starting the SNMP Agent with the SRC CLI*.

6.  Start the SAE.

    See *Chapter 21, Setting Up an SAE with the SRC CLI*.

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

    See *Chapter 34, Defining an Initial Configuration on a Solaris Platform*.

8.  Configure other SRC components.

    Table 7 lists the principle SRC components that you can configure and names the document that provides information about configuring the components, typically from the CLI. To get information about using the C-Web interface to configure components, see the *SRC-PE C-Web Interface Configuration Guide*.

**Table 7: Configuration Information for Other SRC Components**

| Component | Document |
|---|---|
| SRC-ACP | *SRC-PE Network Guide: SAE, Juniper Networks Routers, NIC, and SRC-ACP, Chapter 21, Configuring Admission Control with the SRC CLI* |
| JPS | *SRC-PE Solutions Guide, Chapter 10, Configuring the JPS with the SRC CLI.* |
| C-Web interface | *Chapter 6, Accessing and Using the C-Web Interface* |
| Network information collector (NIC) | *SRC-PE Network Guide: SAE, Juniper Networks Routers, NIC, and SRC-ACP, Chapter 10, Configuring NIC with the SRC CLI* |
| Policies | *SRC-PE Services and Policies Guide, Chapter 10, Configuring and Managing Policies with the SRC CLI* |
| Redirect server | *SRC-PE Subscribers and Subscriptions Guide, Chapter 15, Configuring Traffic Redirection with the SRC CLI* |
| SAE | *SRC-PE Network Guide: SAE, Juniper Networks Routers, NIC, and SRC-ACP, Chapter 2, Configuring the SAE with the SRC CLI* |
| SAE access to external database that stores subscriber data | *SRC-PE Network Guide: SAE, Juniper Networks Routers, NIC, and SRC-ACP, Chapter 2, Configuring the SAE with the SRC CLI* |
| Services | *SRC-PE Services and Policies Guide, Chapter 1, Managing Services with the SRC CLI* |
| Subscribers and subscriptions | *SRC-PE Subscribers and Subscriptions Guide, Chapter 12, Configuring Subscribers and Subscriptions with the SRC CLI* |
| Enterprise Service Portals | *SRC-PE Subscribers and Subscriptions Guide, Chapter 22, Installing and Configuring Enterprise Service Portals* |

## Chapter 5

# Accessing and Starting the SRC CLI

This chapter describes how to configure access to the SRC command-line interface (CLI). Topics include:

- Overview of Configuration for the SRC CLI on page 47

- Changing the Directory Access Configuration for the SRC CLI on page 48

- Starting the SRC CLI on page 50

- Accessing the Policies, Services, and Subscribers SRC CLI on page 51

## Overview of Configuration for the SRC CLI

You can use the SRC CLI on a C-series Controller or a Solaris platform that has the SRC software and the CLI installed.

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

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

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

### *Related Topics*

- *Accessing the Policies, Services, and Subscribers SRC CLI* on page 51

- *Chapter 24, Configuring User Access with the SRC CLI*

- *SRC-PE CLI Command Reference*

## Changing the Directory Access Configuration for the SRC CLI

On Solaris platforms, configure the CLI to use the directory that stores SRC configuration data.

### *Configuration Statements for CLI Directory Access*

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

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

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

The eventing statement is enabled by default.

### *Changing Directory Access Properties*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   For example:

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

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

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

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

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

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

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

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

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

In most cases, you use the default configuration for directory eventing properties. For information about changing directory eventing properties, see *Chapter 30, Configuring Local Properties with the SRC CLI*.

### *Verifying the Configuration for Directory Access*

To verify the configuration for directory connections:

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

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

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

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

## Starting the SRC CLI

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

### *Starting the CLI on a C-series Controller*

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

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

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

   **#ssh my_admin@my_cseries_platform**

2. Start the CLI:

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

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

### *Starting the CLI on a Solaris Platform*

To start the CLI on a Solaris platform:

1. Log into the Solaris platform through a user account that has super-user privileges configured for the SRC software.

2. Start the CLI from the directory in which it is installed.

   ```
   # /opt/UMC/cli/bin/cli
   --- SRC CLI 7.0 build CLI.B.7.0.0.006
    (c) 2005-2006 Juniper Networks Inc.
   user@host>
   ```

## Accessing the Policies, Services, and Subscribers SRC CLI

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

### Configuring Access to the Policies, Services, and Subscribers CLI

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

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

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

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

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

   where:

   - crypt—UNIX crypt, one-way encryption

   - md5—Message Digest 5 (MD5), a 128-bit message digest

   - sha—SHA message digest, a 160-bit message digest

   - plain—No encryption

### Starting the Policies, Services, and Subscribers CLI

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

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

To start the Policies, Services, and Subscribers CLI:

- Enter the enable *component* command.

  user@host> **enable component editor**

## Chapter 6
# Accessing and Using the C-Web Interface

This chapter describes how to configure access to the C-Web interface. Topics include:

- C-Web Overview on page 53

- Navigating the C-Web Interface on page 54

- Starting the C-Web Interface on page 58

- Accessing Policies, Services, and Subscribers with the C-Web Interface on page 58

- Getting Help in the C-Web Interface on page 59

- Changing a Username or Password for the C-Web Interface on page 59

- Enabling Remote Users to Access the C-Web Interface on page 59

- Modifying the Editing Level in the C-Web Interface on page 63

- Displaying Icons for Objects in the C-Web Interface on page 64

- Editing SRC Configurations with the C-Web Interface on page 65

- Modifying Objects in the C-Web Interface on page 67

- Configuring Logging Properties in the C-Web Interface on page 68

- Logging Out of the C-Web Interface on page 69

## C-Web Overview

The C-Web interface lets you monitor, configure, troubleshoot, and manage the SRC components and C-series Controllers. You can use the C-Web interface on a C-series Controller or on a Solaris platform that has the C-Web software installed.

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

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

- Monitoring—Display the current configuration and information about the system and SRC components.

- Configuring—View the current configurations at a glance and configure SRC components on the Solaris platform and the C-series controller.

- Diagnosing—Diagnose problems with the NIC component.

- Managing—Manage files and licenses, enable and disable components, clear certificates and lists, upgrade the software, and reboot the system.

## Navigating the C-Web Interface

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

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

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

### Layout of the C-Web Interface

Each page of the C-Web interface is divided into the following panes, as shown in Figure 13.

**Figure 13: C-Web Layout**
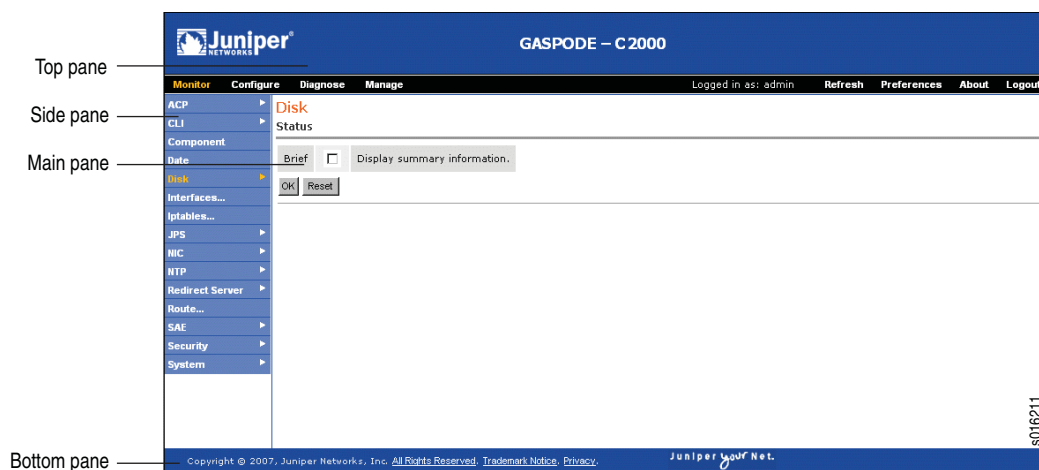
- Top pane—Displays identifying information and links.

- Main pane—Location where you monitor the SRC software or a C-series Controller by entering information in text boxes, making selections, and clicking buttons.

- Side pane—Displays subtasks of the Monitor task currently displayed in the main pane. Click an item to access it in the main pane.

- Bottom pane—Displays copyright and trademark information.

## Elements of the C-Web Interface

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

### Top Pane Elements

The top pane comprises the elements shown in Figure 14 on page 55.

**Figure 14: Top Pane Elements**
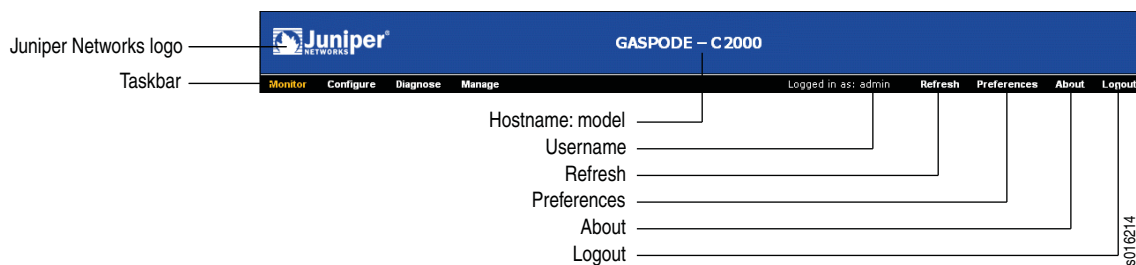


- Juniper Networks logo—Link to http://www.juniper.net in a new browser window.

- Taskbar—Menu of C-Web tasks:

  - Monitor—View monitoring information for core SRC components.

  - Configure—Configure SRC software on the Solaris platform and C-series Controller.

  - Diagnose—Troubleshoot NIC component problems.

  - Manage—Manage files and licenses, upgrade the software, and reboot the system.

- *hostname – model*—Hostname and model of the C-series Controller.

- Logged in as: *username*—Username you used to log in to the C-series Controller or the SRC software.

- Update—Update the display of tasks and objects after modifying SRC software.

- Preferences—Link to C-Web display and configuration preferences, such as the display of Help text.

- About—Link to information about the C-Web interface, such as the version number.

- Logout—Ends your current login session with the C-Web interface and returns you to the login page.

## Main Pane Elements

The main pane comprises the elements shown in Figure 15.

**Figure 15:  Main Pane Elements**
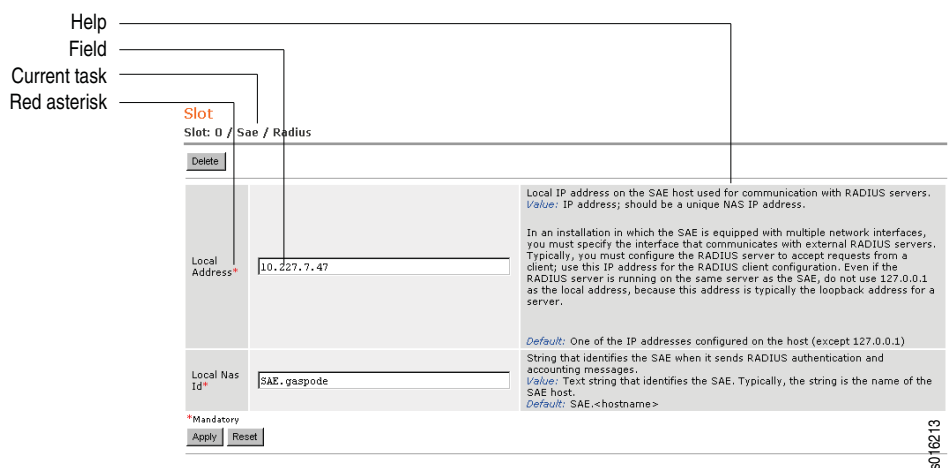


- Help—Displays field-specific information, such as the definition, format, and valid range of data in the field.

- Current task—Shows the successive C-Web tasks and subtasks you selected to display in the current main and side panes.

- Red asterisk (*)—Indicates a required field.

## Side Pane Elements

The side pane comprises the elements shown in Figure 16.

**Figure 16: Side Pane Elements**



C-Web subtasks

C-Web objects

C-Web configuration options
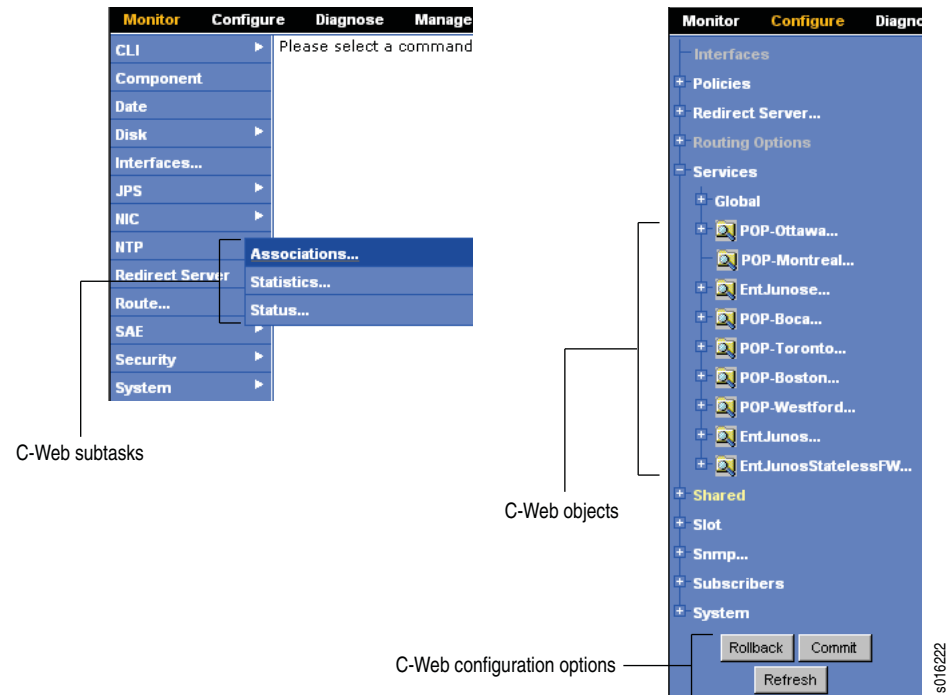
In the Monitor, Diagnose, and Manage side panes, each subtask displays options related to the selected task in the C-Web taskbar. In these side panes, click the arrow signs (>) to expand individual items. Figure 16 shows an example of the Monitor side pane.

In the Configure side pane, each subtask displays options related to the selected task in the C-Web taskbar. Objects represent configuration that you have created. For example, Figure 16 displays objects that represent services. Click the plus signs (+) to expand both individual subtasks and objects. Click the minus signs (–) to hide individual subtasks and objects.

To edit a configuration, click the configuration options buttons at the bottom of the Configure side pane. For more information, see *Editing SRC Configurations with the C-Web Interface* on page 65.

## Starting the C-Web Interface

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

To start the C-Web interface:

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

   **https://**_host_**:port/**

   or

   **http://**_host_**:port/**

   The C-Web interface login page appears.

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

   The Monitor page appears.

## Accessing Policies, Services, and Subscribers with the C-Web Interface

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

### Configuring Access to Policies, Services, and Subscribers with the C-Web Interface

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

1. Click **Configure > System > Services > Editor**.

2. In the Password Encryption box, select the type of password encryption to be used.

3. Click **Apply**.

### Starting Policies, Services, and Subscribers

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

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

To start the Policies, Services, and Subscribers subtasks:

1. Click **Manage > Enable**.

2. From the Component list, select **editor**.

3. Click **OK**.

## Getting Help in the C-Web Interface

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

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

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

### *Enabling Help*

To enable Help to display information:

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

### *Disabling Help*

To disable Help from displaying information:

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

## Changing a Username or Password for the C-Web Interface

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

1. In the C-Web login window, click **Reset**.

2. Type the new entry or entries.

3. Click **Log In**.

## Enabling Remote Users to Access the C-Web Interface

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

### *Accessing the C-Web Interface Through Secure HTTP*

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

See *Chapter 26, Managing Security Digital Certificates*.

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

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

    The HTTP pane appears.

2.  Click **Create**.

3.  To configure HTTPS for an Ethernet port:

    a.  Select the Ethernet port from the list.

    b.  To configure a TCP port, type the value in the Port box, and click **Apply**.

4.  To configure HTTPS for an interface:

    a.  Type a list of incoming network interfaces in the Interface box.

    b.  To configure a TCP port, type the value in the Port box, and click **Apply**.

### *Accessing the C-Web Interface Through HTTP*

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

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

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

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

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

    The HTTP pane appears.

2.  Click **Create**.

3.  To configure HTTP for an Ethernet port:

    a.  Select the Ethernet port from the list.

    b.  To configure a TCP port, type the value in the Port box, and click **Apply**.

4. To configure HTTP for an interface:

   a. Type a list of incoming network interfaces in the Interface box.

   b. To configure a TCP port, type the value in the Port box, and click **Apply**.

### Configuration Statements for Accessing the C-Web Interface Through Secure HTTP

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

See *Chapter 26, Managing Security Digital Certificates*.

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

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

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

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

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

   The default port for HTTPS is 443.

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

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

   You can specify an interface for SRC installations on Solaris platforms as well as on C-series Controllers. On a C-series Controller, use eth0; you can use eth2 or eth3 if installed.

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

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

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

5. Configure logging for the C-Web interface.

   See *SRC-PE Monitoring and Troubleshooting Guide, Chapter 3, Configuring Logging for SRC Components with the CLI*.

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

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

   👉 **NOTE:** Like access to the SRC CLI, we recommend that you not use `root` access. If you do use `root` access, it must be through a secure terminal on a C-series Controller. On Solaris platforms, `root` login is allowed through Telnet.

   See *Chapter 24, Configuring User Access with the SRC CLI*.

## Configuration Statements for Accessing the C-Web Interface Through HTTP

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

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

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

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

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

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

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

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

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

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

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

   You can specify an interface for SRC installations on Solaris platforms as well as on C-series Controllers. On the C-series Controller, use eth0; you can use eth2 or eth3 if installed.

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

4. Configure logging for the C-Web interface.

   See *SRC-PE Monitoring and Troubleshooting Guide, Chapter 3, Configuring Logging for SRC Components with the CLI*.

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

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

   ---

   **NOTE:** Like access to the SRC CLI, we recommend that you not use `root` access. If you do use `root` access, it must be through a secure terminal on a C-series Controller. On Solaris platforms, `root` login is allowed through Telnet.

   ---

   See *Chapter 24, Configuring User Access with the SRC CLI*.

## Modifying the Editing Level in the C-Web Interface

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

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

**Table 8: Editing Levels**

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

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

The editing level can be set for:

■ Specified users in the user profiles.

■ A current user session.

To modify the editing level:

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

## Displaying Icons for Objects in the C-Web Interface

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

You can view icons for interfaces, policies, services, and subscribers. Figure 17 displays an example of the policy icon.

**Figure 17: Policy Icon**
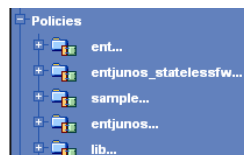


### *Enabling Icons for Objects*

To enable icons:

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

Icons are displayed in the side pane.

### *Disabling Icons for Objects*

To disable icons:

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

The icons are removed from the side pane.

# Editing SRC Configurations with the C-Web Interface

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

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

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

**Figure 18: Configuration Options for the C-Web Interface**
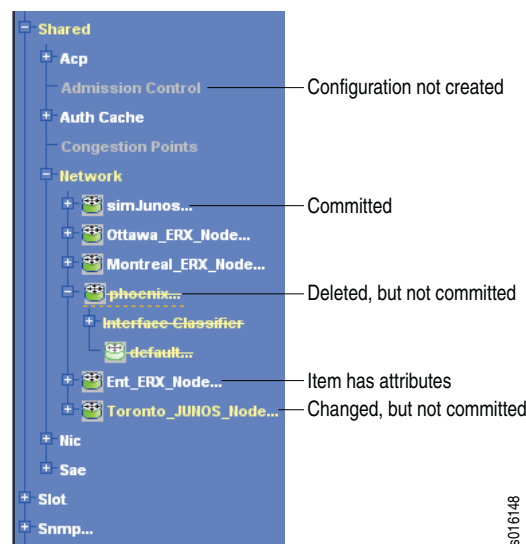


The style of objects in the side pane indicates the status of the configuration. For example:

- White text—Indicates a committed configuration.

- Gray text—Indicates that an object is a configuration that has not been created.

- Orange—Indicates that an item has been changed, but not yet committed.

- Crossed-out orange text—Indicates that an item has been deleted, but not yet committed.

- Red x mark—Indicates an invalid configuration.

## *Loading Configuration Values in the C-Web Interface*

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

Figure 19 shows the main pane of a configuration that has not been created.

**Figure 19: Sample Configuration**



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

To load the configuration values:

1. In the side pane, click an object that does not have a configuration created.

2. In the main pane, click the **Create** button.

## Committing a Configuration

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

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

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

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

## Reverting to a Previous Configuration

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

To revert to the full committed configuration:

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

### Updating the Configuration Data

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

To update the configuration:

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

## Modifying Objects in the C-Web Interface

You can rename, move, or delete any type of object in the C-Web interface.

### Renaming an Object

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

To rename an object:

1. In the main pane, click the **Rename** button.

2. Type a new name for the object in the dialog box. and click **OK**.

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

### Moving an Object

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

To move an object:

1. In the side pane, click the object.

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

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

### Deleting an Object

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

To delete an object:

1. In the side pane, click the object.

2. In the main pane, click **Delete**.

   The object no longer appears in the side pane.

## Configuring Logging Properties in the C-Web Interface

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

### *Configuring File Properties*

To configure file properties for logging:

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

    The Logger pane appears.

2.  From the Create new list, select **Logger**.

3.  Type a name for the logging file in the dialog box, and click **OK**.

4.  In the side pane, expand the logger that you created, and click **File**.

    The File pane appears.

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

### *Configuring Syslog Properties*

To configure system logging properties:

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

    The Logger pane appears.

2.  From the Create new list, select **Logger**.

3.  Type a name for the logging file in the dialog box, and click **OK**.

4.  In the side pane, expand the logger that you created, and click **Syslog**.

    The Syslog pane appears.

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

### *Configuration Statements for Logging for the C-Web Interface*

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

system services web-management logger *name*

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

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

## Logging Out of the C-Web Interface

To end a C-Web session at any time:

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

**Chapter 7**

# Configuring Remote Access to a C-series Controller with the SRC CLI

This chapter describes how to configure access to a C-series Controller.

You can also use the C-Web interface to configure access to a C-series Controller, See *SRC-PE C-Web Interface Configuration Guide, Chapter 1, Configuring Remote Access to a C-series Controller with the C-Web Interface.*

Topics in this chapter include:

## Configuring External Interfaces on a C-series Controller

The C-series Controller provides the following interfaces:

■ Serial port—9600 baud

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

■ Two external Gigabit Ethernet interfaces—eth0 and eth1

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

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

■ Optional two additional Gigabit Ethernet interfaces—eth2 and eth3

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

■ Two USB interfaces

## Configuring Gigabit Ethernet Interfaces for IPv4 with the SRC CLI

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

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

interfaces name unit *unit-number*

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

To configure a Gigabit Ethernet interface to use IPv4:

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

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

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

   For example:

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

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

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

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

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

3. Verify the interface configuration.

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

## Configuring Gigabit Ethernet Interfaces for IPv6 with the SRC CLI

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

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

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

To configure a Gigabit Ethernet interface to use IPv6:

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

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

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

   For example:

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

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

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

   For example:

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

3. Verify the interface configuration.

   ```
   [edit interfaces eth0]
   user@host# show
   unit 0 {
     family {
       inet6 {
         address 10AB:0:0:CD30::/20;
       }
     }
   }
   ```

## Configuring Tunnel Interfaces with the SRC CLI

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

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

- GRE—Generic routing encapsulation. Encapsulates traffic that can use various network protocols within IP. For C-series Controllers, the tunnel interface encapsulates IP packets.

- IP-over-IP—Encapsulates IP packets within IP packets.

- SIT—Encapsulates IPv6 traffic in an IPv4 tunnel. This type of tunnel allows compatibility of IPv6 traffic within an IPv4 network.

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

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

See *Configuring Gigabit Ethernet Interfaces for IPv4 with the SRC CLI* on page 72.

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

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

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

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

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

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

    For example:

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

2.  Configure the type of tunnel.

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

    or

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

    or

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

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

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

    For example:

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

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

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

    For example:

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

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

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

    For example:

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

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

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

    For example:

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

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

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

    For example:

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

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

```
[edit interfaces]
user@host# show
unit 0 {
  family {
    inet6 {
      address 192.2.0.10/24;
    }
  }
}
ip-tunnel {
  tunnel {
      mode ipip;
      destination 192.0.2.20;
      source 192.20.10.5;
      interface eth0;
      ttl 110;
    }
}
```

## Configuring a Static Route to Devices on Other Networks with the SRC CLI

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

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

To configure a static route to another network:

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

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

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

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

To specify that packets to a specified network be dropped:

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

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

## Securing Connections Between a C-series Controller and Remote Hosts

For security reasons, take care to limit the number of open ports you configure for applications and SRC components on the external interfaces. To review the default port settings for SRC components, see *Chapter 34, Defining an Initial Configuration on a Solaris Platform* which provides information about an initial configuration on a Solaris platform.

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

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

| Application | Information About Access Configuration |
| --- | --- |
| SSH | *Configuring a C-series Controller to Accept SSH Connections with the SRC CLI* on page 78 |
| Telnet | *Configuring a C-series Controller to Accept Telnet Connections with the SRC CLI* on page 79 |
| NETCONF | *Configuring a C-series Controller to Accept NETCONF Connections with the SRC CLI* on page 80 |
| C-Web interface | *Chapter 6, Accessing and Using the C-Web Interface* |
| Policies, Services, and Subscribers CLI | *Chapter 5, Accessing and Starting the SRC CLI* |

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

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

- SSH

- Telnet

- FTP by means of a file URL

## Configuring a C-series Controller to Accept SSH Connections with the SRC CLI

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

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

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

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

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

2. (Optional) Specify that SSH version 1 be used.

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

   SSH version 2 is enabled by default.

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

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

   where:

   ■ allow—Allow users to log in to the C-series Controller as root through SSH.

   ■ deny—Disable users from logging in to the C-series Controller as root through SSH.

   ■ deny-password—Allow users to log in to the C-series Controller as root through SSH when the authentication method (for example, RSA authentication) does not require a password. (Default)

## Configuring a C-series Controller to Accept Telnet Connections with the SRC CLI

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

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

system services {
    telnet;
}

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

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

## Configuring a C-series Controller to Accept NETCONF Connections with the SRC CLI

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

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

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

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

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

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

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

**Part 3**

# Managing SRC Licenses

## Chapter 8

# Overview of SRC Licenses

This chapter describes the types of SRC licenses and explains how to obtain licenses. Topics include:

## Types of SRC Licenses

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

- Pilot license—Limits the number of concurrent active subscriber sessions on an SAE. The number of sessions used at any one time cannot exceed the number permitted by the pilot license. The SAE license manager manages pilot licenses. Use the pilot license for field trials of the SRC software.

- Server license—Limits the number of concurrent active SAE service sessions. The server license is managed by the SRC license server, which reads the license, leases a portion of the license on demand to each SAE client, monitors the consumption of the license, and raises alarms when necessary. For server licenses, the SAE client does not involve the directory for license management. Use the server license for a production implementation of the SRC software.

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

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

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

## Obtaining an SRC License

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

### *Pilot License*

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

- Username to be listed in the license key

- Host ID of the SAE host (or the host IDs of all hosts if you have more than one)

- Number of concurrent users that you want to be able to connect to the SAE

You can determine the host ID by issuing one of the following commands:

- Solaris host—/bin/hostid

- C-series Controller—show system information

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

  Hostid        e30a2e07

### *Server License*

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

- Username to be listed in the license key

- Maximum number of concurrently active SAE services that you require

- Time interval for which you need the server license

- IP address or hostname of the license server. The SAE requires access to this IP address or hostname.

**Chapter 9**

# Overview of the SRC License Server

This chapter describes the SRC license server. Each SRC installation uses a single license server to hold and manage the license for a customer. Topics include:

- Overview of the SRC License Server on page 85

- Unsuccessful Connections from the SAE to the SRC License Server on page 87

- SRC License Server Redundancy on page 88

## Overview of the SRC License Server

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

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

For more information about server licenses and an explanation of how to install and configure a server license, see *Chapter 12, Installing Licenses for SRC Software on Solaris Platforms*.

### Server License

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

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

### License Server Errors

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

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

### *License Requests*

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

■ When the new total is below the limit, the license server grants the requested lease to the client.

■ If the new total exceeds the limit, the license server grants leases up to the amount available.

■ If the current total exceeds the license limit, the license server denies all requests.

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

When a lease is granted, it specifies the:

■ Chunk size—Number of active service sessions

■ Lease duration—Length of time allotted to a grant

■ Allocation threshold—A percentage of the license chunk size that defines how many licenses are available for allocation

■ Release threshold—A percentage of the license chunk size that defines when a lease is released

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

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

### Example: License Allocation

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

### Example: License Release Example

License units are released as active service sessions decrease, with the SAE retaining more licenses than it currently needs to avoid fluctuation around the threshold. For example, a lease has a chunk size of 50, a release threshold of 10 %, and four license chunks (200 licenses) allocated to the SAE. In this case:

- If the number of active service sessions drops to 105, the fourth license unit is released, leaving three units and 150 licenses.

- If the number of active service sessions drops to 55, the third license unit is released, leaving two units and 100 licenses.

- If the number of active service sessions drops to 5, the second license unit is released, leaving one unit and 50 licenses.

### *Lease Renewal*

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

### *Directory Location and Access*

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

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

## Unsuccessful Connections from the SAE to the SRC License Server

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

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

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

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

## SRC License Server Redundancy

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

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

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

- If the total number of licenses in use is lower than the licenses limit, all SAEs continue operating in the same manner as before the outage.

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

**Chapter 10**

# Installing Licenses for C-series Controllers

This chapter describes how to install a pilot license from the SRC CLI, how to install a server license for C-series Controllers, and how to configure the SAE to manage server licenses. Topics include:

- Installing a Pilot License from the SRC CLI on page 89

- Installing Server Licenses for C-series Controllers on page 91

- Configuring License Manager for an SAE on a C-series Controller on page 91

## Installing a Pilot License from the SRC CLI

You install pilot licenses on C-series Controllers from the SRC CLI. You can also install pilot licenses for SRC software running on Solaris platforms by using the CLI.

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

Before you install a pilot license, make sure that the Juniper Networks database is running on a C-series Controller. If you are installing the license on a Solaris platform, make sure that the directory server is running.

To install a pilot license:

1. On a C-series Controller on which the Juniper Networks database is configured to have a primary role, or on a Solaris platform that has the SRC software installed, use the request sae import-pilot-license command:

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

   where:

   - *file-name*—Name of the file that contains the SRC license

   - *server-address*—IP address for the primary directory server. For C-series Controllers, this is the platform that has the Juniper Networks database configured to have a primary role.

   - *namespace*—Base DN for the directory. In most cases you can use the default <base>.

   - *authentication-dn*—DN used for directory authentication.

   - *password*—Password used for directory authentication.

2. Verify that a valid license is available:

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


   Type of license: Pilot. Status: OK.

   The following valid licenses are found:

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

### Related Topics

- For information about installing pilot licenses on Solaris platforms by using **instlic** command and SDX Admin, see *Before You Install an SRC License on a Solaris Platform* in *Chapter 12, Installing Licenses for SRC Software on Solaris Platforms*.

## Installing Server Licenses for C-series Controllers

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

To install server licenses for C-series Controllers:

1. From operational mode, enable the license server.

   user@host> **enable component licSrv**

2. Install the server license.

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

3. Verify that a valid license is available.

   user@host> **show sae licenses**

4. Configure license manager for the SAE.

   See *Configuring License Manager for an SAE on a C-series Controller on page 91*.

### *Related Topics*

■ *Chapter 9, Overview of the SRC License Server*

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

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

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

shared sae configuration license-manager directory-access {
    server-address *server-address*;
    server-port *server-port*;
    license-dn *license-dn*;
    authentication-dn *authentication-dn*;
    password *password*;
    (ldaps);
    connection-manager-id *connection-manager-id*;
    event-base-dn *event-base-dn*;
    signature-dn *signature-dn*;
    snmp-agent;
}

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

To configure the SAE license manager:

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

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

2.  Specify the client type.

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

    SDX is the only supported license type.

3.  Specify the path to the cache file.

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

    The default is *var/run/lic_cache.*

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

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

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

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

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

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

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

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

    The default port is 389.

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

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

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

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

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

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

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

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

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

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

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

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

    The default is LICENSE_MANAGER.

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

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

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

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

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

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

    [edit shared sae configuration license-manager directory-access]
    user@host# **set snmp-agen**t

**Chapter 11**

# Setting Up the SRC License Server

This chapter describes how to configure basic properties for the SRC license server on Solaris platforms and how to start, stop, and monitor the server on Solaris platforms. Topics in this chapter include:

## Configuring Initial Settings for the SRC License Server on Solaris Platforms

For server licenses, you configure the initial properties for the license server and install a license, before you can use the SAE. You can also customize license server configuration to send e-mail notifications of alarms, set a threshold for alarms, tune performance of the license server engine, and change directory and file information.

The license server monitors the consumption of the license resources and allocates licenses to client SAEs up to the number supported by the license. The license server obtains most of its information from the directory. A local configuration file, */opt/UMC/licsvr/etc/bootstrap.propertie*s, stores initial configuration information that cannot be stored in the directory, such as the attributes to connect to the directory. Use the information in this section to create and modify the configuration file.

Use the local configuration tool to configure the *bootstrap.properties* file.

To create the local configuration file and configure the properties for the license server:

1. On the SAE host, log in as **root** or as an authorized nonroot admin user.

2. Start the local configuration tool from the license server installation directory.

   **/opt/UMC/licsvr/etc/config -l**

   The first time that you issue this command, it creates the *bootstrap.properties* file and displays the local configuration tool window for the properties.
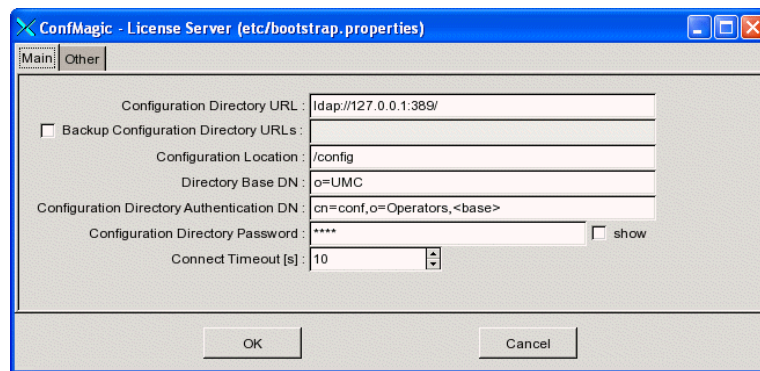


3. In the Main tab, configure directory information.

4. In the Other tab, configure parameters for Java, the object request broker (ORB), and the SNMP agent.

5. Click OK.

### Related Topics

■ For information about using the local configuration tool, see *Chapter 42, Configuring Local Properties*.

■ *Directory Fields for License Server on page 96*

■ *Miscellaneous Fields for License Server on page 98*

### Directory Fields for License Server

In the local configuration tool for License Server, you can modify the following fields in the Main tab.

#### Configuration Directory URL

■ URL of the directory server that stores the license server configuration information.

■ Value—ldap://<URL>

■ Default—ldap://127.0.0.1:389

### Backup Configuration Directory URLs

- URL of a backup directory server that stores the license server configuration information.

- Value—ldap://<URL>

- Default—List of directory URLs, with URLs separated by commas

### Configuration Location

- Name of the directory that stores the license server *bootstrap.properties* file.

- Value—Text string in the format /<DIRECTORY_NAME>

  where <DIRECTORY_NAME> is the name of directory where the license server *bootstrap.properties* file is stored

- Default—*/config*

### Directory Base DN

- Distinguished name (DN) of the root directory for the SAE.

- Value—DN of the root directory for the SAE

- Guidelines—You must set this attribute if you use a directory-naming scheme different from the default.

- Default—*o = umc*

### Configuration Directory Authentication DN

- DN of the entry in the directory that authenticates the license server's directory bind.

- Value—DN of the entry used to authenticate the directory bind for the license server

- Default—*cn = conf, o = operators, <base>*

### Configuration Directory Password

- Authentication password.

- Value—Text string

- Default—conf

### Connect Timeout

- Interval during which a connection must be made.

- Value—Number of seconds in the range 0–2147483647

- Default—10

### Miscellaneous Fields for License Server

In the local configuration tool for License Server, you can modify the following fields in the Other tab.
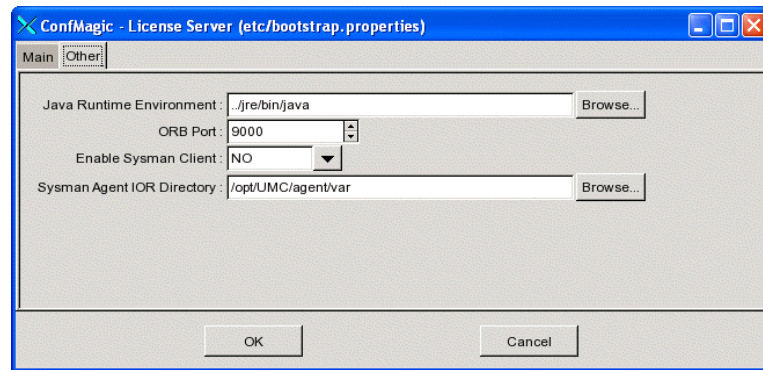


#### Java Runtime Environment

- Path to the Java Runtime Environment (JRE).
- Value—/<path_name>
- Default—*../jre/bin/java*

#### ORB Port

- Port on which the application server ORB listens for requests
- Value—Any valid port number
- Default—9000

#### Enable Sysman Client

- Whether or not you can configure support for viewing license server information with the SNMP agent.
- Value
  - Yes—If you are using the SNMP agent, enables the client.
  - No—Disables client support. Select NO If you are not using the SNMP agent.
- Default—No

#### Sysman Agent IOR Directory

- Folder that contains the interoperable object reference (IOR) file for the license server. The license server writes its object references to this folder, and the SNMP agent discovers license server components by monitoring the license server IOR file in this folder.
- Value—Path to the folder that contains the IOR

- Guidelines—By default, the license server IOR file is in the *var* folder, which is relative to the SNMP agent installation folder (*/opt/UMC/agent*). You need to change this property only if you installed the SNMP agent in a folder other than the default folder, or if you previously changed this property and now need it to point to the folder where the IOR file currently resides.

- Default—*/opt/UMC/agent/var*

## Starting the SRC License Server on Solaris Platforms

After you install the SRC components, start the license server before you start the SAE for the first time. After you have started the license server and the SAE, you can stop and restart either component at any time.

To start the license server:

1.  On the host on which the license server is installed, log in as `root` or as an authorized nonroot user.

2.  Start the license server from its installation directory:

    **/opt/UMC/licsvr/etc/licsvr start**

## Monitoring the SRC License Server on Solaris Platforms

To verify that the license server is running:

1.  On the host on which the license server is installed, log in as `root` or as an authorized nonroot user.

2.  Display the status of the license server from its installation directory:

    **/opt/UMC/licsvr/etc/licsvr status**

## Stopping the SRC License Server on Solaris Platforms

To stop the license server:

1. On the host on which the license server is installed, log in as `root` or as an authorized nonroot user.

2. Stop the license server from its installation directory:

   **/opt/UMC/licsvr/etc/licsvr stop**

## Chapter 12

# Installing Licenses for SRC Software on Solaris Platforms

This chapter describes how to install SRC software licenses on Solaris platforms. Topics include:

- Before You Install an SRC License on a Solaris Platform on page 101

- Installing an SRC Pilot License on a Solaris Platform on page 102

- Installing an SRC Server License on a Solaris Platform on page 104

- Command Options for the SRC instlic and licchk Commands on page 105

## Before You Install an SRC License on a Solaris Platform

Before you install a license:

1. Make sure that the directory server is running.

2. Make sure that the appropriate local properties are configured:

   - Pilot license—If you plan to use the **instlic** command to install the license (recommended), ensure that the SAE local properties have been configured.

     See *Chapter 35, Setting Up an SAE on a Solaris Platform*.

   - Server license

     - Ensure that the SAE local properties have been configured.

       See *Chapter 35, Setting Up an SAE on a Solaris Platform*.

     - Configure initial properties for the license server.

       See *Setting Up the SRC License Server on page 95*.

## Installing an SRC Pilot License on a Solaris Platform

After you configure the SAE local parameters, you can install a pilot license in the directory with either the **instlic** command (recommended) or SDX Admin.

You can also install a pilot license from the SRC CLI, see *Chapter 10, Installing Licenses for C-series Controllers*.

### Installing a Pilot License by Using the instlic Command

To install the pilot license:

1. Save the pilot license provided by Juniper Networks into a text file in the desired directory.

2. Issue the **instlic** command.

    **/opt/UMC/sae/etc/instlic**

    This command has the following syntax; see Table 10 on page 105 for details on the syntax:

    instlic [-h <ldapHost>] [-D <bindDN>] [-b <baseDN>]
    [-w <password>] [-W ] <fileName>

    The installation script reads the license from the specified file.

The following sample command specifies a nondefault host address and base DN, prompts you for the password, and establishes the license contained in the *pilot.txt* file as the license:

    /opt/UMC/sae/etc/instlic -h 10.25.2.4
    -D cn=umcadmin,o=SDXbase -W pilot.txt

### Installing a Pilot License by Using SDX Admin

To install the pilot license:

1. Start SDX Admin.

   For information about starting and using SDX Admin, see *Chapter 43, Using SDX Admin*.

2. In the navigation pane of SDX Admin, expand the **Management** folder, right-click **Licenses**, select **Ne**w, and click **License**.

   The New License dialog box appears.
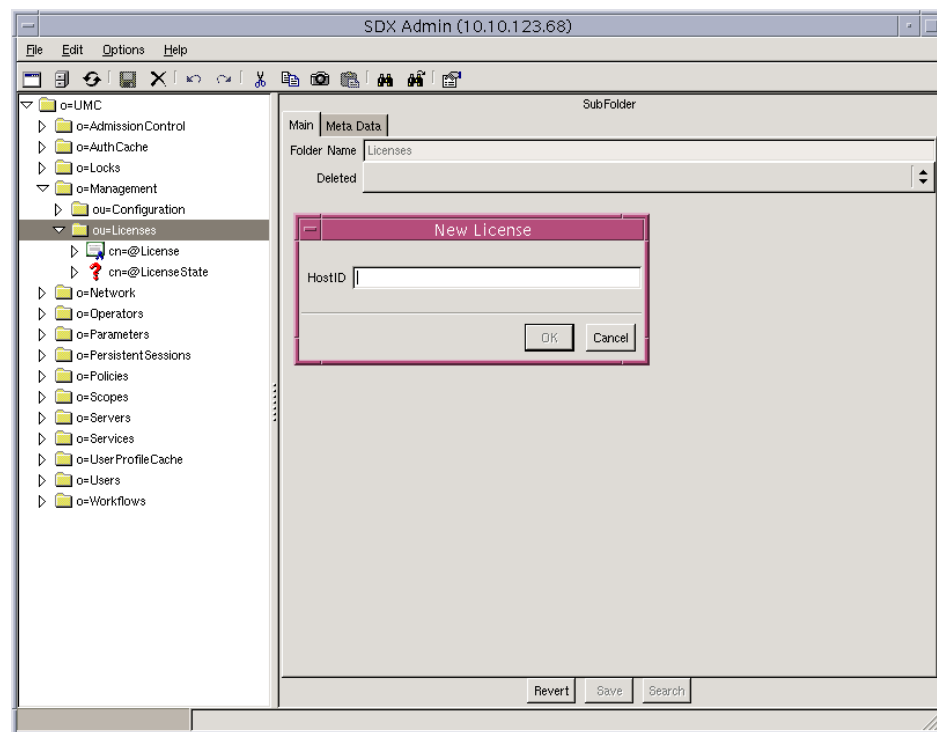


3. Enter the host ID value.

   See the *Chapter 8, Overview of SRC Licenses*.

4. Click **OK**.

   The value appears in the HostID field of the Main tab of the License pane.

5.  Enter the license provided by Juniper Networks in the SSP License field of the Main tab of the License pane, and click **Save**.
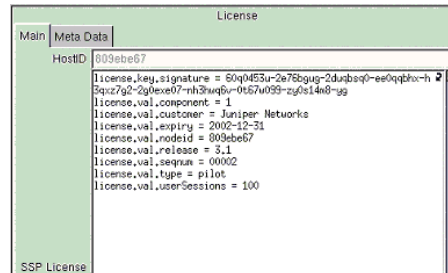


6.  Repeat Steps 3 and 5 for each host with its related host ID and license.

## Installing an SRC Server License on a Solaris Platform

After you configure the SAE local properties and you configure initial properties for the license server, you can install a server license.

To install a server license in the directory:

■ Issue the **instlic** command from the license server's installation directory.

**cd /opt/UMC/licsvr/etc**

This command has the following syntax; see Table 10 on page 105 for details on the syntax:

**instlic** [-h <ldapHost>] [-D <bindDN>] [-b <baseDN>]
[-m ] [-w <password>] [-W ] <fileName>

The **instlic** command applies the name @License to the first license you install; this is the master license. Any subsequent licenses that you install are automatically named by the command as Lic-<#>; <#> is a sequence number starting at 0. SAE clients read the address of the license server from the master license.

When you upgrade the SRC software to a higher release, you must replace the current master license with a new master license obtained from Juniper Networks. The new master license will incorporate the version number of the higher release and a new signature. The **instlic** command automatically renames the old master license to Lic-<#> to retain it as a secondary license.

The following sample command specifies a nondefault host address and base DN, prompts you for the password, and establishes the license contained in the *second.txt* file as the master license:

**/opt/UMC/licsvr/etc/instlic -h 10.25.2.4
-D cn=umcadmin,o=SDXbase -m -W second.txt**

### *Verifying a License*

After you install the license, you can use the **licchk** command to verify the license installation and to verify connectivity to the SRC license server. The command returns the license's relative distinguished name (RDN) and its attributes to a specified file. This command has the following syntax; see Table 10 on page 105 for details on the syntax:

    licchk [-h <ldaphost>] [-D <bindDN>] [-b <baseDN>]
    [-w <password>] -[o <outputFile>]

If you have configured nondefault bind credentials (in the LDAP Connection dialog box) for the directory server, then you must use one or more of the command options to specify the attribute value.

The following sample command specifies a nondefault host address, base DN, and password:

    /opt/UMC/sae/etc/licchk -h 10.13.1.5 -D cn=umcadmin,o=SDXbase -w acp45

If the directory server uses the default bind credentials, you can simply issue the following command:

**/opt/UMC/sae/etc/licchk**

## Command Options for the SRC instlic and licchk Commands

Table 10 defines the options available to the **instlic** and **licchk** commands.

**Table 10: Options for the instlic and licchk Commands**

| Option | Available to Command | Description |
|---|---|---|
| -b < baseDN > | instlic, licchk | Specifies the distinguished name of the base object in the LDAP schema of the directory server. |
| | | The default value is read from */opt/UMC/licsvr/etc/bootstrap.properties*. |
| -D < bindDN > | instlic, licchk | Specifies the distinguished name used for binding to the directory server. |
| | | The default value is read from */opt/UMC/licsvr/etc/bootstrap.properties*. |
| < fileName > | instlic | Required. Specifies the name of the text file that contains the license from Juniper Networks. You can specify either only a filename relative to the current directory or an absolute path that includes the filename. |
| -h < ldapHost > : < port > | instlic, licchk | Specifies the IP address or hostname, and optionally the port number of the directory server. |
| | | The default value is read from */opt/UMC/licsvr/etc/bootstrap.properties*. |
| -H | instlic, licchk | Lists the command options. |
| -m | instlic | Installs the license as the master license (@License). The previous master license is renamed to Lic- < # > . You might use this option if the location of the license server has changed. Option not available for pilot licenses. |
| -o < outputFile > | licchk | Specifies the name of the file in which you store the results of the **licchk** command. |

**Table 10: Options for the instlic and licchk Commands  (continued)**

| Option | Available to Command | Description |
|---|---|---|
| -w < password > | instlic, licchk | Specifies the bind password for authentication with the directory server. The default value is read from */opt/UMC/licsvr/etc/bootstrap.properties.* |
| -W | instlic, licchk | Causes the command to prompt you for the password |

# Chapter 13
# Managing the SRC License Server on Solaris Platforms

This chapter describes how to customize the license server configuration only on a Solaris platform. Topics include:

- Managing Log Files for the SRC License Server on Solaris Platforms on page 107

- Troubleshooting SRC License Server Problems on Solaris Platforms on page 107

## Managing Log Files for the SRC License Server on Solaris Platforms

To clean the log files for the license server and delete the persistent data that the server writes to files or devices:

- Use the se the **stdout** and **stderr** options.

### *Related Topics*

- *SRC-PE Monitoring and Troubleshooting Guide, Chapter 5, Managing SRC Log Files on a Solaris Platform*.

## Troubleshooting SRC License Server Problems on Solaris Platforms

**Problem**   Licensing problems in a distributed environment where the SAE and the license server are installed on different systems.

**Solution**   Use the **licchk** command with the **-h** option.

For example, the output for the following command shows that the SAE does not have connectivity to the specified license server:

**# /opt/UMC/sae/etc/licchk -h 192.2.4.24**
SSC License Key Checker V3.0


Type of license: Server license. Connectivity to the specified SDX License server (192.2.123.68): NOT OK

The following valid licenses are found:

License: cn=@License,ou=LicSvr,ou=Licenses,o=Management,o=UMC
license.val.component = 1
license.val.customer = jnpr1
license.val.expiry = 2005-12-31
license.val.release = 6.*
license.val.seqnum = 00034
license.val.serialnum = 20041206
license.val.server.corbaloc = corbaloc::10.10.123.68:9000/licmanager
license.val.serviceSessions = 100000
license.val.type = server

**Part 4**

# Managing an Environment of C-series Controllers

## Chapter 14

# Configuring System Time on C-Series Controllers with the SRC CLI

This chapter discusses how to configure the system time zone and the system date from the CLI on a C-series Controller. Topics include:

- Setting the Time Zone with the SRC CLI on page 111

- Setting the System Date with the SRC CLI on page 112

## Setting the Time Zone with the SRC CLI

You can set the time zone on a Solaris platform or on a C-series Controller with the SRC CLI. Use one of the following formats:

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

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

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

- GMT offset to set the time zone relative to UTC (GMT) time in the format */Etc/GMToffset*. Time zone files are stored in the /Etc directory.

- A common zone such as UTC, MDT, or EST.

To modify the local time zone:

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

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

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

    [edit system]
    user@host# **set system time-zone America/New_York**

2.  Verify the configuration. For example:

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

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

### *Related Topics*

- *Setting the System Date with the SRC CLI on page 112*

- *NTP Support on C-series Controllers on page 113*

## Setting the System Date with the SRC CLI

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

To set the system date and time:

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

  user@host> **set date** *date*

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

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

### *Related Topics*

- *Setting the Time Zone with the SRC CLI on page 111*

- *NTP Support on C-series Controllers on page 113*

# Chapter 15
# Configuring NTP for C-Series Controllers

This chapter provides information about Network Time Protocol (NTP) support on C-Series Controllers and discusses how to configure NTP for a C-series Controller. Topics include:

- NTP Support on C-series Controllers on page 113

- Configuring NTP on a C-series Controller on page 114

## NTP Support on C-series Controllers

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

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

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

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

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

- Client mode—The local system can be synchronized with the remote system, but the remote system cannot be synchronized with the local system.

■ Symmetric active (peer) mode—The local system and the remote system can synchronize with each other. You use this mode in a network in which either the local system or the remote system might be a better source of time.

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

■ Broadcast mode—The local system sends periodic broadcast messages to a client population at the specified broadcast or multicast address. Typically, you include this statement only when the local system is operating as a transmitter.

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

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

### *Related Topics*

■ *Configuring NTP on a C-series Controller* on page 114

■ *Configuration Statements for NTP on C-series Controllers* on page 117

## Configuring NTP on a C-series Controller

To configure NTP on a C-series Controller:

1. (Recommended) Configure NTP to automatically set the time when it starts.

   ■ See *Specifying Which NTP Server a C-series Controller Contacts on Startup* on page 118.

   ■ See *Specifying a Basic NTP Configuration on a C-series Controller with the C-Web Interface* in *SRC-PE C-Web Interface Configuration Guide, Chapter 2, Configuring NTP on C-Series Controllers with the C-Web Interface*.

2. Specify the time source and the manner in which time is synchronized between systems on the network. Configure NTP to operate in one or more of the following modes:

   ■ Client mode:

      ■ See *Configuring NTP Client Mode for a C-series Controller with the SRC CLI* on page 119.

      ■ See *Configuring NTP Client Mode for a C-Series Controller with the C-Web Interface* in *SRC-PE C-Web Interface Configuration Guide, Chapter 15, Configuring NTP for C-Series Controllers*.

- Symmetric active (peer) mode:

    - See *Configuring an NTP Peer on a C-series Controller with the SRC CLI* on page 120.

    - See *Configuring an NTP Peer for a C-series Controller with the C-Web Interface* in *SRC-PE C-Web Interface Configuration Guide, Chapter 2, Configuring NTP on C-Series Controllers with the C-Web Interface.*

- Broadcast mode:

    - See *Configuring NTP Broadcast Mode on a C-series Controller with the SRC CLI* on page 121.

    - See *Configuring NTP Broadcast Mode on a C-series Controller with the C-Web Interface* in *SRC-PE C-Web Interface Configuration Guide, Chapter 2, Configuring NTP on C-Series Controllers with the C-Web Interface.*

3. (Recommended) Configure NTP authentication.

    - See *Configuring NTP Authentication on a C-series Controller with the SRC CLI* on page 122.

    - See *Specifying an Authentication Key for NTP on C-Series Controllers with the C-Web Interface* in *SRC-PE C-Web Interface Configuration Guide, Chapter 2, Configuring NTP on C-Series Controllers with the C-Web Interface.*

    - See *Configuring NTP Authentication with the C-Web Interface* in *SRC-PE C-Web Interface Configuration Guide, Chapter 2, Configuring NTP on C-Series Controllers with the C-Web Interface.*

4. (Optional) Configure NTP to listen for broadcast messages.

    - See *Configuring NTP as a Broadcast Client on a C-series Controller with the SRC CLI* on page 124.

    - See *Specifying a Basic NTP Configuration on a C-series Controller with the C-Web Interface* in *SRC-PE C-Web Interface Configuration Guide, Chapter 2, Configuring NTP on C-Series Controllers with the C-Web Interface.*

5. (Optional) Configure NTP to listen for multicast messages.

    - See *Configuring NTP as a Multicast Client on a C-series Controller with the SRC CLI* on page 125.

    - See *Configuring NTP as a Multicast Client on a C-series Controller with the C-Web Interface* in *SRC-PE C-Web Interface Configuration Guide, Chapter 2, Configuring NTP on C-Series Controllers with the C-Web Interface.*

### Related Topics

- *NTP Support on C-series Controllers* on page 113

- *Verifying NTP Configuration on a C-series Controller* on page 126

## Chapter 16

# Configuring NTP on C-Series Controllers with the SRC CLI

This chapter discusses how to configure the Network Time Protocol (NTP) on a C-series Controller with the SRC CLI. Topics include:

## Configuration Statements for NTP on C-series Controllers

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

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

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

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

system ntp multicast-client {
    address;
}

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

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

### *Related Topics*

- *SRC-PE CLI Command Reference*

- *NTP Support on C-series Controllers on page 113*

- *Specifying Which NTP Server a C-series Controller Contacts on Startup on page 118*

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

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

To configure the NTP boot server:

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

   [edit]
   user@host# **edit system ntp**

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

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

For example:

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

### *Related Topics*

- *NTP Support on C-series Controllers on page 113*

- *Configuration Statements for NTP on C-series Controllers on page 117*

- *Verifying NTP Configuration on a C-series Controller on page 126*

## Configuring NTP Client Mode for a C-series Controller with the SRC CLI

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

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

To configure NTP to operate in client mode:

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

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

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

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

   [edit system ntp server 192.0.2.30]
   user@host#

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

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

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

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

### *Related Topics*

## Configuring an NTP Peer on a C-series Controller with the SRC CLI

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

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

To configure NTP to operate in symmetric active mode:

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

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

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

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

   [edit system ntp peer 192.0.2.40]
   user@host#

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

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

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

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

### *Related Topics*

## Configuring NTP Broadcast Mode on a C-series Controller with the SRC CLI

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

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

To configure NTP to operate in broadcast mode:

1. From configuration mode, access the configuration statement that configures NTP broadcast, and specify the broadcast address on one of the local networks or a multicast address assigned to NTP. You can specify an IP address or a hostname.

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

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

   For example, to specify the broadcast address of 244.0.1.1:

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

   [edit system ntp broadcast 224.0.1.1]
   user@host#

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

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

3. (Optional) Specify the time-to-live value to transmit.

   [edit system ntp server *address*]
   user@host# **set ttl** *ttl*

### *Related Topics*

## Configuring NTP Authentication on a C-series Controller with the SRC CLI

You can authenticate time synchronization to ensure that a C-series Controller obtains its time services only from known sources. By default, network time synchronization is unauthenticated; the system synchronizes to whatever system appears to have the most accurate time. We highly recommend that you configure authentication of network time services.

Use the following configuration mode statements to configure authentication for NTP on a C-series Controller:

```
system ntp {
    trusted-key [trusted-key...];
}

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

system ntp broadcast address {
    key key;
}

system ntp peer address {
    key key;
}

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

To configure NTP authentication:

1. Specify authentication for other time servers.

   Only time servers transmitting network time packets that contain one of the specified key numbers and whose key matches the value configured for that key number are eligible for synchronization. Other systems can synchronize with the local system without being authenticated.

   [edit system ntp]
   user@host# **set trusted-key** [*trusted-key...*]

   where *trusted-key* is a value in the range 1–2147483647.

For example:

```
[edit system ntp]
user@host# set trusted-key 1
```

2. Depending on the mode configured for NTP, specify a key value at the [edit system ntp server], [edit system ntp peer], or [edit system ntp broadcast] hierarchy level. For example:

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

For example:

```
[edit system ntp server 192.0.2.30]
user@host# set key key1
```

The system transmits the specified authentication key when transmitting packets. The key is necessary if the remote system has authentication enabled so that it can synchronize with the local system.

3. Define the authentication keys by assigning a number to the key and configuring its value.

```
[edit system ntp]
user@host# edit authentication-key key-number
```

```
[edit system ntp authentication-key key-number]
user@host# set value value
```

The *key-number* is the key number for the key. The key number must match on all systems using that particular key for authentication.

For example:

```
[edit system ntp]
user@host# edit authentication-key 1
```

```
[edit system ntp authentication-key 1]
user@host# set value X7VY4ZE
```

4. Verify the configuration.

```
[edit system ntp]
user@host# show
trusted-key 1;
server 192.0.2.30 key 1;
authentication-key 1 {
  value ********;
}
```

### *Related Topics*

- *NTP Support on C-series Controllers on page 113*

- *Specifying Which NTP Server a C-series Controller Contacts on Startup on page 118*

- *Configuration Statements for NTP on C-series Controllers on page 117*

## Configuring NTP as a Broadcast Client on a C-series Controller with the SRC CLI

You can configure NTP on a C-series Controller to listen for broadcast messages on the local network to discover other servers on the same subnet. When NTP receives a broadcast message for the first time, it measures the nominal network delay using a brief client-server exchange with the remote server. It then enters *broadcast client* mode, in which it listens for, and synchronizes with, succeeding broadcast messages.

To avoid accidental or malicious disruption in this mode, both the local and remote systems must use authentication and the same trusted key and key identifier.

To configure NTP to listen for broadcast messages:

1.  From the [edit system ntp] hierarchy level, specify that NTP listen for broadcast messages.

    [edit system ntp]
    user@host# **set broadcast-client**

2.  Authenticate time synchronization to ensure that the local system obtains its time only from known sources.

    See *Configuring NTP Authentication on a C-series Controller with the SRC CLI on page 122*.

3.  Verify the configuration. For example:

    ```
    [edit system ntp]
    user@host# show
    broadcast-client;
    trusted-key 1;
    server 192.0.2.30 key 1;
    authentication-key 1 {
      value ********;
    }
    ```

### *Related Topics*

- *NTP Support on C-series Controllers on page 113*

- *Specifying Which NTP Server a C-series Controller Contacts on Startup on page 118*

- *Configuration Statements for NTP on C-series Controllers on page 117*

## Configuring NTP as a Multicast Client on a C-series Controller with the SRC CLI

You can configure NTP on a C-series Controller to listen for multicast messages on the local network to discover other servers on the same subnet. When NTP receives a multicast message for the first time, it measures the nominal network delay using a brief client-server exchange with the remote server. It then enters *multicast client* mode, in which it listens for, and synchronizes with, succeeding multicast messages.

You can specify one or more IP addresses or hostnames. The hosts then join those multicast groups.

To avoid accidental or malicious disruption in this mode, both the local and remote systems must use authentication and the same trusted key and key identifier.

To configure NTP to listen for multicast messages:

1. From the [edit system ntp] hierarchy level, specify that NTP listen for multicast messages.

   edit system ntp]
   user@host# **set multicast-client** *address*

   For example:

   [edit system ntp]
   user@host# **set multicast-client 224.0.1.1**

2. Authenticate time synchronization to ensure that the local system obtains its time only from known sources.

   See *Configuring NTP Authentication on a C-series Controller with the SRC CLI on page 122*.

3. Verify the configuration. For example:

   ```
   [edit system ntp]
   user@host# show
   multicast-client 224.0.1.1;
   trusted-key 1;
   server 192.0.2.30 key 1;
   authentication-key 1 {
     value ********;
   }
   ```

### Related Topics

- *NTP Support on C-series Controllers on page 113*

- *Specifying Which NTP Server a C-series Controller Contacts on Startup on page 118*

- *Configuration Statements for NTP on C-series Controllers on page 117*

## Verifying NTP Configuration on a C-series Controller

**Purpose**    To verify the configuration for NTP.

**Action**    At the [edit system ntp] hierarchy level, enter the show command. For example:

```
[edit system ntp]
user@host# show
boot-server 192.0.2.20;
multicast-client 192.0.2.15;
trusted-key 1;
server 192.0.2.30 key 1;
server 192.0.2.25;
authentication-key 1 {
  value ********;
}
```

### *Related Topics*

- *NTP Support on C-series Controllers on page 113*

- *Specifying Which NTP Server a C-series Controller Contacts on Startup on page 118*

- *Configuration Statements for NTP on C-series Controllers on page 117*

## Chapter 17

# Configuring System Logging for a C-series Controller with the SRC CLI

This chapter describes how to configure the system log server (also called a syslog server) on a C-series Controller with the SRC CLI.

You can also configure system logging with the C-Web interface. See *SRC-PE C-Web Interface Configuration Guide, Chapter 3, Configuring System Logging for a C-series Controller with the C-Web Interface.*

Topics include:

## Overview of the C-series Controller Log Server

The C-series Controller includes a system log server that you can configure to manage messages generated on the system. These messages record events that occur to system processes and components.

You can configure the system log server on a C-series Controller to send messages about events to:

- A local file

- Other hosts that are running a system log server

- Users who need to be notified about particular error conditions

You configure which groups of messages are to be forwarded by message type and severity level.

### Message Groups

Message groups (also called facilities) define sets of messages generated by the same software process or concerned with a similar condition or activity (such as authentication attempts).

You can configure the following message groups for the system log server:

- any—Messages from all facilities.

- authorization—Authentication and authorization attempts.

- daemon—Actions performed or errors encountered by various system processes.

- ftp—Actions performed or errors encountered by an FTP process.

- kernel—Actions performed or errors encountered by the kernel.

- user—Actions performed or errors encountered by various user processes.

- local7—Actions performed or errors encountered by different SRC processes.

### Severity Levels

You can specify the following severity levels for groups of messages to be forwarded:

- any—Messages for all severity levels.

- emergency—System panic or other condition that causes the system to stop functioning.

- alert—Conditions that require immediate correction.

- critical—Critical conditions, such as hard drive errors.

- error—Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels.

- warning— Conditions that warrant monitoring.

- notice—Conditions that are not errors but might warrant special handling.

- info—Events or nonerror conditions of interest.

- none—Messages are not generated for any condition.

## Before You Configure System Logging with the SRC CLI

Before you configure the syslog server on a C-series Controller, you should be familiar with:

■ The syslog protocol

■ Logging for SRC components

See *SRC-PE Monitoring and Troubleshooting Guide, Chapter 2, Configuring Logging for SRC Components*.

## Configuration Statements for System Logging on a C-series Controller

Use the following configuration statements to configure the system log server at the [edit] hierarchy level.

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

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

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

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

## Saving System Log Messages to a File with the SRC CLI

Use the following statements to configure the system log server to store messages in a file:

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

By default, message files are stored in the */var/log* directory. All log files are rotated daily. When a new log file is created, the previous day's file is compressed and saved. After rotation, the software retains only the last five compressed log files.

To configure the system log server to send messages to a file on the local C-series Controller:

1.  From configuration mode, access the configuration statement that configures the system log server.

    [edit]
    user@host# **edit system syslog**

2.  Specify the name of the file to store messages, and group and severity level for the messages.

    [edit system syslog]
    user@host# **set file** *file-name message-group severity*

    For example, to configure the system log server to save critical messages generated by authentication and authorization attempts to the file named access:

    [edit system syslog]
    user@host# **set file access authorization critical**

## Sending System Log Messages to Other Servers with the SRC CLI

Use the following statements to configure the system log server to send messages to another system log server:

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

Before you configure the system log server to send messages to other system log servers, ensure that the remote system log server is configured to receive messages on the standard UDP port, 514.

To configure the system log server to send messages to another system log server:

1.  From configuration mode, access the configuration statement that configures the system log server.

    [edit]
    user@host# **edit system syslog**

2. Specify the remote system log server to receive messages as well as the groups and severity level for those messages.

   [edit system syslog]
   user@host# **set host** *log-host-name message-group severity*

   For example, to configure the system log server to send error messages generated by processes on the C-series Controller to my-syslog-server:

   [edit system syslog]
   user@host# **set my-syslog-server.mydomain.com local7 error**

## Sending Notifications for System Log Messages to Users with the SRC CLI

Use the following statements to configure the system log server to send notifications to users:

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

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

1. From configuration mode, access the configuration statement that configures the system log server.

   [edit]
   user@host# **edit system syslog**

2. Specify the user to receive notifications and the types of notifications to be sent.

   [edit system syslog]
   user@host# **set user** *user-name message-group severity*

   For example, to configure the system log server to send notifications to admin for conditions that require immediate attention:

   [edit system syslog]
   user@host# **set user admin any critical**

# Chapter 18

# Configuring Static Host Mapping with the SRC CLI

This chapter describes how to configure static host mapping on the Solaris platform or a C-series Controller with the SRC CLI.

You can also configure static host mapping with the C-Web interface. See *SRC-PE C-Web Interface Configuration Guide, Chapter 6, Configuring Static Host Mapping with the C-Web Interface.*

Topics in this chapter include:

- Overview of Static Host Mapping on page 133

- Configuring Static Host Mapping with the SRC CLI on page 133

## Overview of Static Host Mapping

You can configure static host mapping to resolve host names. To configure static host mapping, you map the name to one or more IP addresses and aliases. Static host mapping supports both forward and reverse name lookups.

## Configuring Static Host Mapping with the SRC CLI

Use the following statements to configure static host mapping:

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

To configure static host mapping:

1. From configuration mode, access the configuration statement that configures static host mapping and specify the fully-qualified name of the system.

   [edit]
   user@host# **edit system static-host-mapping** *host-name*

2. Specify the IPv4 or IPv6 addresses to which you want to map the hostname.

   [edit system static-host-mapping *host-name*]
   user@host# **set inet** *inet*

3. (Optional) Specify the aliases for this host.

   [edit system static-host-mapping *host-name*]
   user@host# **set alias** *alias*

# Chapter 19
# Overview of the Juniper Networks Database

This chapter provides a description of the Juniper Networks database included with SRC software. Topics include:

- Overview of the Juniper Networks Database on page 135

## Overview of the Juniper Networks Database

Each C-series Controller contains a Juniper Networks database. The database can store SRC data, SRC sample data, SRC configuration information, and a number of user profiles. You store subscriber data in another database. If you run the SRC software on a Solaris platform, you can install the Juniper Networks database as your SRC data repository on that system.

When the C-series Controller starts for the first time, you must enable the Juniper Networks database. After the database is operational, you can load sample data and perform other configuration activities that use this database.

You can operate this database as a standalone database or as a member of a community of Juniper Networks databases. Typically, you run the database in standalone mode only in testing environments. In standalone mode, the database does not communicate with other Juniper Networks databases; there is no data distribution and no redundancy. In community mode, databases distribute data changes among specified databases. When you have two or more C-series Controllers, enable the Juniper Networks database to run in community mode, and assign a role to each database:

- Primary role—A database that provides read and write access to client applications. It replicates its data and distributes changes to any Juniper Networks databases configured as neighbors.

  We recommend that you configure at least two databases to have a primary role.

- Secondary role—A database that provides read access to client applications. If client applications try to write data to this database, the database refers the client to a primary database.

Neighbors are Juniper Networks databases that receive data from another Juniper Networks database. When you configure a database to be a neighbor, you configure it as one of the following types:

■ Primary neighbor—A database that propagates changes that it receives to other Juniper Networks databases configured as neighbors. A primary neighbor must be assigned a primary role.

We recommend that you configure at least two databases as primary neighbors.

■ Secondary neighbor—A database that only receives database changes. A secondary neighbor must be assigned a secondary role.

When you configure neighbors for the databases, keep in mind the following guidelines:

■ A database assigned a primary role can have primary and secondary neighbors.

■ A database assigned a secondary role must have at least one primary neighbor, but no secondary neighbors. Because a secondary database cannot distribute changes to its neighbors, if you do configure a secondary neighbor for a secondary database, the software does not use the configuration for the secondary neighbor.

To share processing load, you can configure SRC components, such as SRC-ACP, NIC, or SAE, to use a specified database. In the local configuration for SRC components, you configure the URL of the directory.

### Redundancy for a Juniper Networks Database

Protect SRC data by setting up a redundancy scheme for your Juniper Networks databases. Client applications control which database they connect to as their primary database and as their backup database.

Use the following guidelines to plan which databases are assigned primary or secondary roles, and which databases are primary or secondary neighbors:

■ Each Juniper Networks database that is assigned a primary role should have at least one primary neighbor. If a database assigned a primary role become inoperable, a client application fails over to a primary neighbor.

■ Each database that is assigned a secondary role should have at least two primary neighbors.

■ Applications that frequently perform write operations to the database should connect to databases that have a primary role. Applications that perform frequent write operations are the C-Web interface, the SRC CLI, back-office applications that provision data, and in some cases the SRC-ACP.

■ Applications that rarely perform updates, such as the NIC and SAE, can communicate with databases assigned a secondary role. For example, you could configure the NIC and SAE to communicate with the local directory on a C-series Controller, and configure the database on this system to have a secondary role.

### Security for a Juniper Networks Database

You can secure connections to a Juniper Networks database by:

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

- Allowing only LDAPS connections for database replication, but LDAP or LDAPS connections for other applications. In this case. remote SRC components can connect through LDAP or LDAPS.

The type of secure connection you configure determines which ports are open to a Juniper Networks database:

- Remote component access through LDAP—Port 389

- Remote component access through LDAPS—Port 636

- Secure database access for replication—Port 636

- Database access without security for replication—Port 389

- Local component access through LDAP—Port 389

You can also increase the security of your Juniper Networks database by changing the passwords that SRC components use to communicate with the database.

### Related Topics

- For information about configuring the SAE to access subscriber data, see the *SRC-PE Network Guide: SAE, Juniper Networks Routers, NIC, and SRC-ACP, Chapter 2, Configuring the SAE with the SRC CLI*.

- *Configuration Statements for the Juniper Networks Database with the SRC CLI* on page 140

- *Example: Configuration for a Database Community* on page 150

## Chapter 20

# Managing the Juniper Networks Database with the SRC CLI

This chapter describes the Juniper Networks database and how to configure it. Topics include:

## Configuration Statements for the Juniper Networks Database with the SRC CLI

Use the following configuration statements to configure the Juniper Networks database at the [edit] hierarchy level:

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

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

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

☞ The **strict** statement is supported only on C-series Controllers.

*Related Topics*

■ *Overview of the Juniper Networks Database on page 135*

■ *Enabling the Juniper Networks Database to Run in Standalone Mode with the SRC CLI on page 141*

■ *Enabling the Juniper Networks Database to Run in Community Mode with the SRC CLI on page 141*

■ *Securing the Juniper Networks Database with the SRC CLI on page 143*

## Enabling the Juniper Networks Database to Run in Standalone Mode with the SRC CLI

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

Use the following configuration statements to enable the Juniper Networks database on a C-series Controller in standalone mode:

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

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

1.  From configuration mode, access the configuration statement that configures the Juniper Networks database.

    user@host# **edit system ldap server**

2.  Enable standalone mode.

    [edit system ldap server]
    user@host# **set stand-alone**

### Related Topics

- *Overview of the Juniper Networks Database on page 135*

- *Configuration Statements for the Juniper Networks Database with the SRC CLI on page 140*

- *Enabling the Juniper Networks Database to Run in Community Mode with the SRC CLI on page 141*

- *Securing the Juniper Networks Database with the SRC CLI on page 143*

## Enabling the Juniper Networks Database to Run in Community Mode with the SRC CLI

If you are adding a Juniper Networks database to an existing community, see *Adding a Juniper Networks Database to an Established Community with the SRC CLI on page 144*.

Use the following configuration statements to enable the Juniper Networks database on a C-series Controller in community mode:

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

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

1. From configuration mode, access the configuration statement that configures the Juniper Networks database in community mode:

   user@host# **edit system ldap server community**

2. Specify the role of the database as primary or secondary:

   [edit system ldap server community]
   user@host# **set role primary**

   or

   [edit system ldap server community]
   user@host# **set role secondary**

3. Configure primary neighbors. Specify each neighbor by IP address, fully qualified hostname, or a hostname that can be resolved through the domain name system:

   [edit system ldap server community]
   user@host# **set primary-neighbors** *neighbor* …

   For example, set C1 and C2 as primary neighbors:

   [edit system ldap server community]
   user@host# **set primary-neighbors C1 C2**

4. Configure secondary neighbors. Specify each neighbor by IP address, fully qualified hostname, or a hostname that can be resolved through the domain name system:

   [edit system ldap server community]
   user@host# **set secondary-neighbors** *neighbor …*

   For example, set C3 and C4 as secondary neighbors:

   [edit system ldap server community]
   user@host# **set secondary-neighbors C3 C4**

### *Related Topics*

- *Overview of the Juniper Networks Database on page 135*

- *Configuration Statements for the Juniper Networks Database with the SRC CLI on page 140*

- *Enabling the Juniper Networks Database to Run in Standalone Mode with the SRC CLI on page 141*

- *Securing the Juniper Networks Database with the SRC CLI on page 143*

- *Example: Configuration for a Database Community on page 150*

## Securing the Juniper Networks Database with the SRC CLI

You can secure connections to a Juniper Networks database by:

- Allowing only Secure Lightweight Directory Access Protocol (LDAPS) connections from remote systems. In this case, both database replication and remote SRC components connect through LDAPS. Restricting all remote connections to LDAPS is supported only on C-series Controllers.

- Allowing only LDAPS connections for database replication, but LDAP or LDAPS connections for other applications. In this case. remote SRC components can connect through LDAP or LDAPS.

Use the following configuration statements to secure connections to the Juniper Networks database on a C-series Controller:

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

☞ The **strict** statement is supported only on C-series Controllers.

To secure the Juniper Networks database, perform one of the following tasks:

- (Optional) From configuration mode, access the configuration statement that configures the Juniper Networks database to secure connections to other Juniper Networks databases for data replication:

  user@host# **edit system ldap server security enable**

- (Optional) From configuration mode, access the configuration statement that configures the Juniper Networks database to accept connections only through LDAPS:

  user@host# **edit system ldap server security strict**

### *Related Topics*

- *Overview of the Juniper Networks Database on page 135*

- *Securing Communications Between the Juniper Networks Database and SRC Components with the SRC CLI on page 148*

## Changing the Mode of a Juniper Networks Database with the SRC CLI

Because the Juniper Networks database can run in either standalone or community mode, to change modes you must disable the current mode and enable the other mode. Typically, you change from standalone mode, which was used for testing, to community mode for a full deployment.

To change the mode of the Juniper Networks database from standalone to community:

1.  Disable standalone mode:

    [edit system ldap server]
    user@host# **delete stand-alone**

2.  Enable the database in community mode, and configure the role and neighbors.

    See *Enabling the Juniper Networks Database to Run in Community Mode with the SRC CLI on page 141*.

### *Related Topics*

■   *Chapter 19, Overview of the Juniper Networks Database*

■   *Configuration Statements for the Juniper Networks Database with the SRC CLI on page 140*

## Adding a Juniper Networks Database to an Established Community with the SRC CLI

When you add a Juniper Networks database to an existing community, make sure that you configure the primary neighbor relationships from the existing primary databases before you enable the new database.

⚠   If you assign a primary role to a database new to an existing community before you configure the neighbor relationships from existing community databases that have a primary role, you can lose data on neighbor databases that already have a primary role.

To add a Juniper Networks database to an existing community:

1.  On existing databases that have a primary role, configure neighbor relationships for the new database.

    For example, to configure primary neighbors for the existing servers C1 and C2 for the new server C-new:

    On C1:

    [edit system ldap server community]
    user@C1# **set primary-neighbor C-new**

    On C2:

    [edit system ldap server community]
    user@C2# **set primary-neighbor C-new**

2. On the new database, enable the primary role and configure primary neighbors.

   For example, to enable the database in primary role and configure C1 and C2 as primary neighbors:

   [edit]
   user@C-new# **edit system ldap server community**
   [edit system ldap server community]
   user@C-new# **set role primary**
   user@C-new# **set primary-neighbors C1 C2**

### *Related Topics*

- *Overview of the Juniper Networks Database on page 135*

- *Enabling the Juniper Networks Database to Run in Community Mode with the SRC CLI on page 141*

## Promoting a Secondary Database to a Primary Role in a Configuration with One Primary Database with the SRC CLI

Although all communities should have two databases with a primary role, if a community includes one database assigned a primary role and another database assigned a secondary role, promote the database assigned a secondary role to a primary role.

To promote a Juniper Networks database from a secondary role to a primary role:

1. On the database that has a secondary role, set the role to primary.

   For example, if the database on C2 has a secondary role:

   user@C2# **edit system ldap server community**
   [edit system ldap server community]
   user@C2# **set role primary**
   user@C2# **commit**


   C2 already has C1 configured as primary neighbor.

2. On the existing database that has a primary role, remove the neighbor as secondary and add it as primary.

   For example, to remove C2 as a secondary neighbor and add it as a primary neighbor for the database on C1:

   user@C1# **edit system ldap server community**
   [edit system ldap server community]
   user@C1# **set primary-neighbors C2**
   user@C1# **commit**

3. (Optional if you have two databases with a primary role in a community) Switch the role of the database that originally had a secondary role back to secondary:

[edit system ldap server community]
user@C2# **set role secondary**
user@C2# **commit**

### Related Topics

- *Overview of the Juniper Networks Database on page 135*

- *Enabling the Juniper Networks Database to Run in Community Mode with the SRC CLI on page 141*

## Updating Data on a Juniper Networks Database with the SRC CLI

After you bring a Juniper Networks database online after some period of inaccessibility, update the database with any database changes that occurred while the database was offline.

To update data in a neighbor (for example, neighbor1) in a community of Juniper Networks databases:

user@host> **request system ldap community force-update neighbor neighbor1**

### Related Topics

- *Getting Information About Operations in a Juniper Networks Database with the SRC CLI on page 149*

## Synchronizing Data on a Juniper Networks Database with the SRC CLI

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

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

user@host> **request system ldap community initialize neighbor neighbor1**

### Related Topics

- *Updating Data on a Juniper Networks Database with the SRC CLI on page 146*

- *Getting Information About Operations in a Juniper Networks Database with the SRC CLI on page 149*

## Loading Sample Data in to a Juniper Networks Database with the SRC CLI

The SRC software provides sample data that you can load into the Juniper Networks database. Typically, this data is used for testing or for demonstration purposes. You can load sample data for:

- Enterprise service portals

- SNMP traps for the SNMP agent

- Sample applications:

  - Dynamic Service Activator application (in the SRC Application Library)

  - Intrusion Detection and Prevention (IDP) integration application (unsupported sample application in the SRC Application Library)

  - Instant Virtual Extremity (IVE) Host Checker integration application (unsupported sample application in the SRC Application Library)

  - Traffic-Mirroring Application (unsupported sample application in the SRC Application Library)

  - Sample residential portal (unsupported sample application in the SRC Application Library)

    - Equipment registration mode

    - Internet service provider (ISP) mode

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

To load sample data for the Enterprise Manager Portal and the sample enterprise service portal:

user@host> **request system ldap load enterprise-portal**

To load sample data for the SNMP agent:

user@host> **request system ldap load snmp-agent**

To load sample data for the Dynamic Service Activator application:

user@host> **request system ldap load dsa-configuration**

To load sample data for the Intrusion Detection and Prevention (IDP) integration application:

user@host> **request system ldap load idp-configuration**

To load sample data for the Instant Virtual Extremity (IVE) Host Checker integration application:

user@host> **request system ldap load hostchecker-configuration**

To load sample data for the Traffic-Mirroring Application:

user@host> **request system ldap load tm-configuration**

To load sample data for the sample residential portal to demonstrate an application that provides a means for subscribers to directly log in to a subscriber session for their ISP:

user@host> **request system ldap load isp-service-portal**

To load sample data for the sample residential portal to demonstrate an application that provides an association between a subscriber and the equipment being used to make the DHCP connection:

user@host> **request system ldap load equipment-registration**

### *Related Topics*

■   *Overview of the Juniper Networks Database on page 135*

## Securing Communications Between the Juniper Networks Database and SRC Components with the SRC CLI

Communications between SRC components and the Juniper Networks database use password authentication. You can change the default passwords for the following software components to ensure that communications are secure.

■   SRC CLI

■   NIC

■   Configuration for SRC components other than the CLI and the NIC

To change a user password:

> user@host>**request system ldap change-component-password**
> *component-name* **new-password** *new-password*

where *component-name* is:

■   cli—Specifies communication between the SRC CLI and the database

■   conf—Specifies communication about configuration

■   nic—Specifies communication between NIC components and the database

### *Related Topics*

■   *Securing the Juniper Networks Database with the SRC CLI on page 143*

## Verifying Configuration for a Juniper Networks Database with the SRC CLI

To review the configuration for the Juniper Networks database on a C-series Controller:

■ Run the **show system ldap server** command at the [edit] hierarchy level. For example:

```
[edit]
user@host# show system ldap server
community {
 role primary;
 primary-neighbors C2;
}
```

The output indicates the mode, standalone or community. If the database is running in community mode, the output also includes information about the community configuration on this system.

If the command does not display any output, the Juniper Networks database on the system is disabled.

### *Related Topics*

■ *Configuration Statements for the Juniper Networks Database with the SRC CLI on page 140*

■ *Enabling the Juniper Networks Database to Run in Standalone Mode with the SRC CLI on page 141*

■ *Enabling the Juniper Networks Database to Run in Community Mode with the SRC CLI on page 141*

■ *Securing the Juniper Networks Database with the SRC CLI on page 143*

## Getting Information About Operations in a Juniper Networks Database with the SRC CLI

To get information about operations performed on a Juniper Networks database:

```
user@host> show system ldap statistics
Local JDB statistics
Number of Add operations since startup        0
Number of Delete operations since startup     0
Number of Modify operations since startup     0
Number of Rename operations since startup     0
Number of Read operations since startup       265
Number of List operations since startup       129
Number of Subtree Search operations since startup 114
Number of Bind operations                     110
Number of Anonymous Bind operations since startup 94
Number of Compare operations since startup    0
Number of current connections                 3
Number of all connections since startup       110
Number of bind errors since startup           0
Number of all errors since startup            59
```

### *Related Topics*

## Example: Configuration for a Database Community

A community of Juniper Networks databases lets you set up redundancy for client applications that connect to these databases.

This sample configuration describes the tasks for configuring Juniper Networks databases on C-series Controllers:

- Requirements on page 150

- Overview and Sample Topology on page 150

- Configuration on page 151

### *Requirements*

#### Software

Minimum SRC Release 1.0.0

#### Hardware

C2000 or C4000

### *Overview and Sample Topology*

You configure a number of Juniper Networks databases as members of a community to protect data by replicating data from one database to another, and by specifying relationships between databases to support failover if a database that has the primary role for a set of applications becomes inoperable. This example uses C1 and C2 as databases that have a primary role, and C3 as a database that has a secondary role.

Figure 20 shows the sample configuration.

**Figure 20: Sample Community of Juniper Network Databases**
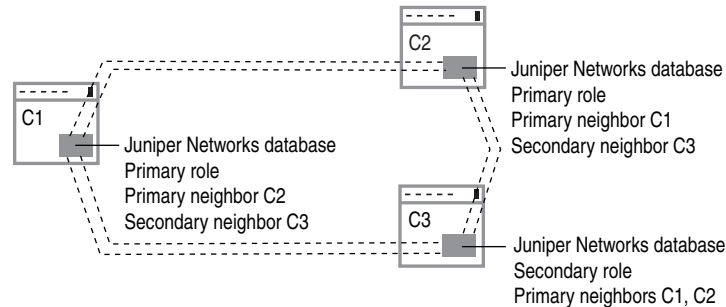


The following configuration shows the configuration statements for databases shown in Figure 20.

## Configuration

### Configuring C1

**Quick Configuration**    To quickly configure a Juniper Networks database, copy the following commands into a text editor, and modify them; then load the configuration from the file.

[edit]
    **set system ldap server community role primary**
    **set system ldap server community primary-neighbors C2**
    **set system ldap server community secondary-neighbors C3**

**Step-by-Step Procedure**    To configure the C1 system:

1. From configuration mode, access the configuration statement that configures the Juniper Networks database in community mode.

   [edit]
   user@C1# **edit system ldap server community**

2. Specify the database role as primary.

   [edit system ldap server community]
   user@C1# **set role primary**

3. Specify primary neighbors.

   [edit system ldap server community]
   user@C1# **set primary-neighbors C2**

4. Specify secondary neighbors.

   [edit system ldap server community]
   user@C1# **set secondary-neighbors C3**

## Configuring C2

**Quick Configuration**  To customize the configuration example for your needs, copy the following commands into a text editor, and modify them; then load the configuration from the file.

[edit]
    **set system ldap server community role primary**
    **set system ldap server community primary-neighbors C1**
    **set system ldap server community secondary-neighbors C3**

**Step-by-Step Procedure**  To configure the C2 system:

1. From configuration mode, access the configuration statement that configures the Juniper Networks database in community mode.

   [edit]
   user@C2# **edit system ldap server community**

2. Specify the database role as primary.

   [edit system ldap server community]
   user@C2# **set role primary**

3. Specify primary neighbors.

   [edit system ldap server community]
   user@C2# **set primary-neighbors C1**

4. Specify secondary neighbors.

   [edit system ldap server community]
   user@C2# **set secondary-neighbors C3**

## Configuring C3

**Quick Configuration**  To customize the configuration example for your needs, copy the following commands into a text editor, and modify them; then load the configuration from the file.

[edit]
    **set system ldap server community role secondary**
    **set system ldap server community primary-neighbors C1 C2**

**Step-by-Step Procedure**  To configure the C3 system:

1. From configuration mode, access the configuration statement that configures the Juniper Networks database in community mode.

   [edit]
   user@C3# **edit system ldap server community**

2.  Specify the database role as primary.

    [edit system ldap server community]
    user@C3# **set role secondary**

3.  Specify primary neighbors.

    [edit system ldap server community]
    user@C3# **set primary-neighbors C1 C2**

### *Related Topics*

- *Overview of the Juniper Networks Database on page 135*

- *Configuration Statements for the Juniper Networks Database with the SRC CLI on page 140*

- *Enabling the Juniper Networks Database to Run in Community Mode with the SRC CLI on page 141*

## Troubleshooting Data Synchronization for Juniper Networks Databases with the SRC CLI

**Problem**   Data in a community of Juniper Networks databases may not be synchronized.

**Solution**  1.  Obtain information about the replication status of Juniper Networks databases in a community by running the show system ldap community on system that runs the primary Juniper Networks database:

   user@host> **show system ldap community**

   The command output indicates that the databases are not synchronized by:

   - Quantity of changes since last startup

   - Start and end time of last update

   - Status of last update

2.  If the databases are not synchronized, initialize neighbors in the community from the primary Juniper Networks database:

   user@host> **request system ldap community initialize neighbor neighbor 1**

   where neighbor1 is the name of the neighbor to be synchronized.

### *Related Topics*

## Recovering Data in a Community with One Primary Database and One Secondary Database with the SRC CLI

In an environment in which a community includes one database assigned a primary role and another database assigned a secondary role, and the primary database is not operative, you must promote the secondary database to primary and reconfigure the inoperative primary database.

1. On the database that has a secondary role, set the role to primary.

   For example, if the database on C2 has a secondary role:

   ```
   user@C2# edit system ldap server community
   [edit system ldap server community]
   user@C2# set role primary
   user@C2# commit
   ```

   C2 already has C1 configured as primary neighbor.

2. On the existing database that has a primary role, remove the neighbor as secondary and add it as primary.

   For example, to configure C1 as a primary database with C2 as a primary neighbor:

   ```
   user@C1# edit system ldap server community
   [edit system ldap server community]
   user@C1# set role primary
   user@C1# delete secondary-neighbors C2
   user@C1# set primary-neighbors C2
   user@C1# commit
   ```

### *Related Topics*

## Chapter 21
# Setting Up an SAE with the SRC CLI

This chapter describes how to initially configure the SAE and how to create grouped SAE configurations with the SRC CLI.

■ To use the SRC CLI to set up an SAE, see *SRC-PE C-Web Interface Configuration Guide, Chapter 8, Setting Up an SAE with the C-Web Interface.*

■ To set up the SAE on a Solaris platform, see *Chapter 35, Setting Up an SAE on a Solaris Platform.*

Topics in this chapter include:

■ Initially Configuring the SAE on page 155

■ Creating Grouped Configurations for the SAE with the SRC CLI on page 156

■ Configuring Local Properties for the SAE with the SRC CLI on page 157

■ Configuring the RADIUS Local IP Address and NAS ID with the SRC CLI on page 159

■ Starting and Stopping the SAE with the SRC CLI on page 159

## Initially Configuring the SAE

To initially configure the SAE:

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

See *Creating Grouped Configurations for the SAE with the SRC CLI* on page 156

■ Configure local properties for the SAE.

See *Configuring Local Properties for the SAE with the SRC CLI* on page 157

■ Configure a local IP address and NAS ID that the SAE uses to communicate with RADIUS servers.

See *Configuring the RADIUS Local IP Address and NAS ID with the SRC CLI* on page 159

■ Configure directory connection properties for the SAE.

See *Configuring Directory Connection Properties* on page 239

■ Configure directory eventing properties for the SAE.

*See Configuring Initial Directory Eventing Properties for SRC Components* on page 240

## Creating Grouped Configurations for the SAE with the SRC CLI

We recommend that you configure the SAE within a group. When you create a configuration group, the software creates a configuration with default values filled in.

Configuration groups allow you to build hierarchies that define different levels of sharing. There is a shared SAE configuration that you configure at the **shared sae configuration** hierarchy level. The configuration is shared with all SAE instances in the SRC network.

You can then create a grouped SAE configuration that is shared with some SAE instances. For example, if you create an SAE group called region within the shared SAE configuration, you could share the SAE configuration with all SAE instances in a particular region.

You can then create a lower-level group called location in the SAE group region, which could be shared with SAE instances in a particular location.

Configuration options that are defined in a lower-level group override options in a higher-level group. This functionality allows you to define general configuration values (such as plug-in definitions) on a higher level and augment or specialize them on a lower level.

### *Configuring an SAE Group*

Use the **shared** option of the **set slot number sae shared** command to add a new group. Use the **shared sae group** *name* command to configure the group.

To configure a group:

1. From configuration mode, add a group. For example, to add a group called REGION-1 in the path /SAE/:

   [edit]
   user@host# **set slot 0 sae shared /SAE/REGION-1**

2. Commit the configuration.

   [edit]
   user@host# **commit**
   commit complete.

3. Configure the group as you would a shared SAE configuration.

```
[edit]
user@host# edit shared sae group REGION-1 ?
Possible completions:
  <[Enter]>               Execute this command
> configuration
> dhcp-classifier          Configure a DHCP classification script
> group                    Group of SAE configuration properties
> user-classifier          Configure a subscriber classification script
  |                        Pipe through a command
```

## Configuring Local Properties for the SAE with the SRC CLI

Use the following configuration statements to configure local properties for the SAE:

slot *number* sae {
    base-dn *base-dn*;
    real-portal-address *real-portal-address*;
    java-runtime-environment *java-runtime-environment*;
    java-heap-size *java-heap-size*;
    java-new-size *java-new-size*;
    java-garbage-collection-options *java-garbage-collection-options*;
    port-offset *port-offset*;
    snmp-agent;
    shared *shared*;
}

To configure local properties on the SAE:

1. From configuration mode, access the SAE RADIUS configuration. This configuration is under the slot 0 hierarchy.

   [edit]
   user@host# **edit slot 0 sae**

2. (Optional) If you store data in the directory in a location other than the default, *o = umc*, change this value.

   [edit slot 0 sae]
   user@host# **set base-dn** *base-dn*

3. Configure the interface on the SAE that the SAE uses to communicate with the router.

   [edit slot 0 sae]
   user@host# **set real-portal-address** *real-portal-address*

4. (Optional. Solaris platform.) If the Java Runtime Environment (JRE) is not in the default location (*../jre/bin/java*) on a Solaris platform, change the directory path to the JRE.

   [edit slot 0 sae]
   user@host# **set java-runtime-environment** *java-runtime-environment*

5.  (Optional) If you encounter problems caused by lack of memory, change the maximum memory size available to the JRE.

    [edit slot 0 sae]
    user@host# **set java-heap-size** *java-heap-size*

6.  Configure the amount of space available to the JRE when the SAE starts.

    [edit slot 0 sae]
    user@host# **set java-new-size** *java-new-size*

7.  Configure the garbage collection functionality of the Java Virtual Machine.

    [edit slot 0 sae]
    user@host# **set java-garbage-collection-options** *java-garbage-collection-options*

8.  If you install multiple instances of the SAE on the same host, set a port offset for SAE instances.

    [edit slot 0 sae]
    user@host# **set port-offset** *port-offset*

9.  (Optional) Enable the SNMP agent to communicate with the SAE.

    [edit slot 0 sae]
    user@host# **set snmp-agent**

10. (Optional) Configure an SAE group configuration.

    [edit slot 0 sae]
    user@host# **set shared** *shared*

11. (Optional) Verify your configuration.

    ```
    [edit slot 0 sae]
    user@host# show
    base-dn o=UMC;
    real-portal-address 10.10.4.24;
    java-runtime-environment ../jre/bin/java;
    java-heap-size 896m;
    java-new-size 22m;
    java-garbage-collection-options "-Xbatch -XX:+UseConcMarkSweepGC
    -XX:CMSInitiatingOccupancyFraction=80 -XX:+UseParNewGC -XX:SurvivorRatio=1
    -XX:InitialTenuringThreshold=8 -XX:MaxTenuringThreshold=10
    -XX:TargetSurvivorRatio=90 -XX:+UseCMSCompactAtFullCollection
    -XX:CMSFullGCsBeforeCompaction=0  -XX:+CMSPermGenSweepingEnabled
    -XX:+CMSClassUnloadingEnabled -XX:+CMSParallelRemarkEnabled";
    port-offset 0;
    snmp-agent;
    shared /SAE/REGION-1;
    ```

## Configuring the RADIUS Local IP Address and NAS ID with the SRC CLI

Use the following configuration statements to set the local RADIUS address and network access server (NAS ID):

```
slot number sae radius {
    local-address local-address;
    local-nas-id local-nas-id;
}
```

To set the local RADIUS address and NAS ID:

1. From configuration mode, access the SAE RADIUS configuration. This configuration is under the slot 0 hierarchy.

   ```
   [edit]
   user@host# edit slot 0 sae radius
   ```

2. Configure the local IP address that the SAE uses to communicate with RADIUS servers.

   ```
   [edit slot 0 sae radius]
   user@host# set local-address local-address
   ```

3. Configure the NAS ID that identifies the SAE when it sends RADIUS authentication and accounting records. Typically, the NAS ID is the name of the SAE host.

   ```
   [edit slot 0 sae radius]
   user@host# set local-nas-id local-nas-id
   ```

4. (Optional) Verify your configuration.

   ```
   [edit slot 0 sae radius]
   user@host# show
   local-address 10.10.4.20;
   local-nas-id SAE.host1;
   ```

## Starting and Stopping the SAE with the SRC CLI

You must configure licenses before you start the SAE. When you start the SAE, the software verifies that a valid license is available. If no license is found, the SAE does not start.

To start the SAE:

- From operational mode, enable the SAE.

  ```
  user@host> enable component sae
  Check license: OK
  Starting sae: may take a few minutes...
  ```

To stop the SAE:

■ From operational mode, disable the SAE.

```
user@host> disable component sae
Shutting down the SAE server: done
```

To verify that the SAE is running:

■ From operational mode, enter the show component command.

```
user@host> show component
Installed Components
Name      Version                                        Status
cli       Release: 7.0 Build: CLI.A.7.0.0.0171           running
acp       Release: 7.0 Build: ACP.A.7.0.0.0174           disabled
jdb       Release: 7.0 Build: DIRXA.A.7.0.0.0176         running
editor    Release: 7.0 Build: EDITOR.A.7.0.0.0176        disabled
redir     Release: 7.0 Build: REDIR.A.7.0.0.0176         disabled
licSvr    Release: 7.0 Build: LICSVR.A.7.0.0.0179        stopped
nic       Release: 7.0 Build: GATEWAY.A.7.0.0.0170       disabled
sae       Release: 7.0 Build: SAE.A.7.0.0.0166           running
www       Release: 7.0 Build: UMC.A.7.0.0.0169           disabled
jps       Release: 7.0 Build: JPS.A.7.0.0.0172           disabled
agent     Release: 7.0 Build: SYSMAN.A.7.0.0.0174        disabled
webadm    Release: 7.0 Build: WEBADM.A.7.0.0.0173        disabled
```

# Chapter 22
# Managing System Software on a C-series Controller

This chapter describes how to upgrade, install, and uninstall system software, create a snapshot of system software, and revert system software on a C-series Controller. Topics include:

- Overview of Software Management on a C-series Controller on page 161
- Before You Upgrade the Software on a C-series Controller on page 162
- Creating a Snapshot of Files on a C-series Controller on page 162
- Upgrading the System Software on a C-series Controller on page 163
- Upgrading SRC Software for a Component on page 165
- Installing SRC Software for a Component on page 165
- Removing an Installed Component on page 165
- Restoring the Files in a Snapshot on page 166

## Overview of Software Management on a C-series Controller

On a C-series Controller you can upgrade all the system software or the software package for a component. You can also install and uninstall a software package for an SRC component. Table 11 lists the names of the packages for the components that run on the C-series Controller.

**Table 11:  Package Names for Components on a C-series Controller**

| Component | Package Name |
|---|---|
| Command-line interface (CLI) | UMCcli |
| C-Web interface | UMCwebadm |
| IP multimedia subsystem | UMCims |
| Java Web server | UMCtomcat |
| Juniper Networks database | UMCjdb |
| Juniper Policy Server (JPS) | UMCjps |
| License Server | UMClicsvr |

**Table 11: Package Names for Components on a C-series Controller (continued)**

| Component | Package Name |
|---|---|
| Network information Collector (NIC) | UMCnic |
| Policies, Services, and Subscribers CLI | UMCeditor |
| Redirect Server | UMCredir |
| Service activation engine (SAE) | UMCsae |
| SNMP agent | UMCagent |
| SRC-ACP | UMCacp |

## Before You Upgrade the Software on a C-series Controller

Before you upgrade system software on a C-series Controller:

- Create a snapshot of the software files currently on the C-series Controller.

  See *Creating a Snapshot of Files on a C-series Controller on page 162*.

- Make sure that other C-series Controllers can carry system load during the upgrade. The system will not be operational during the upgrade.

## Creating a Snapshot of Files on a C-series Controller

You can create a snapshot of the system software to serve as a backup. When you create a snapshot, the software backs up the operating system and the SRC software to a partition on the C-series Controller. You can restore the files in a snapshot to the system software if needed.

To create a snapshot of the system software:

1.  Verify which version of the software is running on the system.

    user@host> **show system information**

2.  Enter the request system snapshot command. Use the verbose option to view information about the snapshot process.

    ```
    user@host> request system snapshot verbose
    Create system snapshot [yes,no] ? (no) yes

    Filesystem label=
    mke2fs 1.35 (28-Feb-2004)
    OS type: Linux
    Block size=4096 (log=2)
    Fragment size=4096 (log=2)
    262144 inodes, 524288 blocks
    26214 blocks (5.00%) reserved for the super user
    First data block=0
    Maximum filesystem blocks=536870912
    16 block groups
    32768 blocks per group, 32768 fragments per group
    16384 inodes per group
    Superblock backups stored on blocks:
            32768, 98304, 163840, 229376, 294912
    ```

```
Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 32 mounts or
180 days, whichever comes first. Use tune2fs -c or -i to override.
  DUMP: Date of this level 0 dump: Thu Oct 19 09:43:44 2006
  DUMP: Dumping /dev/mapper/vg0-root (/) to standard output
restore: cannot open /dev/tty: No such device or address
  DUMP: Label: none
  DUMP: Writing 64 Kilobyte records
  DUMP: mapping (Pass I) [regular files]
  DUMP: mapping (Pass II) [directories]
  DUMP: estimated 1036678 blocks.
  DUMP: Volume 1 started with block 1 at: Thu Oct 19 09:43:45 2006
  DUMP: dumping (Pass III) [directories]
  DUMP: dumping (Pass IV) [regular files]

  DUMP: Volume 1 completed at: Thu Oct 19 09:48:13 2006
  DUMP: Volume 1 1035200 blocks (1010.94MB)
  DUMP: Volume 1 took 0:01:10
  DUMP: Volume 1 transfer rate: 14788 kB/s
  DUMP: 1035200 blocks (1010.94MB)
  DUMP: finished in 70 seconds, throughput 14788 kBytes/sec
  DUMP: Date of this level 0 dump: Thu Oct 19 09:47:02 2006
  DUMP: Date this dump completed:  Thu Oct 19 09:48:13 2006
  DUMP: Average transfer rate: 14788 kB/s
```

## Upgrading the System Software on a C-series Controller

You can upgrade all the system software or the software changes for an SRC component. If an image file (from which you upgrade) contains updates for all components or a number of components, you specify which component to upgrade if you do not want to upgrade all components.

For ease of use, you can manage upgrades for a number of C-series Controllers by copying a complete CD image file to be used for an upgrade to an FTP site in your network. You then upgrade each system by using the files on the FTP site. Alternatively, you can copy the complete CD image to a USB drive and install from there.

To upgrade C-series Controller software:

■ Enter the request system upgrade command.

user@host> **request system upgrade url** *url*

For example:

```
user@host> request system upgrade url ftp://myserver/pub/UMC/7.0.0/B
Setting up Upgrade Process
Setting up repositories
Reading repository metadata in from local files
Resolving Dependencies
--> Populating transaction set with selected packages. Please wait.
---> Downloading header for python-ldap to pack into transaction set.
---> Package python-ldap.i386 0:2.0.6-1 set to be updated
--> Running transaction check

Dependencies Resolved

=============================================================
 Package            Arch      Version       Repository      Size
=============================================================
Updating:
 python-ldap               i386      2.0.6-1        umc-upgrade      150 k

Transaction Summary
=============================================================
Install      0 Package(s)
Update       1 Package(s)
Remove       0 Package(s)
Total download size: 150 k
Downloading Packages:
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction

  Updating  : python-ldap                    ####################### [1/1]

Updated: python-ldap.i386 0:2.0.6-1
Complete!
```

The C-series Controller automatically reboots at the end of the upgrade.

## Upgrading SRC Software for a Component

To upgrade a specified SRC component:

■ Specify the package name for a component when you enter the **request system upgrade** command.

user@host> **request system upgrade url** *url* **package** *package*

For example:

user@host> **request system upgrade url ftp://myserver/pub/UMC/7.0.0/B package UMCnic**

The C-series Controller automatically reboots at the end of the upgrade.

## Installing SRC Software for a Component

To install the software for a component:

■ Specify the package name for a component when you enter the **request system install** command.

user@host> **request system install url** *url* **package** *package*

For example:

user@host> **request system install url ftp://myserver/pub/UMC/7.0.0/B package UMCnic**

## Removing an Installed Component

To remove a component that is installed on a C-series Controller:

■ Specify the package name for a component when you enter the **request system uninstall** command.

user @ host> **request system uninstall package** *package*

For example:

user @ host> **request system uninstall package UMCnic**

## Restoring the Files in a Snapshot

To revert to the system software stored in snapshot files:

■   Enter the request system restore command.

```
user@host> request system restore
WARNING: restoring a snapshot will cause the system to
reboot and replace the software with the data from the
system snapshot.
Rebooting to start restore
```

The C-series Controller reboots twice during a restoration.

## Chapter 23
# Using the Embedded Web Server for Testing on a C-series Controller

This chapter describes how to use the Java Web server on a C-series Controller for testing. Topics include:

- Overview of Java Web Server on C-series Controllers on page 167
- Deploying a Web Application in the Web Server on page 167
- Starting the Web Server on a C-series Controller on page 168
- Restarting the Web Server on a C-series Controller on page 168
- Stopping the Web Server on a C-series Controller on page 168

## Overview of Java Web Server on C-series Controllers

The SRC software on a C-series Controller includes a Java Web server for demonstration purposes. The Web server is not supported for use in production environments. Use a Web server that runs on another system to deploy Web applications to be used with the SRC software.

The Web server listens on port 8080. It can be accessed through the eth0 or eth1 interface.

## Deploying a Web Application in the Web Server

To deploy a Web application in the Web server:

1. Prepare the WAR file on a machine other than the C-series Controller.

2. Copy the WAR file to be deployed to the */opt/UMC/www/webapps* directory on the C-series Controller.

   For example:

   user@host> **file copy ftp://host/path/ssportal.war /opt/UMC/www/webapps**

## Starting the Web Server on a C-series Controller

To start the Web server on a C-series Controller:

user@host> **enable component www**

## Restarting the Web Server on a C-series Controller

To restart the Web server on a C-series Controller:

user@host> **restart component www**

## Stopping the Web Server on a C-series Controller

To stop the Web server on a C-series Controller:

user@host> **disable component www**

**Part 5**

# Managing SRC Access and Security with the CLI

**Chapter 24**

# Configuring User Access with the SRC CLI

This chapter contains information about how to configure user access to the SRC software and how to configure an announcement for users to see at login using the SRC CLI.

You can configure user access to the SRC software using the C-Web interface. See *SRC-PE C-Web Interface Configuration Guide, Chapter 4, Configuring User Access with the C-Web Interface.*

Topics in this chapter include:

- Overview of SRC User Accounts on page 171

- Login Classes for User Accounts with the SRC CLI on page 172

- Configuring Login Classes with the SRC CLI on page 179

- Configuring User Accounts with the SRC CLI on page 183

- Configuring a System Login Announcement with the SRC CLI on page 189

## Overview of SRC User Accounts

All users who can log in to the SRC software must be a member of a login class. With login classes, you define the following:

- Access privileges users have when they are logged in to the SRC software

- Commands and statements that users can and cannot specify

- How long a login session can be idle before it times out and the user is logged out.

You can define any number of login classes. You then apply one login class to an individual user account.

## Login Classes for User Accounts with the SRC CLI

The SRC software provides four predefined login classes to use for configuring user accounts. You can also configure login classes to precisely define access privileges for the user accounts in your SRC environment.

### Access Privilege Level

In the SRC CLI, each top-level command-line interface (CLI) command and each configuration statement have an access privilege level associated with them. Similarly, each task and subtask in the C-Web interface have an access privilege level associated with them. Users can configure and view only those tasks for which they have access privileges. The access privileges for each login class are defined by one or more *permission options*.

Permission options specify which actions are allowed for users assigned to use a login class. More than one permission option can be configured for a login class. Table 12 lists the permission options available when you configure permissions with the SRC CLI and the C-Web interface.

You can use the SRC CLI or the C-Web interface to configure permission options for all commands, statements, tasks, and subtasks. For example, if you configure a user to have the **system** permission class using the C-Web interface, that user will have the same permission when accessing the SRC CLI.

The privilege level for each command and statement is listed in *SRC-PE CLI Command Reference*.

The SRC software also provides a default set of system login classes that have permissions preset. Table 12 on page 172 lists the default system login classes.

**Table 12:  Login Class Permission Options**

| Permission | Description |
|---|---|
| admin | SRC CLI—Can view user account information in configuration mode and with the **show configuration** command. |
| | C-Web interface—Can view user account information by accessing the **Monitor > CLI > Authorization**. |
| admin-control | SRC CLI—Can view user accounts and configure them at the [edit system login] hierarchy level. |
| | C-Web interface—Can view user accounts and configure them by accessing **Configure > System > Login**. |
| all | SRC CLI and C-Web interface—Has all permissions. |
| clear | SRC CLI—Can clear (delete) information learned from the network that is stored in various network databases using the **clear** commands. |
| | C-Web interface—Can clear (delete) information learned from the network that is stored in various network databases by accessing **Manage > Clear**. |
| configure | SRC CLI—Can enter configuration mode using the **configure** command. |
| | C-Web interface—Can access the **Configure** task and subtasks. |

**Table 12: Login Class Permission Options   (continued)**

| Permission | Description |
| --- | --- |
| control | SRC CLI and C-Web interface—Can perform all control-level operations (all operations configured with the -control permission). |
| field | SRC CLI and C-Web interface—Reserved for field (debugging) support. |
| firewall | SRC CLI—Can view the firewall filter configuration in configuration mode. |
| | C-Web interface—Can view the firewall filter configuration by accessing **Monitor > SAE > Services**. |
| firewall-control | SRC CLI—Can view and configure firewall filter information at the [edit firewall] hierarchy level. |
| | C-Web interface—Can view and configure firewall filter information by accessing **Configure > Services**. |
| interface | SRC CLI—Can view the interface configuration in configuration mode and with the show configuration operational mode command. |
| | C-Web interface—Can view the interface configuration by accessing **Monitor > Interfaces**. |
| interface-control | SRC CLI—Can view chassis, class of service, groups, forwarding options, and interfaces configuration information. Can configure chassis, class of service, groups, forwarding options, and interfaces at the [edit] hierarchy level. |
| | C-Web interface—Can view chassis, class of service, groups, forwarding options, and interfaces configuration information. Can configure chassis, class of service, groups, forwarding options, and interfaces by accessing the **Configure** task and subtasks. |
| maintenance | SRC CLI—Can perform system maintenance, including starting a local shell on the system and becoming the superuser in the shell (by issuing the su root command), and can halt and reboot the system (using the request system commands). |
| | C-Web interface—Can perform system maintenance, including halting and reboot the system, by accessing **Manage > Request > System**. |
| network | SRC CLI and C-Web interface—Can access the network by entering the SSH and telnet commands. |
| reset | SRC CLI—Can restart software processes using the restart command, enable components using the enable command, and disable components using the disable command. |
| | C-Web interface—Can restart software processes by accessing **Manage > Restart**, enable components by accessing **Manage > Enable**, and disable components by accessing **Manage > Disable**. |
| routing | SRC CLI—Can view general routing information in configuration and operational modes. |
| | C-Web interface—Can view general routing information by accessing **Monitor > SAE > Route**. |
| routing-control | SRC CLI—Can view and configure general routing at the [edit routing-options] hierarchy level. |
| | C-Web interface—Can view general routing and configure general routing by accessing **Configure > Routing Options**. |
| secret | SRC CLI and C-Web interface—Can view passwords and other authentication keys in the configuration. |

**Table 12:  Login Class Permission Options   (continued)**

| Permission | Description |
| --- | --- |
| secret-control | SRC CLI—Can view passwords and other authentication keys in the configuration and can modify them in configuration mode. |
| | C-Web interface—Can view passwords and other authentication keys in the configuration and can modify them by accessing **Configure > System > Login**. |
| security | SRC CLI—Can view security configuration in configuration mode and with the **show configuration** operational mode command. |
| | C-Web interface—Can view security configuration by accessing **Monitor > Security > Certificate**. |
| security-control | SRC CLI—Can view and configure security information at the [edit security] hierarchy level. |
| | C-Web interface—Can view security information and configure security information by accessing **Manage > Request > Security**. |
| service | SRC CLI and C-Web interface—Can view service and policy definitions. |
| | C-Web interface—Can view service definitions by accessing **Monitor > SAE > Services** and policy definitions by accessing **Monitor > SAE > Policies**. |
| service-control | SRC CLI—Can view and modify service and policy definitions. |
| | C-Web interface—Can view and modify service and policy definitions by accessing **Configure > Services** and **Configure > Policies**. |
| shell | SRC CLI and C-Web interface—Can start a local shell by entering the **start shell** command. |
| snmp | SRC CLI—Can view Simple Network Management Protocol (SNMP) configuration information in configuration and operational modes. |
| | C-Web interface—Can view Simple Network Management Protocol (SNMP) configuration information by accessing **Monitor > SAE > Statistics**. |
| snmp-control | SRC CLI—Can view SNMP configuration information and configure SNMP (at the [edit snmp] hierarchy level). |
| | C-Web interface—Can view SNMP configuration information and configure SNMP by accessing **Configure > SNMP**. |
| subscriber | SRC CLI—Can view information about subscriber definitions. |
| | C-Web interface—Can view information about subscriber definitions by accessing **Monitor > SAE > Subscribers**. |
| subscriber-control | SRC CLI —Can view and control information about subscriber definitions. |
| | C-Web interface—Can view information about subscriber definitions and control information about subscriber definitions by accessing **Configure > Subscribers**. |

**Table 12: Login Class Permission Options   (continued)**

| Permission | Description |
|---|---|
| system | SRC CLI—Can view system-level information in configuration and operational modes. |
| | C-Web interface—Can view system-level configuration information by accessing **Monitor > System**. |
| system-control | SRC CLI—Can view system-level configuration information and configure it at the [**edit system**] hierarchy level. |
| | C-Web interface—Can view system-level configuration and configure it by accessing **Configure > System**. |
| view | SRC CLI—Can use various commands to display current systemwide, routing table, and protocol-specific values and statistics. |
| | C-Web interface—Can access various **Monitor** subtasks to display current systemwide, routing table, and protocol-specific values and statistics. |
| view-configuration | SRC CLI and C-Web interface—Can view all system configurations, excluding any secret configuration. |

When you configure more than one permission, the resulting set of permissions is a combination of all of the permissions set, except for **all** and **control**.

When you configure permissions, include **view** to display information and **configure** to enter configuration mode. Two forms for the permissions control the individual parts of the configuration:

- "Plain" form—Provides read-only capability for that permission type. An example is **interface**.

- Form that ends in **-control**—Provides read and write capability for that permission type. An example is **interface-control**.

## *Predefined Login Classes*

Table 13 lists the system login classes predefined in the SRC software.

**Table 13: Default System Login Classes**

| Login Class | Permission Options Set |
|---|---|
| operator | clear, network, reset, view |
| read-only | view |
| super-user | all |
| unauthorized | None |

☞ **NOTE:** You cannot modify a predefined login class name. If you issue the set command on a predefined class name with the SRC CLI, the software will append -local to the login class name. The following message also appears:

warning: '*<class-name>*' is a predefined class name; changing to '*<class-name>*-local'

**NOTE:** You cannot issue the rename or copy command on a predefined login class with the SRC CLI. Doing so results in the following error message:

error: target '*<classname>*' is a predefined class

## *Access to Individual Commands and Configuration Statements with the SRC CLI*

By default, all top-level CLI commands have associated access privilege levels. Users can execute only those commands and view only those statements for which they have access privileges. For each login class, you can deny or allow the use of specified operational and configuration mode commands that would otherwise be permitted or not allowed by a specified privilege level.

### Regular Expressions for Allow and Deny Statements

You can use extended regular expressions to specify which commands to allow or deny. By using extended regular expressions, you can list a number of commands in each statement.

You specify these regular expressions in the following statements at the [edit system login class] hierarchy level:

- allow-commands

- deny-commands

- allow-configuration

- deny-configuration

Command regular expressions implement the extended (modern) regular expressions as defined in POSIX 1003.2. Table 14 lists common regular expression operators.

**Table 14:  Common Regular Expression Operators to Allow or Deny Operational Mode and Configuration Mode Commands**

| Operator | Match |
|---|---|
| **Operation Mode and Configuration Mode** | |
| \| | One of the two terms on either side of the pipe. |
| ^ | Character at the beginning of an expression. Used to denote where the command begins, where there might be some ambiguity. |
| $ | Character at the end of a command. Used to denote a command that must be matched exactly up to that point. For example, **allow-commands "show interfaces$"** means that the user can issue the **show interfaces** command but cannot issue **show interfaces detail** or **show interfaces extensive**. |
| [ ] | Range of letters or digits. To separate the start and end of a range, use a hyphen ( - ). |
| ( ) | A group of commands, indicating an expression to be evaluated; the result is then evaluated as part of the overall expression. |
| **Configuration Mode Only** | |
| * | 0 or more terms. |
| + | One or more terms. |
| **.** (dot) | Any character except for a space. |

## Guidelines for Using Regular Expressions

Keep in mind the following considerations when using regular expressions to specify which statements or commands to allow or deny:

- Regular expressions are not case-sensitive.

- If a regular expression contains a syntax error, authentication fails and the user cannot log in.

- If a regular expression does not contain any operators, all varieties of the command are allowed.

Follow these guidelines when using regular expressions:

- Enclose the following in quotation marks:

  - A command name or regular expression that contains:

    - Spaces

    - Operators

    - Wildcard characters

■ An extended regular expression that connects two or more terms with the pipe (|) symbol. For example:

[edit system login class *class-name*]
user@host# **set deny-configuration "(system login class) | (system services)"**

■ Do not use spaces between regular expressions separated with parentheses and connected with the pipe (|) symbol.

■ Specify the full paths in the extended regular expressions with the allow-configuration and deny-configuration options.

☞ **NOTE:** You cannot define access to keywords such as set or edit.

## *Timeout Value for Idle Login Sessions*

An idle login session is one in which the CLI operational mode prompt is displayed but there is no input from the keyboard. By default, a login session remains established until a user logs out of the system, even if that session is idle. To close idle sessions automatically, you configure a time limit for each login class. If a session established by a user in that class remains idle for the configured time limit, the session automatically closes.

For users who belong to a login class for which an idle timeout is configured, the CLI displays messages similar to the following when an idle user session times out.

user@host# Session will be closed in 5 minutes if there is no activity.
Warning: session will be closed in 1 minute if there is no activity
Warning: session will be closed in 10 seconds if there is no activity
Idle timeout exceeded: closing session

If you configure a timeout value, the session closes after the specified time has elapsed, except if the user is running commands such as ssh, start shell, or telnet.

The C-Web interface session closes after the specified time has elapsed with no message, and returns to the login window.

## Configuring Login Classes with the SRC CLI

Before you configure a login class:

■ Review the predefined login classes to determine whether you can use one of these classes rather than creating a new one.

See *Predefined Login Classes* on page 175.

■ Make sure you are familiar with how to use regular expressions to specify which commands and configuration statements to allow or deny.

Consider that you can issue one **allow** statement and one **deny** statement for operation mode commands, and one **allow** statement and one **deny** statement for configuration mode commands. Use regular expressions in a statement to specify more than one command in a statement.

See *Regular Expressions for Allow and Deny Statements* on page 176.

### Configuration Statements for Login Classes

Use the following configuration statements to configure login classes at the [edit] hierarchy level:

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

### Configuring a Login Class

To configure a login class:

1. From configuration mode, access the configuration statement that configures login classes, and assign a name to the login class.

   [edit]
   user@host# **edit system login class** *name*

2. Specify the permissions for the login class.

   [edit system login class *name*]
   user@host# **set permissions** *permissions*

   For example, the following statement specifies that the user-account class can configure and view only user accounts:

   [edit system login class user-accounts]
   user@host# **set permissions [configure admin admin-control]**

   The following statement specifies that the network-mgmt class can configure and view only SNMP parameters:

   [edit system login class network-mgmt]
   user@host# **set permissions [configure snmp snmp-control]**

3. (Optional) Configure access to specified operational mode commands that would otherwise be denied.

   [edit system login class *name*]
   user@host# **set** allow-commands *allow-commands*

   For example, the following statement specifies that the network-mgmt class can install system software:

   [edit system login class network-mgmt]
   user@host# **set allow-commands "request system install"**

4. (Optional) Deny access to specified operational mode commands that would otherwise be allowed.

   [edit system login class *class-name*]
   user@host# **set** deny-commands *deny-commands*

   For example, the following statement specifies that the remote class cannot connect to the SRC software through Telnet:

   [edit system login class remote]
   user@host# **set deny-commands telnet**

5.  (Optional) Configure access to specified configuration mode commands that would otherwise be denied.

    [edit system login class *name*]
    user@host# **set** allow-configuration *allow-configuration*

    For example, the following statement specifies that the network-mgmt class can issue configuration mode commands at the [routing-options] hierarchy level:

    [edit system login class network-mgmt]
    user@host# **set allow-configuration "routing options"**

6.  (Optional) Deny access to specified configuration mode commands that would otherwise be allowed.

    [edit system login class *name*]
    user@host# **set** deny-configuration *deny-configuration*

    For example, the following statement specifies that the network-mgmt class does not have access to the [snmp address] hierarchy level:

    [edit system login class network-mgmt]
    user@host# **set deny-configuration "snmp address"**

7.  Specify the number of minutes that a session can be idle before it is automatically closed.

    [edit system login class class-name]
    user@host# **set idle-timeout** *minutes*

8.  Display the results of the configuration.

    ```
    [edit system login]
    user@host# show

    class network-mgmt {
      allow-commands "request system install";
      allow-configuration routing-options;
    deny-configuration "snmp address";
    }
    class remote {
      deny-configuration "system services telnet";
      permissions all;
    }
    ```

### Examples: Configuring Access Privileges for Operational Mode Commands

The following example allows access to the request system reboot command for the login class operator-and-boot that has operator privileges defined by the clear, network, reset, and view permissions.

    [edit system login class operator-and-boot]
    user@host# **set permissions [ clear network reset view ]**
    user@host# **set allow-commands "request system reboot"**

The following example denies access to set commands for the login class operator-no-set that has operator privileges defined by the clear, network, reset, and view permissions.

    [edit system login class operator-no-set]
    user@host# **set permissions [ clear network reset view ]**
    user@host# **set deny-commands "set"**

The following example allows software installation but denies access to the show nic command for the login class operator-no-set that has operator privileges defined by the clear, network, reset, and view permissions.

    [edit system login class operator-and-install-no-nic]
    user@host# **set permissions [ clear network reset view ]**
    user@host# **set allow-commands "request system install**"
    user@host# **set deny-commands "show nic"**

### Examples: Defining Access Privileges for Configuration Mode Commands

The following example does not allow access the C-series Controller through a Telnet session for the login class remote that has permission set to all:

> [edit system login class remote]
> user@host# **set permissions all**
> user@host# **set deny-configuration "system services telnet"**

The following example does not allow access to any login class whose name begins with "m" for the login class local that has permission set to all:

> [edit system login class local]
> user@host# **set permissions all**
> user@host# **set deny-configuration "system login class m.*"**

The following example does not allow access to configuration mode commands at the [system login class] or [system services hierarchy] levels for the login class config-admin that has permission set to all:

> [edit system login class config-admin]
> user@host# **set permissions all**
> user@host# **set deny-configuration "(system login class) | (system services)"**

## Configuring User Accounts with the SRC CLI

User accounts provide one way for users to access the system. For each account, you define the login name for the user, properties for the user account, and authentication information. After you create an account, the software creates a home directory for the user when the user logs in to the system for the first time.

Each user has a home directory on the C-series Controller, which is created the first time that the user logs in. Home directories that have the same name as the user ID are created in the */var/home* directory; for example, the home directory for a user with the user ID Chris_Bee is */var/home/Chris_Bee.*

### *Configuration Statements for User Accounts*

Use the following configuration statements to configure user accounts at the [edit] hierarchy level.

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

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

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

### Configuring a User Account

To configure a user account:

1. From configuration mode, access the configuration statement that configures a user account, and specify a username that identifies the user.

   [edit]
   user@host# **edit system login user** *user-name*

   The username must be unique within the system. Do not include spaces, colons, or commas in the username. For example:

   [edit]
   user@host# **edit system login user JASmith**

   [edit system login user JASmith]
   user@host#

2. Specify the name of the login class that defines the user's access privilege. [edit system login user *user-name]*

   [edit system login user *user-name*]
   user@host# **set class** *class*

   The login class is one of the login classes that you defined in the **class** statement at the [edit system login] hierarchy level, or one of the default classes listed in Table 7 on page 64.

3. Specify the user's full name.

   [edit system login user *user-name*]
   user@host# **set full-name** *full-name*

   If the full name contains spaces, enclose it in quotation marks. Do not include colons or commas. For example:

   [edit system login user JASmith]
   user@host# **set full-name "John A. Smith"**

4. (Optional) Specify a user identifier (UID) for the user.

   [edit system login user *user-name*]
   user@host# **set uid** *uid*

   The identifier must be a number in the range 0 through 64,000 and must be unique within the system. If you do not assign a UID to a username, the software assigns one when you commit the configuration, preferring the lowest available number.

   You must ensure that the UID is unique. However, it is possible to assign the same UID to different users.

5. (Optional) Specify a prompt that the user sees at the SRC CLI.

   [edit system login user *user-name*]
   user@host# **set prompt** *prompt*

6. (Optional) Specify the editing level available to the user. The level determines which configuration commands are visible to the user.

   [edit system login user *user-name*]
   **user@host# set level** (basic | normal | advanced | expert)

   where:

   - basic—Minimal set of configuration statements and commands— only the statements that must be configured are visible.

   - normal—Normal set of configuration statements and commands— the common and basic statements are visible.

   - advanced—All configuration statements and commands, including the common and basic ones, are visible.

   - expert—All configuration statements, including common, basic, and internal statements and commands used for debugging, are visible.

7. (Optional) Specify whether entering a space completes a command.

   [edit system login user *user-name*]
   **user@host# set complete-on-space** (on | off)

   If you do not enter a value, **complete-on-space** is enabled by default.

8. Define the authentication methods that a user can use to log in to a C-series Controller.

   See *Configuring Authentication for User Accounts* on page 186.

9. Display the results of the configuration.

```
[edit system login]
user@host# show
. . .
user JASmith {
  class network-mgmt;
  full-name "John A. Smith";
  uid 507;
  gid 100;
  authentication {
    encrypted-password "{crypt}caZEWDaE1au0c";
  }
  level normal;
  complete-on-space on;
}
```

### Configuring Authentication for User Accounts

You can configure the following types of authentication for user accounts:

- Plain text password—Prompt for a plain text (unencrypted) password. The requirements for plain text passwords are:

  - Can contain between 6 and 128 characters

  - Can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters).

    > **NOTE:** We do not recommend that the password include control characters. We do recommend that the password include at least one change of case or character class.

  If you configure a plain text password, you are prompted to enter and confirm the password.

- Encrypted password—Password encoded with crypt. The format of encrypted passwords is "{crypt} < 13-characters in a-zA-Z0-9./> ".

    > **NOTE:** We recommend that you *do not* enter the password in encrypted format.

- SSH—SSH authentication. For SSH authentication, you can copy the contents of an SSH keys file into a CLI session.

## Configuring a Plain Text Password

To configure a plain text password for a user account:

■  At the [edit system user *user-name*] hierarchy, enter the **set authentication plain text-password** command. For example:

> [edit system user JASmith]
> user@host# **set authentication plain-text-password**
> New password: *type password here*
> Retype new password: *retype password here*

## Configuring SSH Authentication

Before you configure SSH authentication, obtain the contents of SSH key files. You can copy the contents of an SSH keys file into a CLI session:

1.  On a management machine such as a PC or personal workstation, create an ssh-rsa key:

> **ssh-keygen**
> (provide input)
> **cat ~/.ssh/id_rsa.pub**

2.  On the C-series Controller enter the **set system login user testuser authentication ssh-authorized-key** command, and paste in the SSH key:

user@host# **set system login user testuser authentication ssh-authorized-key** "*pasted content of id_rsa.pub*"

For example:

> user@host# **set system login user testuser authentication ssh-authorized-key** "ssh-rsa
> AAAAB3NzaC1yc2EAAAABIwAAAIEAvSqAWNdMTQJS9eqG1eq
>     RANI3ML4hH+u7WX/HP0W82gDSPpjghnt1e5de3D8UkuIIEUBf1obgy/7AK
>     c98FqAIvVp5onCiMg8ELD6
>     RYkgOgo7U6zERB25qy3sK1Rn9NzrB20qLzbvAcZW1NIePmf1R99d/Rge7k
>     B/5k6fq3NOG0fc= id@server" "ssh-rsa
>     AAAAB3NzaC1yc2EAAAABIwAAAIEAxIwe9HfZ78vbdfq1+AY0uCF79yGPxgGu
>     w
>     GZd9QVdT+dniwGh/4HwLITvKd8SYrhmJsyhz5dWuZm94JSwQosm9BVhJw
>     REt39NYIkLWOjGIMkk8Cxw4
>     TkpFfeIz1cSbeFxtFBFVaBbo4YkEv5ItbuxwvbTWURkvsQa2VJXAqIs7z8=
>     id2@server2
>     eriand" "ssh-rsa
>     AAAAB3NzaC1yc2EAAAABIwAAAIEAwwOoUD4m+SazgzF2kRIq5Y2+Ix2zQb
>     CxqBS
>     D1rmW92eLPOQIBv/sEy2d8UNeHpoKot9Px8q9ABriOyONc7vqNsSVnAMyi
>     cQB786uHoabSErVlYscapT
> YvIGg+olbdhKySbSxOoXMehhgoQS0JZxHCbxsQJip7/7vJPCjRGU8Xq0=
> id@server3" ];

### Changing the root Password

An account for the user **root** is always present in the configuration. Only the root user can change the root password.

To change the **root** password:

1.  Log into the SRC software as **root**.

2.  From operational mode, change the **root** password.

    root@host> **set cli password**
    Changing password for user root.
    New UNIX password:

You can also create a regular account for **root** and set the SSH key there. The class for **root** is always super-user—if you create an account for **root**, the class is ignored.

## *Example: User Accounts*

The following example shows the configuration for user accounts for three system users and the template user "remote." All users use one of the default system login classes.

```
system login user philip {
    class super-user;
    full-name "Philip of Macedonia";
    uid 1001;
    authentication {
        encrypted-password "{crypt}6YPqJe88Wz5fQ";
        ssh-authorized-keys [ "ssh-rsa
        AAAAB3NzaC1yc2EAAAABIwAAAIEAvSqAWNdMTQJS9eqG1eq
        RANI3ML4hH+u7WX/HP0W82gDSPpjghnt1e5de3D8UkuIIEUBf1obgy/7AK
        c98FqAIvVp5onCiMg8ELD6
        RYkgOgo7U6zERB25qy3sK1Rn9NzrB20qLzbvAcZW1NIePmf1R99d/Rge7k
        B/5k6fq3NOG0fc= id@server" "ssh-rsa
        AAAAB3NzaC1yc2EAAAABIwAAAIEAxIwe9HfZ78vbdfq1+AY0uCF79yGPxgGu
        w
        GZd9QVdT+dniwGh/4HwLITvKd8SYrhmJsyhz5dWuZm94JSwQosm9BVhJw
        REt39NYIkLWOjGIMkk8Cxw4
        TkpFfeIz1cSbeFxtFBFVaBbo4YkEv5ItbuxwvbTWURkvsQa2VJXAqIs7z8=
        id2@server2
        eriand" "ssh-rsa
        AAAAB3NzaC1yc2EAAAABIwAAAIEAwwOoUD4m+SazgzF2kRIq5Y2+Ix2zQb
        CxqBS
        D1rmW92eLPOQIBv/sEy2d8UNeHpoKot9Px8q9ABriOyONc7vqNsSVnAMyi
        cQB786uHoabSErVIYscapT
        YvIGg+olbdhKySbSxOoXMehhgoQS0JZxHCbxsQJip7/7vJPCjRGU8Xq0=
        id@server3" ];
    }
    user alexander {
        full-name "Alexander the Great";
        uid 1002;
        class view;
        authentication {
            encrypted-password "{crypt}6ZSqJe75Tz5fN";
            ssh-authorized-keys [ "ssh-rsa
```

```
                    AAAAB3NzaC1yc2EAAAABIwAAAIEAvSqAWNdMTQJS9eqG1eq
                    RANI3ML4hH+u7WX/HP0W82gDSPpjghnt1e5de3D8UkuIIEUBf1obgy
                    /7AKc98FqAIvVp5onCiMg8ELD6
                    RYkgOgo7U6zERB25qy3sK1Rn9NzrB20qLzbvAcZW1NIePmf1R99d
                    /Rge7kB/5k6fq3NOG0fc= id@server" "ssh-rsa
                    AAAAB3NzaC1yc2EAAAABIwAAAIEAxlwe9HfZ78vbdfq1+AY0uCF79y
                    GPxgGuw
                    GZd9QVdT+dniwGh/4HwLITvKd8SYrhmJsyhz5dWuZm94JSwQosm9
                    BVhJwREt39NYIkLWOjGIMkk8Cxw4
                    TkpFfeIz1cSbeFxtFBFVaBbo4YkEv5ItbuxwvbTWURkvsQa2VJXA
                    qIs7z8= id2@server2
                    eriand" "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAwwOoUD4m+Sazgz
                    F2kRIq5Y2+Ix2zQbCxqBS
                    D1rmW92eLPOQIBv/sEy2d8UNeHpoKot9Px8q9ABriOyONc7vqNsS
                    VnAMyicQB786uHoabSErVIYscapT
                    YvIGg+olbdhKySbSxOoXMehhgoQS0JZxHCbxsQJip7/7vJPCjRGU
                    8Xq0= id@server3" ];
                  }
              }
              user darius {
                full-name "Darius King of Persia";
                uid 1003;
                class operator;
                authentication {
                  ssh "1024 37 12341234@ecbatana.per";
                }
              }
              user remote {
                full-name "All remote users";
                uid 9999;
                class read-only;
              }
          }
```

# Configuring a System Login Announcement with the SRC CLI

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

To configure a system login announcement:

■   At the [edit system login] hierarchy level, add the **announcement** statement.

[edit system login]
user@host# **set announcement** *text*

If the announcement text contains any spaces, enclose it in quotation marks.

**Chapter 25**

# Authenticating Users on a C-series Controller with the SRC CLI

This chapter describes how to configure RADIUS and TACACS+ authentication for users who access a C-series Controller using the SRC CLI.

You can also use the C-Web interface to configure RADIUS and TACACS+ authentication. See *SRC-PE C-Web Interface Configuration Guide, Chapter 5, Authenticating Users on a C-series Controller with the C-Web Interface*.

Topics in this chapter include:

- Configuring RADIUS and TACACS+ Authentication on a C-series Controller on page 191

- Configuring RADIUS Authentication with the SRC CLI on page 192

- Configuring TACACS+ Authentication with the SRC CLI on page 193

- Configuring More Than One Authentication Method with the SRC CLI on page 194

- Configuring Template Accounts for RADIUS and TACACS+ Authentication with the SRC CLI on page 197

- Example: Configuring System Authentication on page 199

## Configuring RADIUS and TACACS+ Authentication on a C-series Controller

The SRC software always performs password authentication on a C-series Controller. You can configure RADIUS and/or TACACS+ authentication to complement password authentication. In this case, the software performs RADIUS and or TACACS+ authentication before password authentication.

To configure RADIUS and TACACS+ authentication for users who access a C-series Controller:

1. Configure the connection to the RADIUS or TACACS+ server.

   See *Configuring RADIUS Authentication with the SRC CLI* on page 192.

   See *Configuring TACACS+ Authentication with the SRC CLI* on page 193.

2. Configure the authentication order.

   See *Configuring More Than One Authentication Method with the SRC CLI* on page 194.

3. Configure template accounts.

   See *Configuring Template Accounts for RADIUS and TACACS+ Authentication with the SRC CLI* on page 197.

4. (Optional) Configure individual user profiles.

   See *Chapter 24, Configuring User Access with the SRC CLI*.

## Configuring RADIUS Authentication with the SRC CLI

Use the following configuration statements to configure information about one or more RADIUS servers on the network at the [edit] hierarchy level:

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

To configure information about RADIUS servers for authentication:

1. From configuration mode, access the configuration statement that adds a RADIUS server.

   ```
   [edit]
   user@host# edit system radius-server address
   ```

2. Specify a port number on which to contact the RADIUS server.

   ```
   [edit system radius-server address]
   user@host# set port port
   ```

   By default, port number 1812 is used as specified in RFC 2865—Remote Authentication Dial In User Service (RADIUS) (June 2000).

3. Specify a password. Passwords can contain spaces. The secret used by the C-series Controller must match that used by the server.

   ```
   [edit system radius-server address]
   user@host# set secret secret
   ```

4.  (Optional) Specify the amount of time that the C-series Controller waits to receive a response from a RADIUS server.

    [edit system radius-server *address*]
    user@host# **set timeout** *timeout*

    By default, the C-series Controller waits 3 seconds. You can change the timeout to a value from 1 through 90 seconds.

5.  Specify the number of times that the C-series Controller attempts to contact a RADIUS authentication server.

    [edit system radius-server *address*]
    user@host# **set retry** *retry*

    By default, the C-series Controller retry property is set to 3 times. You can change the retry value to a number from 1 through 10 times.

To configure a set of users that share a single account for authorization purposes, you create a template user. See *Configuring Template Accounts for RADIUS and TACACS+ Authentication with the SRC CLI* on page 197.

## Configuring TACACS+ Authentication with the SRC CLI

Use the following configuration statements to configure information about one or more TACACS+ servers on the network at the [edit] hierarchy level:

```
system tacplus-server {
    address address;
    secret secret;
}
```

To configure information about TACACS+ servers for authentication:

1.  From configuration mode, access the configuration statement that adds a RADIUS server.

    [edit]
    user@host# **edit system** tacplus-server

2.  Specify the address of the TACACS+ server.

    [edit system tacplus-server]
    user@host# **set address** *address*

    To configure multiple TACACS+ servers, include multiple values for the **address** option.

3. Specify a secret (password) that the C-series Controller passes to the TACACS + client by including the **secret** statement. Secrets can contain spaces. The secret used by the C-series Controller must match the secret used by the TACACS + server.

[edit system tacplus-server]
user@host# **set secret** *secret*

To configure a set of users that share a single account for authorization purposes, you create a template user. See *Configuring Template Accounts for RADIUS and TACACS + Authentication with the SRC CLI* on page 197.

## Configuring More Than One Authentication Method with the SRC CLI

On a C-series Controller, you can use more than one authentication method. You can configure the C-series Controller to be a RADIUS and TACACS + client by:

■ Configuring RADIUS and TACACS + authentication.

■ Configuring the authentication order to prioritize the order in which the C-series Controller uses configured authentication methods.

For each login attempt, the SRC software tries the authentication methods in the order configured, until the password matches. If one of the authentication methods in the authentication order fails to authenticate a user, the user is denied access to the C-series Controller.

If password authentication does not appear in the prioritized list of authentication methods, the SRC software uses password authentication last. The SRC software always uses password authentication, whether or not it appears in the list of authentication methods to be used. As a result, users can log in to the C-series Controller through password authentication if configured authentication servers are unavailable.

Figure 21 shows three authentication scenarios. In the first two, a user is authenticated while authentication servers are unavailable. In the third scenario, a users is not authenticated by an active server.

**Figure 21: Authentication Order: RADIUS, TACACS+, Password**
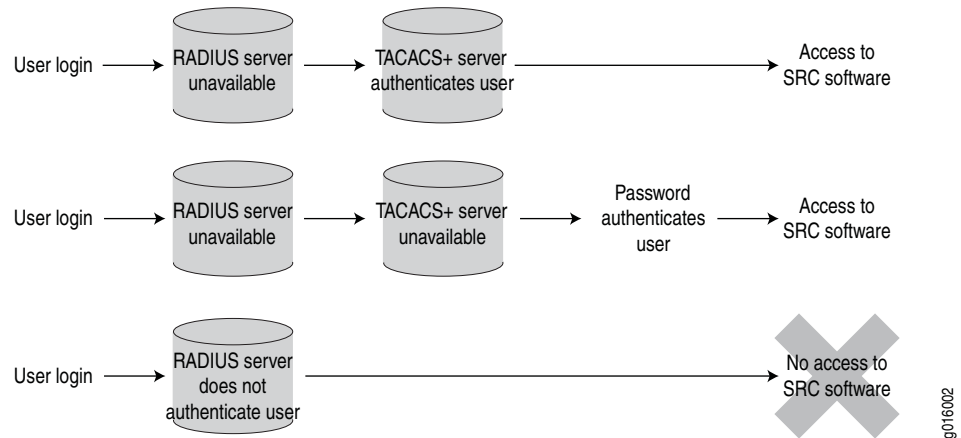


## Configuring Authentication Order

To configure the order in which to use authentication servers:

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

2. Specify the authentication order.

   [edit system]
   user@host# **set authentication-order** [(radius | tacplus | password)]

   Specify one or more of the following in the preferred order, from first authentication method tried to last tried:

   ■ **radius**—Verify the user using RADIUS authentication services.

   ■ **tacplus**—Verify the user using TACACS+ authentication services.

   ■ **password**—Verify the user using the password configured for the user with the **authentication** statement at the [edit system login user] hierarchy level.

If you do not include the **authentication-order** statement, users are verified based on their configured passwords.

### Configuring TACACS+ or RADIUS Authentication

To configure the SRC software to try to authenticate users through TACACS + and, if the TACACS + server is unavailable, to use password authentication:

■ Specify the following authentication order:

[edit]
user@host# **set system authentication-order [tacplus password]**

or

[edit]
user@host# **set system authentication-order tacplus**

To configure the SRC software to try to authenticate users through RADIUS and, if the RADIUS server is unavailable, to use password authentication:

■ Specify the following authentication order:

[edit]
user@host# **set system authentication-order [radius password]**

or

[edit]
user@host# **set system authentication-order radius**

### Configuring TACACS+ and RADIUS Authentication

To configure the SRC software to try to authenticate users through TACACS + and, if the TACACS + server is unavailable, to use RADIUS authentication; and then, if the RADIUS server is unavailable, to use password authentication:

■ Specify the following authentication order:

[edit]
user@host# **set system authentication-order [tacplus radius password]**

or

[edit]
user@host# **set system authentication-order [tacplus radius]**

To configure the SRC software to try to authenticate users through RADIUS and, if the RADIUS server is unavailable, to use TACACS+ authentication; and then, if the TACACS+ server is unavailable, to use password authentication:

■ Specify the following authentication order:

[edit]
user@host# **set system authentication-order [radius tacplus password]**

or

[edit]
user@host# **set system authentication-order [radius tacplus]**

### *Removing an Authentication Method from the Authentication Order*

To delete the radius statement from the authentication order:

■ Enter the following command:

[edit system]
user@host# **delete authentication-order** [(radius | tacplus)]

For example:

[edit system]
user@host# **delete authentication-order radius**

## Configuring Template Accounts for RADIUS and TACACS+ Authentication with the SRC CLI

When a user logs in to the CLI, the following authentication is performed:

■ RADIUS and /or TACSACS+ server authentication

■ Authentication through a user account configured under [system login user]

For authorization purposes, you can use a template account to create a single account that can be shared by a set of users at the same time.

Typically when you use RADIUS and/or TACACS+ authentication, the user account is shared among a group of users who have the same privileges. You create template accounts for sets of users. Template accounts can be named:

■ remote—(Default) A single account that defines user permissions for all users that authenticate through RADIUS or TACACS+

■ *name-of-your-choice*—Account for a group of users

Use a named template account when you need different types of templates. Each template can define a different set of permissions appropriate to a group of users who use that template. For example, you can configure a set of remote users to concurrently share a single UID.

When a user is part of a group that uses a template account, the command-line interface (CLI) username is the login name; however, the privileges, file ownership, and effective username are inherited from the template account.

### Using Named Template Accounts

Template accounts for which you define a name are defined on a C-series Controller and are referenced by the TACACS+ and RADIUS authentication servers through usernames. All users who share a local user template account have the same access privileges.

When a user who accesses the C-series Controller through a name template account logs in:

1. The SRC software issues a request to the authentication server to authenticate the user's login name.

2. If a user is authenticated, the server returns the username to the SRC software.

3. The SRC software determines whether a username is specified for that login name.

4. If there is a username, the SRC software selects the appropriate template.

5. If a user template does not exist for the authenticated user, the C-series Controller uses the remote template.

### Using Remote Template Accounts

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

- Include the system login user remote statement at the [edit] hierarchy level, and specify the "All remote users" for the full-name option:

```
[edit]
system login user remote {
    full-name "All remote users";
    uid uid-value;
    class class-name;
}
```

All users who share the remote template account have the same access privileges.

### Configuring a Local User Template

To configure a local user template and specify the privileges that you want to grant to the local users to whom the template applies:

- Include the **system login user** *local-username* statement at the [edit] hierarchy level, and specify the name of the group for the **full-name** option.

```
[edit]
system login user username {
    full-name "name of group";
    uid uid-value;
    class class-name;
}
```

## Example: Configuring System Authentication

The following example allows login only by:

- Individual user Philip

- Users who have been authenticated by a remote RADIUS server

If a user logs in and is not authenticated by the RADIUS server, the user is denied access to the C-series Controller. However, if the RADIUS server is not available, the user can be authenticated through an SRC password.

In this example, user configuration includes:

- An individual user account for Philip that provides privileges for the **super-user** class after RADIUS authentication.

- A remote user template account for all other users to share the same class and user ID (UID) after RADIUS authentication.

Individual SRC accounts are not configured for other users. When they log in to the system and the RADIUS server authenticates them, they are given access using the same UID 9999 and the same privileges for the **operator** class.

```
[edit]
system {
    authentication-order radius;
    login {
        user philip {
            full-name "Philip";
            uid 1001;
            class super-user;
        }
        user remote {
            full-name "All remote users";
            uid 9999;
            class operator;
        }
    }
}
```

# Chapter 26
# Managing Security Digital Certificates

This chapter describes how digital certificates are used on by the SRC software and how to obtain and delete these certificates. Topics include:

## Overview of Digital Certificates

The SRC software provides support for digital certificates for use by other protocols to protect communications between the SRC software and other applications or network devices. You can manage certificates to:

- Support HTTPS connections between the SRC software and Web browsers.

- Allow BEEP TLS connections between the SRC software and JUNOS routing platforms.

You can use SRC CLI commands to manage certificates manually, or through the Simple Certificate Enrollment Protocol (SCEP).

Certificates are in the format defined in the X.509 standard for public key infrastructure. The certificate requests are in the Public Key Cryptology Standard (PKCS) #10 format.

## Before You Use Digital Certificates

Before you use digital certificates, you should:

- Have a working relationship with a certificate authority (CA).

- Have a good working knowledge of how to work with certificates.

- Decide whether or not to use SCEP to assist with certificate management.

- Identify which connections should be secured by a protocol that requires digital certificates.

- Know how to use the file management commands in the CLI.

## Commands to Manage Digital Certificates

You can use the following operational mode commands to manage digital certificates. Which commands you use depends on whether or not you use SCEP.

- clear security certificate

- clear certificate request

- request security generate-certificate-request

- request security enroll (SCEP)

- request security get-ca-certificate (SCEP)

- request security import-certificate

- show security certificate

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

## Manually Obtaining Digital Certificates

You can manually add digital certificates, or you can use SCEP to help manage how you obtain certificates.

For information about using SCEP to obtain certificates, see *Obtaining Digital Certificates through SCEP on page 204*.

To manually add a signed certificate:

1.  Create a certificate signing request.

    user@host> **request security generate-certificate-request subject** *subject* **password** *password*

    where:

    ■   **subject** is the distinguished name of the SRC host; for example cn=cseries1,ou=pop,o=Juniper,l=kanata,st=Ontario,c=Canada.

    ■   **password** is the password received from the certificate authority for the specified subject.

    By default, this request creates the file **/tmp/certreq.csr** and encodes the file by using Privacy-Enhanced Mail (pem) encoding.

2.  Copy the file generated in Step 1 to another system, and submit the certificate signing request file generated in Step 1 to the certificate authority.

    You can transfer the file through FTP by using the **file copy** command.

    user@host> **file copy** *source_file* **ftp://***username***@***server*[:*port*]**/***destination_file*

    The remote system prompts you for your password.

3.  When you receive the signed certificate, copy the file back to the system to the **/tmp** directory.

    You can transfer the file through FTP, as shown in Step 2.

4. Add the certificate to the SRC configuration.

user@host> **request security import-certificate file-name** *file-name* **identifier** *identifier*

where

- **file-name** is the name of the certificate file in the **/tmp** folder. The file has one of the following extensions:

    - CER—Windows extension

    - PEM—Privacy-Enhanced Mail encoding

    - DER—Binary encoding

    - BER—Binary encoding

- **identifier** is the name of the certificate.

For example, to import the file **sdx.cer** that is identified as web:

user@host> **request security import-certificate file-name sdx.cer identifier web**

5. Verify that the certificate is part of the SRC configuration.

```
user@host> show security certificate
web subject:CN=host
```

If there are no certificates on the system, the CLI displays the following message:

```
user@host> show security certificate
No entity certificates in key store
```

## Obtaining Digital Certificates through SCEP

You can use SCEP to help manage how you obtain digital certificates, or you can manually add certificates.

For information about manually obtaining certificates, see *Manually Obtaining Digital Certificates on page 203*.

To add a signed certificate that you obtain through SCEP:

1. Request a CA certificate through SCEP.

user@host> **request security get-ca-certificate url** *url* **ca_identifier** *ca_identifier*

where:

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

- **ca-identifier** is the identifier that designates the authority.

For example, to request a certificate from the CA authority SdxCA at a specified URL on the server security_server:

```
user@host> request security get-ca-certificate url
http://security_server:8080/ejbca/publicweb/apply/scep/pkiclient.exe
ca-identifier SdxCA

Version: 3
Serial Number: 5721058705923989279
Signature Algorithm: SHA1withRSA
Issuer: CN=SdxCA
Valid From: Wed Sep 06 17:00:55 EDT 2006
Valid Until: Sat Sep 03 17:10:55 EDT 2016
Subject: CN=SdxCA
Public key: RSA
Thumbprint Algorithm: SHA1
Thumbprint: 3c 57 a9 77 af 83 3 e9 c7 1e ee e2 4a e8 ff f3 89 f4 11 a9
Do you want to add the above certificate as a trusted CA [yes,no] ? (no) y
```

2. Request that the certificate authority automatically sign the certificate request.

   user@host> **request security enroll subject** *subject* **password** *password*

   where:

   - **subject** is the distinguished name of the SRC host; for example cn=myhost.

   - **password** is the password received from the certificate authority for the specified subject.

   For example, to request a certificate from the CA authority SdxCA at a specified URL on the server security_server:

   ```
   user@host> request security enroll url
   http://security_server:8080/ejbca/publicweb/apply/scep/pkiclient.exe
   identifier web ca-identifier SdxCA subject cn=myhost password mypassword

   Received certificate:
   Version: 3
   Serial Number: 6822890691617224432
   Signature Algorithm: SHA1withRSA
   Issuer: CN=SdxCA
   Valid From: Tue Sep 19 16:33:11 EDT 2006
   Valid Until: Thu Sep 18 16:43:11 EDT 2008
   Subject: CN=myhost
   Public key: RSA
   Do you want to install the above certificate [yes,no] ? (no) y
   ```

3. Verify that the certificate is part of the SRC configuration.

```
user@host> show security certificate
web subject:CN=myhost
```

If there are no certificates on the system, the CLI displays the following message:

No entity certificates in key store

## Removing a Certificate Request

To remove a certificate request:

1. Review the certificate request files on the system. These files are in the /tmp directory and have the file extension .csr.

2. Issue the **clear security certificate-request** command to remove a file. For example:

user@host> **clear security certificate-request certreq.csr**

## Removing a Certificate

To remove a certificate:

1. Issue the **show security certificate** command to view information about the local certificates. For example:

```
user@host> show security certificate
web subject:CN=myhost
CAcert1 subject:CN=myhost
```

2. Issue the **clear security certificate command** to remove a certificate. Use the trusted option if the certificate is a CA certificate.

clear security certificate <trusted> <identifier *identifier*>

For example:

- To remove the certificate web (that is not a trusted certificate) from myhost:

  user@host>**clear security certificate web**

- To remove a trusted (CA) certificate from myhost:

  user@host>**clear security certificate trusted CAcert1**

## Chapter 27
# Connecting to Remote Hosts from the SRC Software

This chapter describes how to connect to a remote host from the SRC CLI through SSH or Telnet. Topics include:

- Connecting to a Remote Host Through SSH on page 207

- Connecting to a Remote Host Through Telnet on page 207

## Connecting to a Remote Host Through SSH

To connect to a remote host through SSH:

- In operational mode, enter the following command.

  user@host> **ssh host** *host* <v1 | v2>

  where:

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

  - <v1 | v2>—Version of SSH, 1 or 2.

## Connecting to a Remote Host Through Telnet

To connect to a remote host through Telnet:

- In operational mode, enter the following command.

  user@host> **telnet** *host* <**port** *port*>

  where:

  - *host*—Hostname or IP address of the remote host.

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

## Chapter 28
# Configuring and Starting the SNMP Agent with the SRC CLI

This chapter describes how to use the SRC CLI to configure and run the SDX Simple Network Management Protocol (SNMP) agent in the SRC environment. The SNMP agent monitors host resources and the SRC components that use the host resources. You can use the CLI to configure the SNMP agent on a Solaris platform or on a C-series Controller.

You can also use SRC configuration applications to configure the SNMP agent on a Solaris platform. See *Chapter 36, Configuring and Starting the SDX SNMP Agent on a Solaris Platform*.

Topics in this chapter include:

For more information about the SNMP agent, see *SRC-PE Monitoring and Troubleshooting Guide, Chapter 9, Configuring the SNMP Traps with the SRC CLI*.

## Configuration Statements for the SDX SNMP Agent

Use the following configuration statements to configure the SDX SNMP agent at the [edit] hierarchy level.

```
snmp agent {
    trap-history-limit trap-history-limit;
    component-polling-interval component-polling-interval;
    protocol-log-level protocol-log-level;
}

snmp agent initial {
    base-dn base-dn;
    host-id host-id;
}

snmp agent initial directory-connection {
    url url;
    backup-urls [backup-urls...];
    principal principal;
    credentials credentials;
    protocol (ldaps);
    timeout timeout;
    check-interval check-interval;
    blacklist;
    snmp-agent;
}

snmp agent initial directory-eventing {
    eventing;
    signature-dn signature-dn;
    polling-interval polling-interval;
    event-base-dn event-base-dn;
    dispatcher-pool-size dispatcher-pool-size;
}

snmp agent java {
    heap-size heap-size;
}
```

snmp agent logger *name* ...

snmp agent logger *name* file {
    filter *filter*;
    filename *filename*;
    rollover-filename *rollover-filename*;
    maximum-file-size *maximum-file-size*;
}

snmp agent logger *name* syslog {
    filter *filter*;
    host *host*;
    facility *facility*;
    format *format*;
}

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

## Configuring the SDX SNMP Agent

The SNMP agent obtains most of its information from the directory, but you configure the local properties that cannot be stored in the directory.

To configure the local properties for the SDX SNMP agent:

1. Configure general properties for the SDX SNMP agent, including trap history limit, component polling interval, and protocol log level.

   See *Configuring General Properties for the SDX SNMP Agent* on page 212.

2. Configure initial properties for the SDX SNMP agent, including the connection from the SDX SNMP agent to the directory and directory monitoring properties.

   See *Configuring Initial Properties for the SDX SNMP Agent* on page 213.

   See *Configuring Directory Connection Properties for the SDX SNMP Agent* on page 214.

   See *Configuring Directory Monitoring Properties for the SDX SNMP Agent* on page 214.

3. Configure logging destinations for the SDX SNMP agent.

   See *Configuring Logging Destinations for the SDX SNMP Agent* on page 215.

4. (Optional) Configure the Java heap memory for the SDX SNMP agent.

   See *Configuring JRE Properties* on page 216.

After you configure the local properties for the SDX SNMP agent, you can configure the SNMP agent. See *Configuring the SNMP Agent* on page 218.

## Configuring General Properties for the SDX SNMP Agent

Use the following configuration statements to configure general properties for the SDX SNMP agent:

```
snmp agent {
    trap-history-limit trap-history-limit;
    component-polling-interval component-polling-interval;
    protocol-log-level protocol-log-level;
}
```

To configure properties for the SDX SNMP agent:

1. From configuration mode, access the configuration statement that configures the SDX SNMP agent.

   ```
   [edit]
   user@host# edit snmp agent
   ```

2. (Optional) Specify the maximum number of elements stored in the SNMP trap history table.

   ```
   [edit snmp agent]
   user@host# set trap-history-limit trap-history-limit
   ```

3. (Optional) Specify the interval at which an SRC component is polled.

   ```
   [edit snmp agent]
   user@host# set component-polling-interval component-polling-interval
   ```

4. (Optional) Specify the log level for SNMP requests and responses received from the master agent.

   ```
   [edit snmp agent]
   user@host# set protocol-log-level protocol-log-level
   ```

   To enable packet-level logging, set the protocol-log-level option to 9 or less.

5. (Optional) Verify your configuration.

   ```
   [edit snmp agent]
   user@host# show
   ```

   The output indicates the trap history limit, the component polling interval, the protocol log level, the initial properties, the logging destinations, and the Java heap size.

## Configuring Initial Properties for the SDX SNMP Agent

Use the following configuration statements to configure initial properties for the SDX SNMP agent:

snmp agent initial {
    base-dn *base-dn*;
    host-id *host-id*;
}

To configure properties for the SDX SNMP agent:

1. From configuration mode, access the configuration statement that configures the SDX SNMP agent.

   [edit]
   user@host# **edit snmp agent initial**

2. Specify the DN of the directory used for the SNMP agent configuration data.

   [edit snmp agent initial]
   user@host# **set base-dn** *base-dn*

3. Identifies the system management configuration in the directory server that provides the remaining configuration for the SNMP agent.

   [edit snmp agent initial]
   user@host# **set host-id** *host-id*

   If the entry does not exist, the entry and the subentries for the components and traps is automatically created in the system management configuration.

4. (Optional) Verify your configuration.

   ```
   [edit snmp agent initial]
   user@host# show
   base-dn o=UMC;
   host-id POP-ID;
   directory-connection {
     url ldap://127.0.0.1:389/;
     principal cn=sysman,ou=components,o=operators,<base>;
     credentials ********;
   }
   directory-eventing {
     eventing;
   }
   ```

## Configuring Directory Connection Properties for the SDX SNMP Agent

Use the following configuration statements to configure directory connection properties for the SDX SNMP agent:

```
snmp agent initial directory-connection {
    url url;
    backup-urls [backup-urls...];
    principal principal;
    credentials credentials;
    protocol (ldaps);
    timeout timeout;
    check-interval check-interval;
    blacklist;
    snmp-agent;
}
```

To configure directory connection properties:

1.  From configuration mode, access the configuration statement that configures the SDX SNMP agent.

    ```
    [edit]
    user@host# edit snmp agent initial directory-connection
    ```

2.  Specify the directory connection properties.

    ```
    [edit snmp agent initial directory-connection]
    user@host# set ?
    ```

    For more information about the directory connection properties, see *SRC-PE Getting Started Guide, Chapter 30, Configuring Local Properties with the SRC CLI*.

3.  (Optional) Verify your configuration.

    ```
    [edit snmp agent initial directory-connection]
    user@host# show
    url ldap://127.0.0.1:389/;
    principal cn=sysman,ou=components,o=operators,<base>;
    credentials ********;
    ```

## Configuring Directory Monitoring Properties for the SDX SNMP Agent

Use the following configuration statements to configure directory monitoring properties for the SDX SNMP agent:

```
snmp agent initial directory-eventing {
    eventing;
    signature-dn signature-dn;
    polling-interval polling-interval;
    event-base-dn event-base-dn;
    dispatcher-pool-size dispatcher-pool-size;
}
```

To configure properties for the SDX SNMP agent:

1. From configuration mode, access the configuration statement that configures the SDX SNMP agent.

   [edit]
   user@host# **edit snmp agent initial directory-eventing**

2. Specify the properties for the SDX SNMP agent.

   [edit snmp agent initial eventing]
   user@host# **set ?**

   For more information about the directory monitoring properties, see *SRC-PE Getting Started Guide, Chapter 30, Configuring Local Properties with the SRC CLI*.

3. (Optional) Verify your configuration.

   ```
   [edit snmp agent initial directory-eventing]
   user@host# show
   eventing;
   ```

## Configuring Logging Destinations for the SDX SNMP Agent

Use the following configuration statement to configure logging destinations for the SDX SNMP agent:

snmp agent logger *name* ...

To configure logging destinations:

1. From configuration mode, access the configuration statement that configures the SDX SNMP agent.

   [edit]
   user@host# **edit snmp agent**

2. Specify the name and type of logging destination.

   For file-based logging:

   [edit snmp agent]
   user@host# **set logger** *name* **file**

   For syslog-based logging:

   [edit snmp agent]
   user@host# **set logger** *name* **syslog**

For more information about logging, see *SRC-PE Monitoring and Troubleshooting Guide, Chapter 2, Configuring Logging for SRC Components* and *SRC-PE Monitoring and Troubleshooting Guide, Chapter 3, Configuring Logging for SRC Components with the CLI*.

## Configuring JRE Properties

Use the following configuration statements to configure Java Runtime Environment (JRE) properties for the SDX SNMP agent:

```
snmp agent java {
    heap-size heap-size;
}
```

To configure properties for the SDX SNMP agent:

1. From configuration mode, access the configuration statement that configures the SDX SNMP agent.

   ```
   [edit]
   user@host# edit snmp agent java
   ```

2. (Optional) Specify the maximum amount of memory available to the JRE.

   ```
   [edit snmp agent java]
   user@host# set heap-size heap-size
   ```

   Do not change this value unless instructed to do so by Juniper Networks.

3. (Optional) Verify your configuration.

   ```
   [edit snmp agent java]
   user@host# show
   heap-size 160m;
   ```

## Configuration Statements for the SNMP Agent

Use the following configuration statements to configure the SNMP agent at the [edit] hierarchy level.

```
snmp {
    contact contact;
    name name;
    location location;
    description description;
    address [address...];
}

snmp community community {
    authorization (read-only|read-write);
    clients clients;
    oid oid;
}

snmp notify target target-name {
    address address;
    port port;
    community community;
    type (trapv1|trapv2|inform);
}
```

```
snmp v3 snmp-community community-index {
    community-name community-name;
    security-name security-name;
    address address;
}

snmp v3 usm local-engine user username ...

snmp v3 usm local-engine user username authentication-md5 {
    authentication-password authentication-password;
}

snmp v3 usm local-engine user username authentication-sha {
    authentication-password authentication-password;
}

snmp v3 usm local-engine user username privacy-aes {
    privacy-password privacy-password;
}

snmp v3 usm local-engine user username privacy-des {
    privacy-password privacy-password;
}

snmp v3 vacm access group group-name ...

snmp v3 vacm access group group-name default-context-prefix security-model
(any|v1|v2c|usm) ...

snmp v3 vacm access group group-name default-context-prefix security-model
(any|v1|v2c|usm) security-level (authentication|none|privacy) {
    read-view read-view;
    write-view write-view;
}

snmp v3 vacm security-to-group security-model (v1|v2c|usm) ...

snmp v3 vacm security-to-group security-model (v1|v2c|usm) security-name
security-name {
    group-name group-name;
}

snmp view view-name ...

snmp view view-name oid oid {
    (include|exclude);
}
```

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

## Configuring the SNMP Agent

To configure the SNMP agent to control its operation:

1. Configure information supplied by the SNMP agent, including the listening address and system information.

   See *Configuring System Information for the SNMP Agent* on page 218.

2. Configure access control for the SNMP agent, including access for SNMPv3 users, SNMPv1 and SNMPv2 communities (traditional access control), and the view-based access control model (VACM).

   See *Configuring Access Control for SNMPv3 Users* on page 219.

   See *Configuring Access Control for Communities* on page 221.

   See *Configuring Access Control for the VACM* on page 222.

3. Configure active monitoring.

   See *Configuring Notification Targets* on page 227.

## Configuring System Information for the SNMP Agent

Use the following configuration statements to configure information supplied by the SNMP agent:

```
snmp {
    contact contact;
    name name;
    location location;
    description description;
    address [address...];
}
```

To configure properties for the SNMP agent:

1. From configuration mode, access the configuration statement that configures the SNMP agent.

   ```
   [edit]
   user@host# edit snmp
   ```

2. (Optional) Specify the administrative contact for the system being managed by SNMP.

   ```
   [edit snmp]
   user@host# set contact contact
   ```

3. (Optional) Specify the name of the system being managed by SNMP.

   ```
   [edit snmp]
   user@host# set name name
   ```

4.  (Optional) Specify the location of the system being managed by SNMP.

    [edit snmp]
    user@host# **set location** *location*

5.  (Optional) Specify the description of the system being managed by SNMP.

    [edit snmp]
    user@host# **set description** *description*

6.  (Optional) Specify the listening address on which to receive incoming SNMP
    requests.

    [edit snmp]
    user@host# **set address** [*address...*]

    To list more than one IP address, enter the addresses separated by spaces
    within brackets. By default, the SNMP agent listens on all IPv4 interfaces.

7.  (Optional) Verify your configuration.

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

    If you did not configure the SNMP agent, the command displays only the SDX
    SNMP agent configuration.

## Configuring Access Control for SNMPv3 Users

Use the following configuration statements to configure access control for SNMPv3
users:

snmp v3 usm local-engine user *username* ...

snmp v3 usm local-engine user *username* authentication-md5 {
    authentication-password *authentication-password*;
}

snmp v3 usm local-engine user *username* authentication-sha {
    authentication-password *authentication-password*;
}

snmp v3 usm local-engine user *username* privacy-aes {
    privacy-password *privacy-password*;
}

snmp v3 usm local-engine user *username* privacy-des {
    privacy-password *privacy-password*;
}

To configure access control for SNMPv3 users:

1. From configuration mode, access the configuration statement that configures the access control for SNMPv3 users.

   [edit]
   user@host# **edit snmp v3 usm local-engine user** *username*

   Username is the user-based security model (USM) username. By default, no authentication or encryption is specified for the SNMPv3 user.

2. (Optional) Specify the authentication type.

   See *Configuring Authentication* on page 220.

3. (Optional) Specify the encryption.

   See *Configuring Encryption* on page 221.

---

☞ **NOTE:** Before you configure encryption, you must configure the authentication type.

---

4. (Optional) Verify your configuration.

   [edit snmp v3 usm local-engine user *username*]
   user@host# **show**

## *Configuring Authentication*

To configure the authentication type for SNMPv3 users:

1. From configuration mode, access the configuration statement that configures the authentication type.

   To configure MD5 authentication:

   user@host# **edit snmp v3 usm local-engine user** *username* **authentication-md5**

   To configure SHA authentication:

   user@host# **edit snmp v3 usm local-engine user** *username* **authentication-sha**

2. Specify the authentication password.

   user@host# **set authentication-password** *authentication-password*

   The password must be at least eight characters.

### Configuring Encryption

Before you configure encryption, you must configure the authentication type. See *Configuring Authentication* on page 220.

To configure encryption for SNMPv3 users:

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

    To configure AES encryption:

    user@host# **edit snmp v3 usm local-engine user** *username* **privacy-aes**

    To configure DES encryption:

    user@host# **edit snmp v3 usm local-engine user** *username* **privacy-des**

2.  Specify the privacy password.

    user@host# **set privacy-password** *privacy-password*

    The password must be at least eight characters.

## Configuring Access Control for Communities

Use the following configuration statements to configure community strings for traditional access control:

```
snmp community community {
    authorization (read-only|read-write);
    clients clients;
    oid oid;
}
```

To configure community strings:

1.  From configuration mode, access the configuration statement that configures the community string. Community names must be unique.

    [edit]
    user@host# **edit snmp community** *community*

2.  (Optional) Specify the authorization level.

    To specify read-only access:

    [edit snmp community *community*]
    user@host# **set authorization read-only**

    To specify read and write access:

    [edit snmp community *community*]
    user@host# **set authorization read-write**

3. Specify the IP address or subnet of the SNMP client hosts that are authorized to use this community.

[edit snmp community *community*]
user@host# **set clients** *clients*

By default, all clients are allowed.

4. (Optional) Specify the object identifier used to represent a subtree of MIB object to which access is allowed.

[edit snmp community *community*]
user@host# **set oid** *oid*

5. (Optional) Verify your configuration.

```
[edit snmp community community]
user@host# show
```

## Configuring Access Control for the VACM

To configure the access control for the view-based access control model (VACM):

1. Map an SNMPv1 or SNMPv2c community name to a security name.

See *Associating Security Names with a Community* on page 222.

2. Define a named view.

See *Defining Named Views* on page 223.

3. Map from a group of users or communities to a view.

See *Defining Access Privileges for an SNMP Group* on page 224.

4. Map a security name into a named group.

See *Assigning Security Names to Groups* on page 226.

### Associating Security Names with a Community

For SNMPv1 or SNMPv2c packets, you must assign security names to groups at the [edit snmp v3 vacm security-to-group] hierarchy level and you must associate a security name with an SNMP community.

Use the following configuration statements to configure SNMPv1 or SNMPv2c communities for the VACM:

snmp v3 snmp-community *community-index* {
    community-name *community-name*;
    security-name *security-name*;
    address *address*;
}

To configure the community:

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

   [edit]
   user@host# **edit snmp v3 snmp-community** *community-index*

   Unique index that identifies an SNMP community.

2. (Optional) Specify the community string for the SNMPv1 or SNMPv2c community.

   [edit snmp v3 snmp-community *community-index*]
   user@host# **set community-name** *community-name*

   If a community name is not specified, the community index is used.

3. Specify the VACM security name to associate with the community string.

   [edit snmp v3 snmp-community *community-index*]
   user@host# **set security-name** *security-name*

4. (Optional) Specify the IP address or subnet of the SNMP clients that are authorized to use this community.

   [edit snmp v3 snmp-community *community-index*]
   user@host# **set address** *address*

   If an address is not specified, all clients are authorized to use the community.

5. (Optional) Verify your configuration.

   [edit snmp v3 snmp-community *community-index*]
   user@host# **show**

### Defining Named Views

Use the following configuration statements to define named views:

snmp view *view-name* ...

snmp view *view-name* oid *oid* {
    (include|exclude);
}

To configure named views:

1. From configuration mode, access the configuration statement that configures the named views.

   [edit]
   user@host# **edit snmp view** *view-name*

   The view name identifies a group of MIB objects for which to define access.

2. Specify the object identifier (OID) that represents a subtree of MIB objects for the view and whether the OID is included in or excluded from the view.

To include the OID in the view:

[edit snmp view *view-name*]
user@host# **set oid** *oid* **include**

To exclude the OID from the view:

[edit snmp view *view-name*]
user@host# **set oid** *oid* **exclude**

3. (Optional) Verify your configuration.

[edit snmp view *view-name*]
user@host# **show**

### *Defining Access Privileges for an SNMP Group*

Use the following configuration statements to define access privileges for SNMP groups:

snmp v3 vacm access group *group-name* ...

snmp v3 vacm access group *group-name* default-context-prefix security-model (any|v1|v2c|usm) ...

snmp v3 vacm access group *group-name* default-context-prefix security-model (any|v1|v2c|usm) security-level (authentication|none|privacy) {
    read-view *read-view*;
    write-view *write-view*;
}

To configure MIB views with a group for the VACM:

1. From configuration mode, access the configuration statement that configures the VACM group.

[edit]
user@host# **edit snmp v3 vacm access group** *group-name*

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

2. Specify the security model for access privileges.

[edit snmp v3 vacm access group *group-name*]
user@host# **set default-context-prefix security-model** (any|v1|v2c|usm)

To specify any security model:

user@host# **set default-context-prefix security-model any**

To specify the SNMPv1 security model:

user@host# **set default-context-prefix security-model v1**

To specify the SNMPv2c security model:

user@host# **set default-context-prefix security-model v2c**

To specify the SNMPv3 user-based security model (USM):

user@host# **set default-context-prefix security-model usm**

3. Specify the security level for access privileges.

   [edit snmp v3 vacm access group *group-name*]
   user@host# **set default-context-prefix security-model** (any|v1|v2c|usm)
   **security-level** (authentication|none|privacy)

   To specify a security level that provides authentication but no encryption:

   user@host# **set default-context-prefix security-model** (any|v1|v2c|usm)
   **security-level authentication**

   To specify a security level that provides no authentication and no encryption:

   user@host# **set default-context-prefix security-model** (any|v1|v2c|usm)
   **security-level none**

   For SNMPv1 or SNMPv2c access, specify none as the security level.

   To specify a security level that provides authentication and encryption:

   user@host# **set default-context-prefix security-model** (any|v1|v2c|usm)
   **security-level privacy**

4. (Optional) Specify the view used for SNMP read access. You must specify the
   read-view option or the write-view option.

   [edit snmp v3 vacm access group *group-name* default-context-prefix security-model
   (any|v1|v2c|usm) security-level (authentication|none|privacy)]
   user@host# **set read-view** *read-view*

5. (Optional) Specify the view used for SNMP write access. You must specify the
   read-view option or the write-view option.

   [edit snmp v3 vacm access group *group-name* default-context-prefix security-model
   (any|v1|v2c|usm) security-level (authentication|none|privacy)]
   user@host# **set write-view** *write-view*

### Assigning Security Names to Groups

For SNMPv1 or SNMPv2c packets, you must assign security names to groups and you must associate a security name with an SNMP community at the [edit snmp v3 snmp-community *community-index*] hierarchy level.

Use the following configuration statements to assign security names to groups:

snmp v3 vacm security-to-group security-model (v1|v2c|usm) …

snmp v3 vacm security-to-group security-model (v1|v2c|usm) security-name *security-name* {
    group-name *group-name*;
}

To map security names to groups for the VACM:

1. From configuration mode, access the configuration statement that configures the security model for a group.

   user@host# **edit snmp v3 vacm security-to-group security-model** (v1|v2c|usm)

   To specify the SNMPv1 security model:

   user@host# **edit snmp v3 vacm security-to-group security-model v1**

   To specify the SNMPv2c security model:

   user@host# **edit snmp v3 vacm security-to-group security-model v2c**

   To specify the SNMPv3 user-based security model (USM):

   user@host# **edit snmp v3 vacm security-to-group security-model usm**

2. Specify the security name.

   user@host# **edit snmp v3 vacm security-to-group security-model** (v1|v2c|usm) **security-name** *security-name*

   If the security model is USM, the security name is the username configured at the [edit snmp v3 usm local-engine user] hierarchy level.

3. Specify the group to which the security name is assigned.

   [edit snmp v3 vacm security-to-group security-model (v1|v2c|usm) security-name *security-name*]
   user@host# **set group-name** *group-name*

# Configuring Notification Targets

Use the following configuration statements to configure notification targets:

```
snmp notify target target-name {
    address address;
    port port;
    community community;
    type (trapv1|trapv2|inform);
}
```

To configure notification targets:

1.  From configuration mode, access the configuration statement that configures the notification target.

    ```
    [edit]
    user@host# edit snmp notify target target-name
    ```

    Specify the notification target name.

2.  Specify the IPv4 or IPv6 address of the system to receive notifications.

    ```
    [edit snmp notify target target-name]
    user@host# set address address
    ```

3.  (Optional) Specify the SNMP trap port number.

    ```
    [edit snmp notify target target-name]
    user@host# set port port
    ```

4.  Specify the community string used when sending traps.

    ```
    [edit snmp notify target target-name]
    user@host# set community community
    ```

5. Specify the notification types as traps or informs. Traps are unconfirmed notifications. Informs are confirmed notifications.

To specify the notification type as an SNMPv1 trap:

[edit snmp notify target *target-name*]
user@host# **set type trapv1**

To specify the notification type as an SNMPv2 trap:

[edit snmp notify target *target-name*]
user@host# **set type trapv2**

To specify the notification type as an SNMPv2 inform:

[edit snmp notify target *target-name*]
user@host# **set type inform**

6. (Optional) Verify your configuration.

[edit snmp notify target *target-name*]
user@host# **show**

## Operating the SNMP Agent

You must configure the SNMP agent and then manually start the agent. If you attempt to manually start the SNMP agent before it is configured, the software displays a message that the agent has not been configured and cannot start.

The SNMP agent automatically restarts in the event of a host reboot or process failure that stops the agent.

## Starting the SDX SNMP Agent

Before you start the SDX SNMP agent:

1. Perform the initial configuration tasks.

See *Chapter 4, Configuring a C-series Controller*.

2. Configure the SDX SNMP agent.

See *Configuring the SDX SNMP Agent* on page 211.

Manually start the SDX SNMP agent the first time it runs. Thereafter, the agent automatically restarts.

To start the SNMP agent:

user@host> **enable component agent**

The system responds with a start message. If the SNMP agent is already running, the system responds with a warning message indicating that fact.

## Stopping the SDX SNMP Agent

To stop the SNMP agent:

user@host> **disable component agent**

The system responds with a stop message. If the SNMP agent is not running when you issue the command, the software responds with a warning message indicating that fact.

## Monitoring the SDX SNMP Agent

To display the SDX SNMP agent status:

user@host> **show component**

The system responds with a status message.

**Part 6**

# Configuring Operating Properties for Components

## Chapter 29

# Distributing Directory Changes to SRC Components

This chapter provides information about the directory eventing system (DES). Topics include:

- Overview of the Directory Eventing System on page 233

- Managing Directory Communication on page 234

## Overview of the Directory Eventing System

The directory eventing system (DES) provides two functions:

- Automatic notification of changes in the directory

  DES polls the directory periodically to determine changes that affect the configuration or operation of a particular component. If DES finds relevant changes, it automatically provides the changes to the component. However, if DES does not find relevant changes, it does not provide any information.

- Redundancy

  You must define a primary directory for SRC components that require access to a directory. You can also define a list of secondary (backup) directories.

  DES detects when a connection to the primary directory fails, and:

  1. Connects to the first available secondary directory in the specified list.

  2. Reverts to the primary directory when it becomes available.

If a connection to a secondary directory fails, DES:

1. Connects to the primary directory if it is available.

2. If the primary directory is unavailable, connects to the first available directory in the specified list.

DES is not a central service for all SRC components; rather, you configure a DES for an individual SRC component. On a C-series Controller, you configure initial eventing for each component for each slot. Other components such as the SAE and the license manager have additional configuration for directory eventing.

Some components have connections to multiple directories; consequently you must configure DES properties for each connection. For example, the SAE may use different directories for service, configuration, and subscriber information.

DES is a Java Naming and Directory Interface (JNDI)–compliant service and accepts standard JNDI properties. For more information about JNDI, see http://java.sun.com/products/jndi/ .

## Managing Directory Communication

When an SRC component communicates with the directory, that component may pass a time (known as a server timeout) to the directory to specify a time limit for the directory to respond. If the directory is not working correctly, however, it may not respond during this time, and will cause the SRC component to stop operating.

DES recovers if the directory is not working correctly. In addition, you can configure DES to prohibit communications with a directory if that directory repeatedly fails to respond. If you do so, DES starts the following procedure for all communication with the directory:

1. Assigns a client timeout to the communication.

   The client timeout exceeds the server timeout.

2. If the directory does not respond during this time, DES closes the connection to the directory.

3. DES tries to reconnect to the directory and proceeds as follows:

   ■ If DES cannot connect to the directory, it connects to the next available directory specified by the DES redundancy properties.

   ■ If DES can connect to the directory, it contacts the directory again and repeats Steps 1 to 3.

4. If a directory fails to respond 10 times, DES prevents further communication with the directory.

## Chapter 30
# Configuring Local Properties with the SRC CLI

This chapter describes how to use the SRC CLI to configure local properties for SRC components. You can use the CLI to configure local properties on a Solaris platform or on a C-series Controller.

You can also use SRC configuration applications to configure initial properties on a Solaris platform. See the documentation for the component that you are configuring.

Topics in this chapter include:

- Local Properties for SRC Components on page 235

- Configuration Statements for Local Configuration on page 236

- Configuring Basic Local Properties on page 237

- Changing the Location of Data in the Directory on page 238

- Configuring Directory Connection Properties on page 239

- Configuring Initial Directory Eventing Properties for SRC Components on page 240

- Verifying the Local Configuration for a Component on page 242

## Local Properties for SRC Components

Before you configure an SRC component, configure the component's local properties. In many cases you can use the default configuration. From the CLI, local properties are configured for a slot. On a C-series Controller, the slot configuration is applied to the appropriate slot. On a Solaris platform, configuration for slot 0 provides the local configuration; however, the slot is not associated with a hardware slot.

## Configuration Statements for Local Configuration

Use the following configuration statements to configure local properties for a component. You enter these statements at various hierarchy levels for different SRC components. This list shows the configuration common to a number of components. For information about configuration specific to a component, such as SAE, NIC, SRC-ACP, or SNMP, see the documentation for that component.

```
slot number component-name {
    base-dn base-dn;
    java-runtime-environment java-runtime-environment;
    java-heap-size java-heap-size;
    snmp-agent;
}

slot number component-name initial {
    static-dn static-dn;
    dynamic-dn dynamic-dn;
}

slot number component-name initial directory-connection {
    url url;
    backup-urls [backup-urls...];
    principal principal;
    credentials credentials;
    protocol (ldaps);
    timeout timeout;
    check-interval check-interval;
    blacklist;
    snmp-agent;
}

slot number component-name initial directory-eventing {
    eventing;
    signature-dn signature-dn;
    polling-interval polling-interval;
    event-base-dn event-base-dn;
    dispatcher-pool-size dispatcher-pool-size;
}
```

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

## Configuring Basic Local Properties

In most cases you can use the default operating properties. Change the default properties if needed for your environment.

Use the following configuration statements to configure basic local properties for a component:

```
slot number component-name {
    base-dn base-dn;
    java-runtime-environment java-runtime-environment;
    java-heap-size java-heap-size;
    snmp-agent;
}
```

To review the default local configuration and then change values:

1. From configuration mode, access the configuration statement that specifies the slot configuration for a component.

   ```
   [edit]
   user@host# edit slot number nic
   ```

   For example:

   ```
   [edit]
   user@host# edit slot 0 nic
   ```

2. To view the default configuration, run the **show** command. For example:

   ```
   [edit slot 0 nic]
   user@host# show
   base-dn o=umc;
   java-runtime-environment ../jre/bin/java;
   java-heap-size 128m;
   hostname DemoHost;
   initial {
   ```

   > 👉 **NOTE:** The hostname statement is specific to the NIC.

3. (Optional) If you store data in the directory in a location other than the default, *o = umc*, change this value.

   ```
   [edit slot 0 nic]
   user@host> set base-dn base-dn
   ```

4. (Optional) If the Java Runtime Environment (JRE) is not in the default location (*../jre/bin/java*) on a Solaris platform, change the directory path to the JRE.

   ```
   [edit slot 0 nic]
   user@host> set java-runtime-environment java-runtime-environment
   ```

5. (Optional) If you encounter problems caused by lack of memory, change the maximum memory size available to the JRE.

[edit slot 0 nic]
user@host> **set java-heap-size** *java-heap-size*

6. (Optional) Enable viewing of SNMP counters through an SNMP browser.

[edit slot 0 nic]
user@host> **set snmp-agent**

## Changing the Location of Data in the Directory

In most cases, you use the default configuration for the location of SRC data in the directory:

■ Administrator-defined configuration
data—*ou = staticConfiguration,ou = Configuration,o = Management,o = umc*

■ Programmatically defined configuration
data—*ou = dynamicConfiguration,ou = Configuration,o = Management, o = umc*

You can specify the full distinguished name (DN), or a DN relative to a base DN, identified as *< base >*.

You can change the location of data in the directory at the Expert CLI editing level.

Use the following configuration statements to change the location of data for a component in the directory:

slot *number component-name* initial {
    static-dn *static-dn*;
    dynamic-dn *dynamic-dn*;
}

To change the location of data in the directory:

1. From configuration mode, access the configuration statement that specifies the configuration for a component on a slot.

[edit]
user@host# **edit slot** *number* **nic initial**

For example:

[edit]
user@host# **edit slot 0 nic initial**

2. (Optional) Change the location of administrator-defined configuration data in the directory

[edit slot 0 nic initial]
user@host# **set** static-dn *static-dn*

3. (Optional) Change the location of programmatically defined configuration data in the directory.

[edit slot 0 nic initial]
user@host# **set** dynamic-dn *dynamic-dn*

## Configuring Directory Connection Properties

Use the following configuration statements to configure directory properties for a component:

slot *number component-name* initial directory-connection {
    url *url*;
    backup-urls [*backup-urls*...];
    principal *principal*;
    credentials *credentials*;
    protocol (ldaps);
    timeout *timeout*;
    check-interval *check-interval*;
    blacklist;
    snmp-agent;
}

To configure directory connection properties for a component:

1. From configuration mode, access the configuration statement that specifies the directory configuration for a component on a slot.

   user@host# **edit slot** *number component* **initial directory-connection**

   For example:

   user@host# **edit slot 0 nic initial directory-connection**

2. Specify the URL that identifies the location of the primary directory server.

   [edit slot 0 nic initial directory-connection]
   user@host# **set** url *url*

   On a C-series Controller, this value is ldap://127.0.0.1:389.

3. (Optional) Specify URLs that identify the locations of backup directory servers. Backup servers are used if the primary directory server is not accessible.

   [edit slot 0 nic initial directory-connection]
   user@host# **set** backup-urls *directory-backup-url1 directory-backup-url2*

4. Specify the DN that the SRC component uses for authentication to access the directory.

   [edit slot 0 nic initial directory-connection]
   user@host# **set** principal *principal*

5.  Specify the password with which the SRC component accesses the directory.

    [edit slot 0 nic initial directory-connection]
    user@host# **set** credentials *credentials*

6.  (Optional) Specify whether the connection to the directory uses secure LDAP. If you do not configure a security protocol, plain socket is used.

    [edit slot 0 nic initial directory-connection]
    user@host# **set** protocol ldaps

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

    [edit slot 0 nic initial directory-connection]
    user@host# **set timeout** *timeout*

8.  (Optional) Specify the time interval at which the software attempts to connect to the directory.

    [edit slot 0 nic initial directory-connection]
    user@host# **set check-interval** *check-interva*l

9.  (Optional) Enable the directory eventing system to prevent a connection to a directory after the directory fails to respond during an interval in which the directory was polled 10 times.

    [edit slot 0 nic initial directory-connection]
    user@host# **set blacklist**

10. Specify that the SDX SNMP agent exports MIBs for this directory connection.

    [edit slot 0 nic initial directory-connection]
    user@host# **set snmp-agent**

## Configuring Initial Directory Eventing Properties for SRC Components

You can use the default configuration for directory eventing properties, or you can change the configuration to comply with your environment.

For information about the default setting for the directory eventing properties, see the *SRC-PE CLI Command Reference.*

For information about directory eventing, see *Chapter 29, Distributing Directory Changes to SRC Components*.

The following configuration statements configure initial directory eventing properties for a component:

```
slot number sae initial directory-eventing {
    eventing;
    signature-dn signature-dn;
    polling-interval polling-interval;
    event-base-dn event-base-dn;
    dispatcher-pool-size dispatcher-pool-size;
}
```

To change directory eventing configuration:

1. From configuration mode, access the configuration statement that specifies the initial eventing configuration for a component on a slot.

   [edit]
   user@host# **edit slot** *number component* **initial directory-eventing**

   For example:

   [edit]
   user@host# **edit slot 0 nic initial directory-eventing**

2. (Optional; Solaris platform.) Specify the DN of the directory entry that specifies the usedDirectory attribute for the SRC CLI. The usedDirectory attribute identifies the vendor of the directory server.

   [edit slot 0 nic initial directory-eventing]
   user@host# **set signature-dn** *signature-dn*

   Use the default value on a C-series Controller

3. (Optional) Specify an interval at which an SRC component polls the directory to check for directory changes.

   [edit slot 0 nic initial directory-eventing]
   user@host# **set polling-interval** *polling-interval*

4. (Optional) Specify the DN of an entry superior to the data associated with an SRC component in the directory.

   [edit slot 0 nic initial directory-eventing]
   user@host# **set event-base-dn** *event-base-dn*

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

5. (Optional) Specify the number of events that an SRC component can receive simultaneously from the directory.

   [edit slot 0 nic initial directory-eventing]
   user@host# **set dispatcher-pool-size** *dispatcher-pool-size*

## Verifying the Local Configuration for a Component

To verify the local configuration for a component:

1.  From configuration mode, access the configuration statement that configures the slot connection. For example, to verify the slot configuration for the NIC:

    user@host# **edit slot 0 nic**

2.  Run the show command. For example:

```
[edit slot 0 nic ]
user@host# show
base-dn o=umc;
java-runtime-environment ../jre/bin/java;
java-heap-size 128m;
snmp-agent;
hostname DemoHost;
initial {
  dynamic-dn "ou=dynamicConfiguration, ou=Configuration,
o=Management,<base>";
  directory-connection {
    url ldap://127.0.0.1:389/;
    backup-urls ;
    principal cn=nic,ou=Components,o=Operators,<base>;
    credentials ********;
    timeout 10;
    check-interval 60;
  }
  directory-eventing {
    eventing;
    signature-dn <base>;
    polling-interval 15;
    event-base-dn <base>;
    dispatcher-pool-size 1;
  }
  static-dn "l=OnePop,l=NIC, ou=staticConfiguration, ou=Configuration,
o=Management,<base>";
}
```

**Part 7**

# Managing SRC Software on a Solaris Platform

## Chapter 31
# Planning an SRC Installation on a Solaris Platform

This chapter provides information to help you plan an SRC deployment. The chapter describes distribution scenarios for SRC components, including deployment strategies for an enterprise service portal. It also describes SRC architecture and component interactions. Topics include:

## SRC Installation Options and Configurations for Solaris Platforms

Before you install SRC software components on a Solaris platform, plan your implementation. The SRC software comprises a set of interacting software modules that you can install on different hosts and that you can connect to other internetworking devices and applications through a range of standard interfaces.

When you plan your implementation, consider that you can deploy the SAE on one host, a directory on another host, and Policy Editor on a third host. You might want to install only the components needed by an administrator on some hosts, and the components needed by developers on others. For a list of the components you can install and recommended sets of components for different purposes, see *Chapter 33, Installing the SRC Software on a Solaris Platform*.

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

# SRC Component Distribution Scenarios on Solaris Platforms

The distributed architecture of the SRC software offers high scalability and extensive flexibility that allows you to customize the SRC software for your environment. SDX releases 3.1.1 and earlier, in which the SRC software was an integrated application rather than a set of interacting modules, are fully compatible with this distributed architecture.

👉 **NOTE:** This chapter describes some typical scenarios, but they are by no means the only ones; many other variations are possible.

Figure 22 shows an overview installation of all SRC components.

**Figure 22: Installation of All SRC Components**
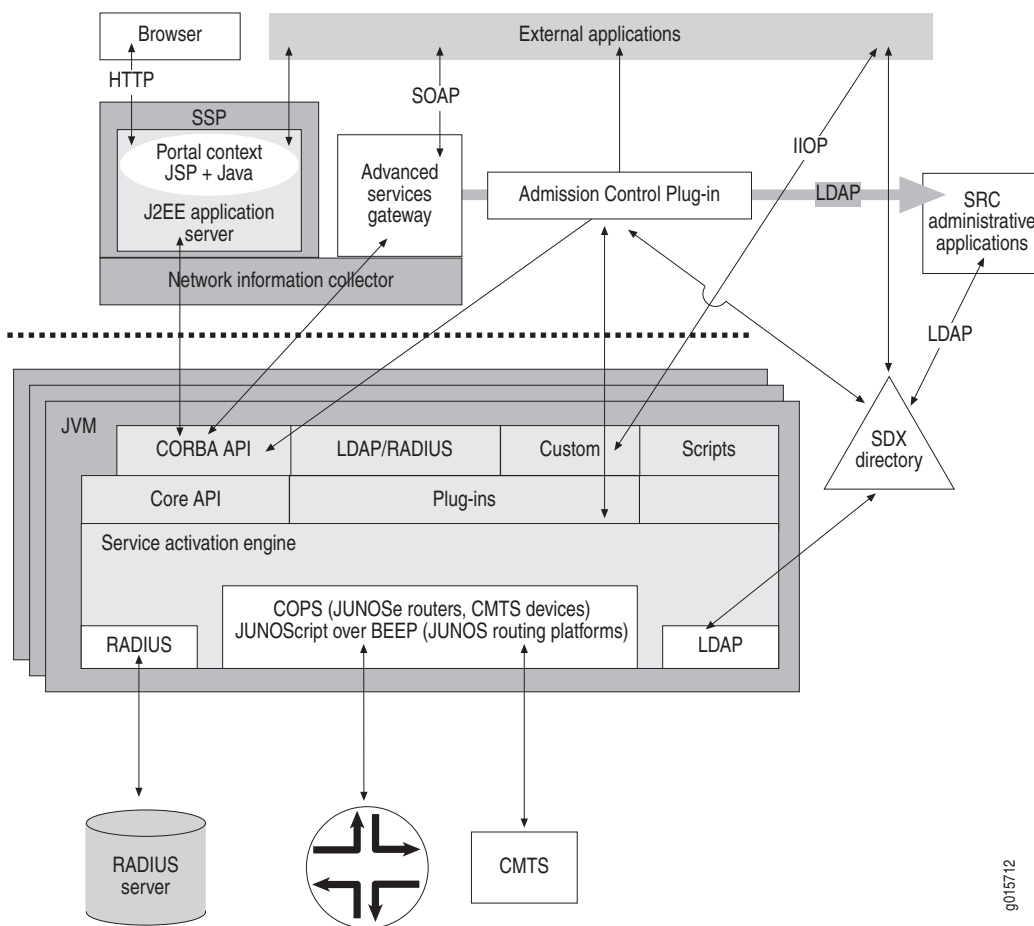


This section covers the following scenarios for distributing SRC components:

- Distributed—An installation that distributes the SRC components among several machines in several locations and provides reliability and scalability

- Regionalized—Distribution scenario for a large service provider that allows regional autonomy

■ Consolidated—Distribution scenario that consolidates network services into regional data centers

■ Single host—A minimal installation that is suitable for small operations, demonstrations, and trials

## Distributed SRC Installation on Solaris Platforms

Figure 23 on page 248 shows a more complicated setup that distributes the SRC components among several machines in several locations, while still providing reliability and scalability.

In the back office, there are:

■ A master directory server running on dedicated hardware

■ SDX Admin and Policy Editor running on as many other machines as desired

■ A pair of network information collector (NIC) hosts running NIC resolvers

■ A Web application server with a portal (a residential portal, an enterprise portal, or an Advanced Services Gateway application)

■ Non-SRC components of the service provider's OSS, which are integrated with the SRC components through the master directory as LDAP clients

In the POPs there are primary and backup hosts that contain identical SAE, RADIUS, directory servers, and NIC hosts. The NIC hosts contain a resolver, directory agent, and SAE agent, and they communicate with the NIC hosts in the back office using Common Object Request Broker Architecture (CORBA). SAE, RADIUS, and directory server components within the hosts communicate through LDAP.

Clients of the NIC host need to determine which remote SAE is managing the subscriber sessions that they need to operate on. The NIC system collects and stores this information. At startup, the SAE stores its CORBA object reference in the directory. The NIC system collects this SAE reference, along with the keys to subscriber sessions (IP addresses and LDAP DNs of the subscriber profiles in the directory) managed by the SAE. Web applications can locate the SAE for a particular subscriber by querying the NIC system.

**Figure 23: Distributed Installation for Reliability and Scalability**
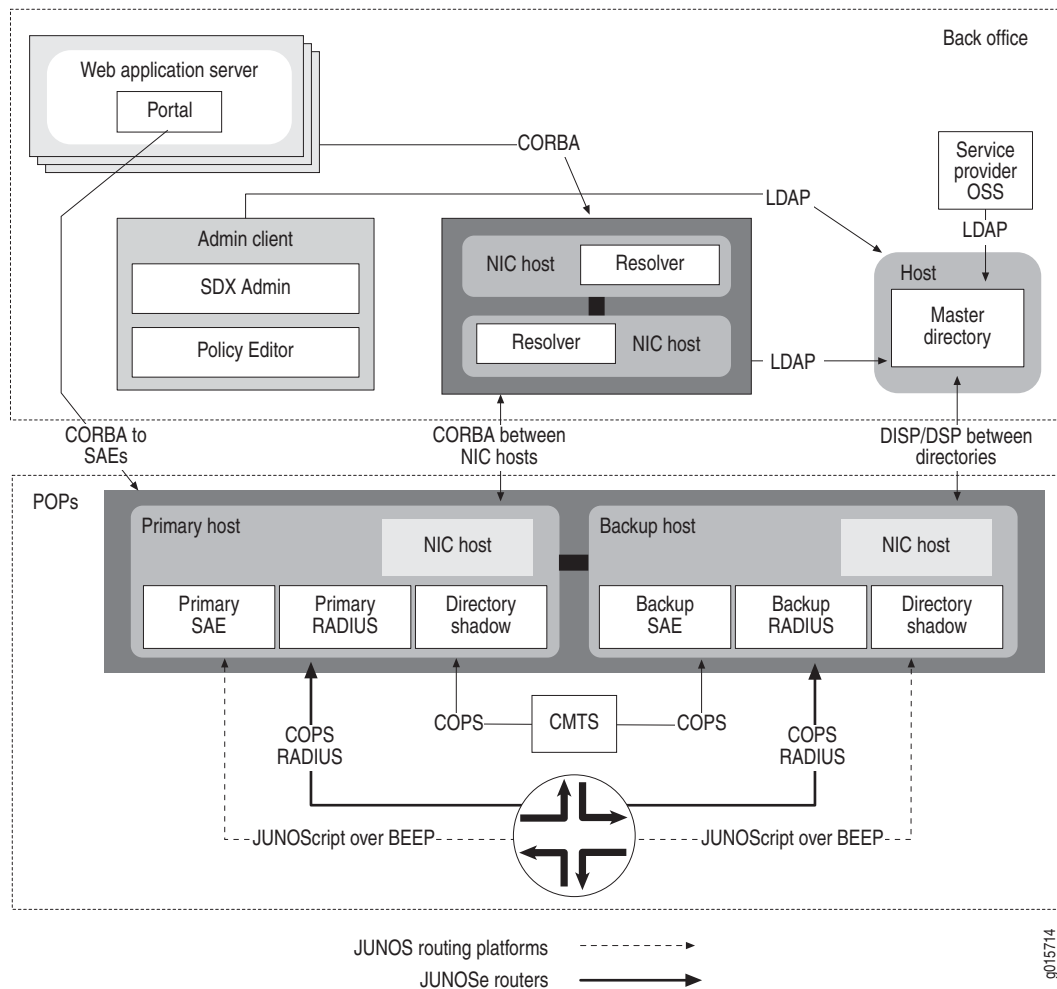


## *Master Directory and Directory Shadows*

The master directory contains all the directory data and handles all update requests, either locally through LDAP or remotely through the Directory Service Protocol (DSP) for X.500 directories, such as DirX, or through equivalent protocols for other directory types.

The information in the master directory is copied to shadow directories in the service provider's point of presence (POP). The system uses Directory Information Shadowing Protocol (DISP) for data transfer for X.500 directories, such as DirX, and equivalent protocols for other directory transfers. This type of distribution puts the directory information for SAEs and RADIUS servers physically close to the servers. A highly reliable LAN connects the hosts and provides good performance.

It is not necessary to include all information in the directory shadows. For instance, only information relevant to a particular POP, such as the information for the subscribers who can actually connect there, may be included. Also, updates generated from an SAE in a particular POP, such as cached logins, may be mastered locally and not propagated to the directory master in the back office. Finally, attributes not relevant to SAE and RADIUS operation—for instance, the subscriber's address—may be filtered from replication to the directory shadows in the POPs.

### Scalability

This setup can be scaled incrementally by replicating the pattern found in the POP as the subscriber base grows.

### Reliability

To avoid a single point of failure in the POPs, the RADIUS, SAE, directory servers, and NIC hosts are installed on identical primary and backup hardware. If the primary host fails, the router switches over to the backup host. Also, the SAE and RADIUS servers (as LDAP clients) and NIC hosts can be configured to switch over to the directory server in the backup host in the POP or to the master directory in the back office. You can configure one or more backup servers for a number of primary servers; such redundancy distributes the load of the routers across several hosts and reduces failover time by limiting the number of subscribers handled by any one host.

This setup avoids service outages in the case of any single network, server, or software failure. Existing subscribers are even unaffected by long periods of disconnection between their POP and the back office. The directory server protocols ensure that all information is properly distributed regardless of the pattern of intermittent connectivity between the sites. Since relatively static directory information is cached locally in the directory shadow in the POP, very high transaction rates for SAE and the RADIUS server are achieved.

### Simplified Management and Security

Additional benefits of this setup at the POP are simplified management because of the use of identical hardware and software, and an added level of security because the SAE, RADIUS, the directory, and NIC hosts are all on the same machine.

**NOTE:** In this and subsequent scenarios, protection of the data in the back office, such as subscriber names and passwords, is a critical issue. Consequently, the back-office site is typically heavily protected by firewalls. One key advantage of this setup is that only directory protocols need be passed through firewalls, and these protocols have rich and flexible security properties.

### *Regionalized Installation*

extends the scheme shown in the last section with an additional layer of directory replication for very large service providers who partition their organization into regions with regional data centers.

A single back office still houses the master directory, some centralized management servers and clients, and a pair of NIC hosts. There are also still primary and backup hosts at the POP, with SAE and RADIUS servers and NIC hosts with a resolver, a directory agent, and an SAE agent.

In this case, there is also a middle layer of regional data centers that house the first level of replication from the master directory in the back office. The regional data centers may also contain a complete set of SRC components and other OSS management components integrated with the local directory. If the local directory fails, these regional components can switch over to the master directory in the back office and switch back once the local failure is corrected. Also, directory administrative controls can be defined to limit the access of regional management operators to an appropriate scope according to the service provider's policies.

**Figure 24: Regionalized Directory Installation for Regional Autonomy**
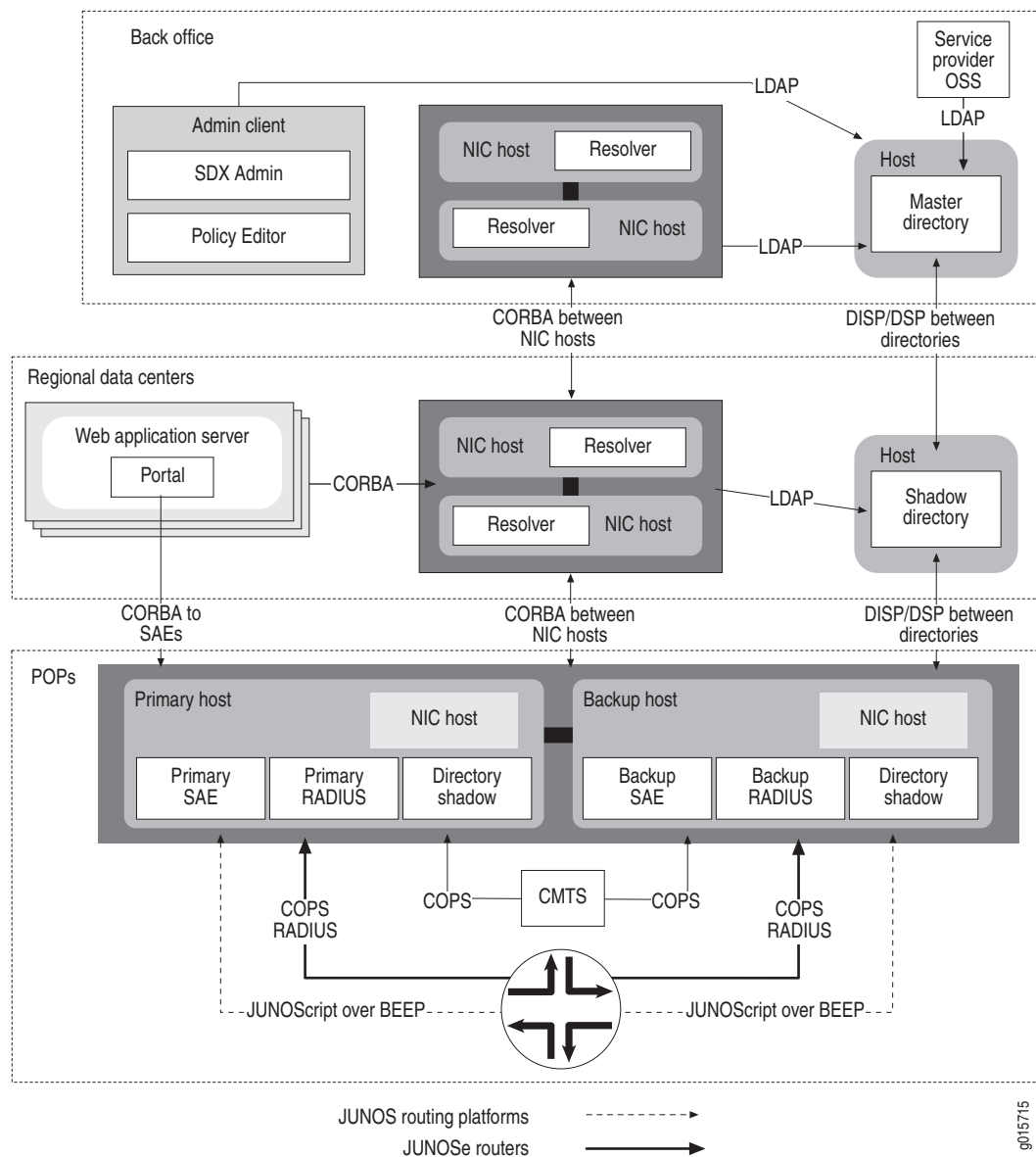
## Consolidated SRC Installation on Solaris Platforms

All the previous scenarios provide top reliability because all the network services—that is, the SAE and RADIUS servers—as well as Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) servers and NIC hosts, are at the same site as the router and are connected by a reliable LAN. However, to maintain this reliability, hardware must be dedicated to this function in every POP, no matter how small, and economies of scale cannot be achieved through consolidation in large hosts.

The SRC software also supports a deployment scenario that allows a trade-off between consolidation of components in large hosts and the risk of less reliable MAN/WAN connections between sites. This scenario, shown in Figure 25 on page 253, consolidates the network services in regional data centers. Here, the regional data center has:

- Two directory servers for reliability.

- A pair of very large SAE hosts that can be used as the primary or backup hosts for different routers in remote POPs.

- A set of RADIUS hosts that can be load balanced across the various routers and the SAEs for the region.

- A pair of NIC hosts.

- A Web application server with a portal (a residential portal, an enterprise portal, or an Advanced Services Gateway application).

**Figure 25: Consolidated Network Services**
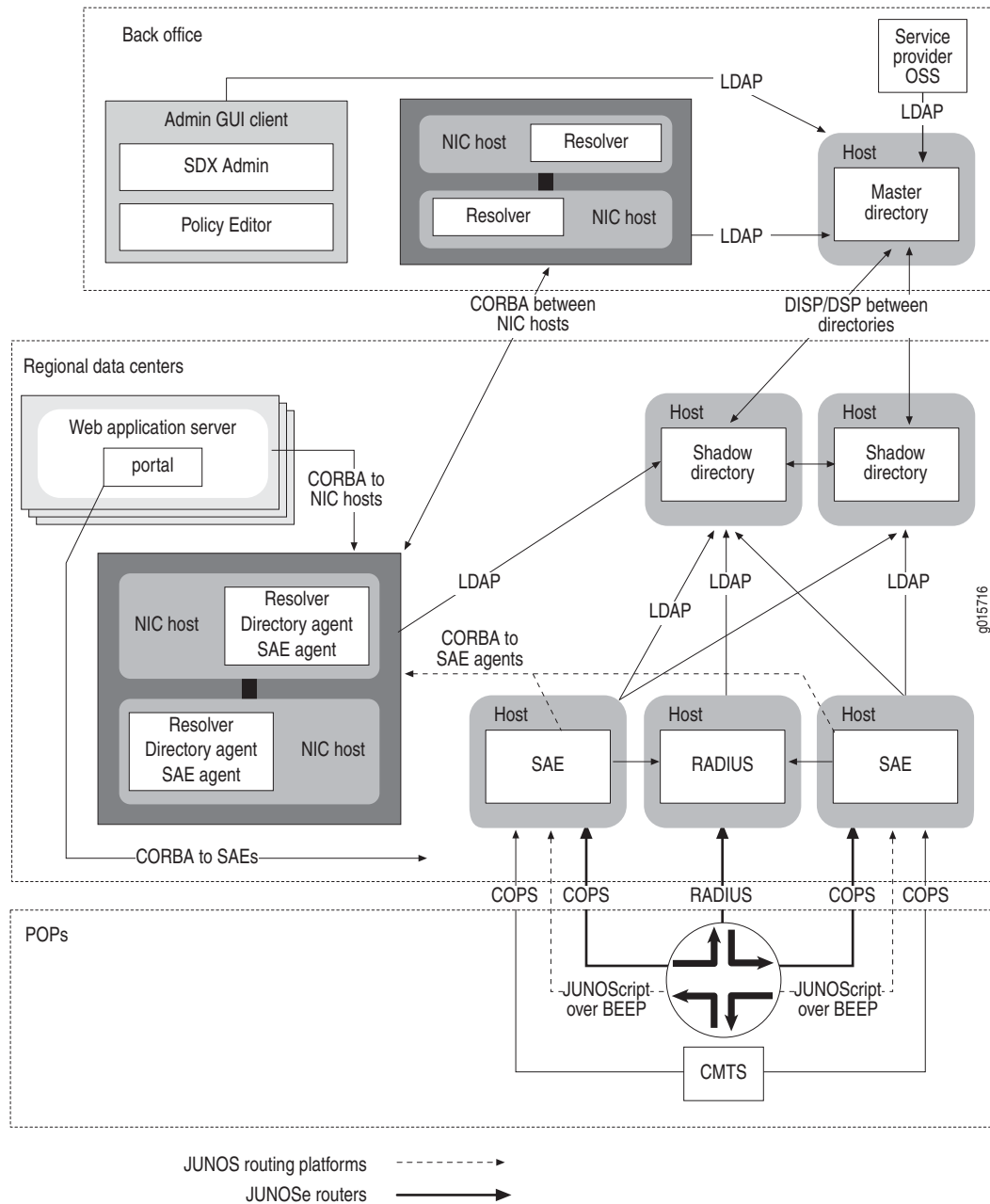


## Redundancy Schemes

The N to 1 and N to M redundancy schemes are even more important in regional data centers because a server could be serving a very large number of subscribers.

### *RADIUS*

Because RADIUS is stateless, it is enough to configure a sufficient number of RADIUS servers for the load and configure both the routers and the SAE to load balance across them.

### *NIC Hosts*

Regional data centers may or may not have one or more NIC hosts. It is up to service providers to add enough NIC hosts to achieve the desired level of availability and performance.

### *COPS Connection*

For the Common Open Policy Service (COPS) connection between the SAE and JUNOSe routers, special care must be taken. During a failover, existing activated services are not affected; but subscribers cannot log in, activate, or deactivate services until failover synchronization is complete. Thus, it may be desirable to configure multiple SAE machines (for example, tens) in the regional data center to limit the number of subscribers served by any one machine. The JUNOSe routers can be configured with primary, secondary, and tertiary COPS servers, so it is possible to configure many failover schemes. It is also possible for SAE servers to redirect existing and new COPS connections to other, more lightly loaded SAE servers. This COPS connection redirection can be triggered manually during a scheduled maintenance window or automatically based on SAE load monitoring.

### *Adding or Replacing Hardware*

Startup is simplified because there is always a pool of SAE hosts to manage any new routers as they are brought online. In the case of a disastrous server failure, the offending hardware can simply be removed and replaced as time and resources allow. Also, in regularly scheduled maintenance windows, incremental software upgrades can be achieved in the same fashion.

## Single-Host SRC Installation for Demonstration

Figure 26 shows a single-host installation that is suitable for demonstrations, trials, and small operations. The directory, Remote Authentication Dial-In User Service (RADIUS) server, SAE, and a Java 2 Enterprise Edition (J2EE) Web application server that contains the portal application are all installed on the same host. The SDX Admin and Policy Editor applications also run locally. The router uses the single RADIUS and SAE servers, and all SRC components act as LDAP clients to the single directory.

**Figure 26: Single-Host Installation for Small Operations**
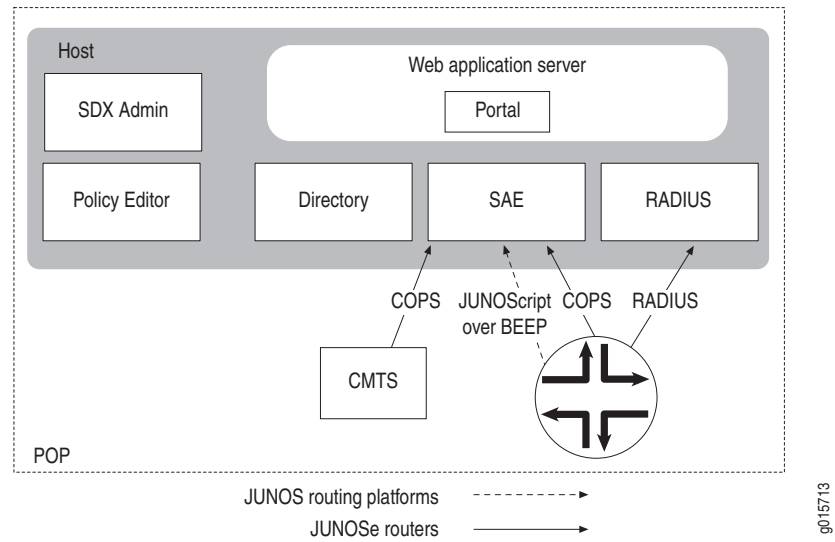
**Chapter 32**

# Before You Install the SRC Software on a Solaris Platform

This chapter provides information and procedures that you should read before you install the SRC software. Topics include:

## Requirements to Install the SRC Software

Before you start to install the SRC software, make sure that you:

- Have a license for the SRC software from Juniper Networks Customer Services and Support. For information about obtaining licenses, see *Chapter 8, Overview of SRC Licenses*.

- Have identified which SRC components to install on various systems in the network.

- Have a solid working knowledge of how to work in a UNIX environment, including how to perform tasks such as starting UNIX sessions, issuing commands on the UNIX command-line interface, mounting CDs, navigating through the file structure, and using a text editor to read and modify text files.

## Required User Privileges to Install the SRC Software

Before you install the software, make sure that you have administrator root permissions on each host where you plan to install and configure SRC software. A root user is typically a system administrator who has the authority to install software and maintain the system.

If you want authorized users to execute commands as if they had root privileges, you can use the UNIX **sudo** command to enable these authorized users.

If you want authorized users with nonroot privileges to be able to configure and administer the SRC software, you can create nonroot users and groups with the UNIX **admintool** utility. See your Solaris documentation for more information. Alternatively, you can use the command described in *Installing the SRC Software on a Solaris Platform in Silent Mode on page 270* to create nonroot users and groups.

☞ **NOTE:** You must install all SRC components as the same administrative user, either all as root or all as the same nonroot user. Installation of some components by the root user and others by a nonroot user causes problems.

## SRC Software Distribution

Juniper Networks provides the SRC software for installation on Solaris platforms on two *SDX-300 Service Deployment System Software CDs*. These CDs contain the component software, supporting applications, and *Release Notes* needed to install and operate the SRC software. Throughout this book, we refer to the software distributed on these CDs as the SRC software distribution.

The *SRC Application Library CD* contains software for optional SRC applications. For information about the SRC Application Library, see the *SRC-PE Application Library Guide.*

The *SDX-300 Service Deployment System Software CDs* are labeled SDX disk 1 and SDX disk 2.

Table 15 describes the contents of SDX disk 1.

**Table 15: Directories on SDX Disk 1**

| Directory | Contents (Directory Name or Description) |
|---|---|
| solaris | Package files to install the SRC software: |
| | omniORB, SMCpython, UMCagent, UMCcli, UMCdirxa, UMCecl, UMCeditor, UMCedsa, UMCiDSa, UMCjboss, UMCjdb, UMCjfds, UMCjps, UMCjre, UMClicsvr, UMCmig, UMCnaming, UMCnetsnmp, UMCnic, UMCoida, UMColdap, UMColdapa, UMCpom, UMCpyadd, UMCredir, UMCredmon, UMCsae, UMCsmg, UMCwebadm |
| solaris9 | Directories for IP Filter: |
| | ipf, ipfx |
| tools | Files for the **verifyInst** command: |
| | criteria.cfg, verifyInst |
| webapp | Web archive (WAR) files for Web applications: |
| | entmgr.war, licsvrAdmin.war, nataddr.war, nicAdmin.war, pomAdmin.war, ssportal.war, tagsEntdemo.war |
| Release_Notes.pdf | Release Notes |
| UMCsdx.bin | SRC GUI installation program |

Table 16 describes the contents of SDX disk 2.

**Table 16: Directories on SDX Disk 2**

| Directory | Contents (Directory Name or Description) |
|---|---|
| gnu | Directory for Java Object Request Broker (ORB): |
| | JacORB |
| SDK | Directories for software development files: |
| | doc, idl, lib, lib-1.3, lib-1.4, mibs, plugin, scriptServices |
| solaris_patches | Directories that contain Solaris patch files: |
| | solaris9, solaris10 |
| Steel_Belted_Radius | Package files to install Steel-Belted Radius: |
| | JNPRsbrsp, UMCsbrspa |
| Unsupported | Directories that contain unsupported software: |
| | ConfEd, RPMS, samples, Solaris, WinNT |

## System Requirements for Installing the SRC Software

All SRC components can typically be installed on a single Sun Solaris host that communicates across a network. The plan for your SRC implementation may require additional hosts to meet scalability and engineering requirements to distribute processing to other systems.

The detailed system requirements for each SRC component can vary greatly from installation to installation. You can consult with Juniper Networks Professional Services to determine the specific requirements for your SRC installation. The specifications depend on your particular needs, the number of customers you plan to service, and system usage. Basic requirements are listed in Table 17.

☞ **NOTE:** To determine the hardware requirements for third-party software, consult the documentation for that software.

You install the components listed in Table 17 on a Sun Solaris host.

For each component, ensure that the system meets the minimum memory requirements and minimum recommended disk space (to install and use a component) listed in Table 17.

**Table 17:  Minimum Memory and Minimum Disk Space Recommended for SRC Components on a Solaris Platform**

| Component Name | Memory | Disk Space | Notes |
|---|---|---|---|
| **Server Components** | | | |
| SAE | 1 GB | 50 MB | |
| Juniper Policy Server | 1 GB | 50 MB | |
| License server | 1 GB | 20 MB | |
| Network information collector (NIC) system | 1 GB | 50 MB | |
| Redundancy monitor system | 1 GB | 20 MB | |
| SNMP agent | 1 GB | 50 MB plus logging space | The SNMP agent does not operate on its own. It runs as a complementary component to other SRC components. |
| **Management Tools** | | | |
| Policy Editor | 1 GB | 5 MB plus logging space | |
| SDX Admin | 1 GB | 10 MB plus logging space | |
| **Infrastructure Components** | | | |
| AAA RADIUS server | 1 GB | 750 MB plus logging space | For exact space requirements for various versions of Steel-Belted Radius, see http://www.juniper.net/techpubs/software/aaa_802/sbr.html |
| JBoss application Web server | 1 GB | 60 MB | For exact space requirements for various versions of JBoss, see http://www.jboss.org/products/jbossas |
| **Captive Portal System** | | | |
| IP filter | 1 GB | 20 MB | |
| Web redirect server | 1 GB | 20 MB | |

## Verifying System Resources with the SRC CLI

You can use an SRC command, **verifyInst**, to verify that the Solaris platform has adequate system resources before and after you install the SRC software. The **verifyInst** command checks the current installation against the following SRC hardware and software requirements on a Solaris platform:

- Disk space for software operation—Platform

- Host OS release version—Processor

- Memory—Swap

The **verifyInst** command is located in the */tools* directory in the SRC software distribution. You can issue the command directly from the CD. If you want to install a local copy on a host, you must copy the complete */tools* directory to the host.

To check system resources for all currently installed components:

- Issue the **verifyInst** command with no arguments:

  **verifyInst**

To check system resources for one or two packages:

- Issue the **verifyInst** command with the package name(s):

  **verifyInst <package-Name> <package_name>**

  For example, to check the UMColdap and UMColdapa packages enter:

  **verifyInst UMColdap UMColdapa**

To check disk space when the SRC software is installed into a directory other then the default (*/opt/UMC*):

- Issue the **verifyInst** command with the **-l** option to specify the directory:

  **verifyInst -l <directory>**

  When you run the **verifyInst** command to check disk space, the command examines the default installation directory (*/opt/UMC*).

  For example, if you installed the SRC software into the */base/SDX* directory, enter:

  **verifyInst -l /base/SDX**

The */tools/criteria.cfg* file specifies default hardware and software requirements.

To use a different file to specify hardware and software requirements:

1. Create a text file that uses the same syntax as the *criteria.cfg* file.

2. Issue the **verifyInst** command with the **-f** option to specify the new file:

   **verifyInst -f <filename>**

   For example, to specify the *my.cfg* file:

   **verifyInst -f my.cfg**

## Network Requirements for the SRC Software

In a network that supports an SRC installation, ensure that:

- The systems on which SRC components run have network connectivity to each other.

- A domain name system (DNS) is configured on the network.

- Clocks on systems on which SRC components run are synchronized.

  Subscriber sessions may not be recognized if the clocks are not synchronized. We strongly recommend that you configure Network Time Protocol (NTP) on every server used for an SRC deployment.

- You define a mechanism to collect log information. Although, you can review the content of log files, we recommend that you use a syslog server for this purpose.

- You identify which router IP interfaces are to be managed as service deployment points.

## SNMP Master Agent Requirements

The SDX SNMP agent cannot act as a master agent, and it can communicate with master agents only by using the Agent Extensibility (AgentX) protocol. The SDX SNMP agent runs as a subagent to an installed AgentX master agent.

## Data Repository

The SRC software provides prepackaged integration for DirX directory server, eTrust Directory, Oracle Internet Directory, and Sun ONE Directory Server through add-on packages specific to a directory. You can also integrate other directories with the SRC software.

For information about the directory servers that you can integrate with the SRC software, see the *SRC-PE Release Notes*.

## RADIUS Choices

Although the SRC software operates with other RADIUS systems, we currently support system integration only with Juniper Networks Steel-Belted Radius/SPE server and Interlink Networks RAD-Series AAA RADIUS.

SRC support for Challenge Handshake Authentication Protocol (CHAP) depends on the integrated RADIUS software. Steel-Belted Radius/SPE server supports CHAP, so when you use the Steel-Belted Radius/SPE server the SRC software supports CHAP.

For information about the RADIUS servers that you can integrate with the SRC software, see the *SRC-PE Release Notes.*

## X-Window Server Software Recommendations

Many of the SRC graphical user interfaces (GUIs) supported on a Solaris platform, such as Policy Editor and SDX Admin, are X-Windows applications and require configuration of the X-Windows server to provide proper font and keyboard behavior. Failure to properly configure the X-Windows server can cause problems in certain circumstances; for example, if you try to use the Japanese locale without having the required Japanese fonts. If you have any questions about X-Windows server configuration, consult technical support or the user documentation for the X-Windows server that you are using.

## Installing Solaris Patches for the UNIX Host

Before you install the SRC software or related components, such as a directory server, make sure that you install the appropriate Sun Solaris patches on the host. Sun Microsystems frequently issues patch clusters. We recommend that you keep your operating system up to date with Sun's recommended patches for the Solaris operating system.

☞ **NOTE:** Review the *SRC-PE Release Notes* for information about the latest patches required to install your Solaris software.

We provide SRC-required Java 2 Platform, Standard Edition (J2SE) patches in a patch cluster in the SRC software distribution. You can find patch clusters and additional information about Solaris and J2SE patches at the following URL:

http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access

See the Sun Solaris documentation for instructions on how to install the operating system and OS patches.

To install the J2SE patches from the SRC software distribution:

1. On the UNIX host, log in as `root`.

2. Place the SDX software disk 2 in the CD drive.

3.  Follow the instructions in the *README* file appropriate to your operating system:

    ■  Solaris 9—*.../solaris_patches/solaris9/README*

    ■  Solaris 10—*.../solaris_patches/solaris10/README*

### Related Topics

■  *Chapter 33, Installing the SRC Software on a Solaris Platform.*

■  *Chapter 39, Upgrading the SRC Software on a Solaris Platform.*

## Chapter 33

# Installing the SRC Software on a Solaris Platform

This chapter describes how to install the SRC software. Topics include:

- Information About Installing IP Filter, Python Libraries, and the SNMP Agent on page 266

- Overview of Steps to Install the SRC Software on page 267

- Logging the Installation Session on page 267

- Installation Feature Sets, Components, and Packages on page 268

- Installation Choices on page 269

- Installing the SRC Software on a Solaris Platform in Silent Mode on page 270

- Installing the SRC Software on a Solaris Platform in Graphical Mode on page 271

- Overview of Installing SRC Components as Solaris Packages on page 277

- Installing SRC Components as Solaris Packages on page 278

- Transferring SRC Packages to Other Hosts on page 278

- Uninstalling the SRC Software on a Solaris Platform on page 279

## Information About Installing IP Filter, Python Libraries, and the SNMP Agent

Before you install the SRC software, make sure that you are familiar with the information in this section about installing IP Filter, Python libraries, and the SNMP agent.

### IP Filter

You must install ipfx (the 64-bit IP Filter package) before you install ipf (the 32-bit IP Filter package). Both packages must be installed for a 64-bit Solaris system.

### Python Libraries

You must install the Python runtime environment (SMCpython) before you install the Python additional libraries (UMCpyadd).

### SNMP Agent

Consider the following factors when installing the SNMP agent:

- If you install the SNMP agent on a host running other SRC components, you must restart the other SRC components after the installation to enable the SNMP agent to manage them.

- If you install the SNMP agent to run under a nonroot user:

  - In the GUI installation program, you can specify authorized nonroot users in the Get User Input window.

  - In a package installation, select the "under a user identification" option when asked where to install UMCagent during the package installation. Provide the login name for the nonroot user when prompted. The SNMP agent is then installed in the home directory of the named user.

  If you install the SNMP agent to run under a nonroot user and later want to start, stop, or monitor the SNMP agent while logged in as the root user, you must use the **smagentroot** command instead of the **smagent** command. Failure to do so may cause the agent to create files, such as log files, that are owned by `root`. If a nonroot user later runs the SNMP agent, the agent will not be able to update these files.

- The SDX SNMP agent cannot act as a master agent, and it can communicate with master agents only by using the Agent Extensibility (AgentX) protocol. The SDX SNMP agent runs as a subagent to an installed AgentX master agent, such as the Net-SNMP agent. The SRC software distribution includes a prepackaged integration for the Net-SNMP agent.

## Overview of Steps to Install the SRC Software

The steps to install the SRC software are independent of the hosts on which you load the software.

To install the SRC software:

1. Complete preinstallation steps. See *Chapter 32, Before You Install the SRC Software on a Solaris Platform*.

2. Install components from the SRC software distribution.

   See one of the following procedures:

   - *Installing the SRC Software on a Solaris Platform in Silent Mode* on page 270

   - *Installing the SRC Software on a Solaris Platform in Graphical Mode* on page 271

   - *Overview of Installing SRC Components as Solaris Packages* on page 277.

3. Install directory software.

   See *SRC-PE Integration Guide: Network Devices, Directories, and RADIUS Servers* for information about directory software.

4. Install RADIUS software.

   See *SRC-PE Integration Guide: Network Devices, Directories, and RADIUS Servers* for information about installing RADIUS software.

5. (For software upgrades only) Reboot your host(s).

6. Define the initial configuration, and start software components.

   See *Chapter 34, Defining an Initial Configuration on a Solaris Platform*.

## Logging the Installation Session

You can log your installation session. UNIX provides several different ways to capture a session.

- If you are using a Telnet or SSH client to connect to the installation host, you can use the logging capabilities of that client to capture the session.

- You can use a terminal that supports logging, such as dtterm. The command **/usr/dt/bin/dtterm -l -lf /tmp/dtterm.log** enables output logging to the file */tmp/dtterm.log*. You must exit the dtterm terminal before it flushes all the output to the file.

■ You can use the UNIX **tee** command to redirect the standard out and standard error to a specified file. For example:

**pkgadd -d /cdrom/cdrom0/solaris 2>&1 | tee -a sessionlog**

■ You can use the UNIX **script** command. The following command sequence captures a **pkgadd** session to the file *capture.txt*; pressing Ctrl + d exits the script:

**script capture.txt**
**pkgadd -d /cdrom/cdrom0/solaris**
**<Ctrl+d>**

See the UNIX **man** pages for **dtterm**, **tee**, and **script** for more information.

When you use the SRC GUI installation program for installation on a Solaris platform, all the installation session output is captured and appended to the log file for the GUI installation program in */opt/UMC/var/InstallerData/solpkg_Install.log*. This file is created if it does not already exist.

## Installation Feature Sets, Components, and Packages

The SRC software contains standard Solaris packages, Java Web Archives, and Java Enterprise Archives. Table 18 lists SRC components available in the various feature sets, the packages that contain the components, and the directories into which SRC components are installed.

**Table 18: Solaris Packages and Installation Directories for All Installation Components**

| Feature Set | Components | Package | Installation Directory |
|---|---|---|---|
| Env | ■ Java Runtime Environment | ■ UMCjre | ■ jre |
| | ■ Python Runtime Environment (includes Python additional libraries) | ■ SMCpython and UMCpyadd | ■ python |
| License Server | ■ License Server | ■ UMClicsvr | ■ licsvr |
| Application and Web Server | ■ JBoss | ■ UMCjboss | ■ jboss |
| SAE System | ■ SAE | ■ UMCsae | ■ sae |
| | ■ System Management Agent | ■ UMCagent | ■ agent |
| SDX Management System | ■ Command Line Interface | ■ UMCcli | ■ cli |
| | ■ SDX Web Administration | ■ UMCwebadm | ■ webadm |
| | ■ SDX Command Line Interface | ■ UMCeditor | ■ editor |
| Captive Portal System | ■ IP Filter (Solaris 9) | ■ ipfx, ipf | ■ ipf |
| | ■ Web Redirect | ■ UMCredir | ■ redir |
| | ■ omniORB | ■ omniORB | ■ omni |
| NIC System | ■ NIC System | ■ UMCnic | ■ nic |
| PDF Viewer | ■ PDF Viewer | ■ UMCxpdf | ■ xpdf |

**Table 18: Solaris Packages and Installation Directories for All Installation Components  (continued)**

| Feature Set | Components | Package | Installation Directory |
|---|---|---|---|
| Admin Workstation | ■ Policy Editor<br>■ SDX Admin<br>■ omniORB | ■ UMCpom<br>■ UMCsmg<br>■ omniORB | ■ pom<br>■ smg<br>■ omni |
| Juniper Policy Server | ■ Juniper Policy Server | ■ UMCjps | ■ jps |
| Redundancy Monitor System | ■ Redundancy Monitor System | ■ UMCredmon | ■ redmon |
| Directory Server | ■ Fedora Directory Server<br>■ COS Naming Service<br>■ Sun ONE Directory Server Add-On<br>■ DirX Add-On<br>■ Oracle Internet Directory Add-On<br>■ eTrust Directory Server Add-On<br>■ Migration | ■ UMCjfds, UMCjdb<br>■ UMCnaming<br>■ UMCiDSa<br>■ UMCdirxa<br>■ UMCoida<br>■ UMCedsa<br>■ UMCmig | ■ jdb<br>■ naming<br>■ conf/iDS<br>■ $DIRX_HOME$<br>■ conf/OID<br>■ conf/etrust<br>■ migration |

## Installation Choices

You can install the SRC software by:

■ Using the installation program—a wrapper around the Solaris packages

■ Installing SRC components as Solaris packages

If you use the SRC installation program, you run the program with or without a GUI.

■ Silent mode does not display the installation GUI.

When you run the command for silent mode, the system prompts you for input in a UNIX window as the various components of the SRC software are installed. Provide input as requested by the program to proceed with the installation.

■ Graphical mode lets you use the GUI shown in to install the software.

You can select which SRC components you want to install and where you want to install them. Buttons at the bottom of the window let you cancel the installation, move to a previous step, and move to the next step. You can move, minimize, or close the window for the installation program.

**Figure 27: Installation Program GUI**
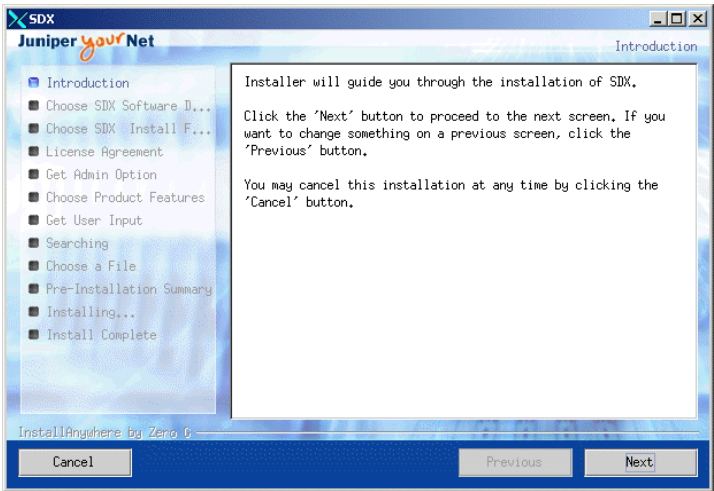


We use the graphical mode to illustrate the installation procedures.

## Installing the SRC Software on a Solaris Platform in Silent Mode

You use the **UMCsdx.bin** command to run the installation program. Table 19 shows the possible inputs to this command.

**Table 19: Command Options for UMCsdx.bin**

| [argument] | default [value] | Notes |
|---|---|---|
| ADMIN_FILE | pkgadd.SSC.default | SDX Admin file |
| INSTALLER_DATA_DIR | /opt/UMC/var/InstallerData | Installation data directory |
| USER_INSTALL_DIR | /opt/UMC | Installation destination directory |
| USER_INPUT_RESULT_1 | sdxuser | User with nonroot privileges who can install the SRC software. See *Logging the Installation Session* on page 267. |
| USER_INPUT-RESULT_2 | staff | Group for users with nonroot privileges who can install the SRC software. See *Logging the Installation Session* on page 267. |
| MEDIAFOLDER | cdrom/cdrom0/SDX | Installation source directory |

To start the installation process in silent mode:

- Enter the following command at the UNIX command line:

  **./UMCsdx.bin -D[*argument*]="[*value*]" -i silent**

If you want nonroot users to configure and administer the SRC software after it is installed, you can define users with nonroot privileges with the USER_INPUT_RESULT_1 and USER_INPUT_RESULT_2 arguments to the command. For example:

> **./UMCsdx.bin -DUSER_INPUT_RESULT_1="sdxuser"**
> **-DUSER_INSTALL_DIR="/opt/UMC" -DMEDIA_FOLDER="/cdrom/cdrom0" -i**
> **silent**

## Installing the SRC Software on a Solaris Platform in Graphical Mode

You can install the SRC software by installation set. In general, an installation set corresponds to a group of software components that provide specific functionality. For example, if you want a particular host to act as an SAE and as a directory server, you could install the SAE and Directory Server installation set on that host.

Table 20 lists the components and feature sets that are included by default for each installation set.

☞ **NOTE:** For a specified installation set, you can select additional components or deselect components. Be careful if you do this; deselecting required components can have undesired results.

**Table 20: Default Installation Set Components**

| Installation Set | Feature Sets and Components |
| --- | --- |
| SDX Demo | ■ Env |
| |   ■ Java Runtime Environment |
| |   ■ Python Runtime Environment |
| | ■ Application and Web Server |
| |   ■ JBoss |
| | ■ SAE System |
| |   ■ SAE |
| |   ■ System Management Agent |
| | ■ SDX Management System |
| |   ■ Command Line Interface |
| |   ■ SDX Web Administration |
| |   ■ SDX Command Line Interface Editor |
| | ■ Captive Portal System |
| |   ■ IP Filter (Solaris 9); the installation program detects the Solaris version on the host and installs the appropriate IP Filter for that OS. |
| |   ■ Web Redirect |
| | ■ PDF Viewer |

**Table 20: Default Installation Set Components  (continued)**

| Installation Set | Feature Sets and Components |
| --- | --- |
|  | ■ Admin Workstation |
|  |    ■ Policy Editor |
|  |    ■ SDX Admin |
|  |    ■ omniORB |
|  | ■ Juniper Policy Server |
|  | ■ Directory Server |
|  |    ■ Fedora Directory Server |
|  |    ■ COS Naming Service |
| SDX License Server | ■ Env |
|  |    ■ Java Runtime Environment |
|  |    ■ Python Runtime Environment |
|  | ■ License Server |
| SAE and Directory Server | ■ Env |
|  |    ■ Java Runtime Environment |
|  |    ■ Python Runtime Environment |
|  | ■ SAE System |
|  |    ■ SAE |
|  |    ■ System Management Agent |
|  | ■ Directory Server |
|  |    ■ Fedora Directory Server |
|  |    ■ COS Naming Service |
| SAE Server | ■ Env |
|  |    ■ Java Runtime Environment |
|  |    ■ Python Runtime Environment |
|  | ■ SAE System |
|  |    ■ SAE |
|  |    ■ System Management Agent |
| Policy Server | ■ Juniper Policy Server |
| Application and Web Server | ■ Env |
|  |    ■ Java Runtime Environment |
|  | ■ Application and Web Server |
|  |    ■ JBoss |
| NIC Server | ■ Env |
|  |    ■ Java Runtime Environment |
|  |    ■ Python Runtime Environment |
|  | ■ NIC System |
| Redundancy Monitor Server | ■ Env |
|  |    ■ Java Runtime Environment |
|  |    ■ Python Runtime Environment |
|  | ■ Redundancy Monitor System |

**Table 20:  Default Installation Set Components  (continued)**

| Installation Set | Feature Sets and Components |
|---|---|
| Captive Portal | ■ Env<br>  ■ Python Runtime Environment<br>■ Captive Portal System<br>  ■ IP Filter (Solaris 9); the installation program detects the Solaris version on the host and installs the appropriate IP Filter for that OS.<br>  ■ Web Redirect<br>  ■ omniORB |
| Administrator WorkStation | ■ Env<br>  ■ Java Runtime Environment<br>  ■ Python Runtime Environment<br>■ PDF Viewer<br>■ Admin Workstation<br>  ■ Policy Editor<br>  ■ SDX Admin<br>  ■ omniORB |
| Directory Server | ■ Directory Server<br>  ■ Fedora Directory Server<br>  ■ COS Naming Service |
| Custom | ■ Env<br>  ■ Java Runtime Environment<br>  ■ Python Runtime Environment<br>■ Application and Web Server<br>  ■ JBoss<br>■ SAE System<br>  ■ SAE<br>  ■ System Management Agent<br>■ SDX Management System<br>  ■ Command Line Interface<br>  ■ SDX Web Administration<br>  ■ SDX Command Line Interface Editor<br>■ PDF Viewer<br>■ Admin Workstation<br>  ■ Policy Editor<br>  ■ SDX Admin<br>  ■ omniORB<br>■ Juniper Policy Server<br>■ Directory Server<br>  ■ Fedora Directory Server<br>  ■ COS Naming Service |

To Install the SRC software from the installation program in graphical mode:

1. On the Solaris platform where you will install the SRC software, log in as `root`.

2. Ensure that the display variable is set.

   **echo $DISPLAY**

3. (Optional) Create nonroot users and groups using the UNIX **admintool** utility to enable nonroot users and groups to administer the SRC software.

4. Load SDX software disk 1, and start the installation program.

   **/cdrom/cdrom0/UMCsdx.bin**

5. Follow the instructions in the various windows.

   a. In the Choose Software Distribution Folder window, specify the location of the software to be installed. You can accept the default location, or specify a different location.

   b. In the Choose SDX Install Folder window, specify the directory into which the software will be installed. The program displays the default installation directory, */opt/UMC*. Although you can specify a different installation directory, you cannot change the location where SRC components are installed within that directory.

   > **NOTE:** All examples in this book presume that you have accepted the default directory.

   > **NOTE:** The SRC software does not support the use of spaces in filenames or directories. If you create files or directories inside the installation directory structure, you must do the following:
   >
   > ■ Ensure that the names do not include spaces.
   >
   > ■ Manage the files and directories outside the context of SRC software.
   >
   > If a filename or directory name includes a space, the removal of various packages will fail.

   c. In the License Agreement window, read then accept the software license for the SRC software. You must accept the license agreement to proceed with the installation.

d. In the Get Admin Option window, select the *admin* file from which the SRC installation program obtains installation parameters. An *admin* file assigns values to various installation parameters to define default installation actions. See the UNIX **man** page for **admin(4)**. You can select one of the following:

- SDX Admin file—Uses SRC installation parameters.

- Solaris Admin file—Uses Solaris default installation parameters from the Solaris default *admin* file. This file is located in */var/sadm/install/admin/default*.

The selected admin option is used to install all the packages. You cannot change admin options for an individual package. The admin selection affects only the current GUI installation instance; if you start the installation program again, the program does have access to any value previously set for the admin option and therefore does not use any previous settings.

e. In the Choose Product Features window, select sets of SRC components to install. You select an installation set that includes one or more feature sets, in part or whole. A feature set includes one or more components. Figure 28 shows how installation sets, feature sets, and components appear in the Choose Product Features window.

**Figure 28: Choose Product Features Window**
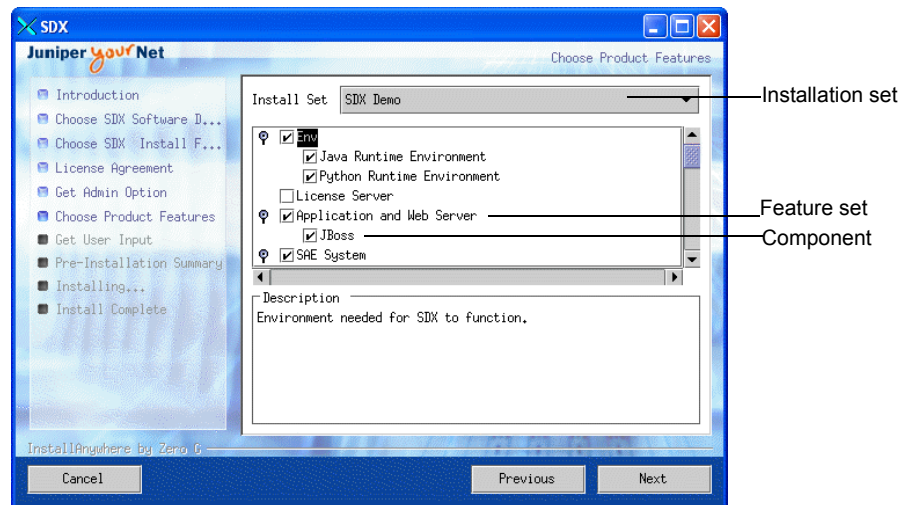


For each installation set, various recommended or required components are selected by default for installation. Click on a package or component to display a brief description.

> **NOTE:** If you install SRC software over an existing installation, the installation program displays a message stating that the existing software will be overwritten.

Table 18 on page 268 lists components for each available feature set, their Solaris package names, and the directories in which each component is installed.

f.  In the Get User Input window, you can specify nonroot users or groups. The users or groups must already exist (created with the UNIX **admintool**), or the installation program returns an error.

> ☞ **NOTE:** Some SRC processes, such as the SAE and the LDAP directory server, use many open files and sockets. You may need to customize the hard and soft limits for the system resources that are used by such SRC processes. Examine your system configuration information and UNIX account holder configuration that runs the SRC processes. See your Solaris system administration documentation for more information about determining the limits of your system configuration and UNIX account holder configuration. The UNIX **man** pages for the **limit(1)** command and the **sysdef(1M)** command also provide useful information.
>
> For example, if you are installing the SRC software in a nonroot environment in a typical Solaris 9 or Solaris 10 installation, the maximum number of file descriptors is too low for nonroot users. The hard limit is 1024, and the soft limit for nonroot users is 256. You can use the UNIX **ulimit** command to increase the number.

g.  In the Preinstallation Summary window, review the feature sets, the components in the feature sets to be installed, and the folder into which the components will be installed. If the list is correct, click Install. The installation program installs the components listed.

The Installing SDX window shows the progress of the installation for the components selected. The installation program opens a UNIX window as it uses the **pkgadd** command to install each component. Messages in the UNIX window request confirmation or other input for installation of a package.

After the installation program finishes installing SRC software components, the Install Complete window displays a message that indicates whether the installation was completed successfully.

6.  In the Install Complete window, click Done when the installation program indicates that the installation is complete.

## Overview of Installing SRC Components as Solaris Packages

The SRC software is constructed as a set of standard Solaris packages. You can use the Solaris package tools directly to install and remove SRC components. The tools are available as standard UNIX commands accessible through a shell command-line interface. See the Software Package Administration documentation for Solaris for detailed information. The *admin* installation file with the following entries is used:

```
mail=
instance=unique
partial=ask
runlevel=ask
idepend=nocheck
rdepend=ask
space=ask
setuid=nocheck
conflict=nocheck
action=nocheck
basedir=default
```

Refer to your Solaris documentation for more information about these settings. Also see the online UNIX **man** pages for the **admin(4)** utility. You cannot configure these settings with the GUI installation program.

⚠️ **CAUTION:** The conflict = nocheck setting results in an automatic overwriting of existing files. If you use directory links (hard or soft), they will be replaced automatically with files from the installation media.

You can install the software into a directory or under a user identification. If you choose to install the software under a user identification, you specify a username. The name of the group associated with the user account must be the same as the username. The installation script expects the username and the group name to be the same.

### Solaris IP Filter Software Installation Notes

If your host system hardware is based on 64-bit processors, then you must install ipfx (the 64-bit IP Filter package) before you install ipf (the 32-bit IP Filter package). Both packages must be installed for a 64-bit Solaris system. For 32-bit processors, install only ipf.

☞ **NOTE:** For Solaris 9, install the packages from the *solaris9* directory.

## Installing SRC Components as Solaris Packages

Table 18 on page 268 lists the Solaris packages for SRC feature sets.

To install individual SRC components as Solaris Packages:

1. On the Solaris platform where you will install the SRC software, log in as `root`.

2. Load SDX software disk 1, and access the CD directory.

   **cd /cdrom/cdrom0/**

3. List the contents of the CD.

   **ls**

   See *Overview of Steps to Install the SRC Software* on page 267 for a list of the directories and their contents on SDX disk 1.

4. Install the components using the UNIX **pkgadd** or **admintool** utility. For example, to install the UMCagent package:

   **pkgadd -d /cdrom/cdrom0/solaris UMCagent**

### *Related Topics*

■ *Chapter 34, Defining an Initial Configuration on a Solaris Platform*

## Transferring SRC Packages to Other Hosts

The SRC software is distributed as packages in the distribution in the file system format. If you want to transfer the packages to another host—for example, by using FTP—you must first convert the file system format to generate a single file that you can then transfer to the host.

You can use the **pkgtrans** tool to translate the file system format of the desired packages to a single file (datastream format). You can optionally compress the file with compression tools such as the UNIX **compress** or **gzip** utilities.

You can use the **md5sum** utility to verify the integrity of the file transfer. The utility computes and checks the MD5 message digest for a file. After packaging the file for transfer, run **md5sum** on the package file to compute an MD5 checksum for the file. Send both the checksum and the file to the destination host by using FTP. After the transfer, run **md5sum** on the destination host to compute a checksum for the transferred file and compare it with the original checksum. If the two checksums do not match, **md5sum** fails, and you know an error occurred in the transfer. You must repeat the transfer. If a transfer log exists, you can examine the log to determine why the transfer has failed before you attempt to retransmit the file. Only when the checksum passes, indicating a successful file transfer, can you use the file for installation.

If you compressed the file before transfer, you must uncompress the transferred file on the destination host. You can either translate the package from datastream format to file system format or use the datastream format directly.

### *Example: Transferring and Installing Packages*

The following sample commands and output illustrate the transfer and installation of the UMCsae and UMCnic packages from the SRC software disk 1 on a source host to the destination host.

■ On the source host:

```
# mount /cdrom/cdrom0
# cd /tmp
# pkgtrans -d /cdrom/cdrom0/solaris /tmp/UMCftp.pkg UMCsae UMCnic
Transferring <UMCsae> package instance
Transferring <UMCnic> package instance
# gzip /tmp/UMC.pkg
# md5sum -b UMCftp.pkg.gz > md5sum.txt
# cat md5sum.txt
588d1fe4ee7d59febef7c26cd441b5bd UMCftp.pkg.gz
```

Now use FTP to transfer the *UMCftp.pkg.gz* and *md5sum.txt* files in binary mode to the destination host, and place them in the */tmp* directory.

■ On the destination host:

```
# cd /tmp
# md5sum -c md5sum.txt
UMCftp.pkg.gz: OK
# gzip -d UMCftp.pkg.gz
# pkgadd -d /tmp/UMCftp.pkg
```

If the checksum had failed, instead of the text above you would see something like the following:

```
# md5sum -c md5sum.txt
UMCftp.pkg.gz: FAILED
md5sum: WARNING: 1 of 1 computed checksum did NOT match
```

## Uninstalling the SRC Software on a Solaris Platform

Use the **uninstall** program only if you installed the SRC software or components with the GUI installation program. If you installed the application or components with the Solaris package tools, you must also use these tools to uninstall the software. You can also use these tools directly to uninstall SRC components that you installed by using the GUI. For example, to remove the NIC package, issue the following command, and respond as prompted by the process:

```
pkgrm UMCnic
```

The GUI program to uninstall the SRC software is a wrapper around the Solaris packages that simplifies the removal of SRC software components.

The **uninstall** program checks whether any processes currently running belong to the component being uninstalled. If the program finds an active process, you can do one of the following:

■ Exit from the **uninstall** program.

■ Have the **uninstall** program force the process to halt. The program generates a warning if halting is not a safe option.

■ Manually stop the process, and then continue to uninstall the software with the **uninstall** program.

When you use the **uninstall** program to uninstall the software, all the session output is captured and appended to a special log file that is created if it does not already exist. The sessions are captured to the file */opt/UMC/var/InstallerData/solpkg_Uninstall.log*.

When the process to uninstall the software has been completed, the Uninstall SDX dialog box displays only components that you did not select for removal. You can verify removal of the selected packages by starting the **uninstall** program again. Packages that were successfully removed will not be displayed. If you previously selected all packages for removal, the program displays an alert indicating that there are no SRC components available for removal.

To uninstall the SRC software by using the GUI program:

1. On the Solaris platform, log in as `root`.

2. Stop all SRC services that are running.

    To stop the SAE:

    **/opt/UMC/sae/etc/sae stop**

    For information how to stop other SRC services, see the associated documentation.

3. Access the directory that contains the **uninstall** program.

    **cd /opt/UMC/uninstall**

4. Start the **uninstall** program.

    **./sh uninstall_SDX**

5. Select one or more of the displayed packages in the Uninstall SDX dialog box, and click Uninstall.

6. Click OK in the Please Confirm dialog to proceed with the package removal.

### *Related Topics*

■ *Overview of Steps to Install the SRC Software* on page 267.

## Chapter 34
# Defining an Initial Configuration on a Solaris Platform

After you install the SRC software, you configure initial settings to get a basic configuration up and running. This chapter describes how to set up an initial configuration. Topics include:

- Configuring Initial SRC Component Settings and Starting Components on page 281

- Saving Logging Information for an SRC Component on page 282

- Starting and Operating the SAE on page 282

- Reviewing Port Settings for SRC Components on page 284

- Enabling Display of Help Topics for SRC Configuration Tools on page 286

- Upgrading the SRC Software from a Previous Release on page 286

## Configuring Initial SRC Component Settings and Starting Components

After you install the SRC software for the first time or upgrade an installation, you configure and start various SRC components.

To perform the initial basic configuration for an SRC environment:

1. Configure the data repository, and optionally load sample data.

   If you are using another directory server, see *SRC-PE Integration Guide: Network Devices, Directories, and RADIUS Servers*.

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

   See *SRC-PE Integration Guide: Network Devices, Directories, and RADIUS Servers* for information about starting RADIUS servers.

3. Configure SAE local properties.

   See *Chapter 35, Setting Up an SAE on a Solaris Platform*.

4. Obtain and install your SRC software license.

   See *Chapter 8, Overview of SRC Licenses*, *Chapter 12, Installing Licenses for SRC Software on Solaris Platforms*, and *Chapter 13, Managing the SRC License Server on Solaris Platforms*.

5. If you are using a license server, start it.

   See *Chapter 13, Managing the SRC License Server on Solaris Platforms*.

6. Configure and start the SDX SNMP Agent.

   See *Chapter 36, Configuring and Starting the SDX SNMP Agent on a Solaris Platform*.

7. Start the SAE.

   See *Starting and Operating the SAE* on page 282.

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

   See *Reviewing Port Settings for SRC Components* on page 284.

9. Configure other SRC components, see *Upgrading the SRC Software from a Previous Release* on page 286.

## Saving Logging Information for an SRC Component

Many SRC server processes (including the SAE server, NIC host server, SNMP agent server, and the license server) have been modified to use a daemon wrapper. The daemon wrapper script writes the output of its child process to the files *<server-install-dir>/stdout* and *<server-install-dir>/stderr*. For example, in the SAE these files are located by default in the */opt/UMC/sae/stdout* and */opt/UMC/sae/stderr* directories. The files include timestamps.

You can rotate these files without stopping the server process. The rotation method uses the standard UNIX method for reopening log files: When you want to rotate the logs, rename the current file and then send a SIGHUP signal to the process. The process ID is stored in the file *<server-install-dir>/var/run/daemon.pid*. For example in SAE, this file is located at */opt/UMC/sae/var/run/daemon.pid*. You can automate log rotation with system tools, such as **logadm** (Solaris 9) or **rotatelog**, see

   http://www.sunfreeware.com

## Starting and Operating the SAE

Starting the SAE is the final step in the SRC software installation and basic configuration process. Before you configure and start the SAE, make sure that you have completed the following:

■ Installed and configured the supporting software.

- Installed, configured, and started the directory

- (Optional) Installed, configured, and started RADIUS servers.

- Started the directory, RADIUS, and license servers.

- Configured local properties for the SAE.

  See *Chapter 35, Setting Up an SAE on a Solaris Platform*.

By default, the SAE sends log events to the system log. You can also enable file loggers to write logs to text files.

For more information, see *SRC-PE Monitoring and Troubleshooting Guide, Chapter 2, Configuring Logging for SRC Components*.

### Starting the SAE for the First Time

Starting the SAE for the first time requires root permission and a special script to add the virtual IP address.

To start the SAE from its host for the first time:

1. On the host on which the SAE is installed, log in as `root` or as an authorized nonroot admin user.

2. Start the SAE from its installation directory

   **/opt/UMC/sae/etc/saeroot start**

Whenever the host subsequently reboots, the installed SRC server components are restarted automatically.

You can also start the SAE from the SRC CLI, see *Chapter 21, Setting Up an SAE with the SRC CLI*.

### Starting the SAE After Initial Startup

Use this procedure to start the SAE anytime after its initial startup.

To start the SAE from its host after the first time:

1. On the host on which the SAE is installed, log in as `root` or as an authorized nonroot admin user.

2. Start the SAE from its installation directory

   **/opt/UMC/sae/etc/sae start**

You can also start the SAE from the SRC CLI, see *Chapter 21, Setting Up an SAE with the SRC CLI*.

### *Monitoring the SAE*

To verify that the SAE is running:

1. On the host on which the SAE is installed, log in as `root` or as an authorized nonroot admin user.

2. Display the status of the SAE from its installation directory

   **/opt/UMC/sae/etc/sae status**

   The system responds with a status message.

### *Stopping the SAE*

To stop the SAE:

1. On the host on which the SAE is installed, log in as `root` or as an authorized nonroot admin user.

2. Stop the SAE from its installation directory

   **/opt/UMC/sae/etc/sae stop**

You can also stop the SAE from the SRC CLI, see *Chapter 21, Setting Up an SAE with the SRC CLI*.

## Reviewing Port Settings for SRC Components

If you use firewall software within your internal network, ensure that firewall settings allow traffic to and from components in your SRC environment. Table 21 lists the default port settings for SRC components.

For information about default port settings for applications in the SRC application library, see *Chapter 1, Installing the SRC Applications* in the *SRC-PE Application Library Guide.*

Table 21: Default Port Settings for SRC Components

| Component | Type of Communication | Default Port Setting |
|---|---|---|
| Applications, such as portals, that use the SAE Common Object Request Broker Architecture (CORBA) remote application programming interface (API) | CORBA remote API connections to the SAE. | TCP 8801 |
| Cable modem termination system (CMTS) devices | Connection requests. | TCP 3918 |

**Table 21: Default Port Settings for SRC Components   (continued)**

| Component | Type of Communication | Default Port Setting |
|---|---|---|
| Sample residential portal with Tomcat[a] | Starting Tomcat server. | TCP 8005 |
| | Apache JServ Protocol (AJP) requests for Tomcat. | TCP 8009 |
| | Responses to incoming HTTP requests from Tomcat. This port is an alternative to port 80. | TCP 8080) |
| JBoss[b] | Remote method invocation (RMI) requests. | TCP 1099 |
| | Communications for the Java Naming and Directory Interface (JNDI). | TCP 1100 |
| License server | Messages from SAEs to the license server. All SAEs in a configuration must be able to reach the license server. | TCP 9000 |
| LDAP | Communications between LDAP and other components in an SRC environment, such as the SAE, NIC, and SNMP. | TCP 389 |
| Network information collector (NIC) | Communications between the NIC host and components, such as portals, that use the NIC. All components that use NIC resolution must be able to reach the NIC host. | TCP 8810 |
| RADIUS | Communications between RADIUS and the SAE. | UDP 1812 |
| | Communications between RADIUS and the SAE for RADIUS accounting. | UDP 1813 |
| Redirect engine | Redirection requests. | TCP 8800 |
| SAE | Common Open Policy Service (COPS) connection from JUNOSe routers. | TCP 3288 |
| | Blocks Extensible Exchange Protocol (BEEP) connection from JUNOS routers. | TCP 3333 |
| | BEEP with Transport Layer Security (TLS) | TCP 3434 |
| | Session store data replication. | TCP 8820 |
| SAE Web Admin | Secure HTTP. | TCP 8443 |
| SNMP agent | SNMP communications between SNMP subagents and the master SNMP agent. | UDP 8030 |
| | SNMP get and set messages. | UDP 161 |
| | SNMP traps. | UDP 162 |

[a] For more information about ports that Tomcat uses, see http://jakarta.apache.org/tomcat
[b] For more information about ports that JBoss uses, see http://www.jboss.org/products/jbossas

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

## Enabling Display of Help Topics for SRC Configuration Tools

In SDX Admin and SDX Policy Editor you can display information about how to use the application from the Help **>** Online Help or the Help **>** Help Contents menu.

To view the online Help:

■ Ensure that a PDF viewer is installed on the Solaris platform.

You can install the UMCxpdf package in the SRC software distribution, or use another PDF viewer that is installed on your system. If you use a PDF viewer other than xpdf, ensure that the PDF viewer is registered on the Solaris system.

For information about how to register a PDF viewers with your Web browser, see the documentation for your Web browser.

## Upgrading the SRC Software from a Previous Release

If you are upgrading the SRC software from a previous release, return to *Chapter 33, Installing the SRC Software on a Solaris Platform*, and complete the upgrade procedure.

After you create the basic SRC configuration for the first time, or after you finish the upgrade procedure, you can configure other SRC components and establish configurations for service providers and enterprises. Table 22 lists the principle SRC components that you can configure and names the chapters that provide information about configuring the component. To get information baout using the C-Web interface to configure components, see the *SRC-PE C-Web Interface Configuration Guide.*

**Table 22: Configuration Information for Other SRC Components**

| Component | Document |
|-----------|----------|
| LDAPS connections between SRC components and the directory | *SRC-PE Integration Guide: Network Devices, Directories, and RADIUS Servers, Chapter 7, Configuring LDAPS for SRC Components* |
| License server for SRC software installed on Solaris platforms | *Chapter 13, Managing the SRC License Server on Solaris Platforms* |
| SNMP agent | *Chapter 28, Configuring and Starting the SNMP Agent with the SRC CLI* |
| | *Chapter 36, Configuring and Starting the SDX SNMP Agent on a Solaris Platform* |
| SAE | *SRC-PE Network Guide: SAE, Juniper Networks Routers, NIC, and SRC-ACP, Chapter 2, Configuring the SAE with the SRC CLI* |
| Logging | *SRC-PE Monitoring and Troubleshooting Guide, Chapter 3, Configuring Logging for SRC Components with the CLI* |
| | *SRC-PE Monitoring and Troubleshooting Guide, Chapter 5, Managing SRC Log Files on a Solaris Platform* |

**Table 22: Configuration Information for Other SRC Components (continued)**

| Component | Document |
|---|---|
| Network information collector (NIC) | *SRC-PE Network Guide: SAE, Juniper Networks Routers, NIC, and SRC-ACP, Chapter 10, Configuring NIC with the SRC CLI* |
| | *SRC-PE Network Guide: SAE, Juniper Networks Routers, NIC, and SRC-ACP, Chapter 11, Configuring NIC on a Solaris Platform* |
| Web applications | *Chapter 38, Installing Web Applications* |
| Services | *SRC-PE Services and Policies Guide, Chapter 1, Managing Services with the SRC CLI* |
| | *SRC-PE Services and Policies Guide, Chapter 2, Managing Services on a Solaris Platform* |
| Subscribers and subscriptions | *SRC-PE Subscribers and Subscriptions Guide, Chapter 12, Configuring Subscribers and Subscriptions with the SRC CLI* |
| | *SRC-PE Subscribers and Subscriptions Guide, Chapter 13, Configuring Subscribers and Subscriptions with SDX Admin* |
| Policies | *SRC-PE Services and Policies Guide, Chapter 10, Configuring and Managing Policies with the SRC CLI* |
| | *SRC-PE Services and Policies Guide, Chapter 11, Configuring and Managing Policies with Policy Editor* |
| Enterprise Service Portals | *SRC-PE Subscribers and Subscriptions Guide, Chapter 22, Installing and Configuring Enterprise Service Portals* |

**Chapter 35**

# Setting Up an SAE on a Solaris Platform

This chapter describes how to configure initial settings for the SAE on a Solaris platform and how to edit the SAE local configuration file.

You can also use the following to set up an SAE:

- To use the SRC CLI, see *Chapter 21, Setting Up an SAE with the SRC CLI*.

- To use the C-Web interface, see *SRC-PE C-Web Interface Configuration Guide, Chapter 8, Setting Up an SAE with the C-Web Interface*.

Topics in this chapter include:

- Configuring SAE Initial Settings on page 289

- Configuring SAE Attributes in Property Files on page 295

## Configuring SAE Initial Settings

Before you configure licenses and before you start the SAE, configure the local parameters for the SAE. These local properties are stored in the default-properties file. The following procedure describes how to use the local configuration tool to configure the SAE local properties.

For information about how to use the local configuration tool, see *Chapter 42, Configuring Local Properties*.

To configure SAE properties that are stored in a local file rather than in the directory:

1. On the SAE host, log in as `root` or as an authorized nonroot admin user.

2. Start the local configuration tool from the SAE installation directory.

   **/opt/UMC/sae/etc/config -l&**

   The local configuration tool window appears.
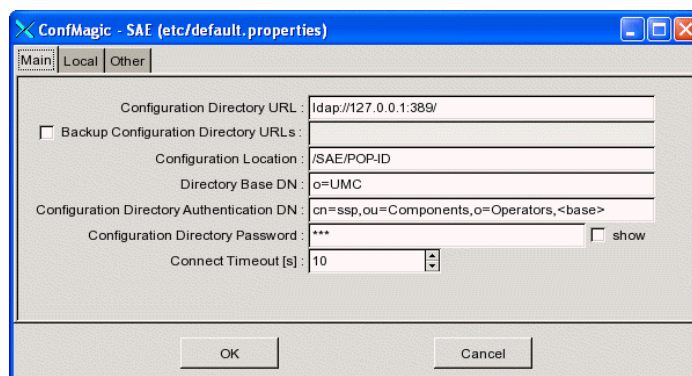


3. Using the field descriptions in the following sections, configure the fields in each tab of the configuration tool window; then click **OK**.

## Directory Fields

Use the Main tab in the local configuration tool for the SAE to specify configuration directory information.

### Configuration Directory URL

- URL of the directory server containing the main SAE configuration data.
- Value—ldap://<URL>
- Default—ldap://127.0.0.1:389

### Backup Configuration Directory URLs

- URL of one or more backup directory servers containing the main SAE configuration data.
- Value—LDAP URL in the format
  ldap:<address>[:<port>][/<path>][?query]
- Guidelines—Use a semicolon (;) to separate URLs for multiple backup directory servers.
- Default—No value

### Configuration Location

- Location of the object holding the SAE configuration data.
- Value—Symbolic name of the SAE

■ Guidelines—Replace /SAE/POP-ID with a symbolic name for the SAE you are configuring. Sensible choices are the hostname of the server or the name of a given location. If you configure multiple servers in a common redundant configuration, the servers should refer to the same configuration object.

■ Default—/SAE/POP-ID

### Directory Base DN

■ Distinguished name (DN) of the root directory for the SAE.

■ Value—DN of the root directory for the SAE

■ Guidelines—You must set this attribute if you use a directory-naming scheme different from the default.

■ Default—*o = umc*

### Configuration Directory Authentication DN

■ DN used for authentication with the directory server.

■ Value—DN used for authentication

■ Guidelines—Replace the default DN with an object that has read/write access to the subtree *ou = Configuration, o = umc*. Access to other parts of the directory is not required.

■ Default—*cn = ssp, ou = Components, o = Operators, o = < base >*

### Configuration Directory Password

■ Password used to authenticate the directory server.

■ Value—Text string

■ Guidelines—The password must match the userPassword attribute of the authentication DN. You can display the password in the clear or as asterisks.

■ Default—ssp

### Connect Timeout

■ Time interval during which connection must be established.

■ Value—Number of seconds in the range 1–2147483647

■ Default—10

### RADIUS and Portal Address Fields

Use the Local tab Main tab in the local configuration tool for the SAE to set the local IP addresses.
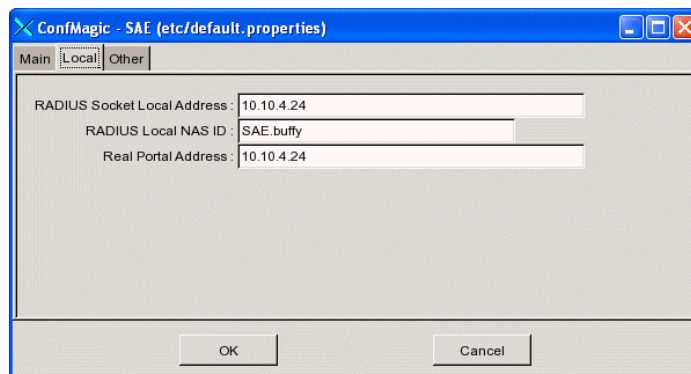


#### RADIUS Socket Local Address

- Local IP address on the SAE host used for communication with RADIUS servers.

- Value—IP address in dotted decimal notation

- Guidelines—In an installation in which the SAE is equipped with multiple network interfaces, you must specify the interface that communicates with external RADIUS servers. Typically, you must configure the RADIUS server to accept requests from a client; use this IP address for the RADIUS client configuration. Even if the RADIUS server is running on the same server as the SAE, do not use 127.0.0.1 as the local address because this address is typically the loopback address for a server. The address that you specify should be a unique network access server (NAS) IP address.

- Default—One of the IP addresses configured on the host (except 127.0.0.1)

#### RADIUS Local NasID

- String identifying the SAE when sending RADIUS authentication and accounting records. Typically, the string is the name of the SAE host.

- Value—Text string that identifies the SAE

- Default—SSP. < hostname >

#### Real Portal Address

- Interface on the SAE that the SAE uses for communication with the router.

- Value—IP address in dotted decimal notation

- Guidelines—If you clear this field, the interface is assumed to be the interface that was used to connect the router driver to the SAE. If the SAE is equipped with multiple network interfaces, you must specify the interfaces that are used to communicate with the router.

- Default—One of the IP addresses configured on the host (except 127.0.0.1), or the field may be empty

### JRE, SNMP, and Port Offset Fields

Use the Other tab Main tab in the local configuration tool for the SAE to configure Java Runtime Environment (JRE) information, enable Simple Network Management Protocol (SNMP), configure the location of the SAE interoperable object reference (IOR) file, and configure the port offset for SAE instances.
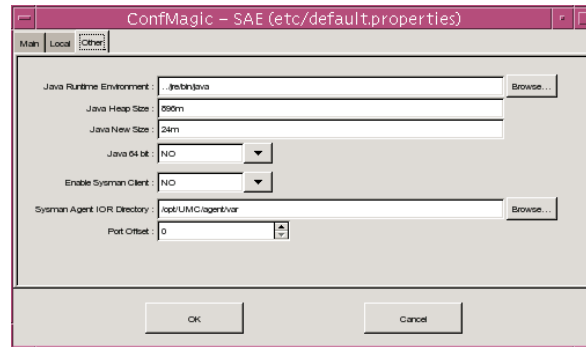


#### Java Runtime Environment

- Path to the JRE.

- Value—Absolute or relative directory path

  This path is the default installation path for the JRE that is distributed with the SRC software and installed with the other SRC components.

- Guidelines—The SRC software requires a JRE that conforms to the Java 2 specification. The SRC software has been tested with Sun's JRE. See the *SRC-PE Release Notes* for information about which version of the Sun JRE is distributed with the SRC software. We expect other JREs to work, but have not verified whether they do.

- Default—*.../jre/bin/java*

- Example

  - */opt/UMC/jre/bin/java*—Absolute path

  - *.../jre/bin/java*—Relative path to the installation directory for the SAE

#### Java Heap Size

- Maximum Java heap (memory) size available to the JRE. The value is inserted when the JRE starts.

- Value—Number of megabytes

- Guidelines—Change this value if you experience problems caused by lack of memory. Set the value lower than the available physical memory to avoid low performance caused by disk swapping.

  See also

    http://java.sun.com/j2se/1.4.2/docs/tooldocs/solaris/java.html

- Default—The value is calculated dynamically to 70 % of the available real memory when you first run the SAE local configuration tool.

### Java New Size

- Amount of space available to the JRE when the component starts.

- Value—Integer in the range 0– < Java heap size > . Specify the value in bytes or add m for megabytes, k for kilobytes, or g for gigabytes. Number of megabytes followed by m. See the documentation for the JRE for valid values.

- Default—24m

### Java 64-Bit

- Specifies whether or not the JRE uses the 64-bit Java virtual machine.

- Value

  - Yes

  - No

- Guidelines—If 64-bit mode is enabled, the Java virtual machine can access more than 4 gigabytes of memory. Enabling 64-bit mode can have negative implications on CPU performance. Please consult the Juniper Technical Assistance Center before you change this value.

- Default—No

### Enable Sysman Client

- Enables the SNMP agent to communicate with the SAE.

- Value

  - Yes—Enabled

  - No—Disabled

- Default—No

### Sysman Agent IOR Directory

- Folder that contains the IOR file for the SAE. The SAE writes its object references to this folder, and the SNMP agent discovers SAE components by monitoring the SAE IOR file in this folder.

- Guidelines—By default, the SAE IOR file is in the *var* folder, which is relative to the SNMP agent installation folder (*/opt/UMC/agent*). You need to change this property only if you installed the SNMP agent in a folder other than the default folder, or if you previously changed this property and now need it to point to the folder where the IOR file currently resides.

- Value—Path to the folder that contains the IOR

- Default—*/opt/UMC/agent/var*

### Port Offset

- Port offset for SAE instances.

- Value—Integer

- Guidelines—Specify a port offset if you install multiple instances of the SAE on the same host.

- Default—0

## Configuring SAE Attributes in Property Files

As an alternative to using the configuration GUIs, you can configure both local SAE properties and SAE properties stored in the directory by editing text files.

To configure the properties files:

1. Access the SAE installation directory.

   **cd /opt/UMC/sae**

2. Edit the SAE local configuration file, *etc/default.properties*, as desired.

3. Retrieve the directory properties, and save them into a filename of your choice.

   **etc/config -g <filename>**

4. Edit the directory properties file as desired.

5. Save the directory properties back into the directory.

   **etc/config -p <filename>**

---

**NOTE:** The **-H** option displays help information for the **config** command.

---

**Chapter 36**

# Configuring and Starting the SDX SNMP Agent on a Solaris Platform

This chapter describes how to configure and run the SDX Simple Network Management Protocol (SNMP) agent on a Solaris platform using the SRC configuration applications. It also describes how to install and use the Net-SNMP agent in the SRC environment.

You can also use the CLI that runs on Solaris platforms and the C-series Controllers to configure the SNMP agents. See *Chapter 28, Configuring and Starting the SNMP Agent with the SRC CLI*.

Topics in the chapter include:

- Configuring the SDX SNMP Agent on page 297

- Operating the SDX SNMP Agent on page 307

- Starting the SDX SNMP Agent on page 308

- Stopping the SDX SNMP Agent on page 308

- Monitoring the SDX SNMP Agent on page 308

- Installing and Using the Net-SNMP Agent in an SRC Environment on page 309

## Configuring the SDX SNMP Agent

The SNMP agent monitors host resources and the SRC components that use the host resources. The SNMP agent obtains most of its information from the directory. A local configuration file primarily stores bootstrapping information that cannot be stored in the directory.

The SDX SNMP agent cannot act as a master agent, and it can communicate with master agents only by using the Agent Extensibility (AgentX) protocol. The SDX SNMP agent runs as a subagent to an installed AgentX master agent, such as the Net-SNMP agent. This setup means that SNMP requests to the master agent for SDX MIB objects (typically on port 161) are automatically redirected to the SDX SNMP agent (on its configured port).

You can use the local configuration tool to configure the SNMP agent.

For information about using the local configuration tool, see *Chapter 42, Configuring Local Properties*.

For more information about the SNMP agent, see *SRC-PE Monitoring and Troubleshooting Guide, Chapter 10, Configuring the SNMP Traps on a Solaris Platform*.

To configure the SNMP agent:

1.  On the SAE host, log in as `root` or as an authorized nonroot admin user.

2.  Start the local configuration tool from the SNMP agent installation directory.

    **/opt/UMC/agent/etc/config -l**

    The SNMP Agent screen appears.
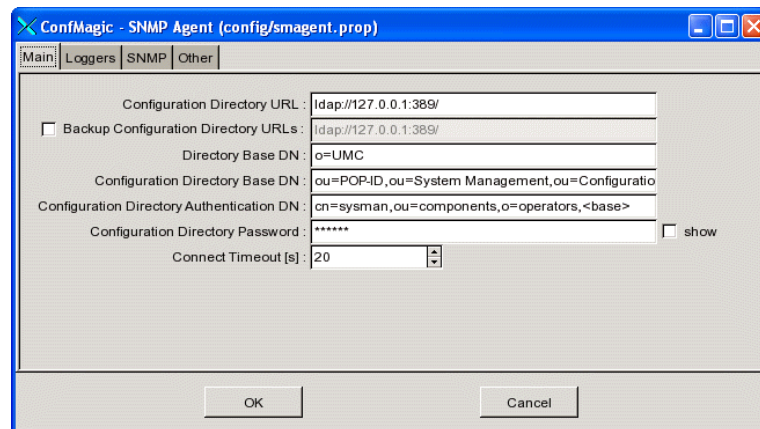


3.  Configure the SNMP agent by completing the fields in the tabs of the SNMP Agent screen. These sections describe the fields for each tab:

    ■  Directory Connection Parameters on page 299—Main tab

    ■  SNMP Agent Logging Fields on page 300—Loggers tab

    ■  Communication with the Master Agent on page 305—SNMP tab

    ■  Other SDX SNMP Agent Parameters on page 306—Other tab

4.  Click **OK** when you have completed the configuration, or click **Cancel** to cancel all changes made since you started the tool.

5.  Restart the SNMP agent for the changes to take effect.

    See *Starting the SDX SNMP Agent* on page 308.

### *Directory Connection Parameters*

Use the Main tab to configure directory connection parameters.

### *Configuration Directory URL*

- URL of the directory server that stores the SNMP agent configuration data.
- Value—URL in the format ldap://<URL>
- Default—ldap://127.0.0.1/389

### *Backup Configuration Directory URLs*

- URL of the backup directory server that stores the SNMP agent configuration data.
- Value—URL in the format ldap://<URL>
- Guidelines—Use a semicolon to separate URLs for multiple backup directory servers. Do not insert spaces on either side of the semicolon.
- Default—ldap://127.0.0.1/389
- Example—ldap://127.153.27.1/389;ldap://192.168.0.1/389

### *Directory Base DN*

- The distinguished name (DN) of the directory used for the SNMP agent configuration data.
- Value—<DN>
- Guidelines—You must set this attribute if you use a directory-naming scheme different from the default.
- Default—*o = umc*

### *Configuration Directory Base DN*

- The DN of the system management configuration in the directory server that provides the remaining configuration for the SNMP agent. If the entry does not exist, the entry and the subentries for the components and traps is automatically created in the system management configuration.
- Value—<DN>
- Guidelines—You can use the special value <base> to refer to the globally configured base DN.
- Default—*ou = POP-ID, ou = System Management, ou = Configuration, o = Management,* <base>

### *Configuration Directory Authentication DN*

- The DN of the entry in the directory server that authenticates the SNMP agent's directory bind.
- Value—<DN>
- Guidelines—You can use the special value <base> to refer to the globally configured base DN.
- Default—*cn = sysman, ou = components, o = operators,* <base>

### Configuration Directory Password

- The password used for authentication with the directory server.
- Value—String
- Default—sysman

### Connect Timeout [s]

- The time limit for establishing a connection to the directory server.
- Value—Number of seconds in the range 1–2147483. If you enter 0 or a negative value, the default configuration of the host's operating system is used.
- Default—20

## SNMP Agent Logging Fields

Use the Loggers tab shown in Figure 29 to configure the SNMP agent logging facility.

For more information about the logging attributes and about cleaning the logs, see *SRC-PE Monitoring and Troubleshooting Guide, Chapter 5, Managing SRC Log Files on a Solaris Platform*.

**Figure 29: Logging Tab of SNMP Agent Local Configuration Tool**



### Severity Levels

Log filters let you specify the level of severity for the event messages to be saved in log files. The event filter provides 128 levels of severity, numbered 1–127. A higher number indicates a higher level of severity. Common levels of severity also have a specific name, as shown in Table 23 on page 301.

Enable info-level logging only when you are initially setting up the SRC software or when you are troubleshooting. Do not leave info-level logging on during normal network operation. Do not enable debug logs unless you have been advised to do so by the Juniper Networks Technical Assistance Center. During normal network operations, enable error-level logging.

**Table 23: Named Severity Levels**

| Name | Severity Level |
| --- | --- |
| logmin | 1 |
| debug | 10 |
| info | 20 |
| notice | 30 |
| warning | 40 |
| error | 50 |
| crit | 60 |
| alert | 70 |
| emerg | 80 |
| panic | 90 |
| logmax | 127 |

### *Error Log Filter*

- Enable or disable the error log, and specify the minimum severity level of event messages saved to the log file.
- Value—Severity level specified by name or number. See *Severity Levels* on page 300. The format is:

  /severity name-

  or

  /severity number-
- Default—/error-

### *Error Log File*

- Filename and path of the log to which error event messages are saved.
- Value—Path and filename of the log file in the format
  < pathname > / < filename.log >
  - < pathname > —Directory in which the log file is stored
  - < filename.log > —Name of the log file
- Default—*var/log/smerror.log*

### Error Rollover File

- Filename of the rollover log file. When the log rollover size is exceeded, the contents of the primary log file are saved to the rollover file.
- Value—Path and filename of the rollover file in the format
  <pathname>/<filename.alt>
  - <pathname>—Directory in which the rollover log file is stored
  - <filename.alt>—Name of the rollover log file
- Default—*var/log/smerror.alt*

### Error Log Rollover Size

- Size of the primary log. If the rollover size is exceeded, the contents of the primary log are saved to the rollover log, overwriting any previous contents. New events are saved to the emptied primary log.
- Value—Number of kilobytes in the range 0–4294967295
- Default—1000000

### Info Log Filter

- Enable or disable the info log, and specify the minimum severity level of event messages saved to the log file.
- Value—Severity level specified by name or number. See *Severity Levels* on page 300. The format is:
  /severity name-
  or
  /severity number-
- Default—/info-

### Info Log File

- Filename and path of the log to which info event messages are saved.
- Value—Path and filename of the log file in the format
  <pathname>/<filename.log>
  - <pathname>—Directory in which the log file is stored
  - <filename.log>—Name of the log file
- Default—*var/log/sminfo.log*

### Info Log Rollover File

- Filename of the rollover log file. When the log rollover size is exceeded, the contents of the primary log file are saved to the rollover file.
- Value—Path and filename of the rollover file in the format
  <pathname>/<filename.alt>
  - <pathname>—Directory in which the log file is stored
  - <filename.alt>—Name of the log file
- Default—*var/log/sminfo.alt*

### Info Log Rollover Size

- Size of the primary info log. When the rollover size is exceeded, the contents of the primary log are saved to the rollover log, overwriting any previous contents. New events are saved to the emptied primary log.

- Value—Number of kilobytes in the range 0–4294967295

- Default—1000000

### Debug Log Filter

- Enable or disable the debug log, and specify the minimum severity level of event messages saved to the log file.

- Value—Severity level specified by name or number. See *Severity Levels* on page 300. The format is:

  /severity name-

  or

  /severity number-

- Default—Disabled

### Debug Log File

- Filename of the log to which event messages are saved.

- Value—Path and filename of the log file in the format
  <pathname>/<filename.log>

  - <pathname>—Directory in which the log file is stored

  - <filename.log>—Name of the log file

- Default—*var/log/debug.log*

### Debug Log Rollover File

- Filename of the rollover log file. When the log rollover size is exceeded, the contents of the primary log file are saved to the rollover file.

- Value—Path and filename of the log file in the format
  <pathname>/<filename.alt>

  - <pathname>—Directory in which the log file is stored

  - <filename.alt>—Name of the log file

- Default—*var/log/debug.alt*

### Debug Log Rollover Size

- Size of the primary log. When the rollover size is exceeded, the contents of the primary log are saved to the rollover log, overwriting any previous contents. New events are saved to the emptied primary log.

- Value—Number of kilobytes in the range 0–4294967295

- Default—1000000

### Error Syslog Filter

- Enable or disable the error system log, and specify the minimum severity level of event messages saved to the log file.

- Value—Severity level specified by name or number. See *Severity Levels* on page 300. The format is:

  /severity name-

  or

  /severity number-

- Default—/error-

### Error Syslog Hostname

- IP address or name of a host that collects error event messages by means of a standard system logging process.

- Value—IP address or hostname

- Default—loghost

### Info Syslog Filter

- Enable or disable the information system log, and specify the minimum severity level of event messages saved to the log file.

- Value—Severity level specified by name or number. See *Severity Levels* on page 300. The format is:

  /severity name-

  or

  /severity number-

- Default—Disabled

### Info Syslog Hostname

- IP address or name of a host that collects warning event messages by means of a standard system logging process.

- Value—IP address or hostname

- Default—loghost

### Communication with the Master Agent

Use the SNMP tab shown in Figure 30 to configure communication with the SNMP master agent.

---

👉 **NOTE:** If you change any of the parameters with the local configuration tool, you must restart the SDX SNMP agent.

---

**Figure 30: SNMP Tab of SNMP Agent Local Configuration Tool**
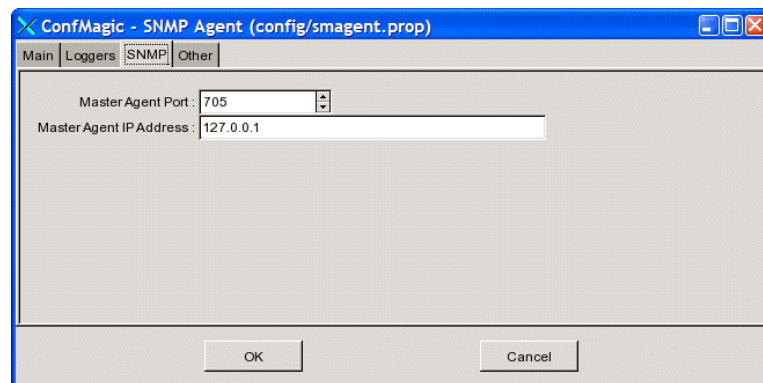


#### Master Agent Port

■ TCP port on which the SDX SNMP agent initiates the AgentX connection with the master agent. You must configure your master agent to accept AgentX connections from the SDX SNMP agent host on this port.

■ Value—TCP port number

■ Default—705

#### Master Agent IP Address

■ IP address of the master agent.

■ Value—IP address

■ Default—127.0.0.1

### Other SDX SNMP Agent Parameters

Use the Other tab, shown in Figure 31, to configure parameters for the Java Runtime Environment (JRE), trap history, and the watchdog program.

**Figure 31:  Other Tab of SNMP Agent Local Configuration Tool**
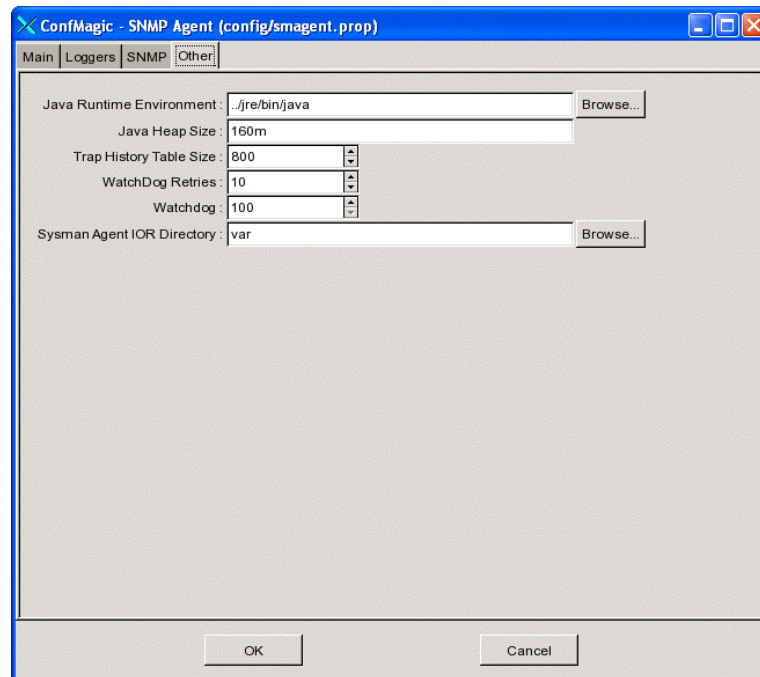


### Java Runtime Environment

- Path to the JRE.
- Value—Directory in which JRE is stored
- Default—*../jre/bin/java*

### Java Heap Size

- Maximum amount of memory available to the JRE.
- Value—Number of megabytes in the format < integer > m
- Guidelines—Change this value if you have problems caused by lack of memory. Set the value lower than the available physical memory to avoid low performance caused by disk swapping.
- Default—160m

### Trap History Table Size

- Maximum number of elements stored in the SNMP trap history table.
- Value—Integer
- Default—800

***WatchDog Retries***

- Number of times the agent watchdog attempts to restart the agent before sending a trap notification that the agent restart has failed.
- Value—Integer in the range 1–2147483647; 0 or a negative value suppresses the trap
- Default—10

***Watchdog***

- Polling interval at which the agent watchdog checks whether the agent is running correctly.
- Value—Number of seconds in the range 0–1000000000
- Default—100

***Sysman Agent IOR Directory***

- Folder that contains the interoperable object reference (IOR) files for SRC components. When the SNMP agent starts, it uses the IOR files in this directory to find SRC components that are already running so that it can connect to them. The SNMP agent also writes its IOR file to this directory so that components that start after the SNMP agent can find and connect to the SNMP agent.
- Value—Path to the folder that contains the IOR files
- Guidelines—By default, the IOR file is in the *var* folder, which is relative to the SNMP agent installation folder (*/opt/UMC/agent*). You need to change this property only if you installed the SNMP agent in a folder other than the default folder, or if you previously changed this property and now need it to point to the folder where the IOR file currently resides.
- Default—*/var*

## Operating the SDX SNMP Agent

The SDX SNMP agent can act as a subagent to any AgentX-enabled master agent that is running.

You must configure the SNMP agent and then manually start the agent. If you attempt to manually start the SNMP agent before it is configured, the software displays a message that the agent has not been configured and cannot start.

The SNMP agent automatically restarts in the event of a host reboot or process failure that stops the agent.

## Starting the SDX SNMP Agent

Before you start the SDX SNMP agent:

1. Start the installed directory server.

   See *Chapter 34, Defining an Initial Configuration on a Solaris Platform*.

2. Configure the SDX SNMP agent.

   See *Configuring the SDX SNMP Agent* on page 297.

Manually start the SDX SNMP agent the first time it runs. Thereafter, the agent automatically restarts.

To start the SNMP agent:

1. On the SNMP agent host, log in as `root` or as an authorized nonroot admin user.

2. Start the SNMP agent from its installation directory.

   **/opt/UMC/agent/etc/smagent start**

   The system responds with a start message. If the SNMP agent is already running, the system responds with a warning message indicating that fact.

## Stopping the SDX SNMP Agent

To stop the SNMP agent:

1. On the SNMP agent host, log in as `root` or as an authorized nonroot admin user.

2. Stop the SNMP agent from its installation directory.

   **/opt/UMC/agent/etc/smagent stop**

   The system responds with a stop message. If the SNMP agent is not running when you issue the command, the software responds with a warning message indicating that fact.

## Monitoring the SDX SNMP Agent

To display the SDX SNMP agent status:

1. On the SNMP agent host, log in as `root` or as an authorized nonroot admin user.

2. Display the status from the SNMP agent installation directory.

   **/opt/UMC/agent/etc/smagent status**

   The system responds with a status message.

### Cleaning SNMP Agent Logs and Process Files

By using the **stdout** and **stderr** options, you can clean the log files for the SNMP agent and delete the persistent data that the agent writes to files or devices.

For more information, see *SRC-PE Monitoring and Troubleshooting Guide, Chapter 5, Managing SRC Log Files on a Solaris Platform*.

### Commands for the Master Agent

Control of the master agent can vary depending on how you have set it up. See the master agent documentation for more information.

### Reading the SNMP Agent MIBs

The master agent may support only certain SNMP versions, such as SNMPv2. For example, if you attempt to read the SNMP agent MIBs in a MIB browser and with SNMPv3 settings, then the reading fails. See the master agent documentation for more information.

## Installing and Using the Net-SNMP Agent in an SRC Environment

The SRC software distribution includes a prepackaged integration for the Net-SNMP agent. For information about using the Net-SNMP master agent in an SRC environment, see:

- *Installing the Net-SNMP Agent* on page 309

- *Configuring the Net-SNMP Agent* on page 310

- *Starting the Net-SNMP Agent* on page 310

- *Stopping the Net-SNMP Agent* on page 310

- *Monitoring the Net-SNMP Agent* on page 310

- *Locating the Log File* on page 310

### Installing the Net-SNMP Agent

Before you install the Net-SNMP agent, you must install the Python Runtime Environment (UMCpython and UMCpyadd packages) and disable all other SNMP master agents.

For more information about installing the SRC software packages, see *Chapter 33, Installing the SRC Software on a Solaris Platform*.

To install the Net-SNMP agent:

1. On the UNIX host where you will install the Net-SNMP agent, log in as `root`.

2. Load SRC software disk 1 in the CD drive.

3. Install the UMCnetsnmp package using the UNIX **pkgadd** tool.

   **pkgadd -d /cdrom/cdrom0/solaris UMCnetsnmp**

   The UMCnetsnmp package is installed in the */opt/UMC/net-snmp* folder. Once installed, the Net-SNMP agent starts up automatically. The Net-SNMP agent also automatically restarts in the event of a host reboot.

### Configuring the Net-SNMP Agent

The configuration file for the Net-SNMP agent is located in the installation directory (by default, */opt/UMC/net-snmp/etc/snmpd.conf*). For more information about configuring the Net-SNMP agent, see the Net-SNMP documentation at:

   http://net-snmp.sourceforge.net/

### Starting the Net-SNMP Agent

To manually start the Net-SNMP agent:

1. On the Net-SNMP agent host, log in as `root` or as an authorized nonroot admin user.

2. Start the Net-SNMP agent from its installation directory.

   **/opt/UMC/net-snmp/etc/snmpd start**

### Stopping the Net-SNMP Agent

To stop the Net-SNMP agent:

1. On the Net-SNMP agent host, log in as `root` or as an authorized nonroot admin user.

2. Stop the Net-SNMP agent from its installation directory.

   **/opt/UMC/net-snmp/etc/snmpd stop**

### Monitoring the Net-SNMP Agent

To display the Net-SNMP agent status:

1. On the Net-SNMP agent host, log in as `root` or as an authorized nonroot admin user.

2. Display the status from the Net-SNMP agent installation directory.

   **/opt/UMC/net-snmp/etc/snmpd status**

### Locating the Log File

The log file for the Net-SNMP agent is located in the installation directory (by default, */opt/UMC/net-snmp/log/snmpd.log*).

**Chapter 37**

# Distributing Directory Changes to SRC Components on a Solaris Platform

This chapter describes how to configure the directory eventing system (DES) on a Solaris platform using the SRC configuration applications that run only on Solaris platforms.

You can also use the CLI that runs on Solaris platforms and the C-series Controller to configure the directory eventing. See *Chapter 30, Configuring Local Properties with the SRC CLI*.

Topics in this chapter include:

## Configuring JNDI Properties for the Directory Eventing System

DES is a Java Naming and Directory Interface (JNDI)–compliant service and accepts standard JNDI properties. For more information about JNDI, see http://java.sun.com/products/jndi/.

To configure JNDI properties for the directory eventing system:

- Use standard DES properties in the format:

  < connectionPrefix > . < standardJNDISuffix >

  Where the variable < connectionPrefix > is a property prefix that depends on the SRC component and the directory to which it connects, and the variable < standardJNDISuffix > is a standard JNDI property.

For example, the property net.juniper.smgt.des.retry_interval is a standard JNDI property that specifies how often the DES for the NIC agent polls the directory.

### *Variables to Customize JNDI Properties for an SRC Component*

If you do not specify values for the standard DES properties, DES accepts the default values. The following list shows the <standardJNDISuffix> variables for the most common standard JNDI properties that you may want to customize for an SRC component.

### *.java.naming.provider.url*

- URL of the primary directory.
- Value—URL in the format ldap:// <host>:389
    - <host> —IP address or name of directory host
- Example—ldap://127.0.0.1:389/

### *.java.naming.security.principal*

- Distinguished name (DN) of the directory entry that defines the username with which the SRC component accesses the directory.
- Value— <DN>
- Example—*cn = nic, ou = Components, o = Operators, <base>*

### *.java.naming.security.credentials*

- Password with which the SRC component accesses 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>.
- Example—admin

### *.java.naming.security.protocol*

- Security protocol (SSL) for the connection.
- Value—ssl

### *.java.naming.factory.initial*

- Name of the Java factory class from which the SRC software creates the LDAP initial context.
- Value—Path to Java factory
- Example—*net.juniper.smgt.lib.des.DESInitialContextFactory*

## Extending the Directory Eventing System for SRC Components

The SRC software defines a number of DES properties that extend the standard set.

- To extend the directory eventing system for SRC components, use the following format for the DES properties:

    <connectionPrefix> .des. <propertySuffix>

Where the variable < connectionPrefix > is a property prefix that depends on the SRC component and the directory to which it connects. The variable < propertySuffix > depends on the DES property.

For example, the property net.juniper.smgt.des.enable_eventing is a property that specifies whether the DES for the NIC agent polls the directory periodically.

## Variables to Configure DES Properties for SRC Components

The following list describes the < propertySuffix > variables for the DES properties that you can configure for SRC components.

### enable_eventing

- Specifies whether the SRC component polls the directory for changes.
- Value
  - True—SRC component polls the directory for changes.
  - False—SRC component does not poll the directory for changes.

### pollinginterval

- Time interval at which the SRC component polls the directory.
- Value—Number of seconds in the range 15–2147483647

### event_baseDN

- DN of an entry superior to the data associated with this SRC component in the directory.
- Value—$o$ = < DN > , < base >
  - < DN >—DN of superior entry
- Guidelines—If you are storing non-SRC data in the directory, and that data changes frequently whereas the SRC data does not, you may need to adjust the default value to improve performance. For optimal performance, set the value to the DN of an entry superior to both the SRC data and the changing non-SRC data.
- Default—$o$ = umc, < base >

### delegate_factory_initial

- Value used by an SRC internal process.
- Value—SRC software sets the value automatically

⚠ **CAUTION:** Do not change this value unless instructed to do so by Juniper Networks.

*connection_pool_size*

- Number of directory connections that DES uses.

- Value—1

> ⚠️ **CAUTION:** Do not change this value unless instructed to do so by Juniper Networks.

*dispatcher_pool_size*

- Number of events that the SRC component can receive from the directory simultaneously.

- Value—Integer in the range 1–2147483647

> ⚠️ **CAUTION:** Some SRC components require a specific value for this property. See the documentation for the component to determine whether you can change this value.

*connection_manager_id*

- DES connection manager within the JNDI framework.

- Value—Text string

- Example—DIRAGENT_POOL_VR

*fake_delete*

- Specifies how DES tracks objects deleted from the directory.

- Value—SRC software sets the value automatically

> ⚠️ **CAUTION:** Do not change this value unless instructed to do so by Juniper Networks.

*show_fake_delete*

- Specifies whether you can view the objects deleted from the directory.

- Value

    - True—Deleted objects are visible.

    - False—Deleted objects are not visible.

- Default—False

> ⚠️ **CAUTION:** Do not change this value unless instructed to do so by Juniper Networks.

### share_connection

- Specifies whether other SRC components running in the same process as this SRC component share a connection to the directory with this SRC component.

- Value—

  - True—SRC components share the connection.

  - False—SRC components do not share the connection.

---

⚠ **CAUTION:** Do not change this value unless instructed to do so by Juniper Networks.

---

### backup_provider

- List of redundant directories.

- Value—List of URLs separated by semicolons; URLs have the format ldap:// < host > :389

  - < host > —IP address or name of the directory host

- Example—ldap://127.0.0.1:389/; ldap://127.0.0.2:389/

### enable_sysman

- Specifies whether the SRC SNMP agent exports MIBs for this directory connection.

- Value

  - True—SNMP agent exports MIBs.

  - False—SNMP agent does not export MIBs.

### connect.timeout

- Maximum time that DES waits for the directory to respond.

- Value—Number of seconds in the range 1–2147483647

### retry_interval

- Time interval at which DES attempts to connect to the directory.

- Value—Number of seconds in the range 10–2147483647

### connectcheck_interval

- Time interval at which DES verifies its connection to the directory.

- Value—Number of seconds in the range 15–2147483647

### signatureDN

■ DN of the directory entry that specifies the usedDirectory attribute. The usedDirectory attribute identifies the type of directory, such as DirX, to which the SRC software is connected. For information about this attribute, see the LDAP schema files in the SRC software distribution in the directory *SDK/doc/ldap* or on the Juniper Networks Web site at

> http://www.juniper.net/techpubs/software/management/sdx

For information about setting this property, see *Identifying the Type of Directory on page 317*.

If the value of signatureDN is not the DN of a directory entry or is the DN of an entry that does not have a usedDirectory attribute, the SRC software logs an error and proceeds as it would for directory types other than DirX. If the value of the usedDirectory attribute does not correspond to a type of directory that the SRC software supports, the SRC software logs an error and proceeds as it would for directory types other than DirX.

■ Value— < DN >

■ Default—GlobalUserDatabase.server.signatureDN  =  *o = umc*

■ Example—GlobalUserDatabase.server.signatureDN  =  *o = SDX, o = Juniper, o = Applications*

### Example

```
java.naming.security.principal =  cn=nic,ou=Components,o=Operators,<base>
java.naming.security.credentials =  {BASE64}bmlj
java.naming.provider.url = ldap://127.0.0.1:389/
java.naming.factory.initial=net.juniper.smgt.lib.des.DESInitialContextFactory
net.juniper.smgt.des.enable_eventing = true
net.juniper.smgt.des.delegate_factory_initial = com.sun.jndi.ldap.LdapCtxFactory
net.juniper.smgt.des.connection_pool_size = 1
net.juniper.smgt.des.connection_manager_id = DIRAGENT_POOL_VR
net.juniper.smgt.des.dispatcher_pool_size = 1
net.juniper.smgt.des.fake_delete = true
net.juniper.smgt.des.show_fake_delete = false
net.juniper.smgt.des.directory_init_delta = 2592000
net.juniper.smgt.des.polling_interval = 30
net.juniper.smgt.des.share_connection=true
net.juniper.smgt.des.event_baseDN = <base>
net.juniper.smgt.des.enable_sysman = false
net.juniper.smgt.des.connect.timeout = 10
net.juniper.smgt.des.retry_interval = 30
net.juniper.smgt.des.connectioncheck_interval = 60
net.juniper.smgt.des.signatureDN = o=umc
```

## Identifying the Type of Directory

The SRC software includes a DES property called signatureDN that identifies the DN of the entry that specifies the LDAP schema attribute usedDirectory. This attribute identifies the type of directory, such as DirX, to which the SRC software connects. For information about this attribute, see the LDAP schema files in the SRC software distribution in the directory *SDK/doc/ldap* or on the Juniper Networks Web site at

http://www.juniper.net/techpubs/software/management/sdx

Identifying the type of directory allows the SRC software to accommodate the different ways that different directories process DES queries, and enables more efficient retrieval of information. In particular, this feature offers benefits for the following tasks:

- Checking whether an object in the directory has not been deleted

- Finding new entries in the directory

If you load the LDAP schema from the SRC software distribution, the SRC software automatically sets the usedDirectory attribute for the type of directory to which it connects. If you use this LDAP schema as the structure for your directory, you can use the default value (*o = umc*) for the signatureDN property, and you do not need to configure the type of directory.

However, if you use a customized LDAP schema rather than the provided LDAP schema, use the following procedure to allow the SRC software to determine the type of directory:

1. Choose the entry that specifies the usedDirectory attribute.

2. Specify a value for the usedDirectory attribute.

3. In the property file of the SRC component that connects to this directory, set the signatureDN property to the DN of the entry with the usedDirectory attribute for the signatureDN property.

   For example, use SDX Admin to configure DES properties for the SAE.

4. Repeat Steps 1 to 3 for each DES connection.

## Enabling Blacklisting for an Unresponsive Directory

For information about how the SRC software can manage connections to an unresponsive directory, see *Chapter 29, Distributing Directory Changes to SRC Components*.

To enable DES to prevent connection to a directory that repeatedly fails to respond:

- Configure the enable_blacklist property.

### *Blacklist Property*

You can enable the following property to blacklist a directory.

#### *enable_blacklist*

- Specifies whether DES prevents connection to a directory if the directory fails to respond during 10 polls.
- Value
  - True—DES prevents connection to the directory.
  - False—DES does not prevent connection to the directory.
- Default—False

## Reestablishing a Connection to a Directory

If DES prevents connection to a directory, do the following to reestablish the connection to the directory.

1. Fix the problem with the directory.

2. Restart the SRC component that communicates with this directory.

## Chapter 38
# Installing Web Applications

This chapter describes how to install Web applications that are included with the SRC software. Topics include:

- Installing Web Applications on page 319

- Removing Web Applications on page 321

- Session Timeouts for Web Applications on page 321

- Access Controls on page 322

## Installing Web Applications

We supply one Web archive (WAR) file for each Web application in the SRC software distribution and the application library CD. You must deploy Web applications in a Web application server.

The exact way you install Web applications depends on the Web application server you are using and the particular Web application. The following procedure provides general steps for installing a Web application:

1. Install the Web application server on the host.

2. Start the Web application server.

3. If the Web application requires configuration of a properties file, complete the following procedure:

   a. Copy the WAR file from the SRC software distribution or application library CD to a temporary folder on the host.

   b. Unpack the WAR file.

      For information about unpacking and packing WAR files, see

      http://java.sun.com/j2se/1.4/docs/guide/jar/

   c. Edit the properties file for the Web application.

   d. Repack the WAR file.

4. Deploy the WAR file by using the procedure appropriate for your Web application server.

   For information about deploying WAR files, see the documentation for your Web application software.

### Installing Web Applications Inside JBoss on a Solaris Platform

SRC software for Solaris platforms provides the JBoss Web application server in the SRC software distribution. JBoss is an open-source Java application server that provides full support for J2EE application programming interfaces (APIs).

To deploy a Web application inside JBoss:

1. Install the *UMCjboss* package from the SRC software distribution.

   For information about using the Solaris **pkgadd** utility to install the package, see *Chapter 33, Installing the SRC Software on a Solaris Platform*.

2. During the installation, choose a JBoss configuration when prompted; typically choose the default configuration.

3. Start JBoss.

   **/etc/init.d/jboss start**

   You can view the log file to observe the process:

   **/opt/UMC/jboss/server/default/log/server.log**

4. Customize the properties file for the Web application.

   For instructions about configuring the property files for the SRC Web applications, see the documentation for that application.

5. Deploy the WAR file by copying it into the JBoss *default/deploy* directory.

   **cp <filename>.war /opt/UMC/jboss/server/default/deploy**

JBoss automatically starts the Web application when a new WAR file is copied into the deploy directory.

### Stopping JBoss

To stop JBoss:

1. On the host on which JBoss is installed, log in as `root` or as an authorized nonroot admin user.

2. Stop JBoss.

   **/etc/init.d/jboss stop**

## Removing Web Applications

The way you remove a Web application depends on the Web application server that you use.

To remove a deployed Web application from JBoss:

■   Remove the WAR file from the JBoss *default/deploy* directory.

## Session Timeouts for Web Applications

For session-based Web applications, a session is started for the Web browser when it connects to a Web server application. A session provides a timeout feature that closes the session on the server when the maximum period of inactivity has passed. The default timeout for many application servers is 30 minutes.

This timeout is reset whenever there is activity on the Web browser, such as refreshing the current page or navigating through other pages under the application's control. Merely keeping a browser window open does not keep the session open, because it does not generate any activity on the browser.

When the session closes, any application-related state must be reestablished by the Web browser. Examples include such items as redoing the login, the parameters of the session, and connection to back-end systems such as directory servers or Common Object Request Broker Architecture (CORBA) servers.

You may be able to customize the session timeout, depending on the type of Web server or Web application server that you are using. See the documentation for your Web server or Web application server for information about configuring these settings.

☞   **NOTE:** Long timeouts or no timeouts not only result in security concerns for the browser, but also result in more resource usage on the servers to keep stale sessions.

The session timeout in *web.xml* used in a J2EE application server might be set as follows:

```
<web-app>
  ...
    <session-config>
      <session-timeout>30</session-timeout>
    </session-config>
  ...
</web-app>
```

## Access Controls

To enforce J2EE-style access controls, Web applications deployed in JBoss must contain a *WEB-INF/jboss-web.xml* file that defines a security domain as shown here:

```
<jboss-web>
<security-domain>java:/jaas/TEST_SECURITY_DOMAIN</security-domain>
</jboss-web>
```

For these Web applications, JBoss performs authentication as defined in the application's deployment descriptor, the *WEB-INF/web.xml* file. Here is the relevant sample portion of a *WEB-INF/web.xml* file:

```
<security-constraint>
   <web-resource-collection>
     <web-resource-name>TEST_WEB_RESOURCE_NAME</web-resource-name>
     <!-- Define the context-relative URL(s) to be protected -->
     <url-pattern>/*</url-pattern>
   </web-resource-collection>
   <auth-constraint>
     <role-name>TEST_ROLE_NAME</role-name>
   </auth-constraint>
</security-constraint>

<login-config>
  <auth-method>BASIC</auth-method>
  <realm-name>TEST_REALM_NAME</realm-name>
</login-config>
```

This *web.xml* file sample directs JBoss to obtain a username and password by using the HTTP BASIC pop-up. The sample shown from the *jboss-web.xml* file directs JBoss to authenticate that username and password by using the login module configured for the security domain, TEST_SECURITY_DOMAIN. You can edit the */opt/UMC/jboss/server/default/conf/login-config.xml* file to change the login module for a particular security domain.

If no login module is defined for TEST_SECURITY_DOMAIN, then the "other" security domain is used by default, as shown in this sample from the *login-config.xml* file:

```
<!--
  The default login configuration used by any security domain that
  does not have a application-policy entry with a matching name.
-->
<application-policy name = "other">
  <authentication>
    <login-module code="org.jboss.security.auth.spi.UsersRolesLoginModule" flag
= "required" />
  </authentication>
</application-policy>
```

The *org.jboss.security.auth.spi.UsersRolesLoginModule* login module authenticates usernames and passwords against the *server/default/conf/users.properties* file. The authenticated username must be a member of the role specified in the *web.xml* file. In our example earlier, this is TEST_ROLE_NAME.

To provide access to the Web application to user "anonymous" with password "secret" with the *jboss-web.xml* and *web.xml* files shown above, the login module requires the following information:

- From *server/default/conf/users.properties*:

  anonymous=secret

- From *server/default/conf/roles.properties*:

  anonymous=TEST_ROLE_NAME

The following Web applications do not have the *jboss-web.xml* file; you must add the file to provide J2EE-style access control:

- *./licenseServer/adminui/WEB-INF*

- *./prepaid/accountAdmin/WEB-INF*

## Chapter 39

# Upgrading the SRC Software on a Solaris Platform

This chapter describes how to upgrade the SRC software from one version of the software to a later version. Topics include:

- Upgrading the SRC Software on Solaris Platforms on page 325

- Overview of Directory Data on Solaris Platforms on page 326

- Overview of the Migration Script on page 326

- Migrating the Directory Data on page 327

## Upgrading the SRC Software on Solaris Platforms

To upgrade the SRC software from an earlier release of the SRC software or SDX software:

1.  Remove previously installed SRC components.

    See *Chapter 33, Installing the SRC Software on a Solaris Platform*.

2.  Remove all other components to be upgraded.

3.  Install the SRC software.

    See *Chapter 33, Installing the SRC Software on a Solaris Platform*.

4.  (Optional) Perform migration procedures to preserve data from a previous installation.

    See Migrating the Directory Data on page 327.

## Overview of Directory Data on Solaris Platforms

When you upgrade from an earlier SRC or SDX release, you must migrate your current directories for the upgraded SRC release.

In this release, we provide procedures to migrate directory data for Sun ONE Directory Server (iPlanet) or DirX from an earlier SRC or SDX software release. If you use Oracle Internet Directory, see the documentation for that product for information about updating directory data.

☞ **NOTE:** The documentation does not describe how to change from one directory type to another when you upgrade to the current SRC release. Contact Juniper Networks Professional Services for assistance if you need to change directory types.

Before you start the migration procedures, you must provide a new host machine for the new software. We refer to this host as the migration host. After you complete the migration procedure, you can transfer the new installation to the original host or use the migration host as your new deployment host.

The migration host must include the following features:

■ Physical attributes, such as memory and CPU, equal to or greater than those available on the original host.

■ A Solaris version compatible with the new SRC release.

■ The Solaris patches appropriate to the Solaris version.

■ The Python runtime environment appropriate to the SRC release from which you are migrating. This is the SMCpython package provided in the SRC software distribution for that release.

## Overview of the Migration Script

The migration script performs different tasks depending on whether you are upgrading your existing directory server to the latest release or keeping the current release.

### Script Tasks Without Directory Server Upgrade

1. Export and convert any existing LDAP objects into a file.

2. Delete the existing objects from the LDAP directory.

3. Delete all obsolete schema elements from the global directory schema.

4. Modify existing schema elements as needed, and add the new schema elements to the global directory schema.

5. Extend the access-control schema. For DirX only, extend the directory information tree (DIT) structure and DIT content rules.

6.  Modify existing data as needed.

7.  Import the modified LDAP objects into the directory.

### *Script Tasks With Directory Server Upgrade*

1.  Export and convert any existing LDAP objects into a file.

2.  Delete the existing objects from the LDAP directory.

3.  Export the existing database into an LDAP Data Interchange Format (LDIF) file in case the databases are not compatible between the current and upgraded versions.

4.  Remove the existing LDAP directory instance and the corresponding directory add-on package.

5.  Install the upgraded directory and the latest directory add-on package (which includes any schema changes).

6.  Import the LDIF file generated from the existing database.

7.  Modify existing data as needed.

8.  Import the modified LDAP objects into the directory.

## Migrating the Directory Data

The migration procedure consists of the following steps:

- Managing Shadowed Directories When Migrating Directory Data on page 328

- Preparing the Migration Host on page 330

- Cloning the Directory Server on page 331

- Installing the UMCmig Migration Package on page 333

- Overview of Directory Data on Solaris Platforms on page 326

- Running the Migration Script on page 334

- Completing the Migration on page 335

- Updating the Original Host on page 336

☞ **NOTE:** If disk shadowing is employed, you must ensure that shadowing is stopped. See *Managing Shadowed Directories When Migrating Directory Data on page 328* for further details.

### Managing Shadowed Directories When Migrating Directory Data

The migration procedure executes only on the primary directory. If you are performing the migration in a shadowed environment setup, then you must ensure that shadowing is terminated before running the migration script.

Perform the following migration procedures:

1. *Running the Migration Script on page 334*

2. *Completing the Migration on page 335*

3. *Updating the Original Host on page 336*

#### DirX Deployment

In a DirX deployment, you must terminate the shadowing agreement by using the **dirxadm** tool as follows:

1. Log in as user `dirx` and access the *customize* directory.

   **su - dirx**
   **cd customize**

2. Start **dirxadm**, perform a bind operation, and terminate the shadowing agreement.

   **dirxadm**
   **dirxadm> sou bind.tcl**
   **dirxadm> ob terminate -dsa <dsa_name> -operationalbindingid <ob-id>**
   **-bindingtype SOB**
   **dirxadm> exit**

   where < dsa_name > is the digital signature algorithm (DSA) of the partner (secondary) directory and < ob-id > is the operational binding ID. Both of these values were established when you established the shadowing agreement.

3. Perform the following migration procedures:

   a. *Running the Migration Script on page 334*

   b. *Completing the Migration on page 335*

   c. *Updating the Original Host on page 336*

#### Updating DirX Secondary Directories

After moving the migrated directory into production, you must update the DirX secondary directories.

1. Uninstall the current UMCdirxa package, and install the most recent one.

2. Log in as user `dirx` and access the *customize* directory.

   **su - dirx**
   **cd customize**

3.  Copy the *dirxabbr-ext.UMC* file.

    **cp <dirx_inst_path>/customize/dirxabbr-ext.UMC**
    **<dirx_inst_path>/client/conf/**

    where  < dirx_inst_path >  specifies the DirX installation directory.

4.  Create the access point of the secondary directory.

    **dirxadm**
    **dirxadm> bind**
    **dirxadm> ob modownacp {AE={ /CN=UMC-DSA2}, PSAP={TS=DSA,**
    **NA='TCP/IP!internet=127.0.0.1+port=21100' } }**
    **dirxadm>exit**

5.  Generate the SDX schema.

    **dirxadm**
    **dirxadm>bind**
    **dirxadm> sou schema.adm**
    **dirxadm>exit**

6.  Establish the shadowing agreements on secondary and primary hosts. Perform
    the following tasks on both secondary and primary host.

    **su - dirx**
    **cd customize**
    **dirxadm**
    **dirxadm> sou bind.tcl**
    **dirxadm> ob establish -dsa <dsa_name> -operationalbindingid <ob-id>**
    **-bindingtype SOB**
    **dirxadm> exit**

## Sun ONE Deployment

To turn off shadowing and restart the directory server for a Sun ONE deployment:

1.  Terminate the shadowing agreements before the migration procedure is
    executed.

2.  Complete the following tasks to migrate the primary directory:

    a.  *Running the Migration Script on page 334*

    b.  *Completing the Migration on page 335*

    c.  *Updating the Original Host on page 336*

3.  Uninstall the primary directory server and all secondary directory servers.

4.  When the primary directory is up and running, set up the supplier directories
    and the shadowing agreements according to the documentation for Sun ONE
    Directory Server.

## *Preparing the Migration Host*

The directory server software and its add-on packages listed in the following table must be installed on both the original host and the migration host.

| Directory Server | Software | Add-On Package |
|---|---|---|
| DirX | Available from Siemens | UMCdirxa |
| Sun ONE (iPlanet) | Available from Sun Microsystems | UMCiDSa |

The software and add-on packages should already be present on the original host.

See the *SRC-PE Integration Guide* for information about installing the DirX or Sun ONE software.

To install the required SRC packages on either host:

1.  From a UNIX window, log in as `root`.

2.  Load the SDX software disk 1.

3.  Start the Solaris software management tool.

    **swmtool**

    The Admintool: Software window appears.

4.  Select and add the desired package(s).

    See the Solaris **man** page for **pkgadd** for more information about this utility.

    See *Chapter 33, Installing the SRC Software on a Solaris Platform* for an example of adding a package.

5.  For Sun ONE (iPlanet) only, perform that software's setup utility.

**NOTE:** If the deployed software is earlier than Release 2.0.2, use the UMColdap or DirX-SV package from the Release 4.x SDX software CD. However, the UMColdapa and UMCdirxa add-on packages must be from SSC Release 2.0.

**NOTE:** Ensure that the directory contents do not change after you save the database on the original host. Additionally, keep the stored directory archives in case the migration fails and you need to restart the migration procedure from the beginning.

### *Cloning the Directory Server*

You must transfer the contents of the original directory to a cloned directory on the migration host. The procedure depends on the type of directory in your current deployment.

### Cloning the DirX Directory Server

To  set up the DirX directory server on the migration host:

1. On the original host, log in as user `dirx`, and access the *customize* subdirectory.

   **cd customize**

2. On the original host, archive the database.

   **dirxadm**
   **dirxadm> source bind.tcl**
   **dirxadm> save -file /tmp/dirxdb**

3. Transfer the archive by using FTP into the */tmp* directory on the migration host.

4. On the migration host, log in as user `dirx`, and access the *customize* subdirectory.

   **cd customize**

5. On the migration host, copy the abbreviation file as described below.

   For SSC 2.x versions:

   **cp dirxabbr-ext.UMC2.0 ../client/conf/**

   For SDX 3.0 and higher versions:

   **cp dirxabbr-ext.UMC ../client/conf/**

6. On the migration host, verify that the DirX server is running. See your DirX documentation for details.

7. On the migration host, restore the archive.

   dirxadm
   dirxadm> source bind.tcl
   dirxadm> restore -file /tmp/dirxdb

### Cloning Sun ONE Directory Server (iPlanet)

To set up Sun ONE Directory Server (iPlanet) on the migration host:

1. On the original host, log in as `root`.

2. On the original host, access the database directory.

   For SSC Release 3.x:

   **cd /opt/UMC/iDS/slapd-ssc**

   For SDX Release 4.0 and higher:

   **cd /opt/UMC/iDS/slapd-sdx**

3. On the original host, back up the database.

   **db2bak /tmp/iDSbak**

4. On the original host, archive the database.

   **tar cfv /tmp/iDSdb.tar /tmp/iDSbak/**

5. Transfer the archive by using FTP into the */tmp* directory on the migration host.

6. On the migration host, log in as `root`.

7. On the migration host, verify that Sun ONE Directory Server (iPlanet) is shut down.

8. On the migration host, extract the archive.

   **tar xfv /tmp/iDSdb.tar**

9. On the migration host, access the database directory.

   For SSC Release 3.x:

   **cd /opt/UMC/iDS/slapd-ssc**

   For SDX Release 4.0 and higher:

   **cd /opt/UMC/iDS/slapd-sdx**

10. On the migration host, restore the saved database.

    **bak2db /tmp/iDSbak**

11. On the migration host, start Sun ONE Directory Server (iPlanet).

    **/opt/UMC/iDS/etc/start-slapd**

### *Installing the UMCmig Migration Package*

The UMCmig package is provided in the SRC software distribution and includes a single migration procedure that handles all migration possibilities. See the Solaris **man** page for **pkgadd** or **smc** for information about using one of these utilities to add a package. By default, the migration files are installed in the */opt/UMC/migration* directory.

### *Customizing Migration*

You must modify the file */etc/migration.conf* to provide the following information. Figure 32 on page 334 shows a sample modified file.

■ Host—IP address of the migration host. In general, this is localhost because you have cloned the production system.

■ Administrator distinguished name (DN)

■ Administrator password—The current administrator's password is specified as a value of the type CurrentPwd. If the password changes between the previously deployed and current releases, the value of NewPwd must be different from the CurrentPwd value. Otherwise, the values are identical.

■ Deployed directory—The migration procedure varies depending on the directory server. Only the  DirX directory server is supported for the migration from SSC 2.x releases. If you migrate from SDX 3.0.x to SDX 3.x, iPlanet Directory Server 4.1.x is also supported.

■ Trap community and version—If you are migrating from SSC 3.0.x, you must provide values for these in the existing trap entries.

**Figure 32: Sample Edited *etc/migration.conf* File**

```
## Configuration file for migration procedure
#
# Current deployed SSC/SDX release.
# CurrentRelease: SSC_2.0.5
# CurrentRelease: SSC_3.0.1
# CurrentRelease: SDX_3.1.0
# CurrentRelease: SDX_4.0.0
# CurrentRelease: SDX_4.1.x
# CurrentRelease: SDX_4.2.x
CurrentRelease: SDX_4.3.x
Host: 127.0.0.1
Port: 389
Base: o=umc
Root: cn=umcadmin,o=umc
CurrentPwd:  admin123
NewPwd:  admin123
# Kind of deployed directory type. Possible values are DirX or
iPlanet
# Type: DirX
Type: iPlanet
# Trap upgrade from SDX 3.0.x to SDX 3.x
Community: public
Version: 1
```

## Running the Migration Script

The entire migration is valid for a single directory deployment.

If the migration is in a large-scale deployment with a shadowed directory setup, before you run the migration script follow the instructions in *Managing Shadowed Directories When Migrating Directory Data on page 328*. After you have completed those tasks, return to this section and continue with the following procedure.

The migration script logs the migration steps in the file */opt/UMC/migration/etc/migration.log*. You can check this file for migration errors.

To run the migration script on the migration host:

1.  On the migration host, log in.

    If DirX is the deployed directory, log in as user `dirx`.

2.  Access the migration directory.

    **cd /opt/UMC/migration**

3.  Start the migration script.

    **sh migrate.sh**

## *Completing the Migration*

Depending on your directory server, you may have additional steps to complete the migration.

### DirX

For DirX, the migration is completed when the migration script successfully terminates. You can now transfer the migrated database to the original host.

### Sun ONE (iPlanet)

For Sun ONE (iPlanet), the migration script displays additional steps that you must manually perform.

1.  Remove the Sun ONE add-on package.

    **pkgrm UMCiDSa**

2.  Remove the Sun ONE Directory instance from its installation directory.

    **/opt/UMC/iDS/uninstall**

3.  Install the latest Sun ONE Directory Server add-on package.

    **pkgadd /cdrom/cdrom0/SDX/solaris/UMCiDSa**

4.  Install the recommended Sun ONE Directory Server release. See the *SRC-PE Release Notes* for the latest recommended version.

    **<Sun-ONE-bin-path>/setup -s -f /opt/UMC/conf/iDS/sdx.inf**

    where < Sun-ONE-bin-path > is the location of the Sun ONE Directory Server binaries.

5.  Configure Sun ONE Directory Server for the SRC software.

---

👉 **NOTE:** Do NOT load the sample database.

---

**/opt/UMC/conf/iDS/load**

6. Access the migration directory.

**cd /opt/UMC/migration**

7. Complete the migration.

---

☞ **NOTE:** This step is required only if you are migrating from a 3.x release to a 4.x or higher release.

---

**sh finalizeMigration.sh**

When you have successfully completed these steps, you can then transfer the migrated database to the original host.

## *Updating the Original Host*

There are two ways to move the migrated data into production:

■  Turn off the original host and replace it with the migration host. This method requires that both hosts be initially set up in the same manner, including hostname and IP address.

■  Transfer the migrated data from the migration host back to the original host. This method requires the following steps:

1. Remove the directory add-on package (UMCdirxa, UMColdapa, or UMCiDSa) to establish a clean directory environment.

2. Remove the directory package.

3. Install the directory server and add-on package from the latest SRC release.

4. For DirX deployment

**cp <dirx_inst_path>/customize/dirxabbr-ext.UMC <dirx_inst_path>/client/co**nf/

where < dirx_inst_path > specifies the DirX installation directory.

5.  For a Sun ONE Directory Server deployment, install and configure the directory server.

    a.  Install the latest Sun ONE Directory Server add-on package.

        **pkgadd /cdrom/cdrom0/SDX/solaris/UMCiDSa**

    b.  Install the recommended Sun ONE Directory Server release. See the *SRC-PE Release Notes* for the latest recommended version.

        **<Sun-ONE-bin-path>/setup -s -f /opt/UMC/conf/iDS/sdx.inf**

        where < Sun-ONE-bin-path > is the location of the Sun ONE Directory Server binaries.

    c.  Configure Sun ONE Directory Server for the SRC software.

---

☞ **NOTE:** Do NOT load the sample database.

---

        **/opt/UMC/conf/iDS/load**

6.  Transfer the data from the migrated computer to the original host. Follow the procedure for your directory.

    See *Cloning the Directory Server on page 331*.

---

☞ **NOTE:** For a DirX deployment, you must skip the step where you copy the abbreviation file, *dirxabbr-ext.UMC20*.

---

# Setting Up Your SRC Environment on a Solaris Platform

After you install the SRC software and perform initial configuration tasks, you are ready to set up your SRC environment. Table 24 provides the names of SRC guides that contain detailed information about configuring or installing SRC components that have been presented in previous sections. All SRC documentation for the current release can be found at the Juniper Networks public Web site: www.juniper.net.

**Table 24: Where to Find Information About SRC Components**

| Component | Document |
|---|---|
| AAA RADIUS server | ■ *SRC-PE Integration Guide*<br>■ *SRC-PE Getting Started Guide* |
| SRC Admission Control Plug-In | ■ *SRC-PE Network Guide* |
| Admission Control Plug-In Administration application | ■ *SRC-PE Network Guide* |
| SRC Advanced Services Gateway (SRC-SG) | ■ *SRC Application Library Guide* |
| APIs | ■ *SRC NETCONF API Guide*<br>■ Online documentation in */SDK/doc* in the SRC software distribution or on the Juniper Networks Web site at<br>http://www.juniper.net/techpubs/software/management/sdx |
| C-Web interface | ■ *SRC-PE Getting Started Guide*<br>■ *SRC-PE Monitoring and Troubleshooting Guide*<br>■ *SRC -PE C-Web Interface Configuration Guide* |
| Directory | ■ *SRC-PE Integration Guide*<br>■ *SRC-PE Getting Started Guide* |
| Enterprise Service Portals | ■ *SRC-PE Subscribers and Subscriptions Guide* |
| IDP integration applications | ■ *SRC Sample Applications Guide* |
| IVE Host Checker integration application | ■ *SRC Sample Applications Guide* |
| J2EE application server | ■ *SRC-PE Getting Started Guide*<br>■ *SRC Application Library Guide* |
| Local configuration tool | ■ *SRC-PE Getting Started Guide* |

**Table 24: Where to Find Information About SRC Components   (continued)**

| Component | Document |
|---|---|
| Monitoring agent application | ■ *SRC Sample Applications Guide* |
| NIC | ■ *SRC-PE Network Guide* <br> ■ *SRC-PE Getting Started Guide* |
| Policy Editor | ■ *SRC-PE Services and Policies Guide* |
| Prepaid service application demonstration | ■ *SRC Sample Applications Guide* |
| SAE | ■ *SRC-PE Network Guide* <br> ■ *SRC-PE Getting Started Guide* |
| SDX Admin | ■ *SRC-PE Getting Started Guide* |
| SNMP agent | ■ *SRC-PE Monitoring and Troubleshooting Guide* <br> ■ *SRC-PE Getting Started Guide* |
| SRC CLI | ■ *SRC-PE CLI User Guide* <br> ■ *SRC-PE Getting Started Guide* |
| Residential portals | ■ *SRC Sample Applications Guide* |
| Traffic-Mirroring Administration Web application | ■ *SRC Application Library Guide* |
| Traffic-Mirroring application | ■ *SRC Sample Applications Guide* |
| SRC-VTAs | ■ *SRC Application Library Guide* |

**Part 8**

# Working with SRC Tools

# Chapter 41
# Using SRC Tools

The SRC software provides a suite of tools to configure and monitor SRC components and processes. Table 25 lists the major configuration and monitoring tools and provides links to where you can find detailed information about the applications.

**Table 25: SRC Configuration and Monitoring Tools**

| SRC Application | Information About Application | Platform Support |
|---|---|---|
| Local configuration tool | *Chapter 42, Configuring Local Properties* | Solaris platform only |
| Policy Editor and management | *SRC-PE Services and Policies Guide, Chapter 7, Using Policy Editor* | Solaris platform only |
| Policies, Services, and Subscribers CLI | *Chapter 5, Accessing and Starting the SRC CLI* | C-series Controller and Solaris platform |
| SDX Admin | *Chapter 43, Using SDX Admin* | Solaris platform only |
| SRC CLI | *Chapter 5, Accessing and Starting the SRC CLI*<br><br>*SRC-PE CLI User Guide* | C-series Controller and Solaris platform |
| C-Web interface | *Chapter 6, Accessing and Using the C-Web Interface*<br><br>*SRC-PE C-Web Interface Configuration Guide* | C-series Controller and Solaris platform |

## Chapter 42

# Configuring Local Properties

This chapter describes how to use the SDX local configuration tool to configure the default properties for SRC components. Topics in this chapter include:

- Overview of SDX Local Configuration Tool on page 345

- Starting the SDX Local Configuration Tool on page 345

- Using GUI Elements in the SDX Local Configuration Tool on page 346

## Overview of SDX Local Configuration Tool

The SDX local configuration tool is a GUI that enables you to configure properties for the SAE, license server, directory, SNMP agent, and other components of the SRC software.

## Starting the SDX Local Configuration Tool

To start the local configuration tool for a component:

- Issue the **config** command from the component's installation directory.

  The first time you issue the command, the local properties file for that component is created from a template. Table 26 lists some commonly used options for this command. If you want the command process to be started in the background and leave the UNIX session window open, you can append the ampersand character (&) to the command option.

**Table 26: Commonly Used Options for the config Command**

| Option | Description |
|---|---|
| -a<br>--apply | Applies the configuration changes made in the local *.*in* startup files to an SAE host. Only necessary if you have previously made changes in the HTTP tab in the directory configuration and want to apply the changes. If the configuration is shared by multiple SAE hosts, you must issue **config -a** on each host where you want the HTTP tab changes to take effect. |
| -D<br>--binddn | Specifies an alternative distinguished name (DN) for binding with the directory. The default is taken from the file *etc/default.properties*. |
| -g<br>--get | Gets the configuration from the directory as a file. |

**Table 26: Commonly Used Options for the config Command (continued)**

| Option | Description |
|--------|-------------|
| -p<br>--put | Puts the configuration into the directory from the file. |
| -H<br>--help | Displays help information. |
| -h<br>--host | Specifies an alternate directory hostname. The default is taken from the file *etc/default.properties.* |
| -l<br>--local | Starts the tool to configure SAE parameters and immediately applies the changes to the local *.in* startup files. If you want to preserve the changes to the file, we recommend that you make the changes to the *.in* files and then start the configuration tool. |
| -w<br>--password | Specifies an alternative password for binding with the directory. The default is taken from the file *etc/default.properties.* |

## Using GUI Elements in the SDX Local Configuration Tool

The local configuration tool uses standard GUI elements. Figure 33 describes buttons commonly used in the local configuration tool.

**Figure 33: GUI Buttons in the Local Configuration Tool**
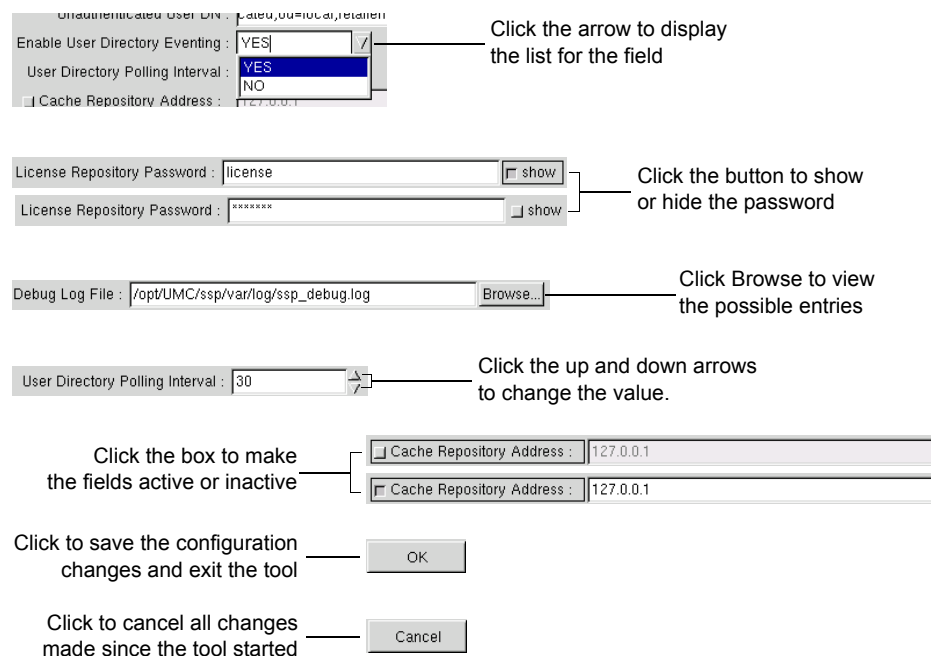
The local configuration tool provides context-sensitive help (tool tips) for fields. Hover the cursor over a field to display the help information for that field. Move the cursor to dismiss the help pop-up.
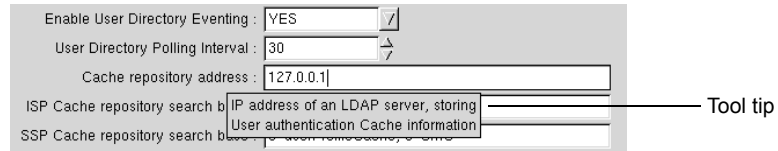


To configure a particular feature, click the tab for that feature at the top of the window. For example, to configure the LDAP parameters, click the LDAP tab.
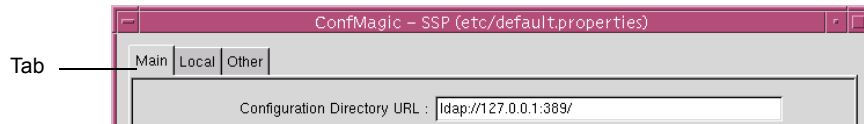
## Chapter 43
# Using SDX Admin

This chapter describes SDX Admin. Topics include:

■ Overview of SDX Admin on page 349

■ Starting SDX Admin on page 350

■ SDX Admin Main Window on page 351

■ General Procedures for Using SDX Admin on page 359

■ SDX Admin Limitations on page 362

■ Internationalization with SDX Admin on page 363

## Overview of SDX Admin

You use SDX Admin to manage the SRC software. You can use SDX Admin to create and modify services, network definitions, and advanced SAE configurations; to configure the system management subagent; and to manage operator accounts. For small installations or demonstrations, you can also use SDX Admin to create and modify subscriber profiles and subscriptions to services. Use this interface to populate the directory with subscriber profiles and services.

## Starting SDX Admin

To display the SDX Admin dialog box:

1. In a UNIX window, issue the command to start SDX Admin.

   **/opt/UMC/smg/bin/sdxadmin**

   The LDAP Connection dialog box appears.
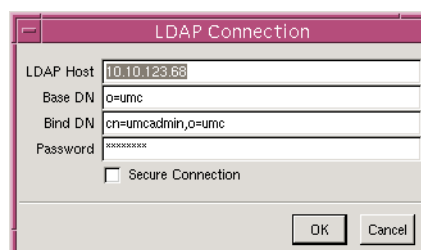


2. Edit or accept the default values for the fields in the LDAP Connection dialog box.

3. Click **OK**.

### *LDAP Connection Fields*

In SDX Admin, you can modify the following fields in the LDAP Connection dialog box.

#### *LDAP Host*

- IP address or hostname of the directory server.
- Value— < IP address or hostname >
- Guidelines—You can connect to only one directory at a time.

#### *Base DN*

- Distinguished name (DN) of the base policy information in the directory server.
- Value—DN
- Default value—$o = umc$

#### *Bind DN*

- DN used for binding to the directory server.
- Value—DN
- Default—$cn = umcadmin, o = umc$

### Password

- Password associated with the bind DN.
- Value— < password >
- Default—admin123

### Secure Connection

- Whether or not the connection is a secure LDAP connection.
- Value
    - Checked—Connection is a secure LDAP connection
    - Unchecked—Connection is a not secure LDAP connection

## SDX Admin Main Window

After you configure the LDAP connection, the main window for SDX Admin appears. The SDX Admin window comprises six main areas, which are illustrated in Figure 34 and described in Table 27.

**Figure 34:  SDX Admin Window Layout**
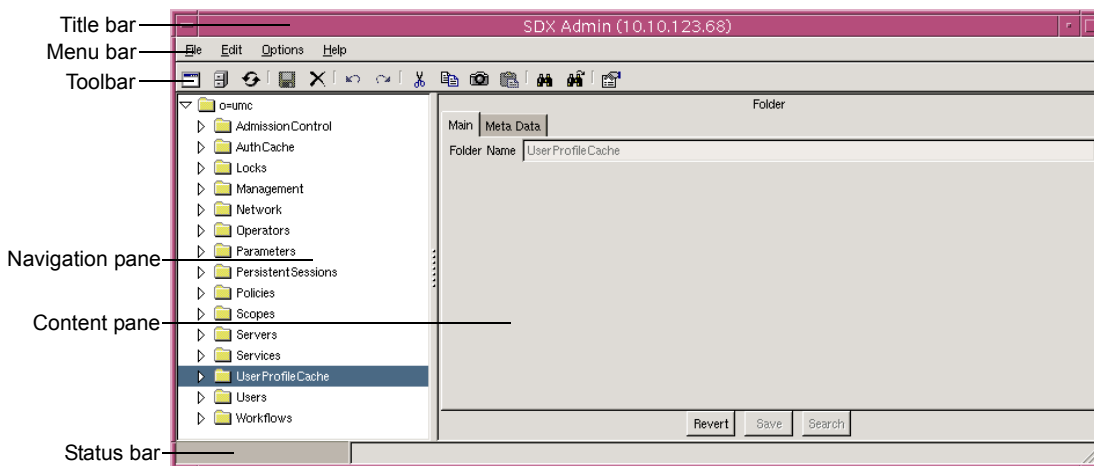


**Table 27:  SDX Admin Window Areas**

| Area | Description |
|---|---|
| Title bar | Displays the name of the current window. Also provides the minimize, maximize, and close window buttons. |
| Menu bar | Displays a menu from which you can select commands from lists. |
| Toolbar | Displays the icons that have the same functionality as the corresponding entries in the main menu. |
| Navigation pane | Displays the objects in a hierarchical format, starting from the top-level folder and moving through the subfolders down to individual objects. Use this pane to navigate through the folders and select objects. |
| Content pane | Displays the details of the object selected in the navigation pane. Use this pane to display and modify information about objects. |

**Table 27: SDX Admin Window Areas   (continued)**

| Area | Description |
|---|---|
| Status bar | Contains a progress indicator on the left side and a message area on the right side. The progress indicator is active for operations that take longer than 1 second (such as loading a large subtree); the message area names the operation that is in progress. |

## *Using the Menu Bar*

The menu bar allows you to execute commands related to each of the menus. See the following tables for information about each menu command.

| Menu | Command | Choose to |
|---|---|---|
| File | New Window | Create a new SDX Admin window and connect it to a directory. |
| | Change Server | Close the current connection to a directory and open new directory connection. |
| | Reload | Get the current tree from the directory again. |
| | Save Entry | Save attributes of the current directory entry. |
| | Close Window | Close the current window. |
| | Exit | Close all windows and terminate SDX Admin. |

| Menu | Command | Choose to |
|---|---|---|
| Edit | Undo: [operation] | Show the most recent operation and cancel it. The text after Undo indicates the most recent operation. If no operation can be canceled, the menu says Can't Undo and is disabled. |
| | Redo | Reinstate the most recent operation that you canceled. |
| | Cut | Cut the currently selected object. |
| | Copy | Copy the currently selected object. |
| | Copy Tree | Copy the currently selected object, including its child entries. |
| | Paste | Paste the object copies from the cut or copy operation as a new child entry below the currently selected object. |
| | Delete | Delete the currently selected object. |
| | Find | Open a dialog box asking for search criteria and search objects in the directory based on the entered criteria. The first found object is selected; the remaining search results are stored. |
| | Find Next | Select the next object that the most recent Find operation has found. If no more objects are available, an error message appears. If no Find operation is in progress, the system starts a new Find operation as if you had selected Find. |

| Menu | Command | Choose to |
|---|---|---|
| Options | Configure | Open the Main Configuration dialog box to configure operational characteristics of the SDX Admin window. |
| | OSM Client Log | Open the OSM Client Reports dialog box to view responses received from the object state manager (OSM) regarding the state of managed objects. |

| Menu | Command | Choose to |
|---|---|---|
| Help | About | View information about the SDX Admin software, including vendor name and software version. |

## Options Menu: Configure

When you click **Configure** in the Options menu, the Main Configuration dialog box opens. Changing the parameters changes the appearance or behavior of SDX Admin or changes the default values it uses. See Table 28.

**Table 28:  Main Configuration Parameters**

| Parameter | Description |
|---|---|
| Encrypt userPassword | From the menu, you can select the default encryption algorithm for the LDAP attribute userPassword. |
| | ■ empty line—no encryption |
| | ■ crypt—password encrypted through UNIX crypt command and stored in */etc/security/passwd* |
| | ■ sha—Secure Hash Algorithm |
| | ■ md5—Message Digest #5 |
| | **NOTE:** You must select an encryption method that your directory server supports. |
| Show Objecttype | Selecting **Yes** shows the < attr > = prefix in the navigation pane. |
| Delete Subtree | Selecting **Yes** means that this operation is available; that is, you can recursively delete all child objects of an object that you select. |
| Subscriber Folder is Subscriber | Selecting **Yes** means that you can subscribe to services from the Subscriber folder. |
| | **NOTE:** Setting this option to Yes can affect performance for some directory servers, such as Sun One (iPlanet) version 5.2. |
| Show Toolbar | Selecting **Yes** means that the toolbar appears in the SDX Admin window. |
| Show Statusbar | Selecting **Yes** means that the status bar appears in the SDX Admin window. |
| LDAP timelimit | Number of seconds allowed for LDAP operations. |
| UNDO levels | Number of commands stored for successive undo operations. |
| OSM Host | Address of server running the object state manager. |
| OSM Port | TCP port number running the object state manager. |
| OSM Transaction ID Prefix | Prefix used when you create transaction objects. |
| OSM Report Server Port | Local port number listening to OSM status reports. |

**Table 28: Main Configuration Parameters  (continued)**

| Parameter | Description |
|---|---|
| Default Trap Receiver | Default value for trap receiver. |
| DirX Server Address | Address of the DirX server. Needed only if the address is different from the LDAP server. |
| SAE Admin Web Application Server | Address and port used for validation of substitutions. Default port is 8443. |
| Tool Path | An alternate path to use for invoking external tools, such as Telnet and SSH, which you can use to manage a router object from an SDX Admin session. Set the Tool Path if these external applications are installed in a path other than the standard path. For example, if the Telnet executable file is installed in the */usr/local/bin* directory, you can list this path for a Tool Path. |
| Enable All Warnings | Displays warning messages again for those messages that do not appear because the `Don't show me this warning again` check box was previously selected for that message. |

## *Using the Toolbar*

Table 29 shows the SDX Admin toolbar icons and the relationship between the icons and the menu commands. The toolbar icons exist in enabled and disabled modes. The mode depends on whether the operation is supported in the context of the selected object and on previous operations. For example, if no object was previously copied or cut, then Paste is disabled.

**Table 29: Toolbar Functions**

| Icon | Corresponding Menu |
|---|---|
| | File > New Window |
| | File > Change Server |
| | File > Reload |
| | File > Save Entry |
| | Edit > Delete |
| | Edit > Undo |
| | Edit > Redo |
| | Edit > Cut |
| | Edit > Copy |

**Table 29: Toolbar Functions (continued)**

| Icon | Corresponding Menu |
|------|-------------------|
| | Edit > Copy Tree |
| | Edit > Paste |
| | Edit > Find |
| | Edit > Find Next |
| | Options > Configure |

## *Using the Navigation Pane*

The directory in the navigation pane consists of nested folders, all contained in the top-level folder. Although you can rename this folder, we use the default name, o = umc, throughout the SRC guides.

The initial installation of the directory creates a set of second-level folders. If it fails to create them (because, for example, of operator error or problems arising from integration with other directories), you must create these folders before you use the application. Different components of the SRC software will not start properly if the basic objects are missing.

To create the required second-level folders, highlight the top-level folder, right-click, and then select **New > Folder** in the pop-up menu that appears. You are prompted for the name of the subfolder that you want to create. Enter the appropriate name. You must create all of the following subfolders, using the names below:

- AdmissionControl

- AggregateServices

- AuthCache

- CongestionPoints

- Locks

- Management

- Network

- Operators

- Parameters

- Persistent Sessions

- Policies

- Scopes

- Servers

- Services

- UserProfileCache

- Users

After you create the second-level folders, the SDX Admin window should appear similar to .

Initially, only the top-level and second-level folders are displayed. To open additional levels of the directory, click on the triangle to the left of the folders.

### Navigation Pane Icons

SDX Admin uses different icons in the navigation pane to differentiate the various objects. Table 30 shows the icons displayed in the navigation pane and lists their related object types. Manipulation of the different objects is explained throughout this guide.

**Table 30:  SDX Admin Navigation Pane Icons**

| Icon | Type |
|------|------|
| | Folder |
| | Traps |
| | Cached Authentication Profile |
| | Configuration |
| | License |
| | Router |
| | Operator Group |
| | Operator |
| | Global Parameter |
| | Policy Group |
| | Policy rule |
| | Service Scope |
| | Access Service/Access Subscription |

**Table 30:  SDX Admin Navigation Pane Icons  (continued)**

| Icon | Type |
|------|------|
| | RADIUS Service/Subscription |
| | Outsource Service/Subscription |
| | SAE (SSP) Service |
| | Retailer |
| | Enterprise Subscriber |
| | Enterprise Site Subscriber |
| | Residential Subscriber |
| | Mutex Group |
| | State Machine |
| | Service Scheduler |

### Using the Content Pane

When you select a folder or an individual object in the navigation pane, the system displays a form in the content pane that shows the attributes of the object (see Figure 35).

**Figure 35: SDX Admin General Window Structure**
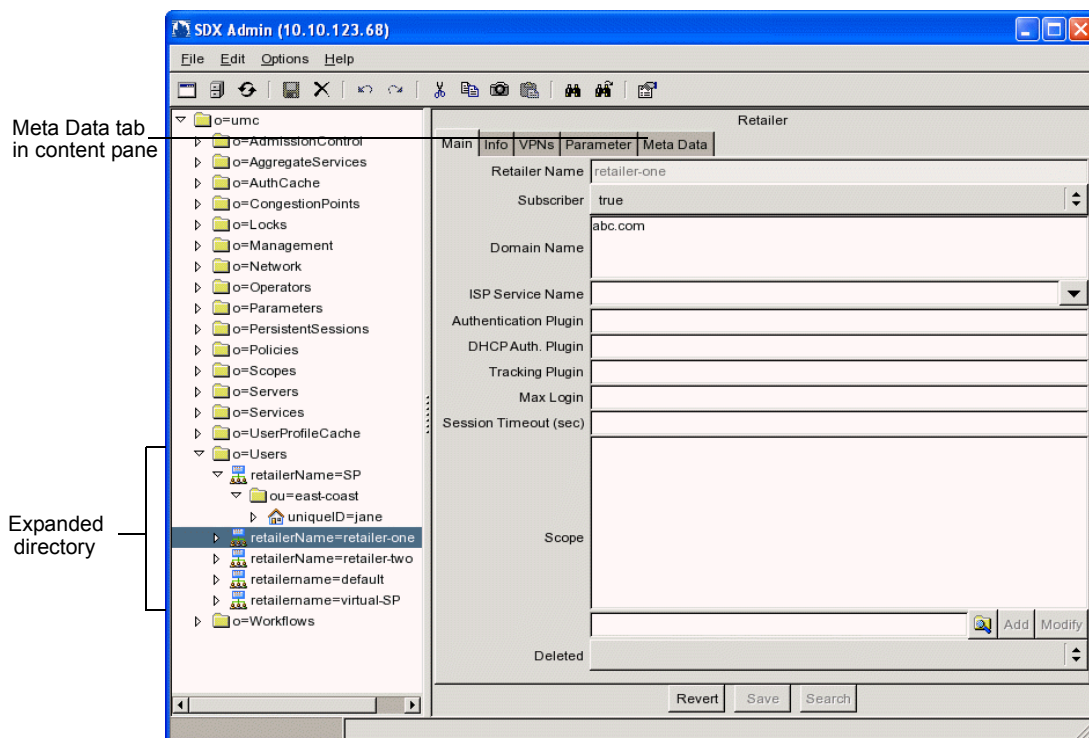


Each object in the navigation pane has an associated Meta Data tab in the content pane (shown in Figure 35). Table 31 describes the Meta Data tab parameters.

**Table 31: Meta Data Tab Parameters**

| Parameter | Description |
|---|---|
| Creation Timestamp | Time when the object was created |
| Creator | Bind DN of the user who created the object |
| Modification Timestamp | Time when the object was last modified |
| Modifier | Bind DN of the user who last modified the object |

## General Procedures for Using SDX Admin

This section describes the general procedures for using SDX Admin.

In the navigation pane:

- To select an object—Move the cursor over the object, and click.

- To expand an object—Click on the triangle to the left of the object. When the object is expanded, the triangle points down.

- To collapse an object—Click on the triangle to the left of the object. When the object is collapsed, the triangle points to the right (toward the object).

In the content pane:

- To revert to (and display) the last saved information for the selected object—Click **Revert**.

- To save the currently displayed information for the selected object—Click **Save**.

### Using Pop-Up Menus

If you select a folder or an individual object in the navigation pane and then right-click, a pop-up menu appears. Available commands relative to the selected object appear. If the command appears dimmed, it is not available. Table 32 lists the menu selections that are available from one or more of the various pop-up menus.
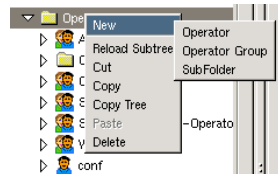


**Table 32: SDX Admin Main Pop-Up Menus**

| Menu Item | Choose to |
|---|---|
| New | Create a new object of the type specified. |
| Edit | Open Policy Editor to edit the selected object. |
| | Available only for some policy objects. See *SRC-PE Services and Policies Guide, Chapter 7, Using Policy Editor* for more information. |
| Congestion Points | Create congestion points and congestion point profiles. |
| Convert Subscriptions | Convert subscriptions from the syntax used in SDX versions earlier that 5.0 to the syntax in SDX 5.0 or greater. or SRC 1.0.0 or greater |
| Discover Network | Search the router and virtual router in a subnet. |
| | Available only for Network object. |
| Reload Subtree | Refresh the navigation pane and reload the subtree from the directory. |
| Cut | Move the selected object (including subtree) to the clipboard. |
| Copy | Create a copy of the selected object (excluding subtree) in the clipboard. |
| Copy Tree | Create a copy of the selected object (including subtree) in the clipboard. |

**Table 32: SDX Admin Main Pop-Up Menus   (continued)**

| Menu Item | Choose to |
|-----------|-----------|
| Paste | Insert the content of the clipboard below the selected object. |
| Delete | Delete the selected object. |

## *Modifying an Entry*

SDX Admin allows you to undo or redo up to 10 operations. You can undo the following operations:

■   New—Creation of a new directory entry, including creation of subentries and modifications of access controls.

■   Paste—Creation of new directory entries by copying existing folders and objects.

■   Delete—Deletion of a directory entry, including modification of dependent entries.

■   Delete subtree—Recursive deletion of a directory entry, including modification of dependent entries.

■   Cut—Recursive deletion of a directory entry, including modification of dependent entries. Undo reverts the directory only to the previous directory state. After you cut an entry, the clipboard contains a copy of what you selected from the directory; any previous content of the clipboard is removed. Undo restores the directory entry (similar to pasting the entry back at the original position) but does not restore the clipboard.

■   Modify—Modification of a single directory entry, including modification of dependent entries. *Modify* means that the content of the object has been changed and saved to the directory. Undo will revert to the previous state of the object.

■   Edit—Modification of a single entry without saving to the directory. Undoing an Edit entry reverts the entry back to the last saved entry from the directory. The difference from Revert is that the edit operation can be redone. When you save the changes to the directory, Edit object becomes a Modify object operation.

The parameters of a highlighted object are displayed in the content pane.

To modify the parameters:

Type in the new value

or

Select a new value from the menu for the parameter.

☞ **NOTE:** Most parameters defined in SDX Admin objects are inherited from higher levels. That is, if you modify a parameter in a parent object, the child object inherits the value. However, SDX Admin does not immediately display the values inherited from the upper level. The inheritance is handled by the SAE at runtime.

### Saving an Entry

Save changes by selecting **Save** in the File menu or by clicking **Save** at the bottom of the form in the content pane. If you do not save changes that you make on the form, the application prompts you to save the changes.

### Reverting an Entry

If you click the **Revert** button, all attributes are loaded from the directory again and displayed.

### Deleting an Entry

Some objects in SDX Admin have a Deleted field that you can set to true or false. If you set this field to true, then the object is deleted from the perspective of any SRC component that uses the directory eventing system. Such components include the enterprise server, the SAE, and the SNMP agent. The object is still present in SDX Admin and in the directory. You can "undelete" such an object by setting the field to false.

To delete an entry, first highlight the object that you want to delete. Then you can delete the object by performing one of the following actions:

■ Right-click and select **Delete**.

■ From the Edit menu, select **Delete**.

The system displays the Delete menu. Click **Yes** to delete the entry.

☞ **NOTE:** Objects that have child entries below them *cannot* be deleted. You must first delete the child entries.

### Searching Text

SDX Admin provides you with a text-searching function.

To search for information:

1. Select a multiline text field in a content pane (for example, the Description field in the Enterprise content pane), and then click **Search** at the bottom of the pane.

   The SDX Admin dialog box appears.
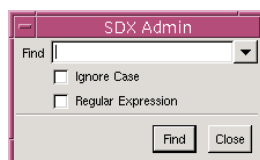


2. Enter the search information in the Find text box.

3. To limit the search, select one of the search criteria (Ignore Case, or Regular Expression); otherwise, click **Find**.

   The system displays the results of the search.

## SDX Admin Limitations

SDX Admin does not automatically check for duplicate inputs, nor does it check for consistency. It allows such entries and does not alert you to these kinds of entries as you make them. Subsequently, SAE functionality can be affected. However, the directory checks some parameters; if the parameters are invalid, they are refused.

### Unique User IDs Only

The user ID that you create *must* be unique. Ensure that you do not create two users with the same name. If you enter a user ID that is in use, the system allows the input, but subsequent customer authentication fails.

### Consistency

Ensure that you consistently enter all values that are required to define a service. If you do not consistently specify a mandatory value, SDX Admin does not warn you of this inconsistency. However, the SAE logs a runtime error, and the service will not work.

### Interdependence

If you modify an attribute related to an object, the dependent objects do not change automatically. For example, the access service object allows you to specify the default value for the primary Domain Name System (DNS) host. If you change this value, current subscriptions to this service are not changed automatically. Where required, you must change the default value manually.

## Internationalization with SDX Admin

SDX Admin allows you to set the language for the SRC interfaces so that information can be displayed in the language of choice. The language environment is set globally on the host that the SDX Admin software is running on. Set the language either at login time or as a system-wide default. For example, the system default for Solaris systems is stored in the file */etc/default/init*. The Solaris login prompt includes a list for choosing the language for the next login session.
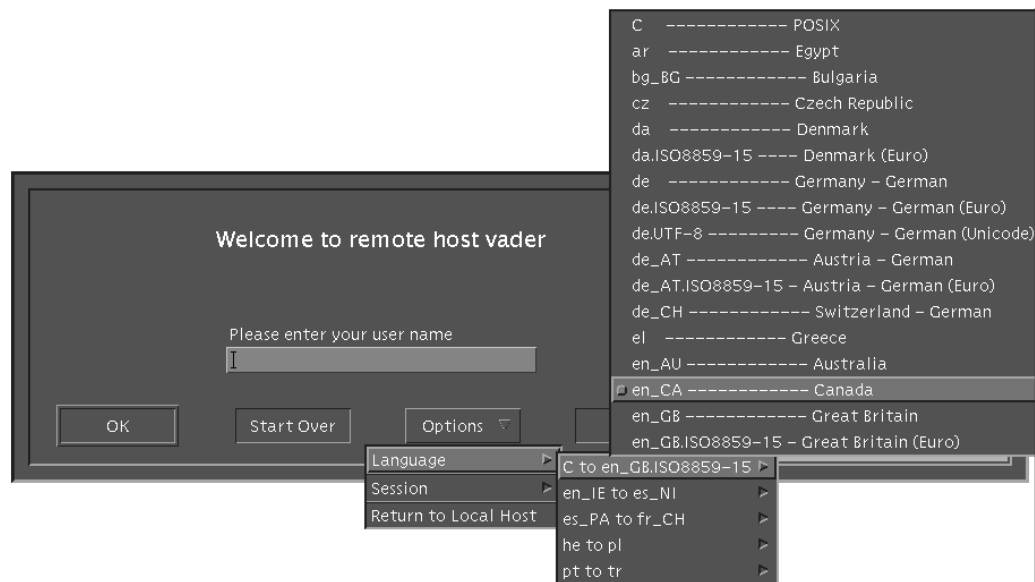


### Locale

To force a particular language, SDX Admin may be started from a shell with the LANG environment variable set to the desired language.

The SDX Admin function has support for translating all user-visible messages and dialogs into local languages. Please contact Juniper Networks support if a particular language is not yet supported.

### Localization of Data Storage

Data entered through SDX Admin is converted to Unicode Transformation Format-8 (UTF-8) encoding and stored in the backend directory. Data retrieved from the backend directory is converted from UTF-8 to the currently selected system encoding (for example, latin-1 for most Western computing environments). If the data contains characters that cannot be displayed in the current language, the character is replaced by a replacement character (for example, ? for ASCII encoding) that is specified by the current language.

**Part 9**
# Reference Material

# Chapter 44
# SRC-Related Abbreviations

The following table includes the abbreviations used throughout the SRC documentation.

| Abbreviation | Description |
| --- | --- |
| 3GPP | 3rd Generation Partnership Project |
| AAA | authentication, authorization, and accounting |
| AATV | authentication/authorization transfer vector |
| ACI | access control information |
| ADSL | asymmetric digital subscriber line |
| AES | Advanced Encryption Standard |
| AH | authentication header |
| API | application programming interface |
| A-RACF | access-resource and admission control function |
| ASCII | American Standard Code for Information Interchange |
| ASP | ■ application service provider<br>■ Adaptive Services PIC |
| ATM | Asynchronous Transfer Mode |
| AVP | attribute value pair |
| BCID | billing correlation identifier |
| BEEP | Blocks Extensible Exchange Protocol |
| BGF | border gateway function |
| BNF | Backus-Naur Format |
| BoD | bandwidth on demand |
| BOOTP | A bootstrap protocol |
| B-RAS | Broadband Remote Access Server |
| CA | certificate authority |
| CHAP | Challenge Handshake Authentication Protocol |
| CIDR | classless interdomain routing |
| CIM | Common Information Model |
| CLEC | competitive local exchange carrier |
| CLI | command-line interface |

| Abbreviation | Description |
| --- | --- |
| CMTS | cable modem termination system |
| COPS | Common Open Policy Service |
| COPS-PR | COPS usage for policy provisioning |
| CORBA | Common Object Request Broker Architecture |
| COS | Common Object Services |
| CoS | class of service |
| CSR | certificate signing request |
| DA | destination address |
| DCE | Distributed Computing Equipment |
| DCU | destination class usage |
| DES | directory eventing system |
| DHCP | Dynamic Host Configuration Protocol |
| DISP | Directory Information Shadowing Protocol |
| DIT | directory information tree |
| DMTF | Distributed Management Task Force |
| DN | distinguished name |
| DNS | Domain Name System |
| DOCSIS | Data over Cable Service Interface Specifications |
| DSCP | Differentiated Services (DiffServ) code point |
| DSL | digital subscriber line |
| DSLAM | digital subscriber line access multiplexer |
| DSML | Directory Services Markup Language |
| DSP | Directory Service Protocol |
| DTD | document type definition |
| EAR | enterprise archive (file format) |
| EGP | exterior gateway protocol |
| EJB | Enterprise JavaBean |
| ESP | Encapsulating Security Payload |
| ETSI | European Telecommunications Standards Institute |
| FEID | financial entity identifier |
| FMC | fixed mobile convergence |
| FSM | finite state machine |
| FTP | File Transfer Protocol |
| GAL | Gateway Application Logic |
| GIF | graphic interchange format |
| GMT | Greenwich Mean Time |
| GRE | generic routing encapsulation |
| GUI | graphical user interface |
| HFC | hybrid fiber coaxial |

| Abbreviation | Description |
|---|---|
| HTML | HyperText Markup Language |
| HTTP | HyperText Transfer Protocol |
| HTTPS | Secure HyperText Transfer Protocol |
| ICMP | Internet Control Message Protocol |
| ID | identification (identifying; identifier) |
| IDE | integrated development environment |
| IDL | interface definition language |
| IDP | Intrusion Detection and Prevention |
| IETF | Internet Engineering Task Force |
| IGMP | Internet Group Management Protocol |
| IIOP | Internet Inter-ORB Protocol |
| ILEC | incumbent local exchange carrier |
| IMAP | Internet Message Access Protocol |
| IMS | IP multimedia subsystem |
| IOR | interoperable object reference |
| IP | Internet Protocol |
| IPCP | Internet Protocol Control Protocol |
| IPSCS | IP Service Control System (product name from Ellacoya Networks) |
| ISDN | Integrated Services Digital Network |
| ISO | International Organization for Standardization |
| ISP | Internet service provider |
| IT | information technology |
| J2EE | Java 2 Platform, Enterprise Edition |
| J2SE | Java 2 Platform, Standard Edition |
| JAR | Java archive (file format) |
| JKS | Java Keystores |
| JMS | Java Message Service |
| JMX | Java Management Extension |
| JNDI | Java Naming and Directory Interface |
| JRE | Java Runtime Environment |
| JSP | JavaServer Pages |
| JVM | Java Virtual Machine |
| KB | kilobyte(s) |
| L2TP | Layer 2 Tunneling Protocol |
| LAN | local area network |
| LAS | local authorization service |
| LDAP | Lightweight Directory Access Protocol |
| LDAPS | LDAP over SSL |
| LDIF | LDAP Data Interchange Format |

| Abbreviation | Description |
|---|---|
| LNS | L2TP network server |
| LSA | link-state advertisement |
| MAC | Media Access Control |
| Mb | megabit(s) |
| MB | megabyte(s) |
| MBeans | manageable JavaBeans |
| MD5 | Message Digest 5 |
| MI | management information |
| MIB | Management Information Base |
| MPLS | Multiprotocol Label Switching |
| MSO | multiple service operator |
| MTU | maximum transmission unit |
| mutex | mutually exclusive |
| NAT | Network Address Translation |
| NBNS | NetBIOS Name Server |
| NGN | next-generation network |
| NIC | network information collector |
| NRTPS | non-real-time polling service |
| OID | object identification |
| ORB | object request broker |
| OS | operating system |
| OSM | object state manager |
| OSMW | object state manager for the Web |
| OSPF | Open shortest Path First |
| OSS | operations support system |
| PCIM | Policy Core Information Model |
| PCMM | PacketCable Multimedia Specification |
| PDF | portable document file |
| PDP | policy decision point |
| PEP | policy enforcement point |
| PFS | Perfect Forward Secrecy |
| PIB | Policy Information Base |
| PIM | Protocol Independent Multicast |
| PKCS | Public Key Cryptology Standard |
| PLP | packet loss priority |
| POP | point of presence |
| PPP | Point-to-Point Protocol |
| PPPoE | Point-to-Point Protocol over Ethernet |
| PTA | PPP Terminated Aggregation |

| Abbreviation | Description |
| --- | --- |
| QoS | quality of service |
| QTP | QoS-tracking plug-in |
| RACS | resource and admission control subsystem |
| RADIUS | Remote Authentication Dial-In User Service |
| RAS | Remote Access Server |
| RCEF | resource control enforcement function |
| RDBMS | relational database management system |
| RDN | relative distinguished name |
| RED | random early detection |
| RF | radio frequency |
| RKS | record-keeping server |
| RPC | remote procedure call |
| RSpec | service request specification |
| RSVP | Resource Reservation Protocol |
| RTPS | real-time polling service |
| RTSP | Real Time Streaming Protocol |
| SA | source address |
| SAC | service activation context |
| SAE | service activation engine |
| SCEP | Simple Certificate Enrollment Protocol |
| SCU | source class usage |
| SDK | Software Development Kit |
| SDX | Service Deployment System (used only to refer to releases earlier than the new SRC 1.0) |
| SHA | Secure Hash Algorithm |
| SID | Oracle System Identifier |
| SIP | Session Initiation Protocol |
| SLE | service logic engine |
| SNMP | Simple Network Management Protocol |
| SOAP | Simple Object Access Protocol |
| SPDF | service policy decision function |
| SPI | ■ security parameter index<br>■ service provider interface |
| SRC | Session and Resource Control (formerly SDX—Service Deployment System) |
| SRC-ACP | SRC Admission Control Plug-In |
| SRC CLI | SRC command-line interface |
| SRC-PE | SRC Policy Engine |
| SRC-SG | SRC SOAP Gateway |
| SRC-TMP | SRC Threat Mitigation Portal |

| Abbreviation | Description |
| --- | --- |
| SRC-VTA | SRC Volume Tracking Application |
| SSL | Secure Sockets Layer |
| SSM | service and subscriber management |
| SSP | Service Selection Portal |
| TCP | Transmission Control Protocol |
| TFTP | Trivial File Transfer Protocol |
| TISPAN | Telecommunications and Internet Converged Services and Protocols for Advanced Networks |
| TLS | Transport Layer Security |
| ToS | type of service |
| TSpec | traffic specification |
| TTL | ■ time to live<br>■ time-to-live |
| UDP | User Datagram Protocol |
| UGS | unsolicited grant service |
| UGS-AD | unsolicited grant service with activity detection |
| UML | Unified Modeling Language |
| URI | Uniform Resource Indicator |
| URL | Uniform Resource Locator |
| UTF-8 | Unicode Transformation Format-8 |
| UUID | universal unique identifier |
| VACM | view-based access control model |
| VLAN | virtual local area network |
| VoIP | voice over Internet Protocol |
| VPN | virtual private network |
| VR | virtual router |
| VSA | vendor-specific attribute (RADIUS) |
| WAR | Web archive (file format) |
| WDSL | Web Services Description Language |
| Wi-Fi | wireless fidelity |
| WINS | Windows Internet Name Service (Microsoft) |
| XDR | External Data Representation Standard |
| XML | Extensible Markup Language |
| XSLT | Extensible Stylesheet Language Transformation |

## Chapter 45

# SRC-Related References

This chapter lists RFCs, draft RFCs, other software standards, hardware standards, and other references that provide information about the protocols and features supported by the SDX software. Topics include:

- RFCs on page 373

- Draft RFCs on page 374

- Other Software Standards on page 374

- URLs on page 375

## RFCs

**Table 33:  RFCs**

| Reference | Protocol or Feature |
|---|---|
| RFC 3494—Lightweight Directory Access Protocol version 2 (LDAPv2) to Historic Status (March 2003) | LDAP |
| RFC 3084—COPS Usage for Policy Provisioning (COPS-PR) | COPS-PR |
| RFC 2882—Network Access Servers Requirements: Extended RADIUS Practices (July 2000) | RADIUS |
| RFC 1305—Network Time Protocol (Version 3) Specification Implementation and Analysis (March 1992) | NTP |
| RFC 2869—RADIUS Extensions (June 2000) | RADIUS |
| RFC 2866—RADIUS Accounting (June 2000) | RADIUS |
| RFC 2865—Remote Authentication Dial In User Service (RADIUS) (June 2000) | RADIUS |
| RFC 2748—The COPS (Common Open Policy Service) Protocol | COPS |
| RFC 2388—Returning Values from Forms: multipart/form-data | multipart/form data |
| RFC 2255—The LDAP URL Format (December 1997) | LDAP |
| RFC 2254—The String Representation of LDAP Search Filters (December 1997) | LDAP |
| RFC 2253—Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names (December 1997) | LDAP |
| RFC 2252—Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions (December 1997) | LDAP |
| RFC 2251—Lightweight Directory Access Protocol (v3) (December 1997) | LDAP |
| RFC 2236—Internet Group Management Protocol, Version 2 (November 1997) | IGMP |
| RFC 2132—DHCP Options and BOOTP Vendor Extensions (March 1997) | DHCP |

**Table 33: RFCs (continued)**

| Reference | Protocol or Feature |
|---|---|
| RFC 2131—Dynamic Host Configuration Protocol (March 1997) | DHCP |
| RFC 1558—White Pages Meeting Report (February 1994) | white pages directory |
| RFC 1213—Management Information Base for Network Management of TCP/IP-based internets: MIB-II (March 1991) | SNMP |
| RFC 793—Transmission Control Protocol (September 1981) | TCP |
| RFC 791—Internet Protocol (September 1981) | IP |

## Draft RFCs

☞ **NOTE:** IETF drafts are valid for only 6 months from the date of issuance. They must be considered as works in progress. Please refer to the IETF Web site at http://www.ietf.org for the latest drafts.

**Table 34: Draft RFCs**

| Reference | Protocol or Feature |
|---|---|
| LDAP Extensions for Scrolling View Browsing of Search Results—draft-ietf-ldapext-ldapv3-vlv-09.txt (June 2003 expiration) | LDAP |
| The syslog Protocol—draft-ietf-syslog-protocol-16.txt (July 2006 expiration) | System logging |

## Other Software Standards

**Table 35: Non-RFC Software Standards**

| Reference | Protocol or Feature |
|---|---|
| CCITT ITU-T Recommendation X.500—Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services (February 2001) | LDAP |
| CCITT ITU-T Recommendation X.501—Information technology - Open Systems Interconnection - The Directory: Models (February 2001) | LDAP |
| PacketCable Multimedia Architecture Framework Technical Report (PKT-TR-MM-ARCH) | PCMM |
| PacketCable Multimedia Specification PKT-SP-MM-I02-040930 | PCMM |
| PacketCable Multimedia Specification PKT-SP-MM-I03-051221 | PCMM |
| PacketCable Security Specifications (PKT-SP-SEC) | PCMM |

## URLs

**Table 36: Juniper Networks URLs**

| Reference | Description |
| --- | --- |
| http://www.juniper.net | Juniper Networks |
| http://www.juniper.net/partners/content_partners.html | J-Partner Content and Applications Alliance Partners List |
| http://www.juniper.net/support | Customer Support Organization |
| http://www.juniper.net/techpubs | SDX documentation |
| http://www.juniper.net/techpubs/docbug/docbugreport.html | Technical Documentation Feedback Form |
| http://www.juniper.net/techpubs/software/junos/junos71/index.html | JUNOS software documentation |
| http://www.juniper.net/techpubs/software/junos/junos84/swconfig84-system-basics/swconfig84-system-basics.pdf | *JUNOS System Basics Configuration Guide, Release 8.4.x* |
| http://www.juniper.net/techpubs/software/erx/junose82/bookpdfs/swconfig-broadband.pdf | *JUNOSe Broadband Access Configuration Guide, Release 8.2.x* |
| http://www.juniper.net/techpubs/software/management/idp/ | Technical documentation for Juniper Networks Intrusion Detection and Prevention (IDP) software |
| http://www.juniper.net/techpubs/software/management/sdx | Technical documentation for the SDX software |
| http://www.juniper.net/techpubs/software/management/sdx/api-index.html | Technical documentation for the SDX application programming Interfaces |
| http://www.juniper.net/techpubs/software/management/security-manager/ | Technical documentation for Juniper Networks NetScreen-Security Manager software |

**Table 37: Third-Party URLs**

| Reference | Protocol or Feature |
| --- | --- |
| ftp://ftp.gtk.org/pub/gtk/python | GTK library for use with Python programs |
| http://cheops.anu.edu.au/~avalon/ip-filter.html | IP Filter |
| http://cui.unige.ch/db-research/Enseignement/analyseinfo/AboutBNF.html | BNF notation |
| http://developer.java.sun.com/developer | JRE |
| http://jakarta.apache.org/tomcat | Servlet container |
| http://jakarta.apache.org/regexp/apidocs/org/apache/regexp/RE.html | Java regular expression documentation |
| http://java.sun.com/j2se/1.4.2/docs/api/java/text/MessageFormat.html | Java message formats |
| http://java.sun.com/j2se/1.4.2/docs/api/java/text/SimpleDateFormat.html | Java date and time format |
| http://java.sun.com/j2se/1.4.1/docs/api/java/util/logging/FileHandler.html | Java logger |
| http://java.sun.com/j2se/1.4.2/docs/api/java/util/regex/Pattern.html | Java regular expression documentation |
| http://java.sun.com/j2se/1.4/docs/guide/intl/encoding.doc.html | Character encoding that a compiler uses when loading Java source files |
| http://java.sun.com/j2se/1.4/docs/guide/jar/ | Web applications |
| http://java.sun.com/j2ee/1.4/docs/tutorial/doc/index.html | Web application |
| http://java.sun.com/j2se/1.4.2/docs/tooldocs/solaris/java.html | Java documentation |
| http://java.sun.com/j2se/1.4.1/docs/tooldocs/solaris/keytool.html | Java keytool documentation |

**Table 37:  Third-Party URLs  (continued)**

| Reference | Protocol or Feature |
|---|---|
| http://java.sun.com/products/jndi/ | Java Naming and Directory Interface (JNDI) |
| http://jsautret.free.fr/luci/index.html | LUCI |
| http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndotnet/html/framewkwinsupp.asp | .NET Framework |
| http://net-snmp.sourceforge.net/ | Net-SNMP agent |
| http://pauillac.inria.fr/~diaz/gnu-prolog/ | GNUPROLOG |
| http://pysnmp.sourceforge.net | pysnmp |
| http://python-ldap.sourceforge.net | LDAP client API for Python |
| http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access | Solaris and J2SE patch clusters |
| http://www.apache.org | Apache Web server and extensions |
| http://docs.sun.com/app/docs/prod/solaris#hic | Sun Solaris documentation |
| http://wp.netscape.com/eng/mozilla/3.0/handbook/javascript/index.html | JavaScript scripting language |
| http://www.eclipse.org | Portal development |
| http://www.entrust.net | Certificate authority |
| http://www.gtk.org | GTK + |
| http://www.interlinknetworks.com | RAD-Series RADIUS Server |
| http://www.jacorb.org/documentation.html | JacORB documentation |
| http://www.jboss.org/products/jbossas | JBoss application server |
| http://www.jython.org | Jython |
| http://www.mozilla.org/rhino | Rhino environment |
| http://www.mysql.com/ | MySQL |
| http://www.omg.org | Object Management Group's CORBA 2.6 standard |
| http://www.opengroup.org/onlinepubs/9629399/apdxa.htm | Universal Unique Identifiers (UUIDs) for the DCE RPC protocol |
| http://www.openssl.org | Certificate authority |
| http://www.oracle.com/appserver/index.html | Oracle Application Server 10g |
| http://www.packetcable.com/specifications/multimedia.html | PacketCable MultiMedia Specification |
| http://www.python.org | Python programming language |
| http://www.python.org/doc/2.0/lib/re-syntax.html | Python regular expression syntax |
| http://docs.python.org/ref/keywords.html | Python keywords |
| http://www.siemens.com/directory | DirX Solutions |
| http://www.sun.com | Sun and Solaris documentation |
| http://www.sun.com/download | Sun ONE Directory Server |
| http://www.sun.com/share/text/termsofuse.html | JRE terms of use |
| http://www.sunfreeware.com | Freeware for Solaris |
| http://www.sysdeo.com/eclipse/tomcatPlugin.html | Portal development |
| http://www.verisign.com | Certificate authority |
| http://www.w3.org/TR/SOAP/ | Simple Object Access Protocol (SOAP) |
| http://www.wi-fialliance.org/opensection/wispr.asp | Wi-Fi WISPr document |

# Index

## Symbols

## A

## B

## C