



SRC PE Software

Getting Started Guide

Release

4.13.x



Modified: 2019-08-21

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Copyright © 2019 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

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

SRC PE Software Getting Started Guide

Release 4.13.x

Copyright © 2019 Juniper Networks, Inc. All rights reserved.

Revision History

August 2019—Revision 1

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

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

SOFTWARE LICENSE

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

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

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

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Abbreviated Table of Contents

	About the Documentation	xix
Part 1	SRC Overview	
Chapter 1	SRC Product Overview	3
Chapter 2	SRC Components	9
Part 2	SRC Software as Virtual Machine	
Chapter 3	Managing the SRC Software as a Virtual Machine	29
Part 3	Managing Your C Series Controller	
Chapter 4	Planning a Deployment of C Series Controllers	41
Chapter 5	Configuring a C Series Controller	45
Chapter 6	Accessing and Starting the SRC CLI	51
Chapter 7	Accessing and Using the C-Web Interface	63
Chapter 8	Configuring Remote Access to a C Series Controller (SRC CLI)	83
Part 4	Managing SRC Licenses	
Chapter 9	Overview of SRC Licenses	105
Chapter 10	Overview of the SRC License Server	107
Chapter 11	Customizing SRC License Server Configuration	113
Chapter 12	Installing Licenses for C Series Controllers	121
Chapter 13	Monitoring License Usage	125
Part 5	Managing an Environment of C Series Controllers	
Chapter 14	Configuring System Time on C Series Controllers (SRC CLI)	133
Chapter 15	Configuring NTP for C Series Controllers	135
Chapter 16	Configuring NTP on C Series Controllers (SRC CLI)	139
Chapter 17	Configuring System Logging for a C Series Controller (SRC CLI)	155
Chapter 18	Configuring Static Host Mapping (SRC CLI)	161
Chapter 19	Overview of the Juniper Networks Database	163
Chapter 20	Managing the Juniper Networks Database (SRC CLI)	167
Chapter 21	Setting Up an SAE (SRC CLI)	189
Chapter 22	Managing System Software on a C Series Controller	199
Chapter 23	Using the Web Application Server on a C Series Controller	215

Part 6	Managing SRC Access and Security (SRC CLI)	
Chapter 24	Configuring User Access (SRC CLI)	235
Chapter 25	Authenticating Users on a C Series Controller (SRC CLI)	259
Chapter 26	Managing Security Digital Certificates	275
Chapter 27	Connecting to Remote Hosts from the SRC Software	283
Chapter 28	Configuring and Starting the SRC SNMP Agent (SRC CLI)	285
Part 7	Configuring Operating Properties for Components	
Chapter 29	Distributing Directory Changes to SRC Components	315
Chapter 30	Configuring Local Properties (SRC CLI)	317
Part 8	Reference Material	
Chapter 31	SRC-Related Abbreviations	329
Chapter 32	SRC-Related References	339

Table of Contents

	About the Documentation	xix
	SRC Documentation and Release Notes	xix
	Audience	xix
	Documentation Conventions	xix
	Documentation Feedback	xxi
	Requesting Technical Support	xxii
	Self-Help Online Tools and Resources	xxii
	Creating a Service Request with JTAC	xxii
Part 1	SRC Overview	
Chapter 1	SRC Product Overview	3
	SRC Product Description	3
	SRC Product Features and Benefits	5
Chapter 2	SRC Components	9
	SRC Component Overview	9
	SRC Server Components	12
	Service Activation Engine	13
	Policy and Service Management	13
	Accounting Support	13
	SAE Extensions	13
	Subscriber Information Collector	13
	Volume Tracking Application	14
	3GPP Gateway	14
	3GPP Gy	14
	Web Application Server	15
	Web Services Gateway	15
	Network Information Collector	15
	Redirect Server	16
	Monitor Components Connectivity	16
	SRC Repository for Data	16
	Juniper Networks Database as a Data Repository on C Series Controllers	17
	Directory as Repository for Subscriber Data	17
	SRC Configuration and Management Tools	17
	SRC CLI	18
	C-Web Interface	18
	Policy and Management	18
	SRC SNMP Agent	19

	SRC Programming Interfaces	19
	NETCONF API	20
	CORBA Plug-In SPI	20
	CORBA Remote API	20
	NIC Access API	20
	SAE Core API	21
	Script Services	21
	Volume Tracking Application (VTA) API	21
	SRC Authentication and Accounting Applications	21
	AAA RADIUS Servers	21
	SRC Admission Control Plug-In	22
	Flat-File Accounting	23
	SRC Demonstration Applications	23
	Enterprise Audit Plug-In	23
	Enterprise Manager Portal	24
	Monitoring Agent Application	24
	Sample Enterprise Service Portal	25
	Residential Service Selection Portals	25
	Other Applications	26
Part 2	SRC Software as Virtual Machine	
Chapter 3	Managing the SRC Software as a Virtual Machine	29
	Virtualized SRC Software Overview	29
	System Requirements for a Virtualized SRC Software	29
	Hard Disk Requirement	30
	Memory Requirements	30
	CPU Requirements	31
	Creating a Virtualized SRC Instance	31
	Creating a Virtualized SRC Instance Using qcow2 Image	32
	Creating a Virtualized SRC Instance Using iso Image	33
	Creating a Virtualized SRC Instance Using the vmdk Image	35
	Creating a Snapshot of qcow2 Image	36
Part 3	Managing Your C Series Controller	
Chapter 4	Planning a Deployment of C Series Controllers	41
	Components in an SRC Deployment	41
	Considerations When Planning a Deployment of C Series Controllers	42
	Deployment Scenario	43
Chapter 5	Configuring a C Series Controller	45
	Before You Begin Configuring the SRC Software on a C Series Controller	45
	Configuring the SRC Software	46
	Configuring SRC Components	47

Chapter 6	Accessing and Starting the SRC CLI	51
	Configuring Access to the SRC CLI Overview	51
	Accessing the SRC CLI When Using an External Directory Server	51
	Configuration Statements for SRC CLI Directory Access	52
	Changing Access to the Directory that Stores SRC Configuration Data	52
	Verifying the Configuration for SRC Directory Access	54
	Starting the SRC CLI	55
	Policies, Services, and Subscribers CLI	56
	Policies, Services, and Subscribers CLI Overview	56
	Configuring Access to the Policies, Services, and Subscribers CLI	56
	Starting the Policies, Services, and Subscribers CLI	57
	Configuring Directory Eventing for Policy Editor	58
	Configuring a Schedule for Executing the Commands or Scripts (SRC CLI)	58
Chapter 7	Accessing and Using the C-Web Interface	63
	C-Web Interface Overview	63
	Navigating the C-Web Interface	64
	Layout of the C-Web Interface	64
	Elements of the C-Web Interface	65
	Top Pane Elements	65
	Main Pane Elements	65
	Side Pane Elements	66
	Accessing the C-Web Interface	67
	Enabling the C-Web Interface	70
	Starting the C-Web Interface	70
	Policies, Services, and Subscribers Subtasks in the C-Web Interface	71
	Policies, Services, and Subscribers Management Subtasks in the C-Web	
	Interface Overview	71
	Configuring Access to Policies, Services, and Subscribers (C-Web	
	Interface)	71
	Starting Policies, Services, and Subscribers	72
	Getting Help in the C-Web Interface	72
	Enabling Help	72
	Disabling Help	72
	Changing a Username or Password for the C-Web Interface	73
	Enabling Remote Users to Access the C-Web Interface	73
	Accessing the C-Web Interface Through Secure HTTP	73
	Accessing the C-Web Interface Through HTTP	73
	Modifying the Editing Level in the C-Web Interface	74
	Displaying Icons for Objects in the C-Web Interface	75
	Enabling Icons for Objects	75
	Disabling Icons for Objects	75
	Editing SRC Configurations (C-Web Interface)	76
	Loading Configuration Values in the C-Web Interface	77
	Committing a Configuration	78
	Reverting to a Previous Configuration	78

	Updating the Configuration Data	78
	Modifying Objects in the C-Web Interface	79
	Copying a Configuration for an Object (C-Web Interface)	79
	Renaming an Object	79
	Moving an Object	80
	Deleting an Object	80
	Configuring Logging Properties in the C-Web Interface	81
	Configuring File Properties	81
	Configuring System Log Properties	81
	Configuration Statements for Logging for the C-Web Interface	82
	Logging Out of the C-Web Interface	82
Chapter 8	Configuring Remote Access to a C Series Controller (SRC CLI)	83
	External Interfaces on a C Series Controller Overview	83
	Tunnel Interfaces	84
	Ethernet Redundancy	84
	Configuring Gigabit Ethernet Interfaces for IPv4 (SRC CLI)	85
	Configuring Gigabit Ethernet Interfaces for IPv6 (SRC CLI)	87
	Configuring Tunnel Interfaces (SRC CLI)	88
	Configuring Ethernet Redundancy (SRC CLI)	90
	Configuring Group Interfaces (SRC CLI)	90
	Configuring the MII Monitor (SRC CLI)	92
	Configuring a Trusted Interface (SRC CLI)	93
	Disabling an Interface (SRC CLI)	94
	Configuring the Virtual IP Address (SRC CLI)	94
	Configuring a Static Route to Devices on Other Networks (SRC CLI)	95
	Securing Connections Between a C Series Controller and Remote Hosts	96
	Configuring a C Series Controller to Accept SSH Connections (SRC CLI)	97
	Configuring a C Series Controller to Accept NETCONF Connections (SRC CLI)	99
	Port Settings for SRC Components	99
Part 4	Managing SRC Licenses	
Chapter 9	Overview of SRC Licenses	105
	Types of SRC Licenses	105
	Obtaining an SRC License	106
Chapter 10	Overview of the SRC License Server	107
	SRC License Server Overview	107
	About the SRC License Server	107
	License Server Errors	107
	License Requests	108
	Example: License Allocation	108
	Example: License Release Example	109
	Lease Renewal	109
	Directory Location and Access	109
	Unsuccessful Connections from the SAE to the SRC License Server	110
	SRC License Server Redundancy	110
	About SRC License Server Alarms	111

Chapter 11	Customizing SRC License Server Configuration	113
	Configuration Statements for SRC License Server Properties	113
	Configuring License Server Alarms (SRC CLI)	114
	Specifying the ORB Configuration for the SRC License Server (SRC CLI)	116
	Configuring the License Server Repository (SRC CLI)	116
	Configuring License Server Properties (SRC CLI)	118
	Configuring the License Server Location (SRC CLI)	119
Chapter 12	Installing Licenses for C Series Controllers	121
	Installing Server Licenses for C Series Controllers (SRC CLI)	121
	Configuring License Manager for an SAE on a C Series Controller (SRC CLI)	122
Chapter 13	Monitoring License Usage	125
	About SRC License Reports	125
	Creating SRC License Usage Reports (SRC CLI)	126
	Sending SRC License Usage Reports to Administrators (SRC CLI)	126
	Monitoring SRC License Usage (SRC CLI)	127
	Removing SRC License Allocated for a Virtual Router (SRC CLI)	128
Part 5	Managing an Environment of C Series Controllers	
Chapter 14	Configuring System Time on C Series Controllers (SRC CLI)	133
	Setting the Time Zone (SRC CLI)	133
	Setting the System Date (SRC CLI)	134
Chapter 15	Configuring NTP for C Series Controllers	135
	NTP Support on C Series Controllers	135
	Configuring NTP on a C Series Controller	136
Chapter 16	Configuring NTP on C Series Controllers (SRC CLI)	139
	Configuration Statements for NTP on C Series Controllers	139
	Specifying Which NTP Server a C Series Controller Contacts on Startup	140
	Configuring NTP Client Mode for a C Series Controller (SRC CLI)	141
	Configuring an NTP Peer on a C Series Controller (SRC CLI)	142
	Configuring NTP Broadcast Mode on a C Series Controller (SRC CLI)	143
	Configuring NTP Authentication on a C Series Controller (SRC CLI)	144
	Configuring NTP as a Broadcast Client on a C Series Controller (SRC CLI)	146
	Configuring NTP as a Multicast Client on a C Series Controller (SRC CLI)	147
	Disabling NTP Monitoring Service (SRC CLI)	148
	Configuring NTP Access Restrictions for a Specific Address (SRC CLI)	149
	Configuring NTP Access Restrictions for All IPv4 Addresses (SRC CLI)	150
	Configuring NTP Access Restrictions for All IPv6 Addresses (SRC CLI)	152
	Verifying NTP Configuration on a C Series Controller	153

Chapter 17	Configuring System Logging for a C Series Controller (SRC CLI)	155
	C Series Controller Log Server Overview	155
	Message Groups	155
	Severity Levels	156
	Before You Configure System Logging (SRC CLI)	156
	Configuration Statements for System Logging on a C Series Controller	157
	Saving System Log Messages to a File (SRC CLI)	157
	Sending System Log Messages to Other Servers (SRC CLI)	158
	Sending Notifications for System Log Messages to Users (SRC CLI)	159
Chapter 18	Configuring Static Host Mapping (SRC CLI)	161
	Static Host Mapping Overview	161
	Configuring Static Host Mapping (SRC CLI)	161
Chapter 19	Overview of the Juniper Networks Database	163
	Juniper Networks Database Overview	163
	Redundancy for a Juniper Networks Database	164
	Security for a Juniper Networks Database	165
Chapter 20	Managing the Juniper Networks Database (SRC CLI)	167
	Configuration Statements for the Juniper Networks Database (SRC CLI)	168
	Enabling the Juniper Networks Database to Run in Standalone Mode (SRC CLI)	168
	Setting a Limit on the Number of Search Results from a Juniper Networks Database (SRC CLI)	169
	Running the Juniper Networks Database in Community Mode (SRC CLI)	170
	Enabling the Juniper Networks Database to Run in Community Mode (SRC CLI)	170
	Configuring the Hostname When Running the Juniper Networks Database in Community Mode (SRC CLI)	172
	Securing the Juniper Networks Database (SRC CLI)	174
	Connecting to Juniper Networks Databases Through LDAPS from an Application Outside the C Series Controller (SRC CLI)	175
	Changing the Mode of a Juniper Networks Database (SRC CLI)	175
	Adding a Juniper Networks Database to an Established Community (SRC CLI)	176
	Promoting a Secondary Database to a Primary Role in a Configuration with One Primary Database (SRC CLI)	177
	Updating Data on a Juniper Networks Database (SRC CLI)	178
	Synchronizing Data on a Juniper Networks Database (SRC CLI)	178
	Loading Sample Data into a Juniper Networks Database (SRC CLI)	179
	Securing Communications Between the Juniper Networks Database and SRC Modules and Components (SRC CLI)	180
	Verifying Configuration for a Juniper Networks Database with the SRC CLI	181
	Getting Information About Operations in a Juniper Networks Database (SRC CLI)	181
	Example: Configuration for a Database Community	182
	Troubleshooting Data Synchronization for Juniper Networks Databases (SRC CLI)	186

	Recovering Data in a Community with One Primary Database and One Secondary Database (SRC CLI)	187
Chapter 21	Setting Up an SAE (SRC CLI)	189
	Initially Configuring the SAE	189
	Grouped Configurations for the SAE	190
	Creating Grouped Configurations for the SAE (SRC CLI)	190
	Configuring an SAE Group	190
	Deleting Default Configurations Within an SAE Group	191
	Configuring Local Properties for the SAE (SRC CLI)	191
	Configuring the RADIUS Local IP Address and NAS ID (SRC CLI)	195
	Starting the SAE (SRC CLI)	196
	Stopping the SAE (SRC CLI)	196
Chapter 22	Managing System Software on a C Series Controller	199
	Software Management on a C Series Controller Overview	199
	Before You Upgrade the Software on a C Series Controller	200
	Creating a Snapshot of Files on a C Series Controller	200
	Upgrading the System Software on a C Series Controller	202
	Upgrading the System Software When Running Redundant SAEs	204
	Preparing the Software Images on the FTP Server	205
	Preparing the CD Image on a Solaris System	205
	Preparing the CD Image on a Linux System	206
	Preparing the Compressed File on a Solaris System	207
	Preparing the Compressed File on a Linux System	207
	Recovering or Installing System Software on a C Series Controller by Using the USB Storage Device Supplied by Juniper Networks	208
	Restoring the Files in a Snapshot	212
	Recovering System Software on a C Series Controller from a System Snapshot (SRC CLI)	212
	Deleting the Files in a Snapshot	213
Chapter 23	Using the Web Application Server on a C Series Controller	215
	Web Application Server on C Series Controllers Overview	215
	Clustering	216
	Local and Shared Configuration	216
	Configuration Statements for the Web Application Server	217
	Configuring the Web Application Server (SRC CLI)	218
	Configuring Local Properties for the Web Application Server (SRC CLI)	219
	Configuring the Web Application Server Shared Cluster Configuration (SRC CLI)	221
	Configuring the Nodes in the Web Application Server Cluster (SRC CLI)	222
	Configuring Remote Access to the Application Server (SRC CLI)	223
	Configuring Access to the Application Server Through Secure HTTP	223
	Configuring Access to the Application Server Through HTTP	224
	Configuring Virtual Hosts for the Web Applications (SRC CLI)	225
	Configuring User Accounts for Web Applications (SRC CLI)	226
	Installing Web Applications in the SRC Web Application Server	228
	Removing Web Applications from the Application Server	228
	Starting the Web Application Server on a C Series Controller	229

	Restarting the Web Application Server on a C Series Controller	229
	Stopping the Web Application Server on a C Series Controller	229
	Viewing Statistics for the Web Application Server (SRC CLI)	229
	Viewing Statistics for the Web Application Server (C-Web Interface)	230
	Viewing the Web Application Server Cluster Status (SRC CLI)	230
	Viewing the Web Application Server Cluster History (SRC CLI)	231
Part 6	Managing SRC Access and Security (SRC CLI)	
Chapter 24	Configuring User Access (SRC CLI)	235
	SRC User Accounts Overview	235
	Login Classes for SRC User Accounts	236
	Login Class Permission Options for the SRC Software	237
	Predefined Login Classes for the SRC Software	241
	Access to Individual Commands and Configuration Statements (SRC CLI)	241
	Regular Expressions for Allow and Deny Statements	242
	Guidelines for Using Regular Expressions	243
	Timeout Value for Idle Login Sessions	243
	Before You Configure Login Classes	244
	Configuring a Login Class (SRC CLI)	244
	Examples: Configuring Access Privileges for SRC Operational Mode	
	Commands	247
	Examples: Defining Access Privileges for SRC Configuration Mode	
	Commands	248
	Configuration Statements for SRC User Accounts	248
	Configuring User Accounts (SRC CLI)	249
	Types of Authentication for SRC User Accounts	251
	Configuring Authentication for SRC User Accounts (SRC CLI)	252
	Configuring a Plain Text Password	252
	Configuring SSH Authentication	253
	Example: SRC User Accounts	254
	Changing the root Password for the SRC Software (SRC CLI)	255
	Recovering the root Password (SRC CLI)	256
	Configuring a System Login Announcement (SRC CLI)	257
Chapter 25	Authenticating Users on a C Series Controller (SRC CLI)	259
	Configuring RADIUS and TACACS+ Authentication on a C Series Controller (SRC	
	CLI)	259
	TACACS+ and RADIUS Authentication/Authorization Attributes	260
	Configuring RADIUS Authentication (SRC CLI)	261
	Configuring TACACS+ Authentication (SRC CLI)	263
	Configuring TACACS+ Authentication (C-Web Interface)	264
	A C Series Controller as a RADIUS Client and TACACS+ Client	264
	Configuring More Than One Authentication Method (SRC CLI)	266
	Configuring Authentication Order	266
	Configuring TACACS+ or RADIUS Authentication	266
	Configuring TACACS+ and RADIUS Authentication	267

	Removing an SRC Authentication Method from the Authentication Order (SRC CLI)	268
	SRC Template Accounts for RADIUS and TACACS+ Authentication	268
	SRC Template Accounts for RADIUS and TACACS+ Authentication Overview	268
	Named Template Accounts	269
	Using Remote Template Accounts (SRC CLI)	269
	Configuring a Local SRC User Template (SRC CLI)	270
	Example: Configuring SRC Authentication	270
	Configuring TACACS+ System Accounting (SRC CLI)	271
	Specifying TACACS+ Auditing and Accounting Events (SRC CLI)	272
	Configuring TACACS+ Server Accounting (SRC CLI)	273
Chapter 26	Managing Security Digital Certificates	275
	Digital Certificates Overview	275
	Before You Use Digital Certificates	276
	Commands to Manage Digital Certificates	276
	Manually Obtaining Digital Certificates (SRC CLI)	277
	Obtaining Digital Certificates through SCEP (SRC CLI)	278
	Removing a Certificate Request	280
	Removing a Certificate	280
Chapter 27	Connecting to Remote Hosts from the SRC Software	283
	Connecting to a Remote Host Through SSH	283
	Connecting to a Remote Host Through Telnet	283
Chapter 28	Configuring and Starting the SRC SNMP Agent (SRC CLI)	285
	Configuration Statements for the SRC SNMP Agent	286
	Configuring the SRC SNMP Agent (SRC CLI)	287
	Configuring General Properties for the SRC SNMP Agent (SRC CLI)	287
	Configuring Initial Properties for the SRC SNMP Agent (SRC CLI)	288
	Configuring Directory Connection Properties for the SRC SNMP Agent (SRC CLI)	290
	Configuring Directory Monitoring Properties for the SRC SNMP Agent (SRC CLI)	291
	Configuring Logging Destinations for the SRC SNMP Agent (SRC CLI)	292
	Configuring JRE Properties (SRC CLI)	292
	Configuration Statements for the SRC SNMP Agent	293
	Configuring the SRC SNMP Agent (SRC CLI)	294
	Configuring System Information for the SRC SNMP Agent (SRC CLI)	295
	Configuring Access Control for SNMPv3 Users (C-Web Interface)	296
	Creating SNMPv3 Users	297
	Configuring Access Privileges for SNMPv3 Users (SRC CLI)	297
	Configuring Authentication for SNMPv3 Users (SRC CLI)	298
	Configuring Encryption for SNMPv3 Users (SRC CLI)	299
	Configuring Access Control for Communities (SRC CLI)	300
	Configuring Access Control for the VACM (SRC CLI)	301
	Associating Security Names with a Community (SRC CLI)	303
	Defining Named Views (SRC CLI)	304
	Defining Access Privileges for an SNMP Group (SRC CLI)	305

	Assigning Security Names to Groups (SRC CLI)	307
	Configuring Notification Targets (SRC CLI)	308
	Operating the SRC SNMP Agent	310
	Starting the SRC SNMP Agent (SRC CLI)	310
	Stopping the SRC SNMP Agent (SRC CLI)	311
	Monitoring the SRC SNMP Agent (SRC CLI)	311
Part 7	Configuring Operating Properties for Components	
Chapter 29	Distributing Directory Changes to SRC Components	315
	Directory Eventing System Overview	315
	Managing Directory Communication	316
Chapter 30	Configuring Local Properties (SRC CLI)	317
	Local Properties for SRC Components	317
	Configuration Statements for Local Configuration	317
	Configuring Basic Local Properties	318
	Changing the Location of Data in the Directory	320
	Configuring Directory Connection Properties	321
	Configuring Initial Directory Eventing Properties for SRC Components	323
	Verifying the Local Configuration for a Component	324
Part 8	Reference Material	
Chapter 31	SRC-Related Abbreviations	329
	SRC-Related Abbreviations	329
Chapter 32	SRC-Related References	339
	SRC-Related References	339
	Draft RFCs	339
	RFCs	339
	Other Software Standards	341
	URLs	341

List of Figures

Part 1	SRC Overview	
Chapter 1	SRC Product Overview	3
	Figure 1: SRC Network with C Series Controllers	4
	Figure 2: SRC-Managed PCMM Network	5
Chapter 2	SRC Components	9
	Figure 3: C-Web Interface for SAE Configuration	18
	Figure 4: Position of SRC ACP in the Network	23
	Figure 5: Sample Page in Enterprise Manager Portal	24
	Figure 6: Sample Residential Web Portal	25
	Figure 7: Sample Login Page for a Residential Portal on a PDA	26
Part 3	Managing Your C Series Controller	
Chapter 4	Planning a Deployment of C Series Controllers	41
	Figure 8: C Series Controller and Related Components	42
	Figure 9: Deployment Scenario for C Series Controllers	44
Chapter 7	Accessing and Using the C-Web Interface	63
	Figure 10: C-Web Layout	64
	Figure 11: Top Pane Elements	65
	Figure 12: Main Pane Elements	66
	Figure 13: Side Pane Elements	67
	Figure 14: Policy Icon	75
	Figure 15: Configuration Options for the C-Web Interface	77
	Figure 16: Sample Configuration	78
Part 5	Managing an Environment of C Series Controllers	
Chapter 20	Managing the Juniper Networks Database (SRC CLI)	167
	Figure 17: Sample Community of Juniper Network Databases	183
Part 6	Managing SRC Access and Security (SRC CLI)	
Chapter 25	Authenticating Users on a C Series Controller (SRC CLI)	259
	Figure 18: Authentication Order: RADIUS, TACACS+, Local Password	265

List of Tables

	About the Documentation	xix
	Table 1: Notice Icons	xx
	Table 2: Text Conventions	xx
Part 1	SRC Overview	
Chapter 1	SRC Product Overview	3
	Table 3: SRC Software Features and Benefits	5
Chapter 2	SRC Components	9
	Table 4: Descriptions of SRC Components	9
	Table 5: Available NIC Resolutions	15
Part 2	SRC Software as Virtual Machine	
Chapter 3	Managing the SRC Software as a Virtual Machine	29
	Table 6: Heap Allocation for SRC Components on a Virtualized SRC Software	30
Part 3	Managing Your C Series Controller	
Chapter 5	Configuring a C Series Controller	45
	Table 7: Configuration Information for Other SRC Components	48
Chapter 6	Accessing and Starting the SRC CLI	51
	Table 8: Values Allowed for the Periodic Strings	60
	Table 9: Available Special Characters	60
	Table 10: Special String Options	61
Chapter 7	Accessing and Using the C-Web Interface	63
	Table 11: Editing Levels	74
Chapter 8	Configuring Remote Access to a C Series Controller (SRC CLI)	83
	Table 12: Applications to Remotely Access the C Series Controller	96
	Table 13: Default Port Settings for SRC Components	99
Part 4	Managing SRC Licenses	
Chapter 10	Overview of the SRC License Server	107
	Table 14: SRC SNMP Warnings and Alarms	111
Chapter 13	Monitoring License Usage	125

	Table 15: Output Fields for the show license-server allocated-licenses Command	128
Part 5	Managing an Environment of C Series Controllers	
Chapter 22	Managing System Software on a C Series Controller	199
	Table 16: Package Names for Components on a C Series Controller	199
Part 6	Managing SRC Access and Security (SRC CLI)	
Chapter 24	Configuring User Access (SRC CLI)	235
	Table 17: Login Class Permission Options	237
	Table 18: Default System Login Classes	241
	Table 19: Common Regular Expression Operators to Allow or Deny Operational Mode and Configuration Mode Commands	242
Chapter 25	Authenticating Users on a C Series Controller (SRC CLI)	259
	Table 20: Supported TACACS+ and RADIUS Authentication/Authorization Attributes	260
	Table 21: Information Published for Events	272
Part 8	Reference Material	
Chapter 31	SRC-Related Abbreviations	329
	Table 22: SRC Software-Related Abbreviations	329
Chapter 32	SRC-Related References	339
	Table 23: Draft RFCs	339
	Table 24: RFCs	339
	Table 25: Non-RFC Software Standards	341
	Table 26: Juniper Networks URLs	341
	Table 27: Third-Party URLs	342

About the Documentation

- SRC Documentation and Release Notes on page xix
- Audience on page xix
- Documentation Conventions on page xix
- Documentation Feedback on page xxi
- Requesting Technical Support on page xxii

SRC Documentation and Release Notes

For a list of related SRC documentation, see <https://www.juniper.net/documentation/>.

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

Audience

This documentation is intended for experienced system and network specialists working with routers running Junos OS and JunosE software in an Internet access environment. We assume that readers know how to use the routers, directories, and RADIUS servers that they will deploy in their SRC networks. If you are using the SRC software in a cable network environment, we assume that you are familiar with the PacketCable Multimedia Specification (PCMM) as defined by Cable Television Laboratories, Inc. (CableLabs) and with the Data-over-Cable Service Interface Specifications (DOCSIS) 1.1 protocol. We also assume that you are familiar with operating a multiple service operator (MSO) multimedia-managed IP network.

Documentation Conventions

[Table 1 on page xx](#) defines the notice icons used in this guide. [Table 2 on page xx](#) defines text conventions used throughout this documentation.

Table 1: Notice Icons







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

Table 2: Text Conventions

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

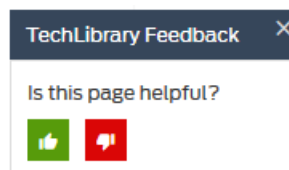
Table 2: Text Conventions (continued)

<i>Italic sans serif typeface</i>	Represents variables in SRC CLI commands.	<code>user@host# set local-address local-address</code>
Angle brackets	In text descriptions, indicate optional keywords or variables.	Another runtime variable is <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.
<i>Italic typeface</i>	<ul style="list-style-type: none"> Emphasizes words. Identifies book names. Identifies distinguished names. Identifies files, directories, and paths in text but not in command examples. 	<ul style="list-style-type: none"> There are two levels of access: <i>user</i> and <i>privileged</i>. <i>SRC PE Getting Started Guide</i> <i>o=Users, o=UMC</i> The <i>/etc/default.properties</i> file.
Backslash	At the end of a line, indicates that the text wraps to the next line.	<code>Plugin.radiusAcct-1.class=\ net.juniper.smgmt.sae.plugin\ RadiusTrackingPluginEvent</code>
Words separated by the symbol	Represent a choice to select one keyword or variable to the left or right of this symbol. (The keyword or variable may be either optional or required.)	<code>diagnostic line</code>

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

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

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

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

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://support.juniper.net/support/requesting-support/>.

PART 1

SRC Overview

- [SRC Product Overview on page 3](#)
- [SRC Components on page 9](#)

CHAPTER 1

SRC Product Overview

- [SRC Product Description on page 3](#)
- [SRC Product Features and Benefits on page 5](#)

SRC Product Description

The Juniper Networks C2000, C3000, C4000, and C5000 systems, collectively referred to as C Series Controllers, are self-contained units with known capacity designed to optimize delivery of the features in the Juniper Networks Session and Resource Control (SRC) software. The model in use determines the number of service session licenses and concurrent subscribers allowed.

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

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

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

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

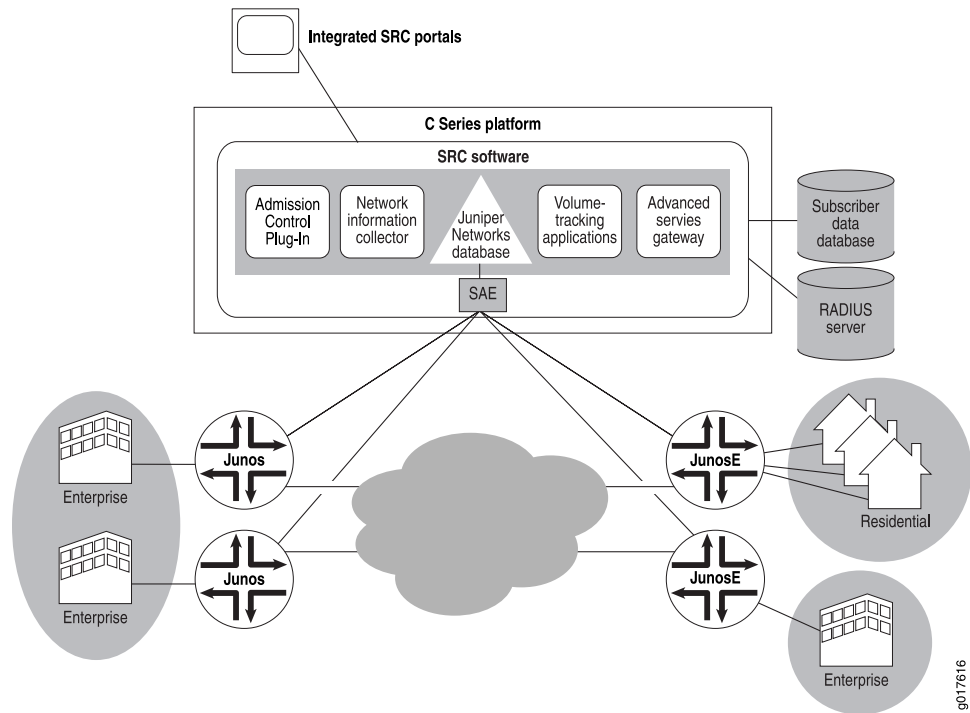
The SRC software is designed to simplify the three major steps in the IP service life-cycle process:

1. Creating innovative, revenue-generating services
2. Delivering numerous on-demand services to subscribers

3. Tracking services with intelligent accounting applications

Figure 1 on page 4 illustrates how the SRC software manages routers running JunosE and Junos OS in an SRC network.

Figure 1: SRC Network with C Series Controllers



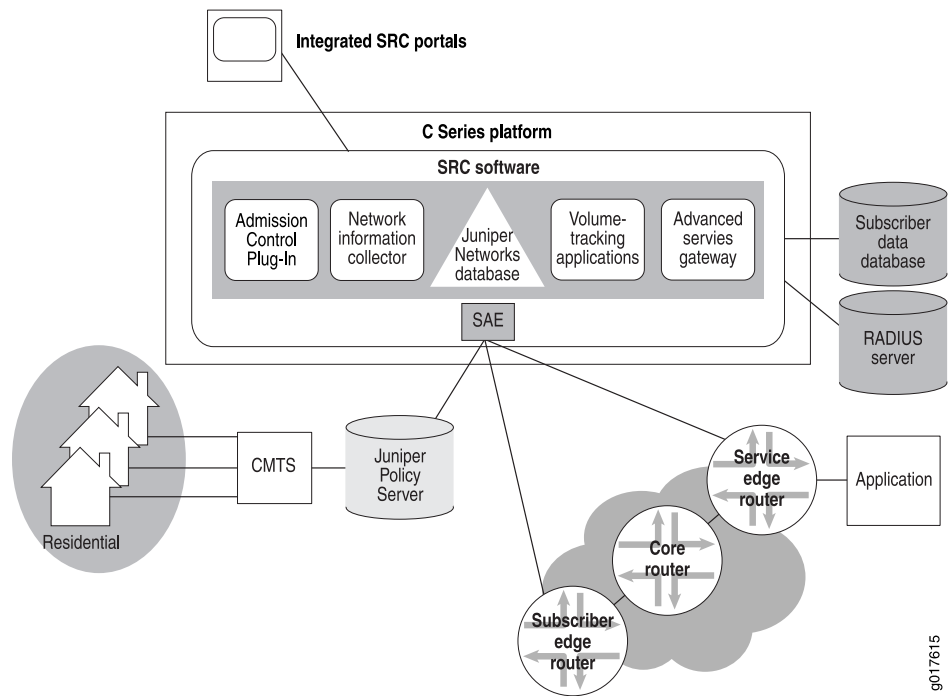
In addition, the SRC software can be used in a PacketCable Multimedia (PCMM) environment to simplify other management tasks, such as:

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

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

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

Figure 2: SRC-Managed PCMM Network



- Related Documentation**
- [SRC Product Features and Benefits on page 5](#)
 - [SRC Component Overview on page 9](#)

SRC Product Features and Benefits

The SRC software provides a host of features for today's Internet service challenges. [Table 3 on page 5](#) lists some of the many features and benefits that service providers need.

Table 3: SRC Software Features and Benefits

Feature	Benefit
Carrier-class architecture	<ul style="list-style-type: none"> • Provides a distributed architecture for flexibility. • Integrates with provider subscriber databases and supports customer profiles to define subscriber groups. • Instantiates each key server multiple times for either load distribution or failover. • Facilitates a variety of wholesale and retail models. • Uses CLI and Web management and monitoring.

Table 3: SRC Software Features and Benefits (continued)

Feature	Benefit
Seamless integration with operations support systems (OSS)	<ul style="list-style-type: none"> • Uses modular design and standards-based interfaces such as HTML/XML, RADIUS, LDAP, Common Object Request Broker Architecture (CORBA), and Simple Object Access Protocol (SOAP). • Supports open interfaces and mediation mechanisms to facilitate system integration with diverse OSS applications, including systems for subscriber management, customer care, order entry, provisioning, billing, security, and sales support. • Ensures smooth integration with back office solutions. (We partner with leading providers of telecommunications, RADIUS/authentication, authorization, and accounting (AAA), and billing systems to offer these services.)
Financial advantages	<ul style="list-style-type: none"> • Avoids the misconception of a one-size-fits-all Internet access model by offering compelling content options with the appropriate level of bandwidth, quality of service (QoS), and network functions (for example, security, traffic prioritization, and filtering). • Allows providers to hold down on capital expenditures and operating expenses by offering a wide range of flexible services, tools, billing models, and revenue streams, and by using the same network infrastructure.
Optimal scalability	<ul style="list-style-type: none"> • Scales for rapidly growing networks and subscriber bases. • Works with routers running JunosE or Junos OS, and PCMM-compliant CMTS devices to automatically provision and support thousands to millions of subscribers in a distributed environment. • Uses zero-touch subscriber provisioning, which removes the roadblocks that can slow large-scale broadband subscriber acquisition.
Easy-to-build wholesale-retail model	<ul style="list-style-type: none"> • Provides a transparent infrastructure to Internet service provider (ISP), application service provider (ASP), and content partners, which lets partners retain ownership and management of their subscriber bases. • Frees partners from the responsibility of handling network operations so that they can focus solely on service delivery.
Intelligent accounting	<ul style="list-style-type: none"> • Tracks service usage to enable rich and creative tariff models. • Supports customer care, rating and billing, security, and sales support systems. • Simplifies the task of collecting and managing retailer and subscriber accounting data. • Uses a configuration interface to choose the policy rules to be used for accounting per interface direction (ingress and egress). • Activates multiple service sessions simultaneously for a given subscriber; each session can be tracked separately. • Supports plug-in software that gives service providers the ability to extend system capabilities. • Allows for flexible accounting rules.
Easy subscriber management	<ul style="list-style-type: none"> • Uses configuration interfaces for service definition and subscriber management. • Uses a directory that acts as a central repository of customer information. The directory stores router information. • Works with routers running JunosE or Junos OS, and PCMM-compliant CMTS to collect subscribers' credentials and queries the RADIUS server for authentication and authorization. • Accommodates and manages a very large number of subscribers (for example, a typical subscriber base may be in the millions).

Table 3: SRC Software Features and Benefits (continued)

Feature	Benefit
Dynamic policy management	<ul style="list-style-type: none"> • Gives subscribers consistent service experience across the network, regardless of the actual network deployment and the mode of connection to the network. • Enables real-time provisioning and collection of subscriber usage data. • Offers high availability based on seamless failover. • Uses configuration interfaces to define policies and store them in a central repository. • Provides robust support for access, QoS, and activation of new services on demand with configurable policies. • Performs dynamic policy decisions while services are activated, leveraging on the directory content to make policy decisions. • Provides end-to-end service levels across the network.
Web-based portal	<ul style="list-style-type: none"> • Creates dynamic webpages, giving subscribers personalized displays to select services on demand. • Offers branding opportunities for network provider/service provider partners. • Identifies subscribers, grants them access to defined services, and maps their selected service(s) to the network by means of dynamically provisioned policies. • Allows portals to be deployed in any application server with support for CORBA or SOAP. • Provides a starting point for rapid portal development through documented sample portals supplied for Java 2 Enterprise Edition (J2EE) application servers.
Easy service creation	<ul style="list-style-type: none"> • Uses the SRC CLI and the C-Web interface to enable the definition of various policy objects. • Uses configuration interfaces to define new services and to create service templates for future use. Service templates provide the service-provisioning information that configures the router for efficient, real-time delivery of that service. • Provides flexible service creation, a reusable service library, and automated service implementation. • Allows providers to define policies once and apply them network-wide.
Service activation engine (SAE)	<ul style="list-style-type: none"> • Translates services into lists of policies to be enforced on the router. • Initiates the service-usage data-collection process. • Customizes services with differentiated QoS and policies. • Collects usage data (time and volume) by subscriber and service to enable differentiated rating and billing.
Flexible open interface support	<ul style="list-style-type: none"> • Allows an external entity or system to control the SRC software's behavior. • Uses application programming interfaces (APIs) to authenticate managers; to navigate among retailers, enterprises, and sites; and to create, delete, activate, and deactivate service sessions. • Provides a Common Open Policy Service for policy provisioning (COPS-PR) interface. • Integrates into a PCMM environment with support for CableLabs PCMM specification. • Extends policies to systems that do not have a supported router driver. • Integrates 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.

Related Documentation • [SRC Product Description on page 3](#)

- [SRC Component Overview on page 9](#)

CHAPTER 2

SRC Components

- [SRC Component Overview on page 9](#)
- [SRC Server Components on page 12](#)
- [SRC Repository for Data on page 16](#)
- [SRC Configuration and Management Tools on page 17](#)
- [SRC Programming Interfaces on page 19](#)
- [SRC Authentication and Accounting Applications on page 21](#)
- [SRC Demonstration Applications on page 23](#)
- [Other Applications on page 26](#)

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 4 on page 9](#) gives a brief description of the components that make up the SRC software.

Table 4: Descriptions of SRC Components

Component	Description
Server Components	
Service activation engine (SAE)	<ul style="list-style-type: none">• Authorizes, activates, and deactivates subscriber and service sessions by interacting with systems such as Juniper Networks routers, cable modem termination system (CMTS) devices, RADIUS servers, and directories.• Collects accounting information about subscribers and services from routers, and stores the information in RADIUS accounting servers, flat files, and other accounting databases.• Provides plug-ins and application programming interfaces (APIs) for starting and stopping subscriber and service sessions and for integrating with systems that authorize subscriber actions and track resource usage.

Table 4: Descriptions of SRC Components (continued)

Component	Description
Subscriber Information Collector (SIC)	The SIC listens for RADIUS accounting events from IP edge devices (accounting clients) and forwards them to a remote AAA server, allowing the SRC software to gain increased subscriber awareness. Additionally, the SIC can optionally edit accounting events before routing them.
Network information collector (NIC)	Collects information about the state of the network and can provide a mapping from a given type of network data to another type of network data.
Redirect Server	Redirects HTTP requests received from IP Filter to a captive portal page.
3GPP Gateway	The SRC Third-Generation Partnership Project (3GPP) gateway is a Diameter-based component in the SRC software, which provides integration with 3GPP Policy and Charging Control environments, to provide fixed-mobile convergence (FMC). The SRC 3GPP gateway provides Gx-based integration with the Policy and Charging Rules Function (PCRF). The SRC 3GPP gateway uses the northbound Gx interface to mediate between the PCRF and Juniper Networks routers like the E Series Broadband Services routers and MX Series routers. The northbound Gx interface on the SRC 3GPP gateway communicates with the PCRF using the Diameter protocol.
3GPP Gy	The SRC 3GPP Gy is a Diameter-based component in the SRC software, which provides Gy-based integration with the Online Charging System (OCS), to provide FMC. The SRC 3GPP Gy uses the northbound Gy interface to handle charging-related information between the OCS and Juniper Networks routers like the E Series Broadband Services routers and MX Series routers. The northbound Gy interface communicates with the OCS using the Diameter protocol.
Web Application Service	The SRC software includes a Web application server that hosts the Web Services Gateway and the Volume Tracking Application (SRC VTA). In production environments, this application server is designed to host only these applications. However, you can load your own applications into this server for testing or demonstration purposes.
Web Services Gateway	<p>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.</p> <p>The Web Services Gateway 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.</p>
Monitor Components Connectivity (MCC)	Monitors the connectivity state between SAEs in a community and between SAE and RADIUS server periodically and collects diagnostic information about the connectivity state of components, such as connection error, connection timeout, and socket read/write timeout.
Repository	
Directory	<p>The SRC software includes the Juniper Networks database, which is a built-in Lightweight Directory Access Protocol (LDAP) directory for storing all SRC data including services, policies, and small subscriber databases.</p> <p>For large subscriber databases, you must supply your own directory.</p>

SRC Configuration and Management Tools

Table 4: Descriptions of SRC Components (continued)

Component	Description
SRC command line interface (CLI)	Provides a way to configure the SRC software on a C Series Controller from a Junos OS–like CLI. The SRC CLI includes the policies, services, and subscribers CLI, which has separate access privileges.
C-Web interface	Provides a way to configure, monitor, and manage the SRC software on a C Series Controller through a Web browser. The C-Web interface includes a policies, services, and subscribers component, which has separate access privileges.
Simple Network Management Protocol (SNMP) agent	Monitors system performance and availability. It runs on all the SRC hosts and makes management information available through SNMP tables and sends notifications by means of SNMP traps.
Service Management Applications (Run on external system)	
IMS Services Gateway	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.
SRC Programming Interfaces	
NETCONF API	Allows you to configure or request information from the NETCONF server on a C Series Controller that runs the SRC software. Applications developed with the NETCONF API run on a system other than a C Series Controller.
CORBA plug-in service provider interface (SPI)	Tracks sessions and enables linking the rest of the service provider's operations support system (OSS) with the SRC software so that the OSS can be notified of events in the life cycle of SAE sessions. Hosted plug-ins only.
CORBA remote API	Provides remote access to the SAE core API. Applications that use these extensions to the SRC software run on a system other than a C Series Controller.
NIC access API	Performs NIC resolutions. Applications that use these extensions to the SRC software run on a system other than a C Series Controller.
SAE core API	Controls the behavior of the SRC software. Applications that use these extensions to the SRC software run on a system other than a C Series Controller.
Script services	Provides an interface to call scripts that supply custom services such as provisioning policies on a number of systems across a network.
VTA API	The Volume Tracking Application (VTA) API is a Simple Object Access Protocol (SOAP) interface that allows developers to create gateway clients and that administrators use to manage VTA subscribers and sessions. The SRC Web Services Gateway allows a gateway client—an application that is not part of the SRC network—to interact with SRC components, such as the VTA, through a SOAP interface.
Authorization and Accounting Applications	
AAA RADIUS servers	Authenticates subscribers and authorizes their access to the requested system or service. Accepts accounting data—time active and volume of data sent—about subscriber and service sessions. RADIUS servers run on a system other than a C Series Controller.

Table 4: Descriptions of SRC Components (continued)

Component	Description
SRC Admission Control Plug-In (SRC ACP)	Authorizes and tracks subscribers' use of network resources associated with services that the SRC application manages.
Flat file accounting	Stores tracking data to accounting flat files that can be made available to external systems that send the data to a rating and billing system.
Volume Tracking Application	<p>The SRC Volume Tracking Application (SRC VTA) is an SRC component that 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.</p> <p>When a subscriber or service exceeds bandwidth limits (or quotas), the SRC VTA can take actions including imposing rate limits on traffic, sending an e-mail notification, or charging extra for additional bandwidth consumed.</p>
Demonstration Applications (available on the Juniper Networks Website)	
Enterprise Audit Plug-In	Defines a callback interface, which receives events when IT managers complete specified operations.
Enterprise Manager Portal	<p>Allows service providers to provision services for enterprise subscribers on routers running JunosE or Junos OS and allows IT managers to manage services.</p> <p>Enterprise Manager Portal can be used with NAT Address Management Portal to allow service providers to manage public IP addresses for use with NAT services on routers running Junos OS and to allow IT managers to make requests about public IP addresses through the Enterprise Manager Portal.</p>
Monitoring Agent application	Integrates IP address managers, such as a DHCP server or a RADIUS server, into an SRC-managed network so that the SAE is notified about subscriber events. The Monitoring Agent application runs on a Solaris platform.
Residential service selection portals	Provides a framework for building Web applications that allow residential and enterprise subscribers to manage their own network services. It comes with several full-featured sample Web applications that are easy to customize and suitable for deployment. The Residential service selection portals run on a Solaris platform.
Sample enterprise service portal	Lets service providers supply an interface to their business customers for managing and provisioning services.

Related Documentation • [SRC Product Description on page 3](#)

SRC Server Components

The SRC server components are:

- [Service Activation Engine on page 13](#)
- [Subscriber Information Collector on page 13](#)

- [Volume Tracking Application on page 14](#)
- [3GPP Gateway on page 14](#)
- [3GPP Gy on page 14](#)
- [Web Application Server on page 15](#)
- [Web Services Gateway on page 15](#)
- [Network Information Collector on page 15](#)
- [Redirect Server on page 16](#)
- [Monitor Components Connectivity on page 16](#)

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 routers running JunosE or Junos OS. 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 webpage.

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.

Subscriber Information Collector

The SIC listens for RADIUS accounting events from IP edge devices (accounting clients), and filters undesired events based on attachment session attributes, providing the SRC software with increased subscriber awareness.

The major components of the SIC are:

- Accounting listeners, which are configured with port numbers and parameters controlling receipt of UDP packets.
- A collection of RADIUS dictionaries.
- A collection of network access server (NAS) clients.
- A collection of RADIUS accounting targets.
- A collection of routing rules.
- A collection of RADIUS network elements. A RADIUS network element contains an ordered list of RADIUS accounting clients, targets or both, along with a failover policy for targets.
- A proxy accounting method that forwards accounting events to a downstream AAA server (network element).
- Components supporting SNMP, statistics, and event logging.

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 imposing rate limits on traffic, sending an e-mail notification, or charging extra for additional bandwidth consumed.

3GPP Gateway

The SRC Third-Generation Partnership Project (3GPP) gateway is a Diameter-based component in the SRC software, which provides integration with 3GPP Policy and Charging Control environments, to provide fixed-mobile convergence (FMC). The SRC 3GPP gateway provides Gx-based integration with the Policy and Charging Rules Function (PCRF). The SRC 3GPP gateway uses the Gx interface to mediate between the PCRF and Juniper Networks routers like the E Series Broadband Services routers and MX Series routers. The Gx interface on the SRC 3GPP gateway communicates with the PCRF using the Diameter protocol.

3GPP Gy

The SRC 3GPP Gy is a Diameter-based component in the SRC software, which provides Gy-based integration with the OCS, to provide FMC. The SRC 3GPP Gy uses the northbound Gy interface to handle charging-related information between the OCS and Juniper Networks routers like the E Series Broadband Services routers and MX Series routers. The northbound Gy interface communicates with the OCS using the Diameter protocol.

Web Application Server

The SRC software on a C Series Controller includes a Web application server that hosts the Dynamic Service Activator and the Volume Tracking Application (SRC VTA). In production environments, this application server is designed to host only these applications. However, you can load your own applications into this server for testing or demonstration purposes. You can control access to applications deployed in the Web application server by configuring virtual hosts. A virtual host contains aliases and lists of the clients that are allowed to access the virtual host.

Web Services Gateway

The Web Services Gateway 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 Web Services Gateway 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.

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 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 5 on page 15](#) shows the NIC resolutions that the standard SRC software can perform. For customized NIC implementations that provide other resolutions, contact Juniper Networks Professional Services.

Table 5: Available NIC Resolutions

Key	Value
Accounting ID of a subscriber	SAE reference

Table 5: Available NIC Resolutions (continued)

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

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

Redirect Server

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

Monitor Components Connectivity

The Monitor Components Connectivity (MCC) component monitors the connectivity state between SAEs in a community and between SAE and RADIUS server periodically and collects diagnostic information about the connectivity state of components, such as connection error, connection timeout, and socket read/write timeout.

Related Documentation

- [SRC Component Overview on page 9](#)

SRC Repository for Data

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

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

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

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

Juniper Networks Database as a Data Repository on C Series Controllers

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

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

Directory as Repository for Subscriber Data

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

Related Documentation

- [SRC Component Overview on page 9](#)

SRC Configuration and Management Tools

The SRC software provides the following configuration and management tools for the SRC module:

- [SRC CLI on page 18](#)
- [C-Web Interface on page 18](#)
- [Policy and Management on page 18](#)
- [SRC SNMP Agent on page 19](#)

SRC CLI

The SRC CLI is the software interface that you use to configure, monitor, and manage a C Series Controller and SRC software, including the SRC module. The SRC CLI uses the same operational model as the Junos OS CLI, which you use to configure and monitor routers running Junos OS.

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 routers running Junos OS.

The C-Web interface supports the configuration, monitoring, and management tasks that you can perform with the SRC CLI. [Figure 3 on page 18](#) shows a C-Web configuration page for the SAE.

Figure 3: C-Web Interface for SAE Configuration



Policy and Management

The SRC software works with Juniper Networks routers and PacketCable Multimedia Specification (PCMM) compliant CMTS platforms to provide differentiated QoS. SRC

policies 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.

For routers running Junos OS, the SRC software supports class-of-service (CoS), firewall filters, policing, stateful firewall, stateless firewall, and Network Address Translation (NAT) services.

For routers running JunosE Software, the SRC software supports policy routing, rate limiting, QoS classification and marking, packet forwarding, and packet filtering.

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

SRC SNMP Agent

The SRC 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 SRC SNMP agent is preconfigured to monitor SRC processes. Additionally, it provides detailed monitoring and configuration of SRC server components such 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.

Related Documentation

- *Monitoring and Troubleshooting Tools Overview*
- *SRC PE Monitoring and Troubleshooting Guide*
- *SRC PE Services and Policies Guide*
- [SRC Component Overview on page 9](#)

SRC Programming Interfaces ---

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

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

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

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

- [NETCONF API on page 20](#)
- [CORBA Plug-In SPI on page 20](#)

- [CORBA Remote API on page 20](#)
- [NIC Access API on page 20](#)
- [SAE Core API on page 21](#)
- [Script Services on page 21](#)
- [Volume Tracking Application \(VTA\) API on page 21](#)

NETCONF API

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

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

CORBA Plug-In SPI

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

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

CORBA Remote API

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

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

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

NIC Access API

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

SAE Core API

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

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

Script Services

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

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

You can use script services to provision policies on a number of systems across a network, including networks that do not contain a router running JunosE or Junos OS.

Volume Tracking Application (VTA) API

The Volume Tracking Application (VTA) API is a Simple Object Access Protocol (SOAP) interface that allows developers to create gateway clients and that administrators use to manage VTA subscribers and sessions. The SRC Web Services Gateway allows a gateway client—an application that is not part of the SRC network—to interact with SRC components, such as the VTA, through a SOAP interface.

Related Documentation • [SRC Component Overview on page 9](#)

SRC Authentication and Accounting Applications

The following components help to provide accounting or authentication:

- [AAA RADIUS Servers on page 21](#)
- [SRC Admission Control Plug-In on page 22](#)
- [Flat-File Accounting on page 23](#)

AAA RADIUS Servers

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

to keep network statistics. The router provides RADIUS accounting and authentication, while the SAE provides SAE accounting and authentication.

We recommend that service providers use a RADIUS server such as the Juniper Networks Steel-Belted Radius/SPE server.

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

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

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

SRC Admission Control Plug-In

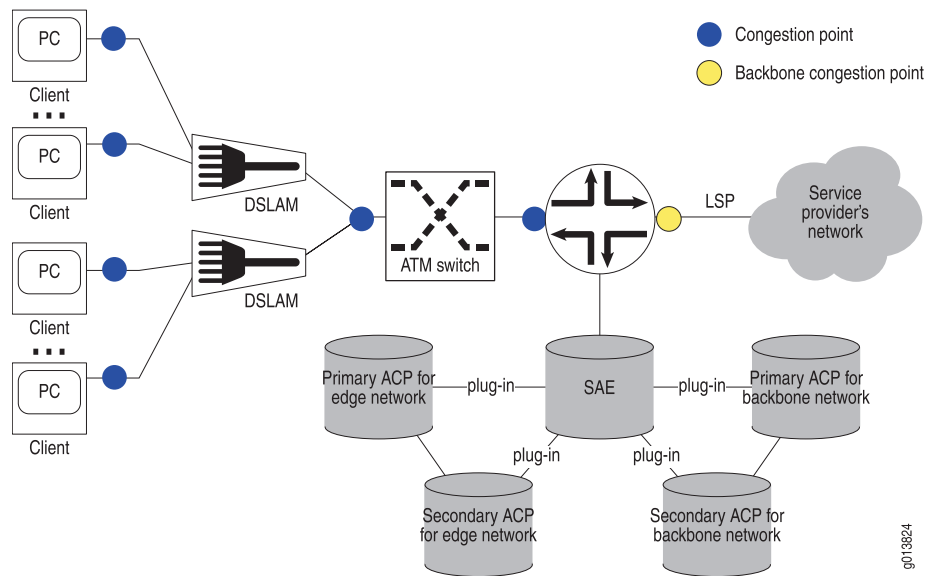
SRC ACP authorizes and tracks subscribers' use of the network resources that are associated with services that the SRC software manages. SRC ACP operates in two separate regions of the SRC network: the *edge* network and the *backbone* network. The edge network is the layer 2 access network through which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

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

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

[Figure 4 on page 23](#) shows a typical network topology.

Figure 4: Position of SRC ACP in the Network



Flat-File Accounting

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

Related Documentation

- [SRC Component Overview on page 9](#)

SRC Demonstration Applications

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

- [Enterprise Audit Plug-In on page 23](#)
- [Enterprise Manager Portal on page 24](#)
- [Monitoring Agent Application on page 24](#)
- [Sample Enterprise Service Portal on page 25](#)
- [Residential Service Selection Portals on page 25](#)

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.

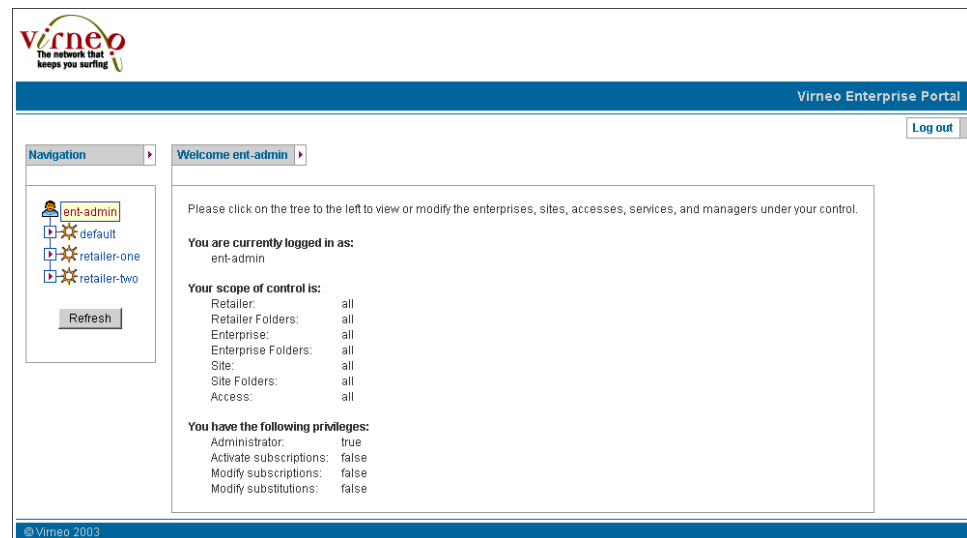
You can write audit plug-in event listeners by implementing the callback interface. A listener performs tasks such as processing received events and then publishing the events to one or more event handlers, such as a log file, system log, or database. Events are sent after the corresponding operations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

Enterprise Manager Portal

Enterprise Manager Portal is an application that allows service providers to provision services for enterprise subscribers on routers running JunosE or Junos OS and that allows IT managers to manage services. This Enterprise Manager Portal is a complete application that requires little customization.

Figure 5 on page 24 shows a sample page in the Enterprise Manager Portal.

Figure 5: Sample Page in Enterprise Manager Portal



You can use the Enterprise Manager Portal with the NAT Address Management Portal to allow service providers to manage public IP addresses for use with NAT services on routers running Junos OS 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.

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

Sample Enterprise Service Portal

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

Residential Service Selection Portals

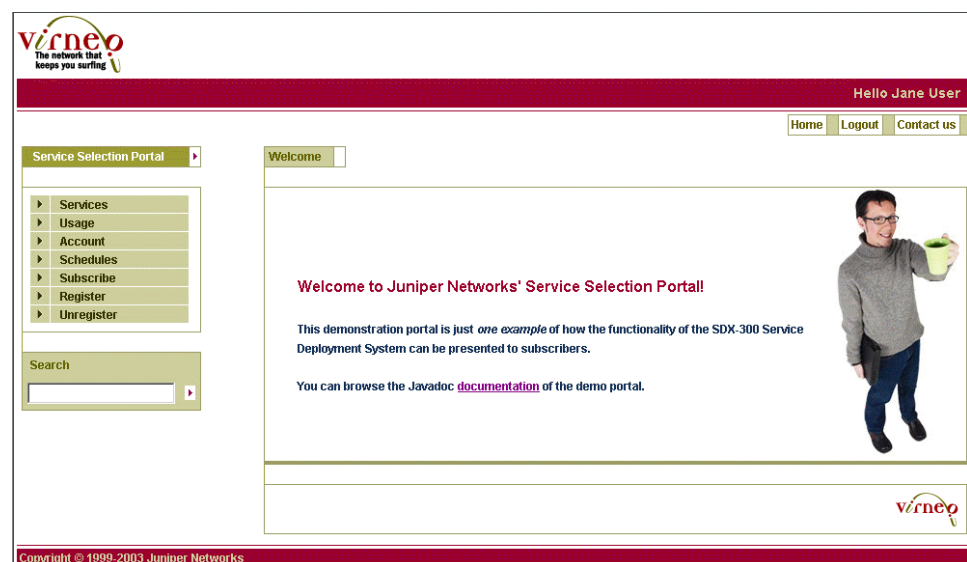
A residential portal is a Web portal application designed for use by individual subscribers to manage their subscriptions to Internet services and to log in to and out of a subscriber session. The portal pages, which are dynamically generated from information stored for subscribers, give subscribers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

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

The SRC software provides examples of residential portals.

Figure 6 on page 25 shows a residential Web portal that could be created with the SRC software.

Figure 6: Sample Residential Web Portal



Web-based residential portals that you develop for the SRC software are compatible with PDAs. [Figure 7 on page 26](#) shows a login page for a sample residential portal that is being accessed from a PDA.

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



Related Documentation

- [SRC Component Overview on page 9](#)

Other Applications

Other companies have created applications for use with the SRC software. For information about applications created by Juniper Networks partners, see <https://www.juniper.net/us/en/partners/>.

Related Documentation

- [SRC Component Overview on page 9](#)

PART 2

SRC Software as Virtual Machine

- [Managing the SRC Software as a Virtual Machine on page 29](#)

CHAPTER 3

Managing the SRC Software as a Virtual Machine

- [Virtualized SRC Software Overview on page 29](#)
- [System Requirements for a Virtualized SRC Software on page 29](#)
- [Creating a Virtualized SRC Instance on page 31](#)
- [Creating a Snapshot of qcow2 Image on page 36](#)

Virtualized SRC Software Overview

You can deploy the SRC software as a virtual machine and manage SRC functionalities. The virtualized SRC software can be created through an iso, qcow2, or vmdk image.



NOTE: All hardware-specific commands (such as show disk status) display an appropriate error message when executed in a virtualized SRC software. Virtualized SRC software does not support hardware-related alarms or traps (such as diskFailure).

The SRC software installation is currently supported and tested over the VMware Workstation 12 Player, VMware Workstation 12 Pro, VMware ESXi 5.5.0, 6.0, and 6.5, and Kernel-based Virtual Machine (KVM) hypervisor on CentOS 7.6.

The SRC software does not have any hypervisor management tool. You can make use of the existing tools such as virsh and virt-manager, VMware vSphere client, and VMware Workstation Player.

Related Documentation

- [SRC Product Description on page 3](#)
- [Creating a Virtualized SRC Instance on page 31](#)
- [System Requirements for a Virtualized SRC Software on page 29](#)

System Requirements for a Virtualized SRC Software

The system requirements for a virtualized SRC software are:



NOTE: We recommend you to allocate CPU cores, RAM, and hard disk space as same as that of C Series Controllers to attain better performance.

- [Hard Disk Requirement on page 30](#)
- [Memory Requirements on page 30](#)
- [CPU Requirements on page 31](#)

Hard Disk Requirement

The qcow2 image and vmdk image (of subtype monolithicSparse) grow in size up to 250 GB when used on a virtual machine, so you must have more than 250 GB of disk space in the host operating system if you use the qcow2 or vmdk image.

If you are using an SRC iso image, we recommend you to have around 250 GB of disk space allocated to the virtualized SRC software to have enough space for system and component logs.

Memory Requirements

[Table 6 on page 30](#) lists the default heap size allocated for SRC components on a virtualized SRC software.

Table 6: Heap Allocation for SRC Components on a Virtualized SRC Software

SRC Component	Default Heap Size on Virtualized SRC Software	Heap Size Adjustable or Not
SRC ACP	64 MB	Yes
SNMP agent	160 MB	No
Web application server	616 MB	No
CLI	200 MB	No
Diameter server	600 MB	No
External subscriber monitor	160 MB	Yes
3GPP Gateway	200 MB	No
IMS Services Gateway	200 MB	No
License server	1 GB or smaller than one-fourth of physical memory	No
NIC	128 MB	Yes
SAE	70% of free memory	Yes

Table 6: Heap Allocation for SRC Components on a Virtualized SRC Software (continued)

SRC Component	Default Heap Size on Virtualized SRC Software	Heap Size Adjustable or Not
C-Web interface	200 MB	No



NOTE: In a virtualized SRC software, the default heap size is set only for the Java components and not for the non-Java components such as redirect server.

The memory requirements of the virtualized SRC software based on the default heap size allocation are:

- At least 2927 MB of memory is required for all Java components other than the SAE and license server.
- Subscriber management capacity of the virtualized SRC software depends on the heap size of the SAE. We recommend you to allocate enough heap size for SAE.
- 1 GB of memory is required for the license server.

CPU Requirements

You must allocate a minimum of one CPU core for a virtualized SRC software. You can allocate CPU cores same as that of C Series Controller to attain better performance. The CPU cores available in C Series Controllers are:

- C2000—4
- C3000—8
- C5000—24

Related Documentation

- [Virtualized SRC Software Overview on page 29](#)

Creating a Virtualized SRC Instance

You can create a virtualized SRC instance by using the iso, qcow2, or vmdk image.



NOTE: We recommend you to create a virtualized SRC instance by using the qcow2 image.

- [Creating a Virtualized SRC Instance Using qcow2 Image on page 32](#)
- [Creating a Virtualized SRC Instance Using iso Image on page 33](#)
- [Creating a Virtualized SRC Instance Using the vmdk Image on page 35](#)

Creating a Virtualized SRC Instance Using qcow2 Image

To create a virtualized SRC instance on the KVM hypervisor by using the qcow2 image:

1. Download the qcow2.gz image from <https://www.juniper.net/support/downloads/?p=src#sw> and place it on the host operating system.

2. Unzip the image on the host operating system.

```
gunzip name.qcow2.gz
```

3. Download the SDK+AppSupport+Demos+Samples.tar.gz file from <https://www.juniper.net/support/downloads/?p=src#sw> and place it on the host operating system.

4. Untar the file to use the create_vm.py script for creating a virtualized SRC instance.

```
tar -xvzf SDK+AppSupport+Demos+Samples.tar.gz
```

5. Execute the create_vm.py script from the path where the SDK+AppSupport+Demos+Samples.tar.gz is extracted.

```
#$cd <sdk_root_folder>/SDK/vSRC/  
#$. /create_vm.py
```



NOTE: The create_vm.py script is not supported for VMware virtual machine creation. To create a virtualized SRC instance on VMware hypervisor, use the iso or vmdk image.

The script requests various details for creating the virtualized SRC instance.

6. Enter the requested details. The details requested by the script are:
 - Name for the virtualized SRC instance
 - Number of CPUs to be allocated for the virtualized SRC instance
 - Memory (in megabytes) to be allocated for the virtualized SRC instance
 - Network configuration details:
 - Number of interfaces to be configured
 - Media access control (MAC) address for each interface. You can enter MAC address or allow the script to create the MAC address automatically.
 - Networking mode for each interface. The supported modes are:

- Direct host device mapping with bridge mode—Use this mode if multiple network interfaces have to be shared with a host device (for example, eth0 for CentOS 6 and enpX/ensX for CentOS 7). This mode is ideal for hosting multiple virtualized SRC instances with multiple interfaces. This is the default mode.
- Direct host device mapping with passthrough mode—In this mode, one-to-one mapping is done between the host device network interface and virtualized SRC instance's network interface. You can use this mode when only one virtualized SRC instance is hosted in the server.
- Shared bridge mapping (bridge has to be manually configured)—In this mode, you have to manually configure the bridge and provide the shared bridge name as an input. This mode provides flexibility to have more complex networking.
- Path of the qcow2 image file

The script creates an xml file with the name of the virtualized SRC instance and creates the virtualized SRC instance by using the **virsh** command. The xml file contains one serial console configuration and one vnc console configuration.



NOTE: You must have the virsh management tool in the host operating system for the script to successfully create the virtualized SRC instance.

7. Log in to the virtualized SRC instance through any hypervisor management tool and set up the initial configuration for the SRC software. For information about the initial configuration, see your *C Series Controller Hardware Guide*.

Creating a Virtualized SRC Instance Using iso Image

To create a virtualized SRC instance on VMware and KVM hypervisors by using the iso image:

1. Download the iso image from <https://www.juniper.net/support/downloads/?p=src#sw> and place it in the host operating system.
2. Start installing the iso image in the virtual machine by using the hypervisor management tool (such as virt-manager, virsh, VMware vSphere client, and VMware Workstation Player). The virtual machine boots from the iso image and prints the following message:

```
Welcome to SRC PE Software Installation.
```

```
WARNING: This system recovery software replaces all data and software
on the system disk image. As a result, any data, including data
previously in the snapshot partition, is lost.
```

```
After you run the system installation software, the virtual image
contains the SRC software, including the SRC operating system,
but no configuration data.
```

To continue, press <TAB> and choose the installation type.

To enable serial console enter following after choosing the Installation type :

```
"console=tty0 console=tty50, 9600
```

To cancel this operation, power off the system and remove the iso image.

boot:

AUTO Manual rescue

boot:

3. At the boot prompt, type the installation option.

- If the typed option is AUTO, the disk space is partitioned automatically and the packages are installed. The following hard disk partition scheme is used:
 - /—8.5 GB
 - /var—50 percent of remaining hard disk space
 - 50 percent of remaining hard disk space can be used for storing snapshots
- If the typed option is Manual, you can define the partition scheme and other general settings (such as language) through the displayed dialog boxes to install the SRC software.



NOTE: You cannot create snapshot or restore snapshot with custom partition scheme. We recommend you to use the `virsh snapshot-create` command on KVM hypervisor and use the **Snapshot** option in the VMware Workstation Pro or VMware ESXi hypervisor to maintain snapshots of disk image.

4. After the successful installation, reboot the virtual machine.



NOTE: On VMware, CentOS 7 and later versions use different schemes for naming network interfaces, for example, `enpX`, `ensX`, and `enoX`. SRC works only with the traditional naming `ethX`. So, it is mandatory to rename the interfaces from `ensX`, `enpX`, or `enoX` to `ethX` and persist interface names with the corresponding MAC addresses. After the software installation is complete, the interface renaming script is executed for renaming the interfaces.

5. (Only for VMware) After the interface renaming script is executed, configure the corresponding MAC address for each network interface (for example, `eth0`, `eth1`).

After verifying the configuration of MAC addresses, reboot the C Series Controller for the changes to take effect.

6. After the virtual machine reboots, set up the initial configuration. For information about the initial configuration, see your *C Series Controller Hardware Guide*.



NOTE: The default username and password for grub menu are “root” and “password”, respectively. You can change the default password by executing the `grub2-setpassword` command in shell mode.

Creating a Virtualized SRC Instance Using the vmdk Image

Virtual Machine Disk (vmdk) is a file format that describes containers for virtual hard disk drives to be used in VMware virtual machines. The vmdk image shipped with the SRC software is of the `monolithicSparse` type, and the image has been tested with `monolithicSparse` and `monolithicFlat` types. If you are using VMware ESXi, either the iso image or the vmdk image of `monolithicFlat` type must be used. To convert the `monolithicSparse` type to the `MonolithicFlat` type, you can use one of the following commands:

- `qemu-img convert -f vmdk vmdk-file-name-MonolithicSparse -O vmdk output-flat-file-name -o subformat={ monolithicFlat }`

You must execute this command in a Linux machine by installing the `qemu-img` tool, and then the output flat file needs to be transferred to the ESXi server.

- `vmkfstools -i MonolithicSparse-file-name output-flat-file-name`

This command can be executed in the ESXi server itself.



NOTE: While using the `qemu-img` or `vmkfstools` command, the output flat file name should not contain the suffix “-flat.vmdk”.



NOTE: The SRC software installation is currently supported and tested over the VMware Workstation 12 Player, VMware Workstation 12 Pro, and VMware ESXi 5.5.0, 6.0, and 6.5.

To create a virtualized SRC instance on VMware hypervisor by using the vmdk image:

1. Download the vmdk image from <https://www.juniper.net/support/downloads/?p=src#sw> and place it in the host operating system.
2. Using VMware vSphere client or VMware workstation player, create a new virtual machine with custom configurations (RAM, CPU, network, and so on). Provide the path of the downloaded vmdk image in the Virtual Disk section.



NOTE: The following settings have been tested by Juniper Networks:

- Network Connection—Bridged Networking
 - I/O Controller Type—LSI Logic
 - Virtual Disk Type—SCSI
 - OS—CentOS (64-bit)
-

3. Power on the virtual machine to start the SRC software.
 4. After the virtual machine boots, set up the initial configuration. For information about the initial configuration, see your *C Series Controller Hardware Guide*.
-



NOTE: You cannot create snapshot or restore snapshot with custom partition scheme. We recommend you to use the **Snapshot** option in the VMware Workstation Pro or VMware ESXi to maintain snapshots of disk image.

The virtual machine gets paused while creating snapshots. We recommend you to disable the Juniper Networks database (jdb component) and components involved in service activities during snapshot creation.

Related Documentation • [Virtualized SRC Software Overview on page 29](#)

Creating a Snapshot of qcow2 Image

You can create and maintain one or more snapshots of the qcow2 image to serve as a backup.

To create a snapshot of the qcow2 image:

- Execute the **snapshot_Qcow2.py** script from the path where the SDK+AppSupport+Demos+Samples.tar.gz is extracted.

The script asks for the name of the virtualized SRC instance and the path where you want to store the snapshot.

```
user@host>cd <sdk_root_folder>/SDK/vSRC/
user@host>./snapshot_Qcow2.py
Enter the name of the VM : VM-name
Enter the path to store backup image : storage-path

Domain snapshot qcow2-snap created
sending incremental file list
SRC-PE-MAIN-A-1614-x86_64.qcow2
      7.35G 100% 150.51MB/s   0:00:46 (xfer#1, to-check=0/1)

sent 7.35G bytes  received 31 bytes  158.09M bytes/sec
total size is 7.35G  speedup is 1.00
Snapshot is created successfully and placed in backup location
Domain lvm3 defined from ./lvm3.xml
```



NOTE: Before creating the snapshot of the qcow2 image, make sure that the hard disk free space is double the size of the qcow2 image. Otherwise, the script displays an error message.

The virtual machine gets paused while creating snapshots. We recommend you to disable the Juniper Networks database (jdb component) and components involved in service activities during snapshot creation.

Related Documentation

- [Virtualized SRC Software Overview on page 29](#)
- [Creating a Virtualized SRC Instance on page 31](#)
- [Creating a Snapshot of Files on a C Series Controller on page 200](#)
- [Restoring the Files in a Snapshot on page 212](#)
- [Deleting the Files in a Snapshot on page 213](#)

PART 3

Managing Your C Series Controller

- [Planning a Deployment of C Series Controllers on page 41](#)
- [Configuring a C Series Controller on page 45](#)
- [Accessing and Starting the SRC CLI on page 51](#)
- [Accessing and Using the C-Web Interface on page 63](#)
- [Configuring Remote Access to a C Series Controller \(SRC CLI\) on page 83](#)

CHAPTER 4

Planning a Deployment of C Series Controllers

- [Components in an SRC Deployment on page 41](#)
- [Considerations When Planning a Deployment of C Series Controllers on page 42](#)
- [Deployment Scenario on page 43](#)

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:

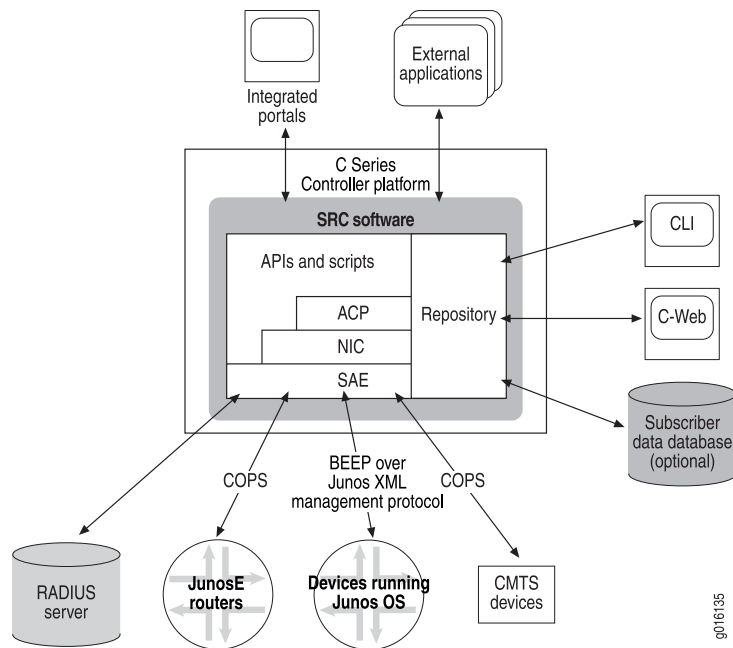
- Admission Control Plug-in
- Juniper Policy Server
- Network information collector
- Redirect server
- SAE
- SNMP agent
- Policies, services, subscribers, and subscriptions management

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

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

[Figure 8 on page 42](#) illustrates the interaction of the various components in an SRC environment that includes a C Series Controller.

Figure 8: C Series Controller and Related Components



- Related Documentation**
- [SRC Server Components on page 12](#)
 - [Considerations When Planning a Deployment of C Series Controllers on page 42](#)
 - [Configuring SRC Components on page 47](#)

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 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—Routers running JunosE Software 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.

**Related
Documentation**

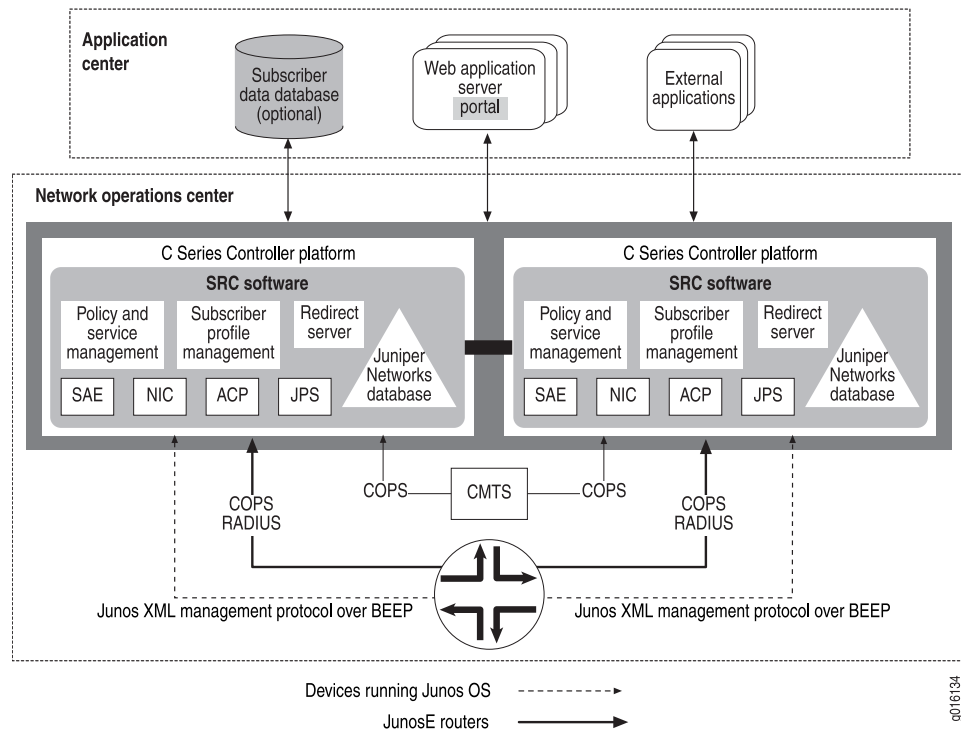
- [SRC Server Components on page 12](#)
- [Components in an SRC Deployment on page 41](#)
- [Before You Begin Configuring the SRC Software on a C Series Controller on page 45](#)

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. Devices, RADIUS servers, and CMTS devices may also reside at the same site or at another location. Subscriber databases and external applications probably reside on servers located with other servers external to a network operations center.

Figure 9 on page 44 shows how C Series Controllers can be deployed. The example shows two platforms in a network operations center. Any number of C Series Controllers can be deployed at one or more sites.

Figure 9: Deployment Scenario for C Series Controllers



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

Related Documentation

- [Components in an SRC Deployment on page 41](#)
- [Considerations When Planning a Deployment of C Series Controllers on page 42](#)
- [Configuring SRC Components on page 47](#)

CHAPTER 5

Configuring a C Series Controller

- [Before You Begin Configuring the SRC Software on a C Series Controller on page 45](#)
- [Configuring the SRC Software on page 46](#)
- [Configuring SRC Components on page 47](#)

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
 - Domain name system
 - Eth0 interface
 - Clock synchronization (Configure the NTP server and verify the clock.)
 - SSH access
- 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.

- 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.

**Related
Documentation**

- *C Series Controller Hardware Guide*
- *Before You Start the SRC CLI*
- [Configuring the SRC Software on page 46](#)
- [Configuring SRC Components on page 47](#)
- [Components in an SRC Deployment on page 41](#)
- *How the SRC Configuration Is Stored*

Configuring the SRC Software

To configure the 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 {
    ssh {
      root-login allow;
    }
  }
}
```

...

Make any updates needed to the initial configuration.

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

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

Do not use the root account for normal operation.

3. If the time zone is not set to the time zone where the system resides, set the time zone.
See [“Setting the Time Zone \(SRC CLI\)” on page 133](#).

4. Configure NTP.

See [“Configuring NTP on a C Series Controller” on page 136.](#)

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

See [“Juniper Networks Database Overview” on page 163.](#)

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 [“External Interfaces on a C Series Controller Overview” on page 83](#), [“Configuring Gigabit Ethernet Interfaces for IPv4 \(SRC CLI\)” on page 85](#), [“Configuring Gigabit Ethernet Interfaces for IPv6 \(SRC CLI\)” on page 87.](#)

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

See [“Configuring a Static Route to Devices on Other Networks \(SRC CLI\)” on page 95.](#)

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

See [“Securing Connections Between a C Series Controller and Remote Hosts” on page 96](#), [“Configuring a C Series Controller to Accept SSH Connections \(SRC CLI\)” on page 97.](#)

9. (Optional) Configure the system log server.

See [“C Series Controller Log Server Overview” on page 155.](#)

10. (Optional) Configure user accounts.

See [“SRC User Accounts Overview” on page 235.](#)

11. Configure components.

See [“Configuring SRC Components” on page 47.](#)

Related Documentation

- [Before You Begin Configuring the SRC Software on a C Series Controller on page 45](#)
- [How the SRC Configuration Is Stored](#)

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.
2. Configure SAE local properties.

See [“Initially Configuring the SAE” on page 189.](#)

3. Obtain your SRC software license.
See [“Types of SRC Licenses” on page 105](#) and [“Obtaining an SRC License” on page 106](#).
4. Install the license, and start the license server if you have a server license.
See [“Installing Server Licenses for C Series Controllers \(SRC CLI\)” on page 121](#).
5. (Optional) Configure and start the SRC SNMP agent.
See [“Configuring the SRC SNMP Agent \(SRC CLI\)” on page 287](#).
6. Start the SAE.
See [“Starting the SAE \(SRC CLI\)” on page 196](#).
7. If you use firewall software on your internal network, review firewall access for SRC components.
See [“Port Settings for SRC Components” on page 99](#).
8. Configure other SRC components.
[Table 7 on page 48](#) lists the principle SRC components that you can configure and names the document that provides information about configuring the components, typically from the CLI.

Table 7: Configuration Information for Other SRC Components

Component	Document
SRC ACP	<i>Configuring SRC ACP (SRC CLI)</i>
C-Web interface	“Enabling the C-Web Interface” on page 70 “Accessing the C-Web Interface” on page 67
Network information collector (NIC)	<i>Configuring the NIC (SRC CLI)</i>
Policies	<i>Configuring Policy Groups (SRC CLI)</i> <i>Configuring Policy Lists (SRC CLI)</i>
Redirect server	<i>Configuring the Redirect Server (SRC CLI)</i>
SAE	“Initially Configuring the SAE” on page 189 <i>Configuring the SAE to Manage Devices Running Junos OS (SRC CLI)</i> <i>Configuring the SAE to Manage JunosE Routers (SRC CLI)</i>
SAE access to external database that stores subscriber data	<i>Configuring LDAP Access to Directory Data (SRC CLI)</i>

Table 7: Configuration Information for Other SRC Components (continued)

Component	Document
Services	<i>Adding a Normal Service (SRC CLI)</i>
	<i>Adding an Infrastructure Service (SRC CLI)</i>
	<i>SRC Aggregate Services Overview</i>
Subscribers and subscriptions	<i>Adding Subscribers (SRC CLI)</i>
	<i>Configuring Subscriptions (SRC CLI)</i>
Enterprise Service Portals	<i>SRC PE Solutions Guide</i>

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

**Related
Documentation**

- [Before You Begin Configuring the SRC Software on a C Series Controller on page 45](#)
- [Configuring the SRC Software on page 46](#)
- [Viewing C Series Controller Information](#)
- [SRC Component Overview on page 9](#)

CHAPTER 6

Accessing and Starting the SRC CLI

- [Configuring Access to the SRC CLI Overview on page 51](#)
- [Configuration Statements for SRC CLI Directory Access on page 52](#)
- [Changing Access to the Directory that Stores SRC Configuration Data on page 52](#)
- [Verifying the Configuration for SRC Directory Access on page 54](#)
- [Starting the SRC CLI on page 55](#)
- [Policies, Services, and Subscribers CLI on page 56](#)
- [Configuring a Schedule for Executing the Commands or Scripts \(SRC CLI\) on page 58](#)

Configuring Access to the SRC CLI Overview

The SRC CLI is the management and configuration interface on C Series Controllers. Most SRC configuration data is stored in the Juniper Networks database on the C Series Controller. When you use the Juniper Networks database, you can use the default configuration to connect to the directory. You can add backup directories and change the password to the directory.

The CLI for policies, services, and subscribers requires that you configure access to and explicitly start the Policies, Services, and Subscribers CLI.

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

- [Accessing the SRC CLI When Using an External Directory Server on page 51](#)

Accessing the SRC CLI When Using an External Directory Server

By default, the SRC software uses the local Juniper Networks database to authenticate access to the SRC CLI. The SRC software can also use an external directory server to authenticate access to the SRC CLI. To use an external directory server to authenticate access to the SRC CLI, you need to define the URL to the external directory server using the **set url url** command under the **[edit system ldap client]** hierarchy. You can also define access to backup directory servers by using the **set backup-urls backup-url-n backup-url-n2** command under this hierarchy. After you configure access to the external directory server, the SRC software uses this server to authenticate access to the SRC CLI instead of the local Juniper Networks database. If the primary external directory server is down and you have configured a backup, the SRC software uses the backup server to authenticate access to the SRC CLI.

- Related Documentation**
- [Policies, Services, and Subscribers CLI Overview on page 56](#)
 - [SRC User Accounts Overview on page 235](#)
 - [Configuration Statements for SRC CLI Directory Access on page 52](#)
 - [SRC PE CLI Command Reference](#)

Configuration Statements for SRC CLI Directory Access

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

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



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

The eventing statement is enabled by default.

- Related Documentation**
- [Changing Access to the Directory that Stores SRC Configuration Data on page 52](#)
 - [Configuring Access to the SRC CLI Overview on page 51](#)

Changing Access to the Directory that Stores SRC Configuration Data

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

```
system ldap client {  
  base-dn base-dn ;  
  url url ;
```

```

backup-urls [ backup-urls ...];
principal principal ;
credentials credentials ;
timeout timeout ;
time-limit time-limit ;
}

```



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

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

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

```

[edit]
user@host# edit system ldap client

```

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

```

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

```

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

```

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

```

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

```

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

```

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

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

```

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

```

For example:

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

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

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

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

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

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

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

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



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

The eventing statement is enabled by default.

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

**Related
Documentation**

- [Verifying the Configuration for SRC Directory Access on page 54](#)
- [Configuring Access to the SRC CLI Overview on page 51](#)
- [Juniper Networks Database Overview on page 163](#)

Verifying the Configuration for SRC Directory Access

Purpose Verify the configuration for directory connections.

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

```
[edit]
```

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

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

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

- Related Documentation**
- [Changing Access to the Directory that Stores SRC Configuration Data on page 52](#)
 - [Viewing Information About the SRC CLI \(C-Web Interface\)](#)

Starting the SRC CLI

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

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

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



NOTE: If you enter an incorrect password, you are prompted to enter an LDAP password.

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 #.

For information about the SRC CLI, see *SRC CLI Overview*.

**Related
Documentation**

- *Before You Start the SRC CLI*
- *Displaying Commands*
- *Viewing Information About the SRC CLI (C-Web Interface)*
- *Understanding SRC Command and Statement Hierarchies*
- [Starting the Policies, Services, and Subscribers CLI on page 57](#)

Policies, Services, and Subscribers CLI

- [Policies, Services, and Subscribers CLI Overview on page 56](#)
- [Configuring Access to the Policies, Services, and Subscribers CLI on page 56](#)
- [Starting the Policies, Services, and Subscribers CLI on page 57](#)
- [Configuring Directory Eventing for Policy Editor on page 58](#)

Policies, Services, and Subscribers CLI Overview

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

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



NOTE: You must not disable the Juniper Networks database (jdb component) when configuring policies with the Policies, Services, and Subscribers Editor.

See Also

- [Configuring Access to the SRC CLI Overview on page 51](#)
- [Configuring Access to the Policies, Services, and Subscribers CLI on page 56](#)
- [Starting the Policies, Services, and Subscribers CLI on page 57](#)

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

- See Also**
- [Starting the Policies, Services, and Subscribers CLI on page 57](#)
 - [Viewing Information about Users Logged Into the SRC Software](#)
 - [Policies, Services, and Subscribers CLI Overview on page 56](#)
 - [Configuring Access to the SRC CLI Overview on page 51](#)

Starting the Policies, Services, and Subscribers CLI

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

See [“Configuring Access to the Policies, Services, and Subscribers CLI” on page 56](#).

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

To start the Policies, Services, and Subscribers CLI:

- Enter the **enable component** command.

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

- See Also**
- [Configuring Access to the Policies, Services, and Subscribers CLI on page 56](#)
 - [Policies, Services, and Subscribers CLI Overview on page 56](#)

Configuring Directory Eventing for Policy Editor

Use the following configuration statements to configure directory eventing for the policy editor:

```
system services editor policy-editor {  
    directory-eventing;  
}
```

To configure directory eventing for the policy editor:

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

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

2. Enable directory eventing for the policy editor to automatically discover the changes in the directory.

```
[edit system services editor policy-editor]  
user@host# set directory-eventing
```

3. (Optional) Verify your configuration.

```
[edit system services editor policy-editor]  
user@host# show  
directory-eventing;
```

- See Also**
- [Starting the Policies, Services, and Subscribers CLI on page 57](#)
 - [Configuring Access to the Policies, Services, and Subscribers CLI on page 56](#)
 - [Viewing Information about Users Logged Into the SRC Software](#)
 - [Policies, Services, and Subscribers CLI Overview on page 56](#)
 - [Configuring Access to the SRC CLI Overview on page 51](#)

Configuring a Schedule for Executing the Commands or Scripts (SRC CLI)

To periodically execute the SRC CLI commands or scripts according to a given schedule, use the **system schedule *schedule-name*** command. You can use the redirection operator (**>**) with the commands or scripts to redirect the command execution output to a file.

Use the following statements to schedule a repetitive task on an SRC system:


```

system schedule schedule-name {
    day-of-week day-of-week;
    month month;
    day-of-month day-of-month;
    hour hour;
    minute minute;
    special (reboot | yearly | annually | monthly | weekly | daily | midnight | hourly);
    command command;
    script script;
}

```

To periodically execute the commands or scripts according to a given schedule:

1. In configuration mode, enter the name of the schedule that is capable of adding schedule entries for the executable scripts or commands. A schedule name can contain alphanumeric characters only. In this sample procedure, **src1cron** is the name of the schedule.

```

[edit]
user@host# edit system schedule src1cron

```

2. (Optional) Enter the day of the week on which you want the command or script sequence to execute. The default value is * (asterisk).

```

[edit system schedule src1cron]
user@host# set day-of-week day-of-week

```

3. (Optional) Enter the month of the year in which you want the command or script sequence to execute. The default value is * (asterisk).

```

[edit system schedule src1cron]
user@host# set month month

```

4. (Optional) Enter the day of the month on which you want the command or script sequence to execute. The default value is * (asterisk).

```

[edit system schedule src1cron]
user@host# set day-of-month day-of-month

```

5. (Optional) Enter the hour of the day at which you want the command or script sequence to execute. The default value is * (asterisk).

```

[edit system schedule src1cron]
user@host# set hour hour

```

6. (Optional) Enter the minute at which you want the command or script sequence to execute. The default value is * (asterisk).

```
[edit system schedule src1cron]
```

```
user@host# set minute minute
```

[Table 8 on page 60](#) lists the values allowed for the periodic strings (such as **day-of-week**, **month**, **day-of-month**, **hour**, and **minute**).

Table 8: Values Allowed for the Periodic Strings

Options	Values
day-of-week	0–7 (where both 0 and 7 mean Sunday) or SUN-SAT
month	1–12 or JAN-DEC
day-of-month	1–31
hour	0–23
minute	0–59

You can use multiple combinations of the special characters described in [Table 9 on page 60](#).

Table 9: Available Special Characters

Special Characters	Meaning
*	Indicates all values. For example, to execute the command or script every hour: user@host# set hour *
/	Indicates the increments of ranges. For example, to execute the command or script at the third minute of the hour and every 15 minutes thereafter: user@host# set minute 3-59/15
,	Indicates to separate the values of a list. For example, to execute the command or script on Mondays, Wednesdays and Fridays: user@host# day of week MON,WED,FRI
-	Indicates the ranges. For example, to execute the command or script every hour from 3 through 10: user@host# set hour 3-10

7. (Optional) Enter the special string values such as **reboot**, **yearly**, **annually**, **monthly**, **weekly**, **daily**, **midnight**, and **hourly** at which you want the command or script sequence to execute.

For example, to execute the command or script at midnight on the first day of each month:

```
[edit system schedule src/cron]
user@host# set special-string monthly
```



NOTE: If you configure both special string values and periodic string values (such as **day-of-week**, **month**, **day-of-month**, **hour**, or **minute** options), a message indicating that both special strings and periodic strings cannot be defined is displayed when you commit the changes.

Table 10 on page 61 lists the special string options.

Table 10: Special String Options

Options	Description
reboot	Executes the command or script at boot and reboot of the system.
yearly	Executes the command or script at midnight, January 1 each year.
annually	Executes the command or script at midnight, January 1 each year.
monthly	Executes the command or script at midnight on the first day of each month.
weekly	Executes the command or script at midnight each Sunday.
daily	Executes the command or script at midnight each day.
midnight	Executes the command or script at midnight each day.
hourly	Executes the command or script at on the first second of every hour.

8. Configure the complete path of the script to be executed for the schedule.



NOTE: The **script** and **command** options are mutually exclusive. You cannot configure both options at the same time.

```
[edit system schedule src/cron]
user@host# set script script
```



NOTE: The CLI editing level must be set to expert by using the `set cli level expert` command for this option.

9. Configure the CLI command to be executed for the schedule.



NOTE:

- The script and command options are mutually exclusive. You cannot configure both options at the same time.

Before you configure a CLI command for the schedule, perform the following steps to make sure that you can configure the CLI command as part of the schedule execution:

1. Enter the CLI command in the shell with the `cli -c "command name"` option.
2. Verify whether the CLI command returns the expected output.

```
[edit system schedule src1cron]
user@host# set command command
```

10. (Optional) Verify your configuration.

```
user@host# show
src1cron {
  command show;
  day-of-month 7;
  day-of-week 5;
  hour 11;
  minute 0;
  month 12;
}
```

- Related Documentation**
- [SRC Script Services Overview](#)
 - [SRC CLI Overview](#)

CHAPTER 7

Accessing and Using the C-Web Interface

- [C-Web Interface Overview on page 63](#)
- [Navigating the C-Web Interface on page 64](#)
- [Accessing the C-Web Interface on page 67](#)
- [Enabling the C-Web Interface on page 70](#)
- [Starting the C-Web Interface on page 70](#)
- [Policies, Services, and Subscribers Subtasks in the C-Web Interface on page 71](#)
- [Getting Help in the C-Web Interface on page 72](#)
- [Changing a Username or Password for the C-Web Interface on page 73](#)
- [Enabling Remote Users to Access the C-Web Interface on page 73](#)
- [Modifying the Editing Level in the C-Web Interface on page 74](#)
- [Displaying Icons for Objects in the C-Web Interface on page 75](#)
- [Editing SRC Configurations \(C-Web Interface\) on page 76](#)
- [Modifying Objects in the C-Web Interface on page 79](#)
- [Configuring Logging Properties in the C-Web Interface on page 81](#)
- [Logging Out of the C-Web Interface on page 82](#)

C-Web Interface Overview

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

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

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

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

- Related Documentation**
- [Navigating the C-Web Interface on page 64](#)
 - [Policies, Services, and Subscribers Management Subtasks in the C-Web Interface Overview on page 71](#)
 - [Accessing the C-Web Interface on page 67](#)

Navigating the C-Web Interface

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

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

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

Layout of the C-Web Interface

Each page of the C-Web interface is divided into the following panes, as shown in [Figure 10 on page 64](#).

Figure 10: C-Web Layout



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

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

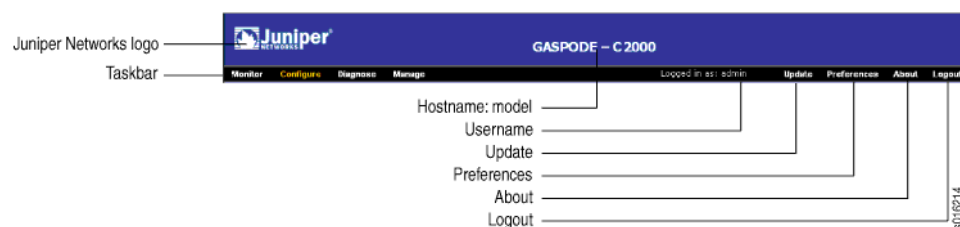
Elements of the C-Web Interface

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

Top Pane Elements

The top pane comprises the elements shown in [Figure 11 on page 65](#).

Figure 11: Top Pane Elements

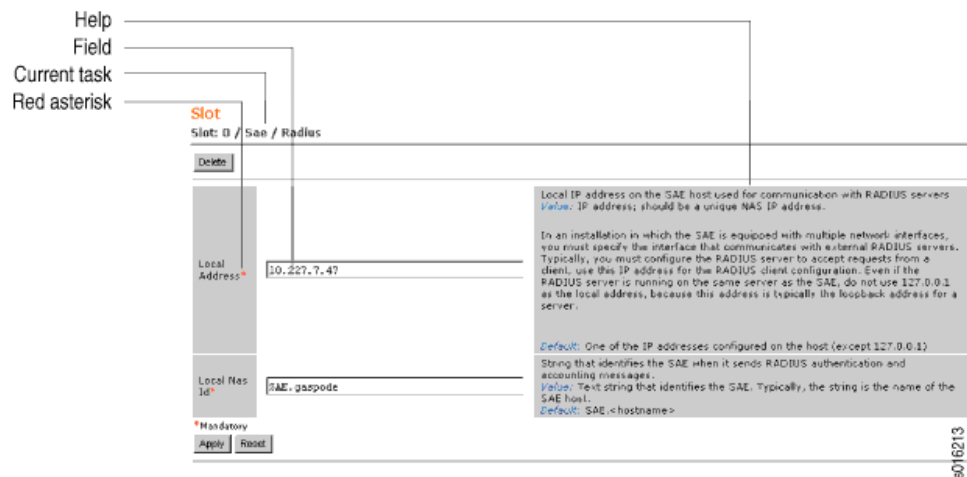


- Juniper Networks logo—Link to <https://www.juniper.net> in a new browser window.
- Taskbar—Menu of C-Web tasks:
 - Monitor—View monitoring information for core SRC components.
 - Configure—Configure SRC software on C Series Controllers.
 - Diagnose—Troubleshoot and test component settings.
 - Manage—Manage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

Main Pane Elements

The main pane comprises the elements shown in [Figure 12 on page 66](#).

Figure 12: Main Pane Elements

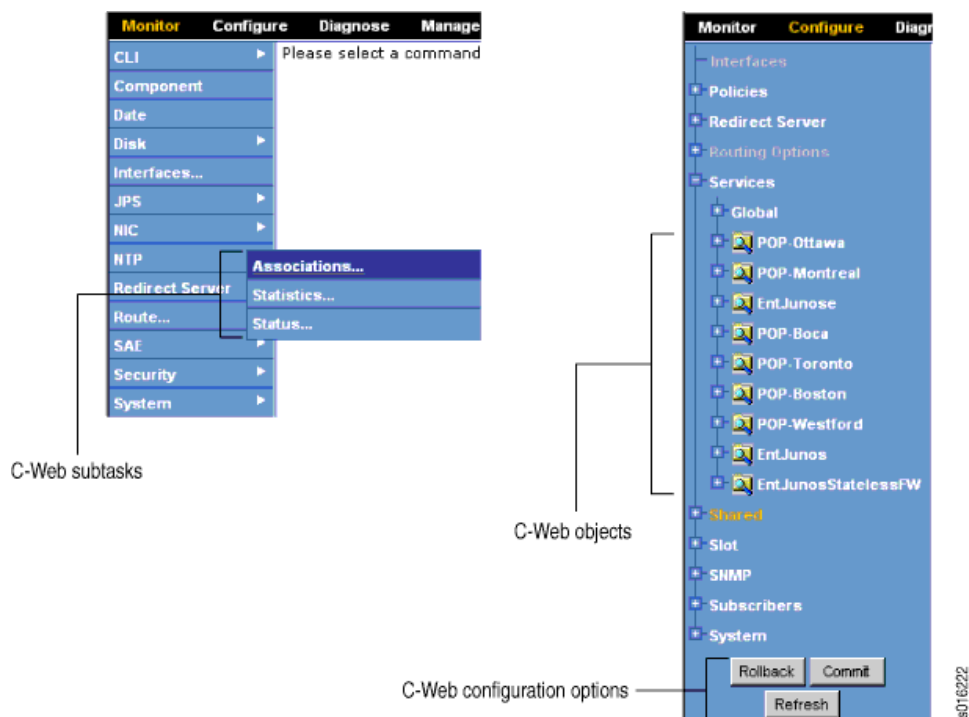


- Help—Displays field-specific information, such as the definition, format, and valid range of data in the field.
- Current task—Shows the successive C-Web tasks and subtasks you selected to display in the current main and side panes.
- Red asterisk (*)—Indicates a required field.

Side Pane Elements

The side pane comprises the elements shown in [Figure 13 on page 67](#).

Figure 13: Side Pane Elements



In the Monitor, Diagnose, and Manage side panes, each subtask displays options related to the selected task in the C-Web taskbar. In these side panes, click the arrow signs (>) to expand individual items. [Figure 13 on page 67](#) shows an example of the Monitor side pane.

In the Configure side pane, each subtask displays options related to the selected task in the C-Web taskbar. Objects represent configuration that you have created. For example, [Figure 13 on page 67](#) displays objects that represent services. Click the plus signs (+) to expand both individual subtasks and objects. Click the minus signs (–) to hide individual subtasks and objects.

To edit a configuration, click the configuration options buttons at the bottom of the Configure side pane. For more information, see [“Editing SRC Configurations \(C-Web Interface\)” on page 76](#).

Related Documentation

- [C-Web Interface Overview on page 63](#)
- [Getting Help in the C-Web Interface on page 72](#)

Accessing the C-Web Interface

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

Configuring Access to 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 [“Digital Certificates Overview” on page 275](#).

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

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

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

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

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

The default port for HTTPS is 443.

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

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

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

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

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

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

5. Configure logging for the C-Web interface.

See *Logging for SRC Components Overview*.

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

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



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

See [“SRC User Accounts Overview”](#) on page 235.

Configuring Access to the C-Web Interface Through HTTP

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

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

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

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

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

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

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

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

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

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

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

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

4. Configure logging for the C-Web interface.

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

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

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



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

**Related
Documentation**

- [Enabling the C-Web Interface on page 70](#)
- [Starting the C-Web Interface on page 70](#)
- [Configuring Access to Policies, Services, and Subscribers \(C-Web Interface\) on page 71](#)
- [Enabling Remote Users to Access the C-Web Interface on page 73](#)

Enabling the C-Web Interface

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

- Enter the **enable component** command.

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

**Related
Documentation**

- [Accessing the C-Web Interface on page 67](#)
- [Starting the C-Web Interface on page 70](#)
- [C-Web Interface Overview on page 63](#)

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.

- Related Documentation**
- [Accessing the C-Web Interface on page 67](#)
 - [Enabling the C-Web Interface on page 70](#)
 - [Logging Out of the C-Web Interface on page 82](#)
 - [C-Web Interface Overview on page 63](#)

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

- [Policies, Services, and Subscribers Management Subtasks in the C-Web Interface Overview on page 71](#)
- [Configuring Access to Policies, Services, and Subscribers \(C-Web Interface\) on page 71](#)
- [Starting Policies, Services, and Subscribers on page 72](#)

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

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

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

- See Also**
- [Getting Help in the C-Web Interface on page 72](#)
 - [*Enabling the Policy Configuration on the C-Web Interface*](#)
 - [*Enabling the Service Configuration on the C-Web Interface*](#)
 - [Starting Policies, Services, and Subscribers on page 72](#)
 - [Configuring Access to Policies, Services, and Subscribers \(C-Web Interface\) on page 71](#)

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

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

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

- See Also**
- [Accessing the C-Web Interface on page 67](#)
 - [Starting Policies, Services, and Subscribers on page 72](#)
 - [Policies, Services, and Subscribers Management Subtasks in the C-Web Interface Overview on page 71](#)

- [Getting Help in the C-Web Interface on page 72](#)

Starting Policies, Services, and Subscribers

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

To start the Policies, Services, and Subscribers subtasks:

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

- See Also**
- [Starting the C-Web Interface on page 70](#)
 - [Modifying the Editing Level in the C-Web Interface on page 74](#)
 - [Policies, Services, and Subscribers Management Subtasks in the C-Web Interface Overview on page 71](#)

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**.

- Related Documentation**
- [C-Web Interface Overview on page 63](#)
 - [Navigating the C-Web Interface on page 64](#)
 - [Policies, Services, and Subscribers Management Subtasks in the C-Web Interface Overview on page 71](#)

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**.

Related Documentation

- [Accessing the C-Web Interface on page 67](#)
- [Configuring Access to Policies, Services, and Subscribers \(C-Web Interface\) on page 71](#)
- [C-Web Interface Overview on page 63](#)
- [Enabling Remote Users to Access the C-Web Interface on page 73](#)

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 [“Digital Certificates Overview” on page 275](#).

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**.

**Related
Documentation**

- [C-Web Interface Overview on page 63](#)
- [Policies, Services, and Subscribers Management Subtasks in the C-Web Interface Overview on page 71](#)
- [Getting Help in the C-Web Interface on page 72](#)

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 11 on page 74](#) describes the editing levels.

Table 11: 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 taskbar, and then click the user level that you want to modify.

Related Documentation

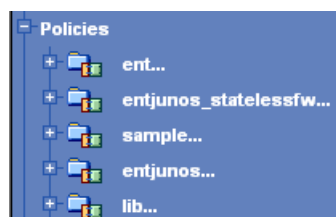
- [Starting Policies, Services, and Subscribers on page 72](#)
- [Editing SRC Configurations \(C-Web Interface\) on page 76](#)

Displaying Icons for Objects in the C-Web Interface

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

You can view icons for interfaces, policies, services, and subscribers. [Figure 14 on page 75](#) displays an example of the policy icon.

Figure 14: Policy Icon



Enabling Icons for Objects

To enable icons:

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

Icons are displayed in the side pane.

Disabling Icons for Objects

To disable icons:

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

The icons are removed from the side pane.

**Related
Documentation**

- [Editing SRC Configurations \(C-Web Interface\) on page 76](#)

Editing SRC Configurations (C-Web Interface)

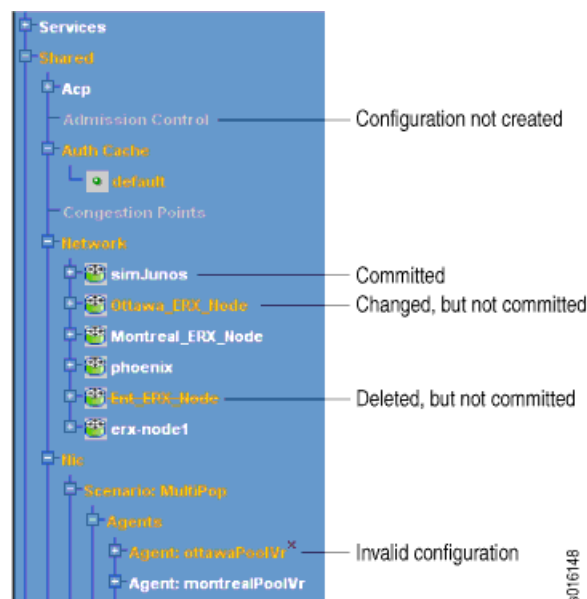
The C-Web interface enables you to edit a graphical version of the SRC CLI configuration statements and hierarchy. In the Configure side pane, each task maps to the top level of the SRC CLI [edit] hierarchy. These tasks include:

- Interfaces—Interface configuration
- Policies—Policy configuration
- Redirect Server—Redirect server properties
- Routing Options—Routing option configuration
- Services—Service configuration
- Shared—Shared configuration properties
- Slot—Local configuration properties
- SNMP—SRC SNMP agent configuration
- Subscribers—Subscriber and subscription configuration
- System—System properties

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

The changes you make to the candidate configuration are visible through the user interface immediately, but they do not take effect on the SRC software or the C Series Controller until you *commit* the changes. [Figure 15 on page 77](#) displays the configuration options for the C-Web interface.

Figure 15: Configuration Options for the C-Web Interface



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

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

Loading Configuration Values in the C-Web Interface

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

Figure 16 on page 78 shows the main pane of a configuration that has not been created.

Figure 16: Sample Configuration

Shared

SAE / Configuration / Aggregate Services

Create

Activation Deactivation Time*	Time to wait before retrying failed activation or deactivation of the fragment service session. <i>Value:</i> Number of seconds in the range 1–2147483647 <i>Default:</i> 900
Failed Notification Retry Time*	Length of time to continue sending failure notifications if an aggregate service cannot reach a fragment service, or a fragment service cannot reach an aggregate service during shutdown of the aggregate service. <i>Value:</i> Number of seconds in the range 1–2147483647 <i>Default:</i> 86400
Keepalive Retry Time*	Time to wait before resending unacknowledged keepalive messages. <i>Value:</i> Number of seconds in the range 1–2147483647 <i>Default:</i> 900
Keepalive Time*	Interval at which keepalive messages are sent from an aggregate service session and an associated fragment service session. <i>Value:</i> Number of seconds in the range 1–2147483647 <i>Default:</i> 86400

*Mandatory

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

To load the configuration values:

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

Committing a Configuration

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

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

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

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

Reverting to a Previous Configuration

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

To revert to the full committed configuration:

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

Updating the Configuration Data

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

To update the configuration:

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

Related Documentation

- [Modifying the Editing Level in the C-Web Interface on page 74](#)
- [Copying a Configuration for an Object \(C-Web Interface\) on page 79](#)

Modifying Objects in the C-Web Interface

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

- [Copying a Configuration for an Object \(C-Web Interface\) on page 79](#)
- [Renaming an Object on page 79](#)
- [Moving an Object on page 80](#)
- [Deleting an Object on page 80](#)

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

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

To copy a configuration to another configuration object:

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

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

See Also

- [Renaming an Object on page 79](#)
- [Moving an Object on page 80](#)
- [Deleting an Object on page 80](#)
- [Displaying Icons for Objects in the C-Web Interface on page 75](#)

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.

- See Also**
- [Copying a Configuration for an Object \(C-Web Interface\) on page 79](#)
 - [Moving an Object on page 80](#)
 - [Deleting an Object on page 80](#)
 - [Displaying Icons for Objects in the C-Web Interface on page 75](#)

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.

- See Also**
- [Copying a Configuration for an Object \(C-Web Interface\) on page 79](#)
 - [Renaming an Object on page 79](#)
 - [Deleting an Object on page 80](#)
 - [Displaying Icons for Objects in the C-Web Interface on page 75](#)

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.

- See Also**
- [Copying a Configuration for an Object \(C-Web Interface\) on page 79](#)
 - [Renaming an Object on page 79](#)
 - [Moving an Object on page 80](#)
 - [Displaying Icons for Objects in the C-Web Interface on page 75](#)

Configuring Logging Properties in the C-Web Interface

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

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

- [Configuring File Properties on page 81](#)
- [Configuring System Log Properties on page 81](#)
- [Configuration Statements for Logging for the C-Web Interface on page 82](#)

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**.

See Also • [Configuring System Log Properties on page 81](#)

Configuring System Log 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 System Log pane appears.

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

See Also • [Configuring File Properties on page 81](#)

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 ;
}
```

See Also • [Configuring File Properties on page 81](#)

Logging Out of the C-Web Interface

To end a C-Web session at any time:

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

Related Documentation

- [Accessing the C-Web Interface on page 67](#)
- [Enabling the C-Web Interface on page 70](#)
- [Starting the C-Web Interface on page 70](#)
- [C-Web Interface Overview on page 63](#)

CHAPTER 8

Configuring Remote Access to a C Series Controller (SRC CLI)

- [External Interfaces on a C Series Controller Overview on page 83](#)
- [Configuring Gigabit Ethernet Interfaces for IPv4 \(SRC CLI\) on page 85](#)
- [Configuring Gigabit Ethernet Interfaces for IPv6 \(SRC CLI\) on page 87](#)
- [Configuring Tunnel Interfaces \(SRC CLI\) on page 88](#)
- [Configuring Ethernet Redundancy \(SRC CLI\) on page 90](#)
- [Configuring a Trusted Interface \(SRC CLI\) on page 93](#)
- [Disabling an Interface \(SRC CLI\) on page 94](#)
- [Configuring the Virtual IP Address \(SRC CLI\) on page 94](#)
- [Configuring a Static Route to Devices on Other Networks \(SRC CLI\) on page 95](#)
- [Securing Connections Between a C Series Controller and Remote Hosts on page 96](#)
- [Configuring a C Series Controller to Accept SSH Connections \(SRC CLI\) on page 97](#)
- [Configuring a C Series Controller to Accept NETCONF Connections \(SRC CLI\) on page 99](#)
- [Port Settings for SRC Components on page 99](#)

External Interfaces on a C Series Controller Overview

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

Tunnel Interfaces

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 router running JunosE Software does not have a direct connection to the C Series Controller.

The C Series Controller supports the following types of tunnel interfaces:

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

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

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

See [“Configuring Gigabit Ethernet Interfaces for IPv4 \(SRC CLI\)”](#) on page 85.

Ethernet Redundancy

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

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

- The group interface name must not be one of the Ethernet interface names (that is, **eth0**, **eth1**, **eth2**, **eth3**).
- If an Ethernet interface is listed inside a group interface, it must not be configured as an interface by itself at the [edit interfaces name unit] hierarchy level.
- Group interface and tunnel interface configurations are mutually exclusive. You cannot configure both types at the same time.

You can group interfaces in the following modes:

- Round-robin policy (**balance-rr**)—Transmits packets in sequential order from the first available device through the last.
- Active-backup policy (**active-backup**)—Creates only one interface that is active. A different interface becomes active if, and only if, the active interface fails.



NOTE: If you configure a primary interface by including the **primary** option at the **[edit interfaces *name* group]** hierarchy level, then the primary interface is always active unless it fails. If a primary interface is deactivated due to a failure, it is reactivated when it recovers.

- XOR policy (**balance-xor**)—Transmits based on the selected transmit hash policy.
- Broadcast policy (**broadcast**)—Transmits everything on all device interfaces.
- IEEE 802.3ad Dynamic link aggregation (**802.3ad**)—Creates aggregation groups that share the same speed and duplex settings.
- Adaptive transmit load balancing (**balance-tlb**)—Creates channel bonding that does not require any special switch support.
- Adaptive load balancing (**balance-alb**)—Includes adaptive transmit load balancing (**balance-tlb**) plus receive load balancing (**rlb**) for IPv4 traffic, and does not require any special switch support.

You can monitor link integrity with the MII monitor.

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

Related Documentation

- [Configuring Ethernet Redundancy \(SRC CLI\) on page 90](#)
- [Configuring Gigabit Ethernet Interfaces for IPv4 \(SRC CLI\) on page 85](#)
- [Configuring Gigabit Ethernet Interfaces for IPv6 \(SRC CLI\) on page 87](#)
- [Configuring Tunnel Interfaces \(SRC CLI\) on page 88](#)

Configuring Gigabit Ethernet Interfaces for IPv4 (SRC CLI)

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

Use the following configuration statements to configure Gigabit Ethernet interfaces to use IPv4 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 inet address 192.2.0.10/24
```

3. Verify the interface configuration.

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

Related Documentation

- [Configuring Gigabit Ethernet Interfaces for IPv4 \(C-Web Interface\)](#)
- [Configuring Gigabit Ethernet Interfaces for IPv6 \(SRC CLI\) on page 87](#)
- [Configuring Tunnel Interfaces \(SRC CLI\) on page 88](#)
- [External Interfaces on a C Series Controller Overview on page 83](#)

Configuring Gigabit Ethernet Interfaces for IPv6 (SRC CLI)

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

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

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

To configure a Gigabit Ethernet interface to use IPv6:

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

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

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

For example:

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

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

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

For example:

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

3. Verify the interface configuration.

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

- Related Documentation**
- [Configuring Gigabit Ethernet Interfaces for IPv6 \(C-Web Interface\)](#)
 - [Configuring Gigabit Ethernet Interfaces for IPv4 \(SRC CLI\) on page 85](#)
 - [Configuring Tunnel Interfaces \(SRC CLI\) on page 88](#)
 - [External Interfaces on a C Series Controller Overview on page 83](#)

Configuring Tunnel Interfaces (SRC CLI)

You can configure tunnel interfaces to use the redirect server in deployments where a router running JunosE Software does not have a direct connection to the C Series Controller.

Before you configure a tunnel interface, configure the interface on the C Series Controller.

See [“Configuring Gigabit Ethernet Interfaces for IPv4 \(SRC CLI\)” on page 85](#)

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;
  }
}
```

- Related Documentation**
- [Configuring Tunnel Interfaces \(C-Web Interface\)](#)
 - [Configuring Gigabit Ethernet Interfaces for IPv6 \(SRC CLI\) on page 87](#)
 - [External Interfaces on a C Series Controller Overview on page 83](#)

Configuring Ethernet Redundancy (SRC CLI)

Tasks to configure Ethernet redundancy are:

- [Configuring Group Interfaces \(SRC CLI\) on page 90](#)
- [Configuring the MII Monitor \(SRC CLI\) on page 92](#)

Configuring Group Interfaces (SRC CLI)

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

Use the following statements to configure the group interface:

```
interfaces name group {
  mode (balance-rr | active-backup | balance-xor | broadcast | 802.3ad | balance-tlb |
    balance-alb);
  lacp-rate (slow | fast);
  interfaces [interfaces...];
}
```



```
primary primary;  
transmit-hash-policy (layer2 | layer3+4);  
}
```

To configure an Ethernet group interface:

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

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

2. Specify the mode in which you want to group the interfaces. By default, the mode is set as **balance-rr**.

You can group interfaces in the following modes:

- Round-robin policy (**balance-rr**)—Transmits packets in sequential order from the first available device through the last.
- Active-backup policy (**active-backup**)—Creates only one interface that is active. A different interface becomes active if, and only if, the active interface fails.



NOTE: If you configure a primary interface by including the **primary** option at the [edit interfaces *name* group] hierarchy level, then the primary interface is always active unless it fails. If a primary interface is deactivated due to a failure, it is reactivated when it recovers.

- XOR policy (**balance-xor**)—Transmits based on the selected transmit hash policy.
- Broadcast policy (**broadcast**)—Transmits everything on all device interfaces.
- IEEE 802.3ad Dynamic link aggregation (**802.3ad**)—Creates aggregation groups that share the same speed and duplex settings.
- Adaptive transmit load balancing (**balance-tlb**)—Creates channel bonding that does not require any special switch support.
- Adaptive load balancing (**balance-alb**)—Includes adaptive transmit load balancing (**balance-tlb**) plus receive load balancing (**rlb**) for IPv4 traffic, and does not require any special switch support.

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

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

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

where:

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

4. Specify the Ethernet interfaces in this group.

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

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

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

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

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

where:

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

7. Configure the unit for the group interface.

- See Also**
- [Disabling an Interface \(SRC CLI\) on page 94](#)
 - [Port Settings for SRC Components on page 99](#)

Configuring the MII Monitor (SRC CLI)

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

Use the following statements to configure MII link monitoring:

```
interfaces name group {
```

```

downdelay downdelay;
updelay mii-monitoring-interval;
mii-monitoring-interval mii-monitoring-interval;
}

```

To configure the MII monitor:

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

```

[edit]
user@host# edit interfaces name group

```

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

```

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

```

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

```

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

```

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

```

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

```

- See Also**
- [Disabling an Interface \(SRC CLI\) on page 94](#)
 - [Port Settings for SRC Components on page 99](#)

- Related Documentation**
- [External Interfaces on a C Series Controller Overview on page 83](#)
 - [Configuring Gigabit Ethernet Interfaces for IPv4 \(SRC CLI\) on page 85](#)
 - [Configuring Gigabit Ethernet Interfaces for IPv6 \(SRC CLI\) on page 87](#)
 - [Configuring Tunnel Interfaces \(SRC CLI\) on page 88](#)
 - [Disabling an Interface \(SRC CLI\) on page 94](#)
 - [Port Settings for SRC Components on page 99](#)

Configuring a Trusted Interface (SRC CLI)

You can configure an interface as a trusted interface. By default, all interfaces except for eth1 are trusted and the eth0 interface is always trusted.

To set an interface as a trusted interface:

1. From configuration mode, access the statement that configures the interface. In this sample procedure, eth1 is the interface.

```
[edit]  
user@host# edit interfaces eth1
```

2. Set the interface as a trusted interface.

```
[edit interfaces eth1]  
user@host# set trusted
```

- Related Documentation**
- [Disabling an Interface \(SRC CLI\) on page 94](#)
 - [Configuring Ethernet Redundancy \(SRC CLI\) on page 90](#)

Disabling an Interface (SRC CLI)

You can disable an interface without removing the interface configuration statements from the configuration.

To disable an interface:

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

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

2. Disable the interface.

```
[edit interfaces name]  
user@host# set disable
```

- Related Documentation**
- [Configuring a Trusted Interface \(SRC CLI\) on page 93](#)
 - [Configuring the Virtual IP Address \(SRC CLI\) on page 94](#)

Configuring the Virtual IP Address (SRC CLI)

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

To configure the virtual IP address:

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

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

2. Specify the protocol family and virtual IP address.

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

For example, to configure a virtual IPv4 address:

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

3. Verify the interface configuration.

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

- Related Documentation**
- [Configuring a Static Route to Devices on Other Networks \(SRC CLI\) on page 95](#)
 - [External Interfaces on a C Series Controller Overview on page 83](#)

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

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

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

To configure a static route to another network:

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

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

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

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

To specify that packets to a specified network be dropped:

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

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

Related Documentation

- [Configuring a Static Route to Devices on Other Networks \(C-Web Interface\)](#)

Securing Connections Between a C Series Controller and Remote Hosts

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

By default, SSH for nonroot users is enabled on C Series Controllers. Otherwise, you configure the C Series Controller to explicitly allow users on remote systems to access it. [Table 12 on page 96](#) lists the applications through which remote users can access a C Series Controller.

Table 12: Applications to Remotely Access the C Series Controller

Application	Information About Access Configuration
SSH	"Configuring a C Series Controller to Accept SSH Connections (SRC CLI)" on page 97
NETCONF	"Configuring a C Series Controller to Accept NETCONF Connections (SRC CLI)" on page 99
C-Web interface	"Accessing the C-Web Interface" on page 67
Policies, Services, and Subscribers CLI	"Configuring Access to the Policies, Services, and Subscribers CLI" on page 56

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

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

- SSH
- FTP by means of a file URL

- Related Documentation**
- [Port Settings for SRC Components on page 99](#)
 - [Connecting to a Remote Host Through SSH on page 283](#)
 - [Connecting to a Remote Host Through Telnet on page 283](#)

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

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

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

```
system services ssh {
  root-login (allow | deny | deny-password);
  port port;
  protocol-version 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 2 be used.

```
[edit system services ssh]
user@host> set protocol-version v2
```



NOTE: SSH version 1 is not supported from SRC 4.12 release. When you upgrade to SRC 4.12 release, SSH version 2 is enabled by default even if you have configured SSH version 1 in the previous SRC release.

3. (Optional) Specify the listening port number for incoming SSH connections. The value range is 1–65,535. By default, the SRC software listens for incoming SSH connections on port 22.

```
[edit system services ssh]
user@host> set port port
```

**NOTE:**

- It is recommended that you configure a value lower than 1024 because only root users can listen on port numbers lower than 1024. This prevents other users from listening on the port. If you configure a value higher than 1024, a warning message is displayed.
- If you set the listening port number to a value other than the default, you must append the “-p” flag to the configured listening port number while logging in to the SRC system. For example, `ssh root@10.212.10.14 -p port`.

4. (Optional) Specify whether or not to allow users to log in as root through SSH:

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

where:

- **allow**—Allows users to log in to the C Series Controller as root through SSH
- **deny**—Prevents users from logging in to the C Series Controller as root through SSH
- **deny-password**—Allows 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. This is the default.



NOTE: We recommend that you do not allow users to log in to the C Series Controller as root through SSH. Instead, you can use the following statement to create a username and password that a user can use to log in to the C Series Controller.

```
system login user user-name {
  class class;
  authentication {
    plain-text-password;
    encrypted-password " password ";
    ssh-authorized-keys [ssh-authorized-keys ...];
  }
}
```

Related Documentation

- [Configuring a C Series Controller to Accept SSH Connections \(C-Web Interface\)](#)
- [Configuring a C Series Controller to Accept NETCONF Connections \(SRC CLI\) on page 99](#)
- [Connecting to a Remote Host Through SSH on page 283](#)
- [Configuring User Accounts \(SRC CLI\) on page 249](#)

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

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

```
system services netconf ssh{
  port port-num;
}
```

To configure the C Series Controller to accept NETCONF connections:

1. From configuration mode, access the configuration statement to enable NETCONF access.

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

2. (Optional) Specify the port used by the SRC NETCONF server. The default port number is 32000.

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

Related Documentation

- [Configuring a C Series Controller to Accept NETCONF Connections \(C-Web Interface\)](#)
- [Configuring a C Series Controller to Accept SSH Connections \(SRC CLI\) on page 97](#)

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 13 on page 99](#) lists the default port settings for SRC components.

Table 13: 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 13: Default Port Settings for SRC Components (continued)

Component	Type of Communication	Default Port Setting
Diameter server	Communications between the MX Series router and the Diameter server.	TCP 3868
Sample residential portal with Tomcat	Starting Tomcat server.	TCP 8005
	Apache JServ Protocol (AJP) requests for Tomcat.	TCP 8009
	Responses to incoming HTTP requests from Tomcat.	TCP 8080)
	This port is an alternative to port 80.	
JBoss	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 Time Protocol (NTP)	Communications between the NTP server and the C Series Controller.	TCP 123
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

Table 13: Default Port Settings for SRC Components (continued)

Component	Type of Communication	Default Port Setting
SAE	Common Open Policy Service (COPS) connection from routers running JunosE Software.	TCP 3288
	Blocks Extensible Exchange Protocol (BEEP) connection from routers running Junos OS.	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 SRC SNMP agent.	UDP 8030
	SNMP get and set messages.	UDP 161
	SNMP traps.	UDP 162
SSH	Secured connection to a C Series Controller.	TCP 22
TACACS	Communications between the TACACS server and the C Series Controllers.	TCP 49

We recommend that you configure NTP to synchronize time on the network. See the documentation for the NTP server for your system.

Related Documentation

- [Configuring Ethernet Redundancy \(SRC CLI\) on page 90](#)
- [Securing Connections Between a C Series Controller and Remote Hosts on page 96](#)

PART 4

Managing SRC Licenses

- [Overview of SRC Licenses on page 105](#)
- [Overview of the SRC License Server on page 107](#)
- [Customizing SRC License Server Configuration on page 113](#)
- [Installing Licenses for C Series Controllers on page 121](#)
- [Monitoring License Usage on page 125](#)

CHAPTER 9

Overview of SRC Licenses

- [Types of SRC Licenses on page 105](#)
- [Obtaining an SRC License on page 106](#)

Types of SRC Licenses

You must obtain a license for the SRC software from the Juniper Networks License Management System. Juniper Networks provides server licenses for the SRC software.

The 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 not imported a server license, the SRC software uses the no license mode. In no license mode, you can create a maximum of 100 current user sessions. If the configured user sessions exceed 100, the SRC software rejects the additional user sessions and logs an error “Number of User sessions has reached the limit” in SAE logs. There is no limitation on the number of service sessions that can be created in the no license mode.

Related Documentation

- [Obtaining an SRC License on page 106](#)
- [Installing Server Licenses for C Series Controllers \(SRC CLI\) on page 121](#)

Obtaining an SRC License

Before you install the SRC software, collect information about the system that will run the SAE and provide this system information to obtain a license.

To obtain a server license, you must log into the Juniper Networks License Management System at https://www.juniper.net/generate_license and provide the following information:

- Authorization code provided with your order
- Serial number of your device on side of the unit
- Hostname of the license server

You can determine the serial number and hostname by issuing this command on a C Series Controller:



.....
NOTE: When you issue the `show system information` command in a virtualized SRC software, the manufacturer, version, and serial number details are not displayed in the output. In addition, the product name is displayed as vSRC.
.....

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

Look for the **Hostname** and **Serial Number** values in the output.

Related Documentation

- [Types of SRC Licenses on page 105](#)
- [Installing Server Licenses for C Series Controllers \(SRC CLI\) on page 121](#)

CHAPTER 10

Overview of the SRC License Server

- [SRC License Server Overview on page 107](#)
- [Unsuccessful Connections from the SAE to the SRC License Server on page 110](#)
- [SRC License Server Redundancy on page 110](#)
- [About SRC License Server Alarms on page 111](#)

SRC License Server Overview

- [About the SRC License Server on page 107](#)
- [License Server Errors on page 107](#)
- [License Requests on page 108](#)
- [Lease Renewal on page 109](#)
- [Directory Location and Access on page 109](#)

About 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.

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:

- Service-session-unit-size—Number of active service sessions
- Lease duration—Length of time allotted to a grant
- Allocation threshold—A percentage of the license service-session-unit-size that defines how many licenses are available for allocation
- Release threshold—A percentage of the license service-session-unit-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 service-session-unit-size of 50 and an allocation threshold of 90%, the SAE requests a second lease when the number of active service sessions reaches 45 ($50 \times 90\%$). Once the lease is granted, if the active service sessions continue to increase, the SAE requests another lease when the number of active service sessions reaches 95, and again at 145.

Example: License Release Example

License units are released as active service sessions decrease, with the SAE retaining more licenses than it currently needs to avoid fluctuation around the threshold. For example, a lease has a service-session-unit-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.

Related Documentation

- [SRC License Server Redundancy on page 110](#)
- [Unsuccessful Connections from the SAE to the SRC License Server on page 110](#)
- [Obtaining an SRC License on page 106](#)
- [Installing Server Licenses for C Series Controllers \(SRC CLI\) on page 121](#)

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 uses the no license mode. In no license mode, you can create a maximum of 100 current user sessions. There is no limitation on the number of service sessions that can be created in the no license mode.

The SAE polls the directory at specified intervals to detect license upgrades or additions. Server licenses are preferred over no license mode. 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 the no license mode 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.

- Related Documentation**
- [Obtaining an SRC License on page 106](#)
 - [SRC License Server Overview on page 107](#)

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.

- Related Documentation**
- [SRC License Server Overview on page 107](#)

About SRC License Server Alarms

The license server provides notifications when licensing thresholds are exceeded. [Table 14 on page 111](#) describes the conditions that prompt a warning or an alarm.

Table 14: SRC SNMP Warnings and Alarms

Condition	Notification to SRC SNMP Agent
Number of licenses in use exceeds a user-defined threshold.	Minor warning SNMP trap
License reaches its expiration date.	saeUserLicenseExpiry warning SNMP event trap
Number of service sessions exceeds the number available.	saeServiceSessionLicense warning SNMP event trap
Number of licenses in use reaches the license limit.	Major warning SNMP trap
Major alarm state continues for 1 week.	Escalation to critical

The license server continues to run during a critical alarm state but denies all requests for licenses. The license server clears the alarm when the alarm is no longer active.

You can configure the license server to send warnings and alarms, and can configure an SNMP host to receive the warnings and alarms.



NOTE: The SRC SNMP agent takes no action when it receives any of these traps. You must determine appropriate measures to resolve these warning states.

- Related Documentation**
- [SRC License Server Overview on page 107](#)
 - [Unsuccessful Connections from the SAE to the SRC License Server on page 110](#)
 - [SNMP Traps Overview](#)
 - [Configuring License Server Alarms \(SRC CLI\) on page 114](#)
 - [Configuration Statements for SRC License Server Properties on page 113](#)

CHAPTER 11

Customizing SRC License Server Configuration

- Configuration Statements for SRC License Server Properties on page 113
- Configuring License Server Alarms (SRC CLI) on page 114
- Specifying the ORB Configuration for the SRC License Server (SRC CLI) on page 116
- Configuring the License Server Repository (SRC CLI) on page 116
- Configuring License Server Properties (SRC CLI) on page 118
- Configuring the License Server Location (SRC CLI) on page 119

Configuration Statements for SRC License Server Properties

Use the following configuration statements to configure license server properties at the [edit] hierarchy level:

```
shared license-server alarm {  
    threshold threshold;  
    report-server report-server;  
}  
  
shared license-server email {  
    server server;  
    alarm-report-address alarm-report-address;  
}  
  
shared license-server corba {  
    orb-configuration-property-file orb-configuration-property-file;  
}  
  
shared license-server repository {  
    ldap-server-address ldap-server-address;  
    server-port server-port;  
    search-base search-base;  
    authentication-dn authentication-dn;  
    password password;  
}
```

```
shared license-server engine {
  service-session-unit-size service-session-unit-size;
  sae-service-unit-size sae-service-unit-size;
  lease-renew-interval lease-renew-interval;
  allocate-license-threshold allocate-license-threshold;
  release-license-threshold release-license-threshold;
}

shared license-server persistence-control {
  root-directory-of-the-license-server root-directory-of-the-license-server;
  work-directory-of-the-license-server work-directory-of-the-license-server;
  license-server-state-cache-file license-server-state-cache-file;
}

shared license-server logging logger name ...

shared license-server logging logger name file-logger {
  filter filter;
  filename filename;
  rollover-filename rollover-filename;
  maximum-file-size maximum-file-size;
}

shared license-server logging logger name syslog-logger {
  filter filter;
  host host;
  facility facility;
  format format;
}
```

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

**Related
Documentation**

- [Logging for SRC Components Overview](#)
- [Configuring License Server Properties \(SRC CLI\) on page 118](#)
- [Specifying the ORB Configuration for the SRC License Server \(SRC CLI\) on page 116](#)
- [SRC License Server Overview on page 107](#)

Configuring License Server Alarms (SRC CLI)

You can configure the license server to send alarms to system administrators through SNMP and e-mail messages.

Use the following configuration statements to configure the license server alarms:

```
shared license-server alarm {
  threshold threshold;
  report-server report-server;
}
```



```
shared license-server email {
  server server;
  alarm-report-address alarm-report-address;
```



NOTE: In most cases, you do not need to change the configuration for the license server. If you change the configuration, do so with care. The software needs to be able to communicate with the license server to operate correctly.

To configure license server alarms:

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

```
[edit]
user@host# edit shared license-server alarm
```

2. Specify the threshold as a percentage of the licensed capacity that, when exceeded, sends SNMP minor traps and initiates e-mail alerts to the system administrator.

```
[edit shared license-server alarm]
user@host# set threshold threshold
```

3. Specify the report server to receive warning traps.

```
[edit shared license-server alarm]
user@host# set report-server report-server
```

To configure an e-mail notification:

1. Access the configuration statement that configures e-mail notification.

```
[edit shared license-server alarm]
user@host# up
```

```
[edit shared license-server]
user@host# edit email
```

2. Specify the SMTP e-mail server to receive alarms and usage reports.

```
[edit shared license-server email]
user@host# set server server;
```

3. Specify an e-mail address of the system administrator to receive warning e-mail messages.

```
[edit shared license-server alarm]
user@host# set alarm-report-address alarm-report-address;
```

Related Documentation

- [SRC License Server Overview on page 107](#)
- [About SRC License Server Alarms on page 111](#)

- [Configuring the License Server Repository \(SRC CLI\) on page 116](#)
- [Configuration Statements for SRC License Server Properties on page 113](#)

Specifying the ORB Configuration for the SRC License Server (SRC CLI)

You can use the object request broker (ORB) configuration to define the location of the property file for the license server. Typically, you do not need to change this property.

Use the following configuration statements to specify the ORB configuration property file for the license server:

```
shared license-server corba {  
  orb-configuration-property-file orb-configuration-property-file;  
}
```



NOTE: In most cases, you do not need to change the configuration for the license server. If you change the configuration, do so with care. The software needs to be able to communicate with the license server to operate correctly.

To specify the ORB configuration:

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

```
[edit]  
user@host# edit shared license-server corba
```

2. Specify the ORB configuration property file.

```
[edit shared license-server corba]  
user@host# set orb-configuration-property-file orb-configuration-property-file
```

Related Documentation

- [SRC License Server Overview on page 107](#)
- [Configuring the License Server Repository \(SRC CLI\) on page 116](#)
- [Configuring License Server Properties \(SRC CLI\) on page 118](#)
- [Configuring the License Server Location \(SRC CLI\) on page 119](#)
- [Configuration Statements for SRC License Server Properties on page 113](#)

Configuring the License Server Repository (SRC CLI)

You can use the license server repository configuration to configure access to the Juniper Networks database for the license server.

Use the following configuration statements to configure the license server repository:

```
shared license-server repository {
  ldap-server-address ldap-server-address;
  server-port server-port;
  search-base search-base;
  authentication-dn authentication-dn;
  password password;
}
```



NOTE: In most cases, you do not need to change the configuration for the license server. If you change the configuration, do so with care. The software needs to be able to communicate with the license server to operate correctly.

To configure the license server repository:

1. From configuration mode, access the configuration statement that configures the license server repository.

```
[edit]
user@host# edit shared license-server repository
```

2. Specify the IP address or the hostname of the LDAP server that stores licensing data.

```
[edit shared license-server repository]
user@host# set ldap-server-address ldap-server-address
```



NOTE: This is a required property. If no value is assigned, the license server does not start. If this value is removed while the license server is running, the server rejects licensing requests. After a new value is entered and the license server connects to the LDAP server, the license server accepts license requests again.

3. Specify the port number of the LDAP server that stores licensing data.

```
[edit shared license-server repository]
user@host# set server-port server-port
```

4. Specify the base directory of the LDAP server that stores licensing data.

```
[edit shared license-server repository]
user@host# set search-base search-base
```

5. Specify the DN used by the SAE to authenticate access to the LDAP server that stores licensing data.

```
[edit shared license-server repository]
user@host# set authentication-dn authentication-dn
```

6. Specify the password used to authenticate access to the LDAP server that stores licensing data.

```
[edit shared license-server repository]
user@host# set password password
```

**Related
Documentation**

- [SRC License Server Overview on page 107](#)
- [Specifying the ORB Configuration for the SRC License Server \(SRC CLI\) on page 116](#)
- [Configuring License Server Properties \(SRC CLI\) on page 118](#)
- [Configuring the License Server Location \(SRC CLI\) on page 119](#)
- [Configuration Statements for SRC License Server Properties on page 113](#)

Configuring License Server Properties (SRC CLI)

You can use the license server engine configuration to configure the general properties for the license server.

Use the following configuration statements to configure the license server general properties:

```
shared license-server engine {
  service-session-unit-size service-session-unit-size;
  sae-service-unit-size sae-service-unit-size;
  lease-renew-interval lease-renew-interval;
  allocate-license-threshold allocate-license-threshold;
  release-license-threshold release-license-threshold;
}
```



NOTE: In most cases, you do not need to change the configuration for the license server. If you change the configuration, do so with care. The software needs to be able to communicate with the license server to operate correctly.

To configure the license server general properties:

1. From configuration mode, access the configuration statement that configures license server general properties.

```
[edit]
user@host# edit shared license-server engine
```

2. Specify the size of each license unit for the service session property; this is the size of the license unit allocated to the SAE.

```
[edit shared license-server engine]
user@host# set service-session-unit-size service-session-unit-size
```

3. (Optional) Specify the size of each license unit for the SAE service property; this is the size of the license unit allocated to the SAE.

```
[edit shared license-server engine]
user@host# set sae-service-unit-size sae-service-unit-size
```

4. Specify the lease period for the licenses that the SAE client receives.

```
[edit shared license-server engine]
user@host# set lease-renew-interval lease-renew-interval
```

5. Specify the license threshold, as a percentage of the serve-session-unit, at which the SAE client obtains more licenses.

```
[edit shared license-server engine]
user@host# set allocate-license-threshold allocate-license-threshold
```

6. Specify the license threshold, as a percentage of the serve-session-unit, at which the SAE client releases one license unit.

```
[edit shared license-server engine]
user@host# set release-license-threshold release-license-threshold
```

Related Documentation

- [SRC License Server Overview on page 107](#)
- [Specifying the ORB Configuration for the SRC License Server \(SRC CLI\) on page 116](#)
- [Configuring the License Server Repository \(SRC CLI\) on page 116](#)
- [Configuring the License Server Location \(SRC CLI\) on page 119](#)
- [Configuration Statements for SRC License Server Properties on page 113](#)

Configuring the License Server Location (SRC CLI)

You can use the persistence control configuration to set the root directory, the working directory, and the cache file for the license server.

Use the following configuration statements to configure the license server location:

```
shared license-server persistence-control {
  root-directory-of-the-license-server root-directory-of-the-license-server;
  work-directory-of-the-license-server work-directory-of-the-license-server;
  license-server-state-cache-file license-server-state-cache-file;
}
```



NOTE: In most cases, you do not need to change the configuration for the license server. If you change the configuration, do so with care. The software needs to be able to communicate with the license server to operate correctly.

To configure the license server location:

1. From configuration mode, access the configuration statement that configures the license server location.

```
[edit]
user@host# edit shared license-server persistence-control
```

2. Specify the root directory of the license server.

```
[edit shared license-server persistence-control]
user@host# set root-directory-of-the-license-server root-directory-of-the-license-server
```

3. Specify the working directory of the license server, in which the license server states are saved.

```
[edit shared license-server persistence-control]
user@host# set work-directory-of-the-license-server
work-directory-of-the-license-server
```

4. Specify the cache file for the license server state information.

```
[edit shared license-server persistence-control]
user@host# set license-server-state-cache-file license-server-state-cache-file
```

Related Documentation

- [SRC License Server Overview on page 107](#)
- [Configuring the License Server Repository \(SRC CLI\) on page 116](#)
- [Configuring License Server Properties \(SRC CLI\) on page 118](#)
- [Configuration Statements for SRC License Server Properties on page 113](#)

CHAPTER 12

Installing Licenses for C Series Controllers

- [Installing Server Licenses for C Series Controllers \(SRC CLI\) on page 121](#)
- [Configuring License Manager for an SAE on a C Series Controller \(SRC CLI\) on page 122](#)

Installing Server Licenses for C Series Controllers (SRC CLI)

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, install the server license.

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

To install the license as the master license.

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

2. Verify that a valid license is available.

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

3. Enable the license server.

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

4. Configure license manager for the SAE.

See [“Configuring License Manager for an SAE on a C Series Controller \(SRC CLI\)” on page 122](#).

Related Documentation

- [Obtaining an SRC License on page 106](#)
- [SRC License Server Overview on page 107](#)

- [Types of SRC Licenses on page 105](#)

Configuring License Manager for an SAE on a C Series Controller (SRC CLI)

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# se password password
```

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

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

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

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

The default is LICENSE_MANAGER.

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

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

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

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

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

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

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

**Related
Documentation**

- [Obtaining an SRC License on page 106](#)
- [Types of SRC Licenses on page 105](#)
- [Unsuccessful Connections from the SAE to the SRC License Server on page 110](#)

CHAPTER 13

Monitoring License Usage

- [About SRC License Reports on page 125](#)
- [Creating SRC License Usage Reports \(SRC CLI\) on page 126](#)
- [Sending SRC License Usage Reports to Administrators \(SRC CLI\) on page 126](#)
- [Monitoring SRC License Usage \(SRC CLI\) on page 127](#)
- [Removing SRC License Allocated for a Virtual Router \(SRC CLI\) on page 128](#)

About SRC License Reports

At the beginning of each month, the SRC software generates a report that provides information about license usage. You can view information about license usage from the CLI or configure the SRC software to send the reports through e-mail to administrators. You can also create a new license usage report at any time. The system stores only one license usage report per month. When you create a report, the system replaces a previous report generated in the same month with the new one.

The report lists the date the report was created, and for each license the customer identification information, the license serial number, and the number of licenses installed. It also lists the number of concurrent active SAE service sessions (maximum number of license units) that can be allocated, and the maximum number of concurrent active SAE service sessions allocated since the license was installed or since the last license usage report was created.

The system stores license usage reports in files. The filename syntax for reports is report-year-month.txt; for example, **report-2008-12.txt**. The following sample license usage report shows the format of the report. The message is sent best-effort; therefore, there is no guarantee that the signature in the report can be trusted.

```
License-Usage Report
Date: 2008-08-01
Customer: <customer>
Serial Number: <sn>
Installed: #####
-----BEGIN SIGNATURE-----
<Base-64 encoded signature>
-----END SIGNATURE-----
```

For example:

```
License-Usage Report
Date: 2008-11-01
Customer: MyCompany
Serial Number: <sn>
Installed: #####
-----BEGIN SIGNATURE-----
<Base-64 encoded signature>
-----END SIGNATURE-----
```

**Related
Documentation**

- [SRC License Server Overview on page 107](#)
- [Creating SRC License Usage Reports \(SRC CLI\) on page 126](#)
- [Sending SRC License Usage Reports to Administrators \(SRC CLI\) on page 126](#)

Creating SRC License Usage Reports (SRC CLI)

Create a report to compare the maximum number of concurrent active SAE service sessions in use since the last report with the number of sessions allowed by the server license.

The SRC software generates a report at the beginning of each month. You can create a new report at any time. If you configured reports to be sent through e-mail, the SRC software sends a report after you create it.

To create a license usage report:

```
user@host> request license usage-report

Generated Usage Report
```

**Related
Documentation**

- [Monitoring SRC License Usage \(SRC CLI\) on page 127](#)
- [Sending SRC License Usage Reports to Administrators \(SRC CLI\) on page 126](#)

Sending SRC License Usage Reports to Administrators (SRC CLI)

Send license usage reports to system administrators or others to have them monitor the maximum number of concurrent active SAE service sessions and compare that number with the number allowed by the server license.

To specify users to receive SRC license usage reports:

1. From configuration mode, access the configuration statement for license server e-mail configuration.

```
[edit]
user@host# edit shared license-server email
```

- Specify the e-mail server. for example:

```
[edit shared license-server email]
user@host> set server my-server.mycompany.com
```

- Specify one or more e-mail addresses. Use commas to separate addresses. For example:

```
[edit shared license-server email]
user@host> set usage-report-address CBee@mycompany.com, SJones@mycompany.com,
JSmith@mycompany.com
```

- Related Documentation**
- [Creating SRC License Usage Reports \(SRC CLI\) on page 126](#)
 - [About SRC License Reports on page 125](#)

Monitoring SRC License Usage (SRC CLI)

Purpose Monitor the maximum number of concurrent service sessions in use per virtual router since the last time a usage report was generated, and compare this number with the maximum number of sessions allowed by the SRC server license.

Action View the maximum concurrent service sessions for all licenses allocated.

```
user@host> show license allocated

Allocated Licenses
Virtual router name default@junos1
Enforcement type    service sessions
Granted             50
Last Granted        Wed Nov 19 08:37:43 EST 2008
Expiration           Wed Nov 19 08:37:43 EST 2008

Allocated Licenses
Virtual router name default@junose_vr1
Enforcement type    service sessions
Granted             0
```

Meaning [Table 15 on page 128](#) describes the output fields for the **show license-server allocated-licenses** command. Output fields are listed in the order in which they appear.

Table 15: Output Fields for the show license-server allocated-licenses Command

Field Name	Field Description
Allocated Licenses	Section of the output that provides license information for a particular virtual router
Virtual router name	Virtual router associated with an SRC server license
Enforcement type	Type of enforcement provided by the license. For SRC, the only license type is service sessions.
Granted	Maximum number of concurrent active SAE service sessions allocated by the SAE.
Last granted	Last time the SAE allocated a license unit that specifies the number of concurrent active SAE service sessions allowed.
Expiration	Time at which the allocation ends.

Related Documentation

- [Creating SRC License Usage Reports \(SRC CLI\) on page 126](#)
- [Sending SRC License Usage Reports to Administrators \(SRC CLI\) on page 126](#)
- [Removing SRC License Allocated for a Virtual Router \(SRC CLI\) on page 128](#)

Removing SRC License Allocated for a Virtual Router (SRC CLI)

Remove the license allocated for a virtual router to prevent licenses from getting completely used up.

When the licenses allocated for existing virtual routers become inactive, it results in preventing new service sessions being created for another virtual router due to exhaustion of licenses. Use the **request sae license remove-allocated virtual-router *virtual-router-name*** command to remove licenses for an inactive router driver.



NOTE: When inactive, the virtual router is not listed in the **show sae drivers** command output.

To remove a license allocated for a virtual router:

1. View the licenses allocated for each and every virtual router.

```
user@host> show license allocated

Allocated Licenses
Virtual router name default@junos1
Enforcement type    service sessions
Granted            50
```

Last Granted	Wed Nov 19 08:37:43 EST 2016
Expiration	Wed Nov 29 08:37:43 EST 2016

2. Remove the allocated license.

```
user@host> request sae license remove-allocated virtual-router default@junos1
License has been removed for vr = default@junos1
```



NOTE: This command is applicable only for the inactive router drivers and virtual routers managed by the same SAE.

You can use the **show license allocated** command to verify whether the license has been removed.

Related Documentation

- [Monitoring SRC License Usage \(SRC CLI\) on page 127](#)
- [Creating SRC License Usage Reports \(SRC CLI\) on page 126](#)
- [About SRC License Reports on page 125](#)

PART 5

Managing an Environment of C Series Controllers

- [Configuring System Time on C Series Controllers \(SRC CLI\) on page 133](#)
- [Configuring NTP for C Series Controllers on page 135](#)
- [Configuring NTP on C Series Controllers \(SRC CLI\) on page 139](#)
- [Configuring System Logging for a C Series Controller \(SRC CLI\) on page 155](#)
- [Configuring Static Host Mapping \(SRC CLI\) on page 161](#)
- [Overview of the Juniper Networks Database on page 163](#)
- [Managing the Juniper Networks Database \(SRC CLI\) on page 167](#)
- [Setting Up an SAE \(SRC CLI\) on page 189](#)
- [Managing System Software on a C Series Controller on page 199](#)
- [Using the Web Application Server on a C Series Controller on page 215](#)

Configuring System Time on C Series Controllers (SRC CLI)

- [Setting the Time Zone \(SRC CLI\) on page 133](#)
- [Setting the System Date \(SRC CLI\) on page 134](#)

Setting the Time Zone (SRC CLI)

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

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

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

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

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

To modify the local time zone:

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

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

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

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

2. Verify the configuration. For example:

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

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

**Related
Documentation**

- [Setting the System Date \(SRC CLI\) on page 134](#)
- [Viewing the System Date and Time \(C-Web Interface\)](#)
- [NTP Support on C Series Controllers on page 135](#)

Setting the System Date (SRC CLI)

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

To set the system date and time:

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

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

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

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

**Related
Documentation**

- [Setting the Time Zone \(SRC CLI\) on page 133](#)
- [Viewing the System Date and Time \(C-Web Interface\)](#)
- [NTP Support on C Series Controllers on page 135](#)

Configuring NTP for C Series Controllers

- [NTP Support on C Series Controllers on page 135](#)
- [Configuring NTP on a C Series Controller on page 136](#)

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 Documentation

- [Configuring NTP on a C Series Controller on page 136](#)
- [Viewing NTP Peers \(SRC CLI\)](#)
- [Viewing NTP Peers \(C-Web Interface\)](#)
- [Configuration Statements for NTP on C Series Controllers on page 139](#)

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 140](#).
 - See [Specifying a Basic NTP Configuration on a C Series Controller \(C-Web Interface\)](#).
2. Specify the time source and the manner in which time is synchronized between systems on the network. Configure NTP to operate in one or more of the following modes:
 - Client mode:
 - See [“Configuring NTP Client Mode for a C Series Controller \(SRC CLI\)” on page 141](#).
 - See [Configuring NTP Client Mode for a C Series Controller \(C-Web Interface\)](#).
 - Symmetric active (peer) mode:
 - See [“Configuring an NTP Peer on a C Series Controller \(SRC CLI\)” on page 142](#).
 - See [Configuring an NTP Peer for a C Series Controller \(C-Web Interface\)](#).
 - Broadcast mode:
 - See [“Configuring NTP Broadcast Mode on a C Series Controller \(SRC CLI\)” on page 143](#).

- See *Configuring NTP Broadcast Mode on a C Series Controller (C-Web Interface)*.
3. (Recommended) Configure NTP authentication.
 - See *Specifying an Authentication Key for NTP on C Series Controllers (C-Web Interface)*.
 - See *Configuring NTP Authentication (C-Web Interface)*.
 4. (Optional) Configure NTP to listen for broadcast messages.
 - See [“Configuring NTP as a Broadcast Client on a C Series Controller \(SRC CLI\)” on page 146](#).
 - See *Specifying a Basic NTP Configuration on a C Series Controller (C-Web Interface)*.
 5. (Optional) Configure NTP to listen for multicast messages.
 - See [“Configuring NTP as a Multicast Client on a C Series Controller \(SRC CLI\)” on page 147](#).
 - See *Configuring NTP as a Multicast Client on a C Series Controller (C-Web Interface)*.
 6. (Optional) Disable NTP monitoring service on C Series Controllers.
 - See [“Disabling NTP Monitoring Service \(SRC CLI\)” on page 148](#).

Related Documentation

- [NTP Support on C Series Controllers on page 135](#)
- [Configuration Statements for NTP on C Series Controllers on page 139](#)
- [Verifying NTP Configuration on a C Series Controller on page 153](#)

CHAPTER 16

Configuring NTP on C Series Controllers (SRC CLI)

- [Configuration Statements for NTP on C Series Controllers on page 139](#)
- [Specifying Which NTP Server a C Series Controller Contacts on Startup on page 140](#)
- [Configuring NTP Client Mode for a C Series Controller \(SRC CLI\) on page 141](#)
- [Configuring an NTP Peer on a C Series Controller \(SRC CLI\) on page 142](#)
- [Configuring NTP Broadcast Mode on a C Series Controller \(SRC CLI\) on page 143](#)
- [Configuring NTP Authentication on a C Series Controller \(SRC CLI\) on page 144](#)
- [Configuring NTP as a Broadcast Client on a C Series Controller \(SRC CLI\) on page 146](#)
- [Configuring NTP as a Multicast Client on a C Series Controller \(SRC CLI\) on page 147](#)
- [Disabling NTP Monitoring Service \(SRC CLI\) on page 148](#)
- [Configuring NTP Access Restrictions for a Specific Address \(SRC CLI\) on page 149](#)
- [Configuring NTP Access Restrictions for All IPv4 Addresses \(SRC CLI\) on page 150](#)
- [Configuring NTP Access Restrictions for All IPv6 Addresses \(SRC CLI\) on page 152](#)
- [Verifying NTP Configuration on a C Series Controller on page 153](#)

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;  
    disable-monitor;  
    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
Documentation**

- [SRC PE CLI Command Reference](#)
- [Configuring NTP on a C Series Controller on page 136](#)
- [NTP Support on C Series Controllers on page 135](#)

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
Documentation**

- [NTP Support on C Series Controllers on page 135](#)
- [Verifying NTP Configuration on a C Series Controller on page 153](#)

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

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

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

To configure NTP to operate in client mode:

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

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

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

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

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

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

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

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

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

**Related
Documentation**

- [Configuring NTP Client Mode for a C Series Controller \(C-Web Interface\)](#)
- [Specifying Which NTP Server a C Series Controller Contacts on Startup on page 140](#)
- [Verifying NTP Configuration on a C Series Controller on page 153](#)
- [NTP Support on C Series Controllers on page 135](#)

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

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

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

To configure NTP to operate in symmetric active mode:

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

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

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

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

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

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

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

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

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

Related Documentation

- [Configuring an NTP Peer for a C Series Controller \(C-Web Interface\)](#)
- [Specifying Which NTP Server a C Series Controller Contacts on Startup on page 140](#)
- [Verifying NTP Configuration on a C Series Controller on page 153](#)
- [NTP Support on C Series Controllers on page 135](#)

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

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

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

To configure NTP to operate in broadcast mode:

1. From configuration mode, access the configuration statement that configures NTP broadcast, and specify the broadcast address on one of the local networks or a multicast address assigned to NTP. You can specify an IP address or a hostname.

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

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

For example, to specify the broadcast address of 224.0.1.1:

```
[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 Documentation

- [Configuring NTP Broadcast Mode on a C Series Controller \(C-Web Interface\)](#)
- [Specifying Which NTP Server a C Series Controller Contacts on Startup on page 140](#)
- [Verifying NTP Configuration on a C Series Controller on page 153](#)
- [NTP Support on C Series Controllers on page 135](#)

Configuring NTP Authentication on a C Series Controller (SRC CLI)

You can authenticate time synchronization to ensure that a C Series Controller obtains its time services only from known sources. By default, network time synchronization is unauthenticated; the system synchronizes to whatever system appears to have the most accurate time. We highly recommend that you configure authentication of network time services.

Use the following configuration mode statements to configure authentication for NTP on a C Series Controller:

```
system ntp {  
    trusted-key [trusted-key...];  
}  
  
system ntp authentication-key key-number {  
    value value;  
}  
  
system ntp broadcast address {  
    key key ;  
}  
  
system ntp peer address {  
    key key;  
}  
  
system ntp server address {  
    key key;  
}
```

To configure NTP authentication:

1. Specify authentication for other time servers.

Only time servers transmitting network time packets that contain one of the specified key numbers and whose key matches the value configured for that key number are eligible for synchronization. Other systems can synchronize with the local system without being authenticated.

```
[edit system ntp]  
user@host# set trusted-key [trusted-key...]
```

where **trusted-key** is a value in the range 1–2147483647.

For example:

```
[edit system ntp]
user@host# set trusted-key 1
```

2. Depending on the mode configured for NTP, specify a key value at the **[edit system ntp server]**, **[edit system ntp peer]**, or **[edit system ntp broadcast]** hierarchy level. For example:

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

For example:

```
[edit system ntp server 192.0.2.30]
user@host# set key key1
```

The system transmits the specified authentication key when transmitting packets. The key is necessary if the remote system has authentication enabled so that it can synchronize with the local system.

3. Define the authentication keys by assigning a number to the key and configuring its value.

```
[edit system ntp]
user@host# edit authentication-key key-number
```

```
[edit system ntp authentication-key key-number ]
user@host# set value value
```

The **key-number** is the key number for the key. The key number must match on all systems using that particular key for authentication.

For example:

```
[edit system ntp]
user@host# edit authentication-key 1
```

```
[edit system ntp authentication-key 1]
user@host# set value X7VY4ZE
```

4. Verify the configuration.

```
[edit system ntp]
user@host# show
trusted-key 1;
server 192.0.2.30 key 1;
authentication-key 1 {
  value *****;
}
```

**Related
Documentation**

- [Configuring NTP Authentication \(C-Web Interface\)](#)
- [Specifying Which NTP Server a C Series Controller Contacts on Startup on page 140](#)
- [NTP Support on C Series Controllers on page 135](#)

Configuring NTP as a Broadcast Client on a C Series Controller (SRC CLI)

You can configure NTP on a C Series Controller to listen for broadcast messages on the local network to discover other servers on the same subnet. When NTP receives a broadcast message for the first time, it measures the nominal network delay using a brief client-server exchange with the remote server. It then enters *broadcast client* mode, in which it listens for, and synchronizes with, succeeding broadcast messages.

To avoid accidental or malicious disruption in this mode, both the local and remote systems must use authentication and the same trusted key and key identifier.

To configure NTP to listen for broadcast messages:

1. From the **[edit system ntp]** hierarchy level, specify that NTP listen for broadcast messages.

```
[edit system ntp]
user@host# set broadcast-client
```

2. Authenticate time synchronization to ensure that the local system obtains its time only from known sources.

See [“Configuring NTP Authentication on a C Series Controller \(SRC CLI\)” on page 144](#).

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 Documentation**
- [Specifying Which NTP Server a C Series Controller Contacts on Startup on page 140](#)
 - [NTP Support on C Series Controllers on page 135](#)

Configuring NTP as a Multicast Client on a C Series Controller (SRC CLI)

You can configure NTP on a C Series Controller to listen for multicast messages on the local network to discover other servers on the same subnet. When NTP receives a multicast message for the first time, it measures the nominal network delay using a brief client-server exchange with the remote server. It then enters *multicast client* mode, in which it listens for, and synchronizes with, succeeding multicast messages.

You can specify one or more IP addresses or hostnames. The hosts then join those multicast groups.

To avoid accidental or malicious disruption in this mode, both the local and remote systems must use authentication and the same trusted key and key identifier.

To configure NTP to listen for multicast messages:

1. From the **[edit system ntp]** hierarchy level, specify that NTP listen for multicast messages.

```
edit system ntp]
user@host# set multicast-client address
```

For example:

```
[edit system ntp]
user@host# set multicast-client 224.0.1.1
```

2. Authenticate time synchronization to ensure that the local system obtains its time only from known sources.

See “[Configuring NTP Authentication on a C Series Controller \(SRC CLI\)](#)” on page 144.

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 Documentation**
- [Configuring NTP as a Multicast Client on a C Series Controller \(C-Web Interface\)](#)
 - [Specifying Which NTP Server a C Series Controller Contacts on Startup on page 140](#)
 - [NTP Support on C Series Controllers on page 135](#)

Disabling NTP Monitoring Service (SRC CLI)

You can disable NTP monitoring feature to protect the network from flood attacks. If you disable the monitoring feature, the attackers cannot flood requests (that can cause Denial of Service) to the NTP server. By default, the monitoring feature is enabled on C Series Controllers.

Use the following configuration statements to disable the NTP monitoring service on C Series Controllers:

To disable the NTP monitoring service on C Series Controllers:

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

```
[edit]
user@host# set system ntp;
```

2. Disable the NTP monitoring service on C Series Controllers.

```
[edit system ntp]
user@host# set disable-monitor;
```

- Related Documentation**
- [Configuration Statements for NTP on C Series Controllers on page 139](#)
 - [NTP Support on C Series Controllers on page 135](#)
 - [Configuring NTP on a C Series Controller on page 136](#)

Configuring NTP Access Restrictions for a Specific Address (SRC CLI)

By default, all the clients (any IPv4 or IPv6 addresses of any network) except localhost are restricted to access the NTP server. Some of the CLI commands (for example, **show ntp status**) will work only if the access to the localhost is allowed. So, we recommend you to not delete the access to the localhost. You can use the **system ntp restrict address address** command to allow access for specific addresses to your NTP server and to configure NTP access restriction options for those addresses.

```
system ntp restrict address address {
    mask mask;
    kod;
    nomodify;
    nopeer;
    noquery;
    notrap;
}
```

To configure NTP access restrictions for a specific address:

1. From configuration mode, access the configuration statement that restricts NTP access for a specific address.

```
[edit]
user@host# set system ntp restrict address address ;
```

2. Specify the subnet mask of the host.

```
[edit system ntp restrict address address ]
user@host# set mask mask;
```

3. Specify whether to send a kiss-of-death packet if the client limit has exceeded.

```
[edit system ntp restrict address address ]
user@host# set kod;
```

4. Specify whether to restrict the client from making any changes to the NTP configurations.

```
[edit system ntp restrict address address ]
user@host# set nomodify;
```

5. Specify whether to prevent the client from establishing a peer association.

```
[edit system ntp restrict address address ]
user@host# set nopeer;
```

6. Specify whether to prevent the client from performing ntpq and ntpdc queries, but not time queries.

```
[edit system ntp restrict address address ]
user@host# set noquery;
```

7. Specify whether to prevent the client from configuring control message traps.

```
[edit system ntp restrict address address ]
user@host# set notrap;
```

Related Documentation

- [Configuration Statements for NTP on C Series Controllers on page 139](#)
- [NTP Support on C Series Controllers on page 135](#)
- [Configuring NTP on a C Series Controller on page 136](#)
- [Configuring NTP Access Restrictions for All IPv4 Addresses \(SRC CLI\) on page 150](#)
- [Configuring NTP Access Restrictions for All IPv6 Addresses \(SRC CLI\) on page 152](#)

Configuring NTP Access Restrictions for All IPv4 Addresses (SRC CLI)

By default, all the clients (any IPv4 or IPv6 addresses of any network) except localhost are restricted to access the NTP server. Some of the CLI commands (for example, **show ntp status**) will work only if the access to the localhost is allowed. So, we recommend you to not delete the access to the localhost. You can use the **system ntp restrict default-v4** command to allow access for all IPv4 addresses to your NTP server and to configure NTP access restriction options for IPv4 addresses.



NOTE: We recommend you to not delete or change the default restrictions available for the **edit system ntp restrict default-v4** command to avoid vulnerabilities.

```
system ntp restrict default-v4{
  kod;
  nomodify;
  nopeer;
  noquery;
  notrap;
}
```

To configure NTP access restrictions for all IPv4 addresses:

1. From configuration mode, access the configuration statement that restricts NTP access for all IPv4 addresses.

```
[edit]
user@host# edit system ntp restrict default-v4
```

2. Specify whether to send a kiss-of-death packet if the client limit has exceeded.

```
[edit system ntp restrict default-v4]  
user@host# set kod;
```

3. Specify whether to restrict the client from making any changes to NTP configurations.

```
[edit system ntp restrict default-v4]  
user@host# set nomodify;
```

4. Specify whether to prevent the client from establishing a peer association.

```
[edit system ntp restrict default-v4]  
user@host# set nopeer;
```

5. Specify whether to prevent the client from performing ntpq and ntpdc queries, but not time queries.

```
[edit system ntp restrict default-v4]  
user@host# set noquery;
```

6. Specify whether to prevent the client from configuring control message traps.

```
[edit system ntp restrict default-v4]  
user@host# set notrap;
```

**Related
Documentation**

- [Configuration Statements for NTP on C Series Controllers on page 139](#)
- [NTP Support on C Series Controllers on page 135](#)
- [Configuring NTP on a C Series Controller on page 136](#)
- [Configuring NTP Access Restrictions for All IPv6 Addresses \(SRC CLI\) on page 152](#)
- [Configuring NTP Access Restrictions for a Specific Address \(SRC CLI\) on page 149](#)

Configuring NTP Access Restrictions for All IPv6 Addresses (SRC CLI)

By default, all the clients (any IPv4 or IPv6 addresses of any network) except localhost are restricted to access the NTP server. Some of the CLI commands (for example, **show ntp status**) will work only if the access to the localhost is allowed. So, we recommend you to not delete the access to the localhost. You can use the **system ntp restrict default-v6** command to allow access for all IPv6 addresses to your NTP server and to configure NTP access restriction options for IPv6 addresses.



NOTE: We recommend you to not delete or change the default restrictions available for the **system ntp restrict default-v6** command to avoid vulnerabilities.

```
system ntp restrict default-v6{
  kod;
  nomodify;
  nopeer;
  noquery;
  notrap;
}
```

To configure NTP access restrictions for all IPv6 addresses:

1. From configuration mode, access the configuration statement that restricts NTP access for all IPv6 addresses.

```
[edit]
user@host# edit system ntp restrict default-v6;
```

2. Specify whether to send a kiss-of-death packet if the client limit has exceeded.

```
[edit system ntp restrict default-v6]
user@host# set kod;
```

3. Specify whether to restrict the client from making any changes to the NTP configurations.

```
[edit system ntp restrict default-v6]
user@host# set nomodify;
```

4. Specify whether to prevent the client from establishing a peer association.

```
[edit system ntp restrict default-v6]
user@host# set nopeer;
```

- Specify whether to prevent the client from performing ntpq and ntpdc queries, but not time queries.

```
[edit system ntp restrict default-v6]
user@host# set noquery;
```

- Specify whether to prevent the client from configuring control message traps.

```
[edit system ntp restrict default-v6]
user@host# set notrap;
```

Related Documentation

- [Configuration Statements for NTP on C Series Controllers on page 139](#)
- [NTP Support on C Series Controllers on page 135](#)
- [Configuring NTP on a C Series Controller on page 136](#)
- [Configuring NTP Access Restrictions for All IPv4 Addresses \(SRC CLI\) on page 150](#)
- [Configuring NTP Access Restrictions for a Specific Address \(SRC CLI\) on page 149](#)

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;
disable-monitor;
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 Documentation

- [Specifying Which NTP Server a C Series Controller Contacts on Startup on page 140](#)
- [NTP Support on C Series Controllers on page 135](#)

CHAPTER 17

Configuring System Logging for a C Series Controller (SRC CLI)

- [C Series Controller Log Server Overview on page 155](#)
- [Before You Configure System Logging \(SRC CLI\) on page 156](#)
- [Configuration Statements for System Logging on a C Series Controller on page 157](#)
- [Saving System Log Messages to a File \(SRC CLI\) on page 157](#)
- [Sending System Log Messages to Other Servers \(SRC CLI\) on page 158](#)
- [Sending Notifications for System Log Messages to Users \(SRC CLI\) on page 159](#)

C Series Controller Log Server Overview

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 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.

Related Documentation

- [Before You Configure System Logging \(SRC CLI\) on page 156](#)
- [Configuration Statements for System Logging on a C Series Controller on page 157](#)
- [Saving System Log Messages to a File \(C-Web Interface\)](#)
- [Sending System Log Messages to Other Servers \(C-Web Interface\)](#)
- [Sending Notifications for System Log Messages to Users \(C-Web Interface\)](#)

Before You Configure System Logging (SRC CLI)

Before you configure the system log server on a C Series Controller, you should be familiar with:

- The system log protocol
- Logging for SRC components

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

Related Documentation

- [C Series Controller Log Server Overview on page 155](#)

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*.

Related Documentation

- [Saving System Log Messages to a File \(SRC CLI\) on page 157](#)
- [Sending System Log Messages to Other Servers \(SRC CLI\) on page 158](#)
- [Sending Notifications for System Log Messages to Users \(SRC CLI\) on page 159](#)
- [C Series Controller Log Server Overview on page 155](#)

Saving System Log Messages to a File (SRC CLI)

Use the following statements to configure the system log server to store messages in a file:

```
system syslog file file-name (any | authorization | daemon | ftp | kernel | user | local7) {
    (any | emergency | alert | critical | error | warning | notice | info | none);
}
```

By default, message files are stored in the `/var/log` directory. Log files are rotated and compressed according to the settings in the `logrotate` utility.

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
```

Related Documentation

- [Saving System Log Messages to a File \(C-Web Interface\)](#)
- [Sending System Log Messages to Other Servers \(SRC CLI\) on page 158](#)
- [Sending Notifications for System Log Messages to Users \(SRC CLI\) on page 159](#)
- [C Series Controller Log Server Overview on page 155](#)
- [Rotating Log Files](#)

Sending System Log Messages to Other Servers (SRC CLI)

Use the following statements to configure the system log server to send messages to another system log server:

```
system syslog host log-host-name (any | authorization | daemon | ftp | kernel | user | local7)
{
  (any | emergency | alert | critical | error | warning | notice | info | none);
}
```

Before you configure the system log server to send messages to other system log servers, ensure that the remote system log server is configured to receive messages on the standard UDP port, 514.

To configure the system log server to send messages to another system log server:

1. From configuration mode, access the configuration statement that configures the system log server.

```
[edit]
user@host# edit system syslog
```

2. Specify the remote system log server to receive messages as well as the groups and severity level for those messages.

```
[edit system syslog]
```

```
user@host# set host log-host-name message-group severity
```

For example, to configure the system log server to send error messages generated by processes on the C Series Controller to my-syslog-server:

```
[edit system syslog]
user@host# set my-syslog-server.mydomain.com local7 error
```

Related Documentation

- [Sending System Log Messages to Other Servers \(C-Web Interface\)](#)
- [Saving System Log Messages to a File \(SRC CLI\) on page 157](#)
- [Sending Notifications for System Log Messages to Users \(SRC CLI\) on page 159](#)
- [C Series Controller Log Server Overview on page 155](#)

Sending Notifications for System Log Messages to Users (SRC CLI)

Use the following statements to configure the system log server to send notifications to users:

```
system syslog user user-name (any | authorization | daemon | ftp | kernel | user |
local7) {
  (any | emergency | alert | critical | error | warning | notice | info | none);
}
```

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

1. From configuration mode, access the configuration statement that configures the system log server.

```
[edit]
user@host# edit system syslog
```

2. Specify the user to receive notifications and the types of notifications to be sent.

```
[edit system syslog]
user@host# set user user-name message-group severity
```

For example, to configure the system log server to send notifications to admin for conditions that require immediate attention:

```
[edit system syslog]
user@host# set user admin any critical
```

**Related
Documentation**

- *[Sending Notifications for System Log Messages to Users \(C-Web Interface\)](#)*
- [Saving System Log Messages to a File \(SRC CLI\) on page 157](#)
- [Sending System Log Messages to Other Servers \(SRC CLI\) on page 158](#)
- [C Series Controller Log Server Overview on page 155](#)

Configuring Static Host Mapping (SRC CLI)

- [Static Host Mapping Overview on page 161](#)
- [Configuring Static Host Mapping \(SRC CLI\) on page 161](#)

Static Host Mapping Overview

You can configure static host mapping to resolve hostnames. 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.

**Related
Documentation**

- [Configuring Static Host Mapping \(C-Web Interface\)](#)
- [Configuring Static Host Mapping \(SRC CLI\) on page 161](#)

Configuring Static Host Mapping (SRC CLI)

Use the following statements to configure static host mapping:

```
system static-host-mapping host-name {  
    inet [inet...];  
    alias [alias...];  
}
```

To configure static host mapping:

1. From configuration mode, access the configuration statement that configures static host mapping and specify the fully-qualified name of the system.

```
[edit]  
user@host# edit system static-host-mapping host-name
```

2. Specify the IPv4 or IPv6 addresses to which you want to map the hostname.

```
[edit system static-host-mapping host-name]  
user@host# set inet inet
```

3. (Optional) Specify the aliases for this host.

```
[edit system static-host-mapping host-name]  
user@host# set alias alias
```

**Related
Documentation**

- *Configuring Static Host Mapping (C-Web Interface)*
- [Static Host Mapping Overview on page 161](#)

CHAPTER 19

Overview of the Juniper Networks Database

- [Juniper Networks Database Overview on page 163](#)

Juniper Networks Database Overview

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.

The Juniper Networks database is designed to store a limited number of subscriber entries that may be shared among your subscribers. If you need to have dedicated entries for each subscriber, you can configure the SRC software to use an external directory. We recommend that an external directory store the subscriber data in environments that have more than 1000 subscribers with an average of 3 subscriptions per subscriber.

You can also set a limit on the maximum number of search results that the server returns to a client in response to a search operation. You must set the size limit on the basis of the total number of available entries in the Juniper Networks Database.

When the C Series Controller starts for the first time, you must enable the Juniper Networks database. After the database is operational, you can load sample data and perform other configuration activities that use this database.

You can operate this database as a standalone database or as a member of a community of Juniper Networks databases. Typically, you run the database in standalone mode only in testing environments. In standalone mode, the database does not communicate with other Juniper Networks databases; there is no data distribution and no redundancy. In community mode, databases distribute data changes among specified databases. When you have two or more C Series Controllers, enable the Juniper Networks database to run in community mode, and assign a role to each database:

- **Primary role**—A database that provides read-and-write access to client applications. It replicates its data and distributes changes to any Juniper Networks databases configured as neighbors.

We recommend that you configure at least two databases to have a primary role.

- Secondary role—A database that provides read access to client applications. If client applications try to write data to this database, the database refers the client to a primary database.

Neighbors are Juniper Networks databases that receive data from another Juniper Networks database. When you configure a database to be a neighbor, you configure it as one of the following types:

- Primary neighbor—A database that propagates changes that it receives to other Juniper Networks databases configured as neighbors. A primary neighbor must be assigned a primary role.

We recommend that you configure at least two databases as primary neighbors.

- Secondary neighbor—A database that only receives database changes. A secondary neighbor must be assigned a secondary role.

When you configure neighbors for the databases, keep in mind the following guidelines:

- A database assigned a primary role can have primary and secondary neighbors.
- A database assigned a secondary role must have at least one primary neighbor, but no secondary neighbors. Because a secondary database cannot distribute changes to its neighbors, if you do configure a secondary neighbor for a secondary database, the software does not use the configuration for the secondary neighbor.

To share processing load, you can configure 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.

For information about configuring the SAE to access subscriber data, see *Configuring LDAP Access to Directory Data (SRC CLI)*.

Related Documentation

- [Adding a Juniper Networks Database to an Established Community \(SRC CLI\) on page 176](#)
- [Configuration Statements for the Juniper Networks Database \(SRC CLI\) on page 168](#)
- [Viewing Statistics for the Juniper Networks Database \(C-Web Interface\)](#)
- [Example: Configuration for a Database Community on page 182](#)
- [Setting a Limit on the Number of Search Results from a Juniper Networks Database \(SRC CLI\) on page 169](#)

CHAPTER 20

Managing the Juniper Networks Database (SRC CLI)

- [Configuration Statements for the Juniper Networks Database \(SRC CLI\) on page 168](#)
- [Enabling the Juniper Networks Database to Run in Standalone Mode \(SRC CLI\) on page 168](#)
- [Setting a Limit on the Number of Search Results from a Juniper Networks Database \(SRC CLI\) on page 169](#)
- [Running the Juniper Networks Database in Community Mode \(SRC CLI\) on page 170](#)
- [Securing the Juniper Networks Database \(SRC CLI\) on page 174](#)
- [Connecting to Juniper Networks Databases Through LDAPS from an Application Outside the C Series Controller \(SRC CLI\) on page 175](#)
- [Changing the Mode of a Juniper Networks Database \(SRC CLI\) on page 175](#)
- [Adding a Juniper Networks Database to an Established Community \(SRC CLI\) on page 176](#)
- [Promoting a Secondary Database to a Primary Role in a Configuration with One Primary Database \(SRC CLI\) on page 177](#)
- [Updating Data on a Juniper Networks Database \(SRC CLI\) on page 178](#)
- [Synchronizing Data on a Juniper Networks Database \(SRC CLI\) on page 178](#)
- [Loading Sample Data into a Juniper Networks Database \(SRC CLI\) on page 179](#)
- [Securing Communications Between the Juniper Networks Database and SRC Modules and Components \(SRC CLI\) on page 180](#)
- [Verifying Configuration for a Juniper Networks Database with the SRC CLI on page 181](#)
- [Getting Information About Operations in a Juniper Networks Database \(SRC CLI\) on page 181](#)
- [Example: Configuration for a Database Community on page 182](#)
- [Troubleshooting Data Synchronization for Juniper Networks Databases \(SRC CLI\) on page 186](#)
- [Recovering Data in a Community with One Primary Database and One Secondary Database \(SRC CLI\) on page 187](#)

Configuration Statements for the Juniper Networks Database (SRC CLI)

Use the following configuration statements to configure the Juniper Networks database at the **[edit]** hierarchy level:

```
system ldap server {
  maximum-entries-returned maximum-entries-returned;
  stand-alone;
}
system ldap server community {
  role (primary | secondary);
  primary-neighbors [primary-neighbor...];
  primary-connection-type (clear | secure);
  secondary-neighbors [secondary-neighbor...];
  secondary-connection-type (clear | secure);
}
maximum-entries-returned maximum-entries-returned;
system ldap server security {
  (enable | strict);
}
```



NOTE: The strict statement is supported only on C Series Controllers.

Related Documentation

- [Enabling the Juniper Networks Database to Run in Standalone Mode \(SRC CLI\) on page 168](#)
- [Enabling the Juniper Networks Database to Run in Community Mode \(SRC CLI\) on page 170](#)
- [Securing the Juniper Networks Database \(SRC CLI\) on page 174](#)
- [Juniper Networks Database Overview on page 163](#)
- [Setting a Limit on the Number of Search Results from a Juniper Networks Database \(SRC CLI\) on page 169](#)
- [Verifying Configuration for a Juniper Networks Database with the SRC CLI on page 181](#)

Enabling the Juniper Networks Database to Run in Standalone Mode (SRC CLI)

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

Use the following configuration statements to enable the Juniper Networks database on a C Series Controller in standalone mode:

```
system ldap server {
  stand-alone;
```

```
}
```

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

1. From configuration mode, access the configuration statement that configures the Juniper Networks database.

```
user@host# edit system ldap server
```

2. Enable standalone mode.

```
[edit system ldap server]
user@host# set stand-alone
```

Related Documentation

- [Enabling the Juniper Networks Database to Run in Standalone Mode \(C-Web Interface\)](#)
- [Enabling the Juniper Networks Database to Run in Community Mode \(SRC CLI\) on page 170](#)
- [Securing the Juniper Networks Database \(SRC CLI\) on page 174](#)
- [Configuration Statements for the Juniper Networks Database \(SRC CLI\) on page 168](#)
- [Juniper Networks Database Overview on page 163](#)

Setting a Limit on the Number of Search Results from a Juniper Networks Database (SRC CLI)

You can set a limit on the maximum number of search results that the server returns to a client in response to a search operation. You must set the size limit on the basis of the total number of available entries in the Juniper Networks Database. The size limit value range is -1 through 2,147,483,647. By default, the size limit is set to 2000 in the `dse.ldif` file.

If the size limit you set is lower than the number of available matching entries, the server returns all matching search results to the client with an error message indicating that you have exceeded the size limit. If you set the size limit to -1, there is no restriction on the number of search results and the server returns all matching search results to the client.

Use the following configuration statements to specify the maximum number of search results to return in response to a search operation:

```
system ldap server {
  maximum-entries-returned maximum-entries-returned;
}
```

To configure the limit on the number of search results from a Juniper Networks Database:

1. From configuration mode, access the configuration statement that configures the Juniper Networks database.

```
user@host# edit system ldap server
```

2. Specify the maximum number of search results to return in response to a search operation.

```
[edit system ldap server]  
user@host# set maximum-entries-returned maximum-entries-returned
```

**Related
Documentation**

- [Configuration Statements for the Juniper Networks Database \(SRC CLI\) on page 168](#)
- [Juniper Networks Database Overview on page 163](#)

Running the Juniper Networks Database in Community Mode (SRC CLI)

- [Enabling the Juniper Networks Database to Run in Community Mode \(SRC CLI\) on page 170](#)
- [Configuring the Hostname When Running the Juniper Networks Database in Community Mode \(SRC CLI\) on page 172](#)

Enabling the Juniper Networks Database to Run in Community Mode (SRC CLI)

If you are adding a Juniper Networks database to an existing community, see [“Adding a Juniper Networks Database to an Established Community \(SRC CLI\)” on page 176](#).

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...];  
  primary-connection-type (clear | secure);  
  secondary-neighbors [secondary-neighbor...];  
  secondary-connection-type (clear | secure);  
}
```

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. Specify the connection type of the configured primary neighbors as clear or secure:

```
[edit system ldap server community]
user@host# set primary-connection-type clear
```

or

```
[edit system ldap server community]
user@host# set primary-connection-type secure
```

Where:

- clear—Sets LDAP as a data replication protocol between SRC and the LDAP nodes that are configured in the primary neighbors.
 - secure—Sets LDAPS as a data replication protocol between SRC and the LDAP nodes that are configured in the primary neighbors.
5. 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
```

6. Specify the connection type of the configured secondary neighbors as clear or secure:

```
[edit system ldap server community]
```

```
user@host# set secondary-connection-type clear
```

or

```
[edit system ldap server community]
```

```
user@host# set secondary-connection-type secure
```

Where:

- clear—Sets LDAP as a data replication protocol between SRC and the LDAP nodes that are configured in the secondary neighbors.
- secure—Sets LDAPS as a data replication protocol between SRC and the LDAP nodes that are configured in the secondary neighbors.

- See Also**
- [Configuring the Juniper Networks Database to Run in Community Mode \(C-Web Interface\)](#)
 - [Enabling the Juniper Networks Database to Run in Standalone Mode \(SRC CLI\) on page 168](#)
 - [Securing the Juniper Networks Database \(SRC CLI\) on page 174](#)
 - [Viewing Information About the Juniper Networks Database in Community Mode \(C-Web Interface\)](#)
 - [Configuration Statements for the Juniper Networks Database \(SRC CLI\) on page 168](#)
 - [Example: Configuration for a Database Community on page 182](#)
 - [Juniper Networks Database Overview on page 163](#)

Configuring the Hostname When Running the Juniper Networks Database in Community Mode (SRC CLI)

If you run Juniper Networks databases in community mode, all C Series Controllers that have a Juniper Networks database configured to be part of a community require hostname configuration.

You can either configure Domain Name System (DNS) and enter the controller names into DNS or configure the controller names as static hostnames in all C Series Controllers.

To configure each C Series Controller to use DNS:

1. Navigate to the **[edit system]** hierarchy level.

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

2. Specify the name of a name server.

```
[edit system]
user@host# set name-server name-server
```

where *name-server* is the IP address of a DNS name server.

To configure static hostnames for each C Series Controller:

1. Navigate to the **[edit system]** hierarchy level.

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

2. Specify the name of a C Series Controller as the static hostname.

```
[edit system]
user@host# set static-host-mapping host-name
```

where *host-name* is the fully qualified name.

- See Also**
- [Configuring the Juniper Networks Database to Run in Community Mode \(C-Web Interface\)](#)
 - [Securing the Juniper Networks Database \(SRC CLI\) on page 174](#)
 - [Viewing Information About the Juniper Networks Database in Community Mode \(C-Web Interface\)](#)
 - [Configuration Statements for the Juniper Networks Database \(SRC CLI\) on page 168](#)
 - [Example: Configuration for a Database Community on page 182](#)

- Related Documentation**
- [Configuring the Juniper Networks Database to Run in Community Mode \(C-Web Interface\)](#)
 - [Enabling the Juniper Networks Database to Run in Standalone Mode \(SRC CLI\) on page 168](#)
 - [Securing the Juniper Networks Database \(SRC CLI\) on page 174](#)
 - [Viewing Information About the Juniper Networks Database in Community Mode \(C-Web Interface\)](#)
 - [Configuration Statements for the Juniper Networks Database \(SRC CLI\) on page 168](#)
 - [Example: Configuration for a Database Community on page 182](#)
 - [Juniper Networks Database Overview on page 163](#)

Securing the Juniper Networks Database (SRC CLI)

You can secure connections to a Juniper Networks database by:

- Allowing only Secure Lightweight Directory Access Protocol (LDAPS) connections from remote systems. In this case, both database replication and remote SRC components connect through LDAPS. Restricting all remote connections to LDAPS is supported only on C Series Controllers.
- Allowing only LDAPS connections for database replication, but LDAP or LDAPS connections for other applications. In this case, remote SRC components can connect through LDAP or LDAPS.

Use the following configuration statements to secure connections to the Juniper Networks database on a C Series Controller:

```
system ldap server security {  
  (enable | strict);  
}
```



NOTE: 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 Documentation

- [Securing the Juniper Networks Database \(C-Web Interface\)](#)
- [Securing Communications Between the Juniper Networks Database and SRC Modules and Components \(SRC CLI\) on page 180](#)
- [Configuration Statements for the Juniper Networks Database \(SRC CLI\) on page 168](#)
- [Juniper Networks Database Overview on page 163](#)

Connecting to Juniper Networks Databases Through LDAPS from an Application Outside the C Series Controller (SRC CLI)

To connect to Juniper Networks databases through LDAPS from an application outside the C Series Controller, you must import the Juniper Networks database CA certificate into the application's trusted CA certificate store.

Use the following configuration statements to export the Juniper Networks database CA certificate to a file in ASCII format and then import the CA certificate into the trusted CA certificate store:

1. Export the Juniper Networks database CA certificate:

```
[edit system ldap server]
user@host# request system ldap security export-certificate file-name
```

2. Import the CA certificate into the trusted CA certificate store:

```
[edit system ldap server]
user@host# request system security import-certificate file-name
```

Related Documentation

- [Securing the Juniper Networks Database \(C-Web Interface\)](#)
- [Securing Communications Between the Juniper Networks Database and SRC Modules and Components \(SRC CLI\) on page 180](#)
- [Configuration Statements for the Juniper Networks Database \(SRC CLI\) on page 168](#)
- [Juniper Networks Database Overview on page 163](#)

Changing the Mode of a Juniper Networks Database (SRC CLI)

Because the Juniper Networks database (jdb component) 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 mode:

1. Disable standalone mode:

```
[edit system ldap server]
user@host# delete stand-alone
```

2. Enable the database in community mode, and configure the role and neighbors.

See [“Enabling the Juniper Networks Database to Run in Community Mode \(SRC CLI\)”](#) on page 170.



NOTE: You must configure the Juniper Networks database either in standalone or community mode. Otherwise, the commit is not successful and when you commit the changes, a message indicating that the jdb component is not configured is displayed.

Related Documentation

- [Enabling the Juniper Networks Database to Run in Standalone Mode \(SRC CLI\)](#) on page 168
- [Configuration Statements for the Juniper Networks Database \(SRC CLI\)](#) on page 168
- [Juniper Networks Database Overview](#) on page 163

Adding a Juniper Networks Database to an Established Community (SRC CLI)

When you add a Juniper Networks database to an existing community, make sure that you configure the primary neighbor relationships from the existing primary databases before you enable the new database.



WARNING: If you assign a primary role to a database new to an existing community before you configure the neighbor relationships from existing community databases that have a primary role, you can lose data on neighbor databases that already have a primary role.

To add a Juniper Networks database to an existing community:

1. On existing databases that have a primary role, configure neighbor relationships for the new database.

For example, to configure primary neighbors for the existing servers C1 and C2 for the new server C-new:

On C1:

```
[edit system ldap server community]
user@C1# set primary-neighbor C-new
```

On C2:

```
[edit system ldap server community]
user@C2# set primary-neighbor C-new
```

2. On the new database, enable the primary role and configure primary neighbors.

For example, to enable the database in primary role and configure C1 and C2 as primary neighbors:

```
[edit]
user@C-new# edit system ldap server community
[edit system ldap server community]
user@C-new# set role primary

user@C-new# set primary-neighbors C1 C2
```

Related Documentation

- [Adding a Juniper Networks Database to an Established Community \(C-Web Interface\)](#)
- [Enabling the Juniper Networks Database to Run in Community Mode \(SRC CLI\) on page 170](#)
- [Configuration Statements for the Juniper Networks Database \(SRC CLI\) on page 168](#)
- [Juniper Networks Database Overview on page 163](#)

Promoting a Secondary Database to a Primary Role in a Configuration with One Primary Database (SRC CLI)

Although all communities should have two databases with a primary role, if a community includes one database assigned a primary role and another database assigned a secondary role, promote the database assigned a secondary role to a primary role.

To promote a Juniper Networks database from a secondary role to a primary role:

1. On the database that has a secondary role, set the role to primary.

For example, if the database on C2 has a secondary role:

```
user@C2# edit system ldap server community
[edit system ldap server community]
user@C2# set role primary
user@C2# commit
```

C2 already has C1 configured as primary neighbor.

2. On the existing database that has a primary role, remove the neighbor as secondary and add it as primary.

For example, to remove C2 as a secondary neighbor and add it as a primary neighbor for the database on C1:

```
user@C1# edit system ldap server community
[edit system ldap server community]
user@C1# set primary-neighbors C2
user@C1# commit
```

3. (Optional if you have two databases with a primary role in a community) Switch the role of the database that originally had a secondary role back to secondary:

```
[edit system ldap server community]
user@C2# set role secondary
user@C2# commit
```

**Related
Documentation**

- [Promoting a Secondary Database to a Primary Role in a Configuration with One Primary Database \(C-Web Interface\)](#)
- [Enabling the Juniper Networks Database to Run in Community Mode \(SRC CLI\) on page 170](#)
- [Recovering Data in a Community with One Primary Database and One Secondary Database \(SRC CLI\) on page 187](#)
- [Configuration Statements for the Juniper Networks Database \(SRC CLI\) on page 168](#)
- [Juniper Networks Database Overview on page 163](#)

Updating Data on a Juniper Networks Database (SRC CLI)

After you bring a Juniper Networks database online after some period of inaccessibility, update the database with any database changes that occurred while the database was offline.

To update data in a neighbor (for example, neighbor1) in a community of Juniper Networks databases:

```
user@host> request system ldap community force-update neighbor neighbor1
```

**Related
Documentation**

- [Updating Data on a Juniper Networks Database \(C-Web Interface\)](#)
- [Synchronizing Data on a Juniper Networks Database \(SRC CLI\) on page 178](#)
- [Getting Information About Operations in a Juniper Networks Database \(SRC CLI\) on page 181](#)
- [Juniper Networks Database Overview on page 163](#)

Synchronizing Data on a Juniper Networks Database (SRC CLI)

You can initialize a Juniper Networks database with data from a neighbor. This process takes the following actions on the database to be initialized:

- Removes any existing data
- Copies data from the system on which the **request system ldap community initialize neighbor** command is run

To replace data on a neighbor database (for example, neighbor1):

- On the system that contains the source database to be replicated:

```
user@host> request system ldap community initialize neighbor neighbor1
```

Related Documentation

- [Synchronizing Data on a Juniper Networks Database \(C-Web Interface\)](#)
- [Updating Data on a Juniper Networks Database \(SRC CLI\) on page 178](#)
- [Troubleshooting Data Synchronization for Juniper Networks Databases \(SRC CLI\) on page 186](#)
- [Getting Information About Operations in a Juniper Networks Database \(SRC CLI\) on page 181](#)
- [Juniper Networks Database Overview on page 163](#)

Loading Sample Data into a Juniper Networks Database (SRC CLI)

The SRC software provides SRC 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 SRC SNMP agent
- Sample applications:
 - Sample residential portal (unsupported sample application)
 - Equipment registration mode
 - Internet service provider (ISP) mode

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

To load sample data for new entries, including deleted entries, from the specified file:

- Enter the **request system ldap load merge** command.

If you do not specify an option, **merge** is the default option.

To load sample data for all entries from the specified file:

- Enter the **request system ldap load replace** command.

This option will overwrite all existing entries.

To load sample data for the Volume Tracking Application (VTA) component:

```
user@host> request system ldap load vta-configuration
```

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 SRC 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
```

**Related
Documentation**

- [Loading Sample Data into a Juniper Networks Database \(C-Web Interface\)](#)
- [Getting Information About Operations in a Juniper Networks Database \(SRC CLI\) on page 181](#)
- [Juniper Networks Database Overview on page 163](#)

Securing Communications Between the Juniper Networks Database and SRC Modules and Components (SRC CLI)

Communications between SRC components and the Juniper Networks database use password authentication. You can change the default passwords for the following software components to ensure that communications are secure.

- SRC CLI
- NIC
- Configuration for SRC components other than the CLI and the NIC

To change a user password:

```
user@host> request system ldap change-component-password component-name  
new-password new-password
```

where *component-name* is:

- cli—Specifies communication between the SRC CLI and the database
- conf—Specifies communication about configuration
- nic—Specifies communication between NIC components and the database

**Related
Documentation**

- [Securing Communications Between the Juniper Networks Database and SRC Modules and Components \(C-Web Interface\)](#)
- [Securing the Juniper Networks Database \(SRC CLI\) on page 174](#)

- [Juniper Networks Database Overview on page 163](#)

Verifying Configuration for a Juniper Networks Database with the SRC CLI

Purpose Review the configuration for the Juniper Networks database on a C Series Controller.

Action • Run the **show system ldap server** command at the [edit] hierarchy level. For example:

```
[edit]
user@host# show system ldap server
community {
  primary-connection-type clear;
  primary-neighbors C2;
  role primary;
}
maximum-entries-returned 3000;
```

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 Documentation**
- [Enabling the Juniper Networks Database to Run in Standalone Mode \(SRC CLI\) on page 168](#)
 - [Enabling the Juniper Networks Database to Run in Community Mode \(SRC CLI\) on page 170](#)
 - [Securing the Juniper Networks Database \(SRC CLI\) on page 174](#)
 - [Configuration Statements for the Juniper Networks Database \(SRC CLI\) on page 168](#)
 - [Juniper Networks Database Overview on page 163](#)

Getting Information About Operations in a Juniper Networks Database (SRC CLI)

Purpose Get information about operations performed on a Juniper Networks database.

```
Action user@host> show system ldap statistics
Local JDB statistics
Number of Add operations since startup          0
Number of Delete operations since startup       0
Number of Modify operations since startup       0
Number of Rename operations since startup       0
Number of Read operations since startup        265
Number of List operations since startup         129
Number of Subtree Search operations since startup 114
Number of Bind operations                     110
Number of Anonymous Bind operations since startup 94
Number of Compare operations since startup      0
Number of current connections                  3
Number of all connections since startup        110
Number of bind errors since startup            0
Number of all errors since startup             59
```

- Related Documentation**
- [Troubleshooting Data Synchronization for Juniper Networks Databases \(SRC CLI\) on page 186](#)
 - [Updating Data on a Juniper Networks Database \(SRC CLI\) on page 178](#)
 - [Recovering Data in a Community with One Primary Database and One Secondary Database \(SRC CLI\) on page 187](#)
 - [Juniper Networks Database Overview on page 163](#)

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 182](#)
- [Overview and Sample Topology on page 183](#)
- [Configuration on page 183](#)

Requirements

Software

Hardware

Minimum SRC Release 1.0.0

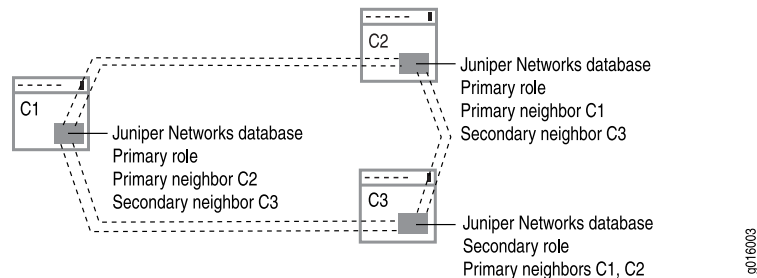
C2000 or C4000

Overview and Sample Topology

You configure a number of Juniper Networks databases as members of a community to protect data by replicating data from one database to another, and by specifying relationships between databases to support failover if a database that has the primary role for a set of applications becomes inoperable. This example uses C1 and C2 as databases that have a primary role, and C3 as a database that has a secondary role.

Figure 17 on page 183 shows the sample configuration.

Figure 17: Sample Community of Juniper Network Databases



The following configuration shows the configuration statements for databases shown in Figure 17 on page 183.

Configuration

- [Configuring C1 on page 183](#)
- [Configuring C2 on page 184](#)
- [Configuring C3 on page 185](#)

Configuring C1

CLI Quick Configuration

To quickly configure a Juniper Networks database, copy the following commands into a text editor, and modify them; then load the configuration from the file.

```
[edit]
set system ldap server community role primary
set system ldap server community primary-neighbors C2
set system ldap server community primary-connection-type clear
set system ldap server community secondary-neighbors C3
set system ldap server community secondary-connection-type clear
```

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 the connection type of the primary neighbors as clear.

```
[edit system ldap server community]
user@C1# set primary-connection-type clear
```

5. Specify secondary neighbors.

```
[edit system ldap server community]
user@C1# set secondary-neighbors C3
```

6. Specify the connection type of the secondary neighbors as clear.

```
[edit system ldap server community]
user@C1# set secondary-connection-type clear
```

Configuring C2

CLI Quick Configuration To customize the configuration example for your needs, copy the following commands into a text editor, and modify them; then load the configuration from the file.

```
[edit]
set system ldap server community role primary
set system ldap server community primary-neighbors C1
set system ldap server community primary-connection-type clear
set system ldap server community secondary-neighbors C3
set system ldap server community secondary-connection-type clear
```

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 the connection type of the primary neighbors as clear.

```
[edit system ldap server community]
user@C1# set primary-connection-type clear
```

5. Specify secondary neighbors.

```
[edit system ldap server community]
user@C2# set secondary-neighbors C3
```

6. Specify the connection type of the secondary neighbors as clear.

```
[edit system ldap server community]
user@C1# set secondary-connection-type clear
```

Configuring C3

CLI Quick Configuration To customize the configuration example for your needs, copy the following commands into a text editor, and modify them; then load the configuration from the file.

```
[edit]
set system ldap server community role secondary
set system ldap server community primary-neighbors C1 C2
set system ldap server community primary-connection-type clear
```

**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
```

4. Specify the connection type of the primary neighbors as clear.

```
[edit system ldap server community]  
user@C1# set primary-connection-type clear
```

**Related
Documentation**

- [Enabling the Juniper Networks Database to Run in Community Mode \(SRC CLI\) on page 170](#)
- [Configuration Statements for the Juniper Networks Database \(SRC CLI\) on page 168](#)
- [Juniper Networks Database Overview on page 163](#)

Troubleshooting Data Synchronization for Juniper Networks Databases (SRC CLI)

Problem **Description:** 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 neighbor1
```

where neighbor1 is the name of the neighbor to be synchronized.

**Related
Documentation**

- [Recovering Data in a Community with One Primary Database and One Secondary Database \(SRC CLI\) on page 187](#)
- [Promoting a Secondary Database to a Primary Role in a Configuration with One Primary Database \(SRC CLI\) on page 177](#)
- [Synchronizing Data on a Juniper Networks Database \(SRC CLI\) on page 178](#)
- [Updating Data on a Juniper Networks Database \(SRC CLI\) on page 178](#)
- [Juniper Networks Database Overview on page 163](#)

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

In an environment in which a community includes one database assigned a primary role and another database assigned a secondary role, and the primary database is not operative, you must promote the secondary database to primary and reconfigure the inoperative primary database.

1. On the database that has a secondary role, set the role to primary.

For example, if the database on C2 has a secondary role:

```
user@C2# edit system ldap server community
[edit system ldap server community]
user@C2# set role primary
user@C2# commit
```

C2 already has C1 configured as primary neighbor.

2. On the existing database that has a primary role, remove the neighbor as secondary and add it as primary.

For example, to configure C1 as a primary database with C2 as a primary neighbor:

```
user@C1# edit system ldap server community
[edit system ldap server community]
user@C1# set role primary
user@C1# delete secondary-neighbors C2
user@C1# set primary-neighbors C2
user@C1# commit
```

**Related
Documentation**

- [Recovering Data in a Community with One Primary Database and One Secondary Database \(C-Web Interface\)](#)
- [Promoting a Secondary Database to a Primary Role in a Configuration with One Primary Database \(SRC CLI\) on page 177](#)
- [Troubleshooting Data Synchronization for Juniper Networks Databases \(SRC CLI\) on page 186](#)
- [Juniper Networks Database Overview on page 163](#)

CHAPTER 21

Setting Up an SAE (SRC CLI)

- [Initially Configuring the SAE on page 189](#)
- [Grouped Configurations for the SAE on page 190](#)
- [Configuring Local Properties for the SAE \(SRC CLI\) on page 191](#)
- [Configuring the RADIUS Local IP Address and NAS ID \(SRC CLI\) on page 195](#)
- [Starting the SAE \(SRC CLI\) on page 196](#)
- [Stopping the SAE \(SRC CLI\) on page 196](#)

Initially Configuring the SAE

To initially configure the SAE:

- (Optional) Create a configuration group for the SAE.
See [“Creating Grouped Configurations for the SAE \(SRC CLI\)” on page 190](#)
- Configure local properties for the SAE.
See [“Configuring Local Properties for the SAE \(SRC CLI\)” on page 191](#)
- Configure a local IP address and NAS ID that the SAE uses to communicate with RADIUS servers.
See [“Configuring the RADIUS Local IP Address and NAS ID \(SRC CLI\)” on page 195](#)
- Configure directory connection properties for the SAE.
- Configure directory eventing properties for the SAE.
See [Configuring Initial Directory Eventing Properties for SRC Components on page 323](#)

Related Documentation

- [Initially Configuring the SAE \(C-Web Interface\)](#)
- [Reloading the SAE Configuration \(SRC CLI\)](#)
- [Starting the SAE \(SRC CLI\) on page 196](#)

Grouped Configurations for the SAE

- [Creating Grouped Configurations for the SAE \(SRC CLI\) on page 190](#)
- [Configuring an SAE Group on page 190](#)
- [Deleting Default Configurations Within an SAE Group on page 191](#)

Creating Grouped Configurations for the SAE (SRC CLI)

We recommend that you configure the SAE within a group. When you create a configuration group, the software creates a configuration with default values filled in.

Configuration groups allow you to build hierarchies that define different levels of sharing. There is a shared SAE configuration that you configure at the **shared saeconfiguration** 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.

- See Also**
- [Initially Configuring the SAE on page 189](#)
 - [Configuring an SAE Group on page 190](#)
 - [Configuring Local Properties for the SAE \(SRC CLI\) on page 191](#)
 - [Configuring the RADIUS Local IP Address and NAS ID \(SRC CLI\) on page 195](#)
 - [Deleting Default Configurations Within an SAE Group](#)

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
```

- See Also**
- [Configuring an SAE Group \(C-Web Interface\)](#)
 - [Creating Grouped Configurations for the SAE \(SRC CLI\) on page 190](#)
 - [Initially Configuring the SAE on page 189](#)
 - [Deleting Default Configurations Within an SAE Group](#)
 - [Configuring Local Properties for the SAE \(SRC CLI\) on page 191](#)

Deleting Default Configurations Within an SAE Group

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

If there are multiple SAE groups and you delete a default configuration in more than one group, the software adds the default configurations only to the group that is currently set with the **set slot 0 sae shared** command.

- See Also**
- [Creating Grouped Configurations for the SAE \(SRC CLI\) on page 190](#)
 - [Configuring an SAE Group on page 190](#)
 - [Configuring an SAE Group \(C-Web Interface\)](#)
 - [Initially Configuring the SAE \(C-Web Interface\)](#)
 - [Initially Configuring the SAE on page 189](#)

Configuring Local Properties for the SAE (SRC CLI)

Use the following configuration statements to configure local properties for the SAE:

```
slot number sae {  
  base-dn base-dn ;  
  real-portal-address real-portal-address ;  
  java-runtime-environment java-runtime-environment ;  
  java-min-heap-size java-min-heap-size ;  
  java-heap-size java-heap-size ;  
  java-min-new-size java-min-new-size ;  
  java-new-size java-new-size ;  
  java-min-heap-size-percentage java-min-heap-size-percentage ;  
  java-heap-size-percentage java-heap-size-percentage ;  
  java-min-new-size-percentage java-min-new-size-percentage ;  
  java-new-size-percentage java-new-size-percentage ;  
  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) Configure the percentage of total memory that should be allocated to the minimum heap memory size of SAE process.

```
[edit slot 0 sae]  
user@host# set java-min-heap-size-percentage java-min-heap-size-percentage
```



NOTE: You cannot configure the *java-min-heap-size* option manually. This option is automatically configured based on the value set to the *java-min-heap-size-percentage* option.

5. (Optional) If you encounter problems caused by lack of memory, change the percentage of total memory that should be allocated to the maximum heap memory size of SAE process.

[edit slot 0 sae]

user@host# set java-heap-size-percentage *java-heap-size-percentage*



NOTE: You cannot configure the `java-heap-size` option manually. This option is automatically configured based on the value set to the `java-heap-size-percentage` option.

6. Configure the percentage of total memory that should be allocated to the minimum young generation size of SAE process.

[edit slot 0 sae]

user@host# set java-min-new-size-percentage *java-min-new-size-percentage*



NOTE: You cannot configure the `java-min-new-size` option manually. This option is automatically configured based on the value set to the `java-min-new-size-percentage` option.

7. Configure the percentage of total memory that should be allocated to the maximum young generation size of SAE process.

[edit slot 0 sae]

user@host# set java-new-size-percentage *java-new-size-percentage*



NOTE: You cannot configure the `java-new-size` option manually. This option is automatically configured based on the value set to the `java-new-size-percentage` option.



NOTE: SAE restart is required if the `java-min-heap-size-percentage`, `java-heap-size-percentage`, `java-min-new-size-percentage`, or `java-new-size-percentage` option is changed. When upgrading from SRC 4.11 or earlier versions, if the heap value set to `java-min-heap-size`, `java-heap-size`, `java-min-new-size`, or `java-new-size` is less than 1 percent of total memory, then the `java-min-heap-size-percentage`, `java-heap-size-percentage`, `java-min-new-size-percentage`, or `java-new-size-percentage` value will be set to 1%, respectively. If the heap value is greater than the total memory, then the percentage value will be set to 100%.

8. 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
```

9. 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
```

10. (Optional) Enable the SRC SNMP agent to communicate with the SAE.

```
[edit slot 0 sae]
user@host# set snmp-agent
```

11. (Optional) Configure an SAE group configuration.

```
[edit slot 0 sae]
user@host# set shared shared
```

12. (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 20527m;
java-heap-size-percentage 85;
java-min-heap-size 1932m;
java-min-heap-size-percentage 8;
java-min-new-size 241m;
java-min-new-size-percentage 1;
java-new-size 966m;
java-new-size-percentage 4;
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;
```

Related Documentation

- [Configuring Local Properties for the SAE \(C-Web Interface\)](#)
- [Configuring the RADIUS Local IP Address and NAS ID \(SRC CLI\) on page 195](#)

- [Configuring an SAE Group on page 190](#)
- [Initially Configuring the SAE on page 189](#)
- [Creating Grouped Configurations for the SAE \(SRC CLI\) on page 190](#)

Configuring the RADIUS Local IP Address and NAS ID (SRC CLI)

Use the following configuration statements to set the local RADIUS address and network access server (NAS ID):

```
slot number sae radius {
    local-address local-address ;
    local-nas-id local-nas-id ;
}
```

To set the local RADIUS address and NAS ID:

1. From configuration mode, access the SAE RADIUS configuration. This configuration is under the slot 0 hierarchy.

```
[edit]
user@host# edit slot 0 sae radius
```

2. Configure the local IP address that the SAE uses to communicate with RADIUS servers.

```
[edit slot 0 sae radius]
user@host# set local-address local-address
```

3. Configure the NAS ID that identifies the SAE when it sends RADIUS authentication and accounting records. Typically, the NAS ID is the name of the SAE host.

```
[edit slot 0 sae radius]
user@host# set local-nas-id local-nas-id
```

4. (Optional) Verify your configuration.

```
[edit slot 0 sae radius]
user@host# show
local-address 10.10.4.20;
local-nas-id SAE.host1;
```

Related Documentation

- [Configuring the RADIUS Local IP Address and NAS ID \(C-Web Interface\)](#)
- [Configuring Local Properties for the SAE \(SRC CLI\) on page 191](#)
- [Configuring an SAE Group on page 190](#)

- [Initially Configuring the SAE on page 189](#)
- [Creating Grouped Configurations for the SAE \(SRC CLI\) on page 190](#)

Starting the SAE (SRC CLI)

You must configure licenses before you start the SAE. When you start the SAE, the software verifies that a valid license is available. If no license is found, the SAE does not start.

To start the SAE:

- From operational mode, enable the SAE.

```
user@host> enable component sae
Check license: OK
Starting sae: may take a few minutes...
```



NOTE:

- Before executing the **show sae** commands, you must ensure that the SAE is started and running. The CLI may become inoperative if some of the **show sae** commands are executed immediately after enabling the SAE without waiting for the SAE to start. If the CLI is inoperative, press Ctrl+c and execute the **show** command again.
 - If you want to use the default SAE group (POP-ID) with the default values, enable the SAE without configuring the SAE local properties and creating an SAE group.
-

For information about monitoring SAE data with the SRC CLI, see *Viewing Information About the Directory Blacklist (SRC CLI)*.

Related Documentation

- [Starting the SAE \(C-Web Interface\)](#)
- [Stopping the SAE \(SRC CLI\) on page 196](#)
- [Initially Configuring the SAE on page 189](#)
- [Obtaining an SRC License on page 106](#)

Stopping the SAE (SRC CLI)

To stop the SAE:

- From operational mode, disable the SAE.

```
user@host> disable component sae
```

Shutting down the SAE server: done

To verify that the SAE is running:

- From operational mode, enter the **show component** command.

```
user@host> show component
Installed Components
Name      Version      Status
acp        Release: 7.8 Build: ACP.A.MAIN.1480      disabled
activity   Release: 7.8 Build: ACTIVITY.A.MAIN.1480  running
agent      Release: 7.8 Build: SYSMAN.A.MAIN.1480     disabled
appsvr     Release: 7.8 Build: JBOSS.A.MAIN.1480     disabled
cli        Release: MAIN Build: CLI.A.MAIN.1480       running
diameter   Release: 7.8 Build: DIAMETER.A.MAIN.1480  running
dsa        Release: 7.8 Build: GATEWAYAPPS.A.MAIN.1480 disabled
editor     Release: 7.8 Build: EDITOR.A.MAIN.1480    running
extsubmon  Release: 7.8 Build: MONAGENT.A.MAIN.1480   disabled
gw-3gpp    Release: 7.8 Build: 3GPPGW.A.MAIN.1480    disabled
gy-3gpp    Release: 7.8 Build: 3GPPGY.A.MAIN.1480    running
ims        Release: 7.8 Build: IMS.A.MAIN.1480       disabled
jdb        Release: 7.8 Build: DIRXA.A.MAIN.1480     running
licSvr     Release: 7.8 Build: LICSVR.A.MAIN.1480    disabled
naming     Release: 7.8 Build: NAMING.A.MAIN.1480    running
nic        Release: 7.8 Build: GATEWAY.A.MAIN.1480    running
redir      Release: 7.8 Build: REDIR.A.MAIN.1480     disabled
sae        Release: 7.8 Build: SAE.A.MAIN.1480       running
sic        Release: 7.8 Build: SICCLI.A.MAIN.1480    disabled
vta        Release: 7.8 Build: VTA.A.MAIN.1480       disabled
webadm     Release: 7.8 Build: WEBADM.A.MAIN.1480    disabled
```

For information about monitoring SAE data with the SRC CLI, see *Viewing Information About the Directory Blacklist (SRC CLI)*.

- Related Documentation**
- [Stopping the SAE \(C-Web Interface\)](#)
 - [Starting the SAE \(SRC CLI\) on page 196](#)
 - [Initially Configuring the SAE on page 189](#)

CHAPTER 22

Managing System Software on a C Series Controller

- [Software Management on a C Series Controller Overview on page 199](#)
- [Before You Upgrade the Software on a C Series Controller on page 200](#)
- [Creating a Snapshot of Files on a C Series Controller on page 200](#)
- [Upgrading the System Software on a C Series Controller on page 202](#)
- [Upgrading the System Software When Running Redundant SAEs on page 204](#)
- [Preparing the Software Images on the FTP Server on page 205](#)
- [Recovering or Installing System Software on a C Series Controller by Using the USB Storage Device Supplied by Juniper Networks on page 208](#)
- [Restoring the Files in a Snapshot on page 212](#)
- [Recovering System Software on a C Series Controller from a System Snapshot \(SRC CLI\) on page 212](#)
- [Deleting the Files in a Snapshot on page 213](#)

Software Management on a C Series Controller Overview

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 16 on page 199](#) lists the names of the packages for the components that run on the C Series Controller.

Table 16: Package Names for Components on a C Series Controller

Component	Package Name
Application server	UMCjboss
Command-line interface (CLI)	UMCcli
C-Web interface	UMCwebadm
External Subscriber Monitor	UMCmonagent
IP multimedia subsystem	UMCims

Table 16: Package Names for Components on a C Series Controller (continued)

Component	Package Name
Juniper Networks database	UMCjdb
License server	UMClicsvr
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

Related Documentation

- [Before You Upgrade the Software on a C Series Controller on page 200](#)
- [SRC Component Overview on page 9](#)
- [Configuring the SRC Software on page 46](#)
- [Configuring SRC Components on page 47](#)

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 200](#).
- Make sure that other C Series Controllers can carry system load during the upgrade.
The system is not operational during the upgrade.

Related Documentation

- [Configuring the SRC Software on page 46](#)
- [Software Management on a C Series Controller Overview on page 199](#)

Creating a Snapshot of Files on a C Series Controller

You can create one or more snapshots 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.



NOTE: When you issue the **show system information** command in a virtualized SRC software, the manufacturer, version, and serial number details are not displayed in the output. In addition, the product name is displayed as vSRC.

```
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 (1010.94 MB)
DUMP: Volume 1 took 0:01:10
DUMP: Volume 1 transfer rate: 14788 Kbps
DUMP: 1035200 blocks (1010.94 MB)
DUMP: finished in 70 seconds, throughput 14788 KBps
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 Kbps
```

3. Verify information about the snapshot.

```
user@host> show system snapshot
```

Related Documentation

- [Before You Upgrade the Software on a C Series Controller on page 200](#)
- [Restoring the Files in a Snapshot on page 212](#)
- [Deleting the Files in a Snapshot on page 213](#)
- [Software Management on a C Series Controller Overview on page 199](#)

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.

However, it is recommended that you upgrade a number of components together rather than individual components separately.

For example:

```
user@host>request system install package upgrade url ftp://myserver/SRC-PE-4.0.0-R3.iso
```

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 contents of the CD to a USB drive and install from there.



NOTE: You cannot upgrade the C Series Controller software to Release 4.13.0 from an earlier release by using the `request system upgrade url url` command, because SRC 4.13.0 release uses a different operating system (CentOS 7.6). You must reimage the controller by using the USB storage device. For more information about using the USB storage device to reimage the controller, see [“Recovering or Installing System Software on a C Series Controller by Using the USB Storage Device Supplied by Juniper Networks”](#) on page 208.

When you install the SRC software from the USB storage device, all system software, including the operating system, is installed, and the system hard drives are partitioned. As a result, any data, including data previously in the snapshot partition (if you do not select the `retainsnapshot` option at the boot prompt during the installation), is lost.

To upgrade C Series Controller software:

- Enter the `request system upgrade` command.

```
user@host> request system upgrade url url
```

where *url* is one of the following:

- `ftp://host/path`—Path on an FTP site or on the local system
- `usb:`—Local USB disk

For example:

```
user@host> request system upgrade url ftp://myserver/SRC-PE-4.0.0R3.iso or .tar.gz
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.

Related Documentation

- [Before You Upgrade the Software on a C Series Controller on page 200](#)
- [Preparing the Software Images on the FTP Server on page 205](#)
- [Restoring the Files in a Snapshot on page 212](#)
- [Software Management on a C Series Controller Overview on page 199](#)
- [Recovering System Software on a C Series Controller from a System Snapshot \(SRC CLI\) on page 212](#)
- [Recovering or Installing System Software on a C Series Controller by Using the USB Storage Device Supplied by Juniper Networks on page 208](#)

Upgrading the System Software When Running Redundant SAEs

When running the SRC software with redundant SAEs, we recommend that you run the same release of the SRC software on all C Series Controllers in the same Juniper Networks database community. Mixing SRC software releases in a network may cause shared configuration data to be placed in the Juniper Networks database that is not compatible with all versions of the SRC software. As a result, when running redundant SAEs, we recommend that you postpone any planned configuration changes to the C Series Controllers until you complete the SRC software upgrade on all C Series Controllers running in the Juniper Networks database community.

Use the following procedure to upgrade the SRC software on C Series Controllers in a network environment running redundant SAEs. Perform this procedure on each C Series Controller in a serial fashion.

1. For each router managed by the SAE, issue the **request sae shutdown device** command to shut down the device driver and force a graceful failover to the redundant SAE.
2. Disable the SAE by issuing the **disable component sae** command.
3. Upgrade the SRC software by issuing the **request system upgrade url url** command.
4. Reenable the SAE by issuing the **enable component sae** command.

Related Documentation

- [Upgrading the System Software on a C Series Controller on page 202](#)
- [Software Management on a C Series Controller Overview on page 199](#)
- [Before You Upgrade the Software on a C Series Controller on page 200](#)

Preparing the Software Images on the FTP Server

For easier management of upgrades or installations, you can copy the software image to an FTP site in your network. For more information, see the following procedures:

- [Preparing the CD Image on a Solaris System on page 205](#)
- [Preparing the CD Image on a Linux System on page 206](#)
- [Preparing the Compressed File on a Solaris System on page 207](#)
- [Preparing the Compressed File on a Linux System on page 207](#)

Preparing the CD Image on a Solaris System

To prepare the CD image on a Solaris system:

1. Attach and mount the CD image from the FTP server.

```
# lofiadm -a pathname/filename
# mount -F hsfs /dev/lofi/1 /mnt
```

2. Copy the CD image to your FTP server.

```
# cp -r /mnt pathname
```

3. Unmount and detach from the FTP server.

```
# umount /mnt
# lofiadm -d /dev/lofi/1
```

For example:

```
# lofiadm -a /ftp/public/SRC-PE-4.0.0-R-3-x86_64.iso
# mount -F hsfs /dev/lofi/1 /mnt
# cp -r /mnt /ftp/SRC-PE-4.0.0-R-3-x86_64
# umount /mnt
# lofiadm -d /dev/lofi/1
```

- See Also**
- [Recovering or Installing System Software on a C Series Controller by Using the USB Storage Device Supplied by Juniper Networks on page 208](#)
 - [Recovering System Software on a C Series Controller from a System Snapshot \(SRC CLI\) on page 212](#)
 - [Software Management on a C Series Controller Overview on page 199](#)
 - [Before You Upgrade the Software on a C Series Controller on page 200](#)
 - [Upgrading the System Software on a C Series Controller on page 202](#)

Preparing the CD Image on a Linux System

To prepare the CD image on a Linux system:

1. Mount the CD image from the FTP server.

```
# mount -o ro,loop filename /mnt
```

2. Copy the CD image to your FTP server.

```
# cp -r /mnt pathname
```

3. Unmount from the FTP server.

```
# umount /mnt
```

For example:

```
# mount -o ro,loop SRC-PE-4.0.0-R-3-x86_64.iso /mnt
# cp -r /mnt /ftp/SRC-PE-4.0.0-R-3-x86_64
# umount /mnt
```

- See Also**
- [Recovering or Installing System Software on a C Series Controller by Using the USB Storage Device Supplied by Juniper Networks on page 208](#)
 - [Recovering System Software on a C Series Controller from a System Snapshot \(SRC CLI\) on page 212](#)
 - [Software Management on a C Series Controller Overview on page 199](#)
 - [Before You Upgrade the Software on a C Series Controller on page 200](#)
 - [Upgrading the System Software on a C Series Controller on page 202](#)

Preparing the Compressed File on a Solaris System

To prepare the compressed file on a Solaris system:

1. Change directory to the FTP server where the compressed file is located.

```
# cd pathname
```

2. Uncompress the file.

```
# gunzip pathname/filename
```

3. Extract the archive file.

```
# tar xf pathname/filename
```

For example:

```
# cd /ftp  
# gunzip /ftp/SRC-PE-4.0.0-R-3-x86_64.tgz  
# tar xf /ftp/SRC-PE-4.0.0-R-3-x86_64.tar
```

- See Also**
- [Recovering or Installing System Software on a C Series Controller by Using the USB Storage Device Supplied by Juniper Networks on page 208](#)
 - [Recovering System Software on a C Series Controller from a System Snapshot \(SRC CLI\) on page 212](#)
 - [Software Management on a C Series Controller Overview on page 199](#)
 - [Before You Upgrade the Software on a C Series Controller on page 200](#)
 - [Upgrading the System Software on a C Series Controller on page 202](#)

Preparing the Compressed File on a Linux System

To prepare the compressed file on a Linux system:

- Extract the archive file from the compressed file on the FTP server.

```
# tar -C pathname -zxf filename
```

For example:

```
# tar -C /ftp/ -zxf SRC-PE-4.0.0-R-3-x86_64.tgz
```

- See Also**
- [Recovering or Installing System Software on a C Series Controller by Using the USB Storage Device Supplied by Juniper Networks on page 208](#)

- [Recovering System Software on a C Series Controller from a System Snapshot \(SRC CLI\) on page 212](#)
- [Software Management on a C Series Controller Overview on page 199](#)
- [Before You Upgrade the Software on a C Series Controller on page 200](#)
- [Upgrading the System Software on a C Series Controller on page 202](#)

Related Documentation

- [Recovering or Installing System Software on a C Series Controller by Using the USB Storage Device Supplied by Juniper Networks on page 208](#)
- [Recovering System Software on a C Series Controller from a System Snapshot \(SRC CLI\) on page 212](#)
- [Software Management on a C Series Controller Overview on page 199](#)
- [Before You Upgrade the Software on a C Series Controller on page 200](#)
- [Upgrading the System Software on a C Series Controller on page 202](#)

Recovering or Installing System Software on a C Series Controller by Using the USB Storage Device Supplied by Juniper Networks

You can recover system software by using the USB storage device supplied with the C Series Controller.



NOTE:

- Starting from SRC Release 4.5, the USB storage device supplied with the C Series Controller is a read/write or read-only device. Prior to SRC Release 4.5, Juniper Networks shipped the C Series Controller with only a read-only USB storage device that contains a copy of the system software.
- Using the read-only USB storage device supplied by Juniper Networks, you can only recover the system software; whereas, by using the read/write USB storage device, you can create an installation medium and back up the system configuration.
- To determine whether the USB storage device you received from Juniper Networks is a read-only or read/write device, contact Juniper Networks Technical Assistance Center (JTAC).

Using the read/write USB storage device supplied by Juniper Networks, you can create an installation medium that can be updated to the desired release and used to reimage a C Series Controller. You need to download the image file from the Juniper Networks Support website onto your Linux workstation, uncompress the software, and then copy the software image onto your Juniper Networks external USB (4-gigabyte) storage device.



CAUTION: When you install the SRC software from the supplied USB storage device, all system software, including the operating system, is installed, and the system hard drives are partitioned. As a result, any data, including data previously in the snapshot partition (if you do not select the `retainsnapshot` option at the boot prompt during the installation), is lost.

You can back up the system configuration to the read/write USB storage device supplied by Juniper Networks or to an external system (such as a computer running a Linux or Windows operating system, or a USB device) by using the `save` and `file copy` commands. The term “USB device” in this case refers to the customer-supplied read/write USB storage device. This should not be confused with the “USB storage device” supplied by Juniper Networks with each C Series Controller. You can also recover the configuration by using the `load` command. For information about managing the SRC configuration, see the *SRC PE CLI User Guide*. For information about how to specify a filename, see *Specifying Filenames and URLs*.

To create an installation medium by using the read/write USB storage device:

1. In a Web browser, go to <https://www.juniper.net/support/products/src/>.
The **SRC** page appears.
2. Click the **Software** tab and select the image file that you want to download.
A login screen appears.
3. Enter your username and password and press **Enter**.
4. Log in and save the image file to your Linux workstation.
5. Uncompress the image file on your Linux workstation.
`gunzip name.*img.gz`
6. Insert the read/write USB (4-gigabyte) storage device supplied by Juniper Networks into your Linux workstation.
7. Determine the system device of the USB storage device by using the `dmesg | less` command.

```
dmesg | less
```

```
scsi 1:0:0:0: Direct-Access          USB Flash Memory 1.04 PQ: 0 ANSI: 0
CCS
usb-storage: device scan complete
sd 1:0:0:0: [sdb] 2004992 512-byte hardware sectors: (1.02 GB/979 MiB)
sd 1:0:0:0: [sdb] Write Protect is off
sd 1:0:0:0: [sdb] Mode Sense: 23 00 00 00
sd 1:0:0:0: [sdb] Assuming drive cache: write through
sd 1:0:0:0: [sdb] Assuming drive cache: write through
```

```
sdb: sdb1
sd 1:0:0:0: [sdb] Attached SCSI removable disk
```



NOTE: In this case, **sdb** is the system device of the USB storage device.

8. Copy the software image that you just downloaded to your Linux workstation onto your external USB storage device by using the **dd** command.

```
dd if=name.img of=/dev/usb-device
```

In this case,

```
dd if=name.img of=/dev/sdb
```

9. Remove the USB storage device from the Linux workstation.

To boot the system from the supplied USB storage device and install the SRC software on a C Series Controller:



CAUTION: After you complete this procedure, remember to disconnect the USB storage device. Failure to do so can result in the loss of configuration and data if the system loses power or is rebooted.

1. Plug the USB storage device into the USB port on the C Series Controller.

2. Connect a console terminal to the C Series Controller.

See your *C Series Controller Hardware Guide*.

3. Power on the system.

The controller starts up from the USB storage device and prints the following message.

```
SRC software -- System recovery software for SRC C series platforms.
```

```
WARNING: This system recovery software replaces all data and software
on the system hard drives. As a result, any data, including data
previously in the snapshot partition(if retainsnapshot is not selected), is
lost.
```

```
After you run the system recovery software, the C-series platform
contains the SRC software, including the C-series operating system,
but no configuration data.
```

```
To continue, press <Enter>.
```

```
To retain the software previously in the snapshot partition, type retainsnapshot
and press <Enter>
```


To cancel this operation, power off the C-series platform and remove the USB storage device from the USB port.
boot:

4. At the boot prompt, enter **retainsnapshot** and press the **Enter** key to retain the snapshot of the system software stored in the snapshot partition. If you do not want to retain the snapshot, press the **Enter** key, or follow the instructions on the screen to cancel the operation.
5. When the software installation is complete, unplug the USB storage device from the USB port and reboot the C Series Controller.



NOTE: CentOS 7 and later versions use different schemes for naming network interfaces, for example, enpX, ensX, and enoX. SRC works only with the traditional naming ethX. So, it is mandatory to rename the interfaces from ensX, enpX, or enoX to ethX and persist interface names with the corresponding MAC addresses. After the software installation is complete, the interface renaming script is executed for renaming the interfaces.

6. After the interface renaming script is executed, configure the corresponding MAC address for each network interface (for example, eth0, eth1). After verifying the configuration of MAC addresses, reboot the C Series Controller for the changes to take effect.
7. After the C Series Controller reboots and the software installation is complete, set up the initial configuration.

See your *C Series Controller Hardware Guide*.



NOTE: The default username and password for grub menu are “root” and “password”, respectively. You can change the default password by executing the **grub2-setpassword** command in shell mode.

Related Documentation

- [Before You Upgrade the Software on a C Series Controller on page 200](#)
- [Preparing the Software Images on the FTP Server on page 205](#)
- [Restoring the Files in a Snapshot on page 212](#)
- [Software Management on a C Series Controller Overview on page 199](#)
- [Recovering System Software on a C Series Controller from a System Snapshot \(SRC CLI\) on page 212](#)
- [Upgrading the System Software on a C Series Controller on page 202](#)

Restoring the Files in a Snapshot

To revert to the system software stored in snapshot files:

- Enter the **request system restore** command.

The output lists the available snapshots. Enter the specific number of the snapshot which you want to restore.

```
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.

Available Snapshots:
1:Snapshot of SRC-PE Release MAIN [VMAIN.A-1616] taken 2016-04-22 12:29:47 -
2623 MB
2:Snapshot of SRC-PE Release MAIN [VMAIN.A-1616] taken 2016-04-22 12:32:36 -
2623 MB
Select the snapshot[1,2,...,n] ? Snapshot-number
```

The C Series Controller reboots twice during a restoration.

Related Documentation

- [Creating a Snapshot of Files on a C Series Controller on page 200](#)
- [Deleting the Files in a Snapshot on page 213](#)
- [Upgrading the System Software on a C Series Controller on page 202](#)
- [Recovering or Installing System Software on a C Series Controller by Using the USB Storage Device Supplied by Juniper Networks on page 208](#)
- [Software Management on a C Series Controller Overview on page 199](#)

Recovering System Software on a C Series Controller from a System Snapshot (SRC CLI)

If you encounter a software failure on a C Series Controller, in most cases you can recover from the failure by restoring the software from a snapshot by using the **request system restore** command.

If, however, the operating system on the main partition on a C Series Controller is damaged, the operating system tries to boot from the snapshot partition. If the system does not boot from the snapshot partition, you can try to manually reboot the system and use the software snapshot.

If a software failure damages the snapshot partition on a C Series Controller, you can boot the system from the USB storage device supplied with the C Series Controller. After the system boots, it installs the system software from the USB storage device. The USB

storage device supplied with the C Series Controller contains a copy of the system software. For more information, see [“Recovering or Installing System Software on a C Series Controller by Using the USB Storage Device Supplied by Juniper Networks” on page 208](#).

To boot a C Series Controller from the system snapshot:

1. Connect a console terminal to the C Series Controller.
See your *C Series Controller Hardware Guide*.
2. Initiate a system reboot in one of the following ways:
 - Power off and then power on the C Series Controller.
 - To enter the boot menu, press the Spacebar on the console when the **Press any key to continue** prompt is displayed.
3. From the boot menu, select the backup partition.

If a software failure damages the boot partition on a C Series Controller, you can install the system software from the USB storage device that is supplied with a C Series Controller.

Related Documentation

- [Before You Upgrade the Software on a C Series Controller on page 200](#)
- [Preparing the Software Images on the FTP Server on page 205](#)
- [Restoring the Files in a Snapshot on page 212](#)
- [Software Management on a C Series Controller Overview on page 199](#)
- [Upgrading the System Software on a C Series Controller on page 202](#)
- [Recovering or Installing System Software on a C Series Controller by Using the USB Storage Device Supplied by Juniper Networks on page 208](#)

Deleting the Files in a Snapshot

To delete the files in a snapshot:

- Execute the **request system delete** command.

The output lists the available snapshots. Enter the specific number of the snapshot which you want to delete.

```
user@host> request system delete
```

```
WARNING: deleting a snapshot will cause the system to
erase every data related to the snapshot.
```

```
Available Snapshots:
```

```
1:Snapshot of SRC-PE Release MAIN [VMAIN.A-1616] taken 2016-04-22 12:29:47 -
2623 MB
```

```
2:Snapshot of SRC-PE Release MAIN [VMAIN.A-1616] taken 2016-04-22 12:32:36 -
```

2623 MB

Select the snapshot[1,2,...,n] ? *Snapshot-number*

**Related
Documentation**

- [Creating a Snapshot of Files on a C Series Controller on page 200](#)
- [Restoring the Files in a Snapshot on page 212](#)
- [Software Management on a C Series Controller Overview on page 199](#)

CHAPTER 23

Using the Web Application Server on a C Series Controller

- [Web Application Server on C Series Controllers Overview on page 215](#)
- [Configuration Statements for the Web Application Server on page 217](#)
- [Configuring the Web Application Server \(SRC CLI\) on page 218](#)
- [Configuring Local Properties for the Web Application Server \(SRC CLI\) on page 219](#)
- [Configuring the Web Application Server Shared Cluster Configuration \(SRC CLI\) on page 221](#)
- [Configuring the Nodes in the Web Application Server Cluster \(SRC CLI\) on page 222](#)
- [Configuring Remote Access to the Application Server \(SRC CLI\) on page 223](#)
- [Configuring Virtual Hosts for the Web Applications \(SRC CLI\) on page 225](#)
- [Configuring User Accounts for Web Applications \(SRC CLI\) on page 226](#)
- [Installing Web Applications in the SRC Web Application Server on page 228](#)
- [Removing Web Applications from the Application Server on page 228](#)
- [Starting the Web Application Server on a C Series Controller on page 229](#)
- [Restarting the Web Application Server on a C Series Controller on page 229](#)
- [Stopping the Web Application Server on a C Series Controller on page 229](#)
- [Viewing Statistics for the Web Application Server \(SRC CLI\) on page 229](#)
- [Viewing Statistics for the Web Application Server \(C-Web Interface\) on page 230](#)
- [Viewing the Web Application Server Cluster Status \(SRC CLI\) on page 230](#)
- [Viewing the Web Application Server Cluster History \(SRC CLI\) on page 231](#)

Web Application Server on C Series Controllers Overview

The SRC software on a C Series Controller includes a Web application server that hosts the Web Services Gateway and the Volume Tracking Application (SRC VTA). In production environments, this application server is designed to host only these applications. However, you can load your own applications into this server for testing or demonstration purposes.

By default, the SRC Web application server listens on port 8080 for HTTP connections on the `eth0` interface (interface to the trusted network) and on the configured ports for HTTP and HTTPS connections on the `eth1` interface (interface to the untrusted network).

You can control access to applications deployed in the Web application server by configuring virtual hosts. A virtual host contains aliases and lists of the clients that are allowed to access the virtual host.

The aliases are DNS names or IP addresses that appear in the host part of the URLs used by clients to access a Web application. When the Web application server receives a request for an application, it searches for the virtual host with the alias that matches the host in the URL. If a virtual host is found, the Web application server verifies that the application is deployed on this virtual host and the client making the request is allowed to access the virtual host. If no virtual host is found, or if access to the application or client is not allowed by the virtual host, the request is rejected and the client receives an error code.

By default, SRC applications use the virtual host `eth0`. You must configure this virtual host and the following aliases:

- The IP address assigned to `eth0`.
- The name for the SRC host configured at the `[edit system host-name]` and `[edit system domain-name]` hierarchy levels.

For this reason, if you want to access the `eth0` virtual host with URLs containing the DNS name of your SRC host, you must configure your SRC hostname in your DNS server.

You configure the built-in applications, such as Dynamic Service Activator, to deploy the application to a specific virtual host. Other applications that you can load for demonstration purposes are automatically deployed on the built-in virtual host `eth0`.

Clustering

The SRC Web application server supports clustering, which provides reliability through failover and load balancing. The nodes in the cluster automatically discover one another on startup and automatically synchronize their state with the rest of the group. The cluster configuration is part of the shared SRC configuration and is stored in the Juniper Networks database. You can configure several Web application server clusters. However, a single SRC Web application server instance belong to only one cluster; it cannot belong to more than one cluster.

Local and Shared Configuration

If you want a Web application server instance to be part of a cluster, you need to specify the cluster name in the local configuration by using the `[edit slot 0 application-server]` configuration statement. This statement points to the shared configuration stored in the Juniper Networks database. The Web application shared configuration is specified using the `[edit shared application-server cluster cluster-name]` configuration statement.

Storing the cluster configuration in the Juniper Networks database ensures that all nodes in the cluster share the same configuration, including the unique identifier of each node,

and the shared cluster name. All nodes must be specified within the same Juniper Networks database community name.

The configuration of the application server cluster lists the information about each application server node. When the application server is started, the system retrieves the shared application server cluster configuration and generates the appropriate startup script for the application server node. If no cluster is defined, the application server is started in “all” mode, but without the cluster parameters.



NOTE: If you change the shared-cluster configuration, you must restart the local Web application server.

By default, the intra-cluster communication is done through multicasting and UDP is used as the channel stack protocol. If multicasting is not an option for deployment, you can use TCP as the channel stack. The shared cluster configuration is valid only if the following conditions are fulfilled:

- The multicast-address is configured and either the channel stack is not set (the system uses UDP by default) or the channel stack is set to UDP.
- The channel stack is set to TCP and the multicast-address is not configured.

Related Documentation

- [Configuring the Web Application Server \(SRC CLI\) on page 218](#)
- [Configuration Statements for the Web Application Server on page 217](#)

Configuration Statements for the Web Application Server

Use the following configuration statements to configure the operating properties for the Web application server at the **[edit]** hierarchy level.

```
slot number application-server {
    java-garbage-collection-options java-garbage-collection-options;
    java-heap-size java-heap-size;
    shared-cluster shared-cluster
    corba-request-timeout corba-request-timeout
}
```

```
shared application-server cluster name {
    channel-stack (udp|tcp);
    multicast-address multicast-address;
}
```

```
shared application-server cluster name nodes node address {
    node-id node-id;
}
```

```
slot number application-server web http {
```

```
port port;  
interface interface;  
}
```

```
slot number application-server web https {  
  local-certificate local-certificate;  
  port port;  
  interface interface;  
}
```

```
slot number application-server web virtual-host host-name {  
  alias alias;  
  allow-address allow-address;  
  allow-host allow-host;  
  deny-address deny-address;  
  deny-host deny-host;  
}
```

```
shared application-server user name
```

```
shared application-server user name authentication {  
  encrypted-password encrypted-password;  
  plain-text-password;  
}
```

**Related
Documentation**

- [Configuring the Web Application Server \(SRC CLI\) on page 218](#)
- [Configuring Remote Access to the Application Server \(SRC CLI\) on page 223](#)
- [Configuring Virtual Hosts for the Web Applications \(SRC CLI\) on page 225](#)
- [Configuring User Accounts for Web Applications \(SRC CLI\) on page 226](#)
- [Web Application Server on C Series Controllers Overview on page 215](#)

Configuring the Web Application Server (SRC CLI)

Tasks to configure the Web application server are:

1. Configure the Web application server shared cluster configuration.
[See “Configuring the Web Application Server Shared Cluster Configuration \(SRC CLI\)” on page 221.](#)
2. Configure the operating properties.
[See “Configuring Local Properties for the Web Application Server \(SRC CLI\)” on page 219.](#)
3. Configure the nodes of the Web application server cluster.
[See “Configuring the Nodes in the Web Application Server Cluster \(SRC CLI\)” on page 222.](#)

4. Configure remote access to the application server.
See [“Configuring Remote Access to the Application Server \(SRC CLI\)” on page 223](#).
5. Configure the virtual host for the Web application, including whether to allow or deny access by specific remote clients.
See [“Configuring Virtual Hosts for the Web Applications \(SRC CLI\)” on page 225](#).
6. Configure the user accounts for the Web application.
See [“Configuring User Accounts for Web Applications \(SRC CLI\)” on page 226](#).

Related Documentation

- [Web Application Server on C Series Controllers Overview on page 215](#)
- [Configuring the Web Application Server Shared Cluster Configuration \(SRC CLI\) on page 221](#)
- [Configuring the Nodes in the Web Application Server Cluster \(SRC CLI\) on page 222](#)

Configuring Local Properties for the Web Application Server (SRC CLI)

To configure basic local properties:

1. From configuration mode, access the configuration statement that configures the local properties.

```
user@host# edit slot 0 application-server
```

2. (Available at the Advanced editing level.) Configure the garbage collection functionality of the Java Virtual Machine.

```
[edit slot 0 application-server]
user@host# set java-garbage-collection-options java-garbage-collection-options
```

3. (Optional. Available at the Advanced editing level.) If you encounter problems caused by lack of memory, change the maximum memory size available to the JRE.

```
[edit slot 0 application-server]
user@host# set java-heap-size java-heap-size
```

4. (Optional) Configure the cluster name. Specify the shared-cluster as `/application-server/shared-cluster`.

```
[edit slot 0 application-server]
user@host# set shared-cluster /application-server/shared-cluster
```

For example, to configure a shared cluster called cluster-1:

```
[edit slot 0 application-server]
```

```
user@host# set shared-cluster /application-server/cluster-1
```



NOTE: If you change the shared cluster name, you must restart the local application server for the change to take effect.

5. (Optional. Available at the Advanced editing level.) Configure the time duration that the CORBA request must wait for a response before timing out. By default, the value is set to 125000 milliseconds.

```
[edit slot 0 application-server]
```

```
user@host# set corba-request-timeout corba-request-timeout
```



NOTE: You must ensure that the CORBA request time-out value is greater than the message time-out interval of the configured router driver. You can configure the message time-out interval of the router driver by including the *message-timeout* option under the *[edit shared sae group group-name configuration driver device-driver]* hierarchy level.

6. (Optional) Verify your configuration.

```
[edit slot 0 application-server]
```

```
user@host# show
```

```
corba-request-timeout 125000;
java-garbage-collection-options '-Dsun.rmi.dgc.client.gcInterval=36000000
-Dsun.rmi.dgc.server.gcInterval=36000000';
java-heap-size 666m;
shared-cluster /application-server/cluster-1;
web {
  http {
    interface eth0;
    port 8080;
  }
  virtual-host eth0;
}
```

Related Documentation

- [Configuring the Web Application Server Shared Cluster Configuration \(SRC CLI\) on page 221](#)
- [Configuring the Nodes in the Web Application Server Cluster \(SRC CLI\) on page 222](#)
- [Web Application Server on C Series Controllers Overview on page 215](#)

Configuring the Web Application Server Shared Cluster Configuration (SRC CLI)

Use the following statements to configure a Web application server shared cluster configuration:

```
shared application-server cluster name {
  channel-stack (udp|tcp);
  multicast-address multicast-address;
}
```

To configure the Web application server shared cluster configuration:

1. From configuration mode, access the statement that configures the shared cluster configuration. The name you specify must match the name you configured for the local configuration at the **[edit slot 0 application-server]** hierarchy level.

```
user@host# edit shared application-server cluster name
```

For example, if you have the following local configuration:

```
[edit slot 0 application-server]
shared-cluster /application-server/cluster-1
```

You need to specify cluster-1 as the cluster name for the shared configuration:

```
user@host# edit shared application-server cluster cluster-1
```

2. Configure the channel stack.

```
[edit shared application-server cluster cluster-1]
user@host# set channel-stack (udp|tcp)
```

3. (Optional) Specify the multicast address. The multicast address is required only if UDP is selected as the channel stack.

```
[edit shared application-server cluster cluster-1]
user@host# set multicast-address multicast-address
```

4. (Optional) Verify your configuration.

```
[edit shared application-server cluster cluster-1]
user@host# show
```

```
channel-stack tcp;
[edit shared application-server cluster cluster-1]
user@host#
```

**Related
Documentation**

- [Web Application Server on C Series Controllers Overview on page 215](#)
- [Configuring the Nodes in the Web Application Server Cluster \(SRC CLI\) on page 222](#)
- [Configuring the Web Application Server \(SRC CLI\) on page 218](#)
- [Configuring Local Properties for the Web Application Server \(SRC CLI\) on page 219](#)
- [Viewing the Web Application Server Cluster Status \(SRC CLI\) on page 230](#)

Configuring the Nodes in the Web Application Server Cluster (SRC CLI)

Use the following statements to configure the nodes in the Web application server cluster:

```
shared application-server cluster name nodes node address {  
    node-id node-id;  
}
```

To configure the Web application server cluster nodes:

1. From configuration mode, access the statement that configures the cluster nodes and specify the IP address of the node.

```
user@host# shared application-server cluster name nodes node address {
```

2. Configure the node ID for the node. The node ID is a random number you assign to the node. Each node must have a unique node ID specified as the integer type.

```
[edit shared application-server cluster name nodes node address]  
user@host# set node-id node-id
```

3. (Optional) Verify your configuration.

```
[edit shared application-server cluster name nodes node address]  
user@host# show
```

Following is a sample output of the cluster node configuration:

```
channel-stack udp;  
multicast-address 255.255.100.100;  
nodes {  
    node 10.1.2.3 {  
        node-id 2;  
    }  
    node 10.1.2.4 {  
        node-id 1;  
    }  
    node 10.1.2.5 {  
        node-id 4;  
    }  
}
```

Related Documentation

- [Web Application Server on C Series Controllers Overview on page 215](#)
- [Configuring the Web Application Server Shared Cluster Configuration \(SRC CLI\) on page 221](#)
- [Configuring the Web Application Server \(SRC CLI\) on page 218](#)
- [Configuring Local Properties for the Web Application Server \(SRC CLI\) on page 219](#)

Configuring Remote Access to the Application Server (SRC CLI)

Before you can start using the application server, you need to configure and enable access to the application server. You can make the application server accessible through secure HTTP (HTTPS) or HTTP.

- [Configuring Access to the Application Server Through Secure HTTP on page 223](#)
- [Configuring Access to the Application Server Through HTTP on page 224](#)

Configuring Access to the Application Server Through Secure HTTP

Before you configure access to the application server through HTTPS, obtain a digital security certificate on the system.

To make the application server accessible through HTTPS:

1. From configuration mode, access the statement that configures access through HTTPS.

```
user@host# edit slot 0 application-server web https
```

2. Specify which TCP port is to receive incoming connection requests for the application server.

```
[edit slot 0 application-server web https]
user@host# set port port
```

3. Specify the interface to be used for connections to the application server.

```
[edit slot 0 application-server web https]
user@host# set interface interface
```

On a C Series Controller, use **eth1** for built-in Web applications; you can use **eth0** for demonstration applications.

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

```
[edit slot 0 application-server web https]
user@host# set local-certificate local-certificate
```

5. Configure the secure connection protocol to be used by the application server. You can specify more than one protocol in this option.

```
[edit slot 0 application-server web https]
user@host# set protocol (TLSv1 | TLSv1.1 | TLSv1.2)
```



NOTE: While upgrading to SRC 4.12.0 release, by default all three protocol versions TLSv1, TLSv1.1, and TLSv1.2 are enabled for backward compatibility. We recommend you to configure TLSv1.2 alone to avoid vulnerabilities.

6. (Optional) Configure user accounts to allow specified clients to authenticate with the application server.

- See Also**
- [Configuring the Web Application Server \(SRC CLI\) on page 218](#)
 - [Configuring User Accounts for Web Applications \(SRC CLI\) on page 226](#)
 - [Web Application Server on C Series Controllers Overview on page 215](#)
 - [Digital Certificates Overview on page 275](#)
 - [Configuring Access to the Application Server Through HTTP on page 224](#)

Configuring Access to the Application Server Through HTTP

To make the application server accessible through HTTP:

1. From configuration mode, access the statement that configures access through HTTP.

```
user@host# edit slot 0 application-server web http
```

2. Specify which TCP port is to receive incoming connection requests for the application server.

```
[edit slot 0 application-server web http]
user@host# set port port
```

3. Specify the interface to be used for connections to the application server.

```
[edit slot 0 application-server web http]
user@host# set interface interface
```

On a C Series Controller, use **eth1** for built-in Web applications; you can use **eth0** for demonstration applications.

4. (Optional) Configure user accounts to allow specified clients to authenticate with the application server.

- See Also**
- [Configuring the Web Application Server \(SRC CLI\) on page 218](#)
 - [Configuring User Accounts for Web Applications \(SRC CLI\) on page 226](#)
 - [Web Application Server on C Series Controllers Overview on page 215](#)
 - [Digital Certificates Overview on page 275](#)
 - [Configuring Access to the Application Server Through Secure HTTP on page 223](#)

- Related Documentation**
- [Configuring the Web Application Server \(SRC CLI\) on page 218](#)
 - [Configuring User Accounts for Web Applications \(SRC CLI\) on page 226](#)
 - [Web Application Server on C Series Controllers Overview on page 215](#)
 - [Digital Certificates Overview on page 275](#)

Configuring Virtual Hosts for the Web Applications (SRC CLI)

Use the following configuration statements to configure virtual hosts at the **[edit]** hierarchy level:

```
slot number application-server web virtual-host host-name {
    alias [alias...];
    allow-address [allow-address...];
    allow-host [allow-host...];
    deny-address [deny-address...];
    deny-host [deny-host...];
}
```

To configure virtual hosts for the Web applications:

1. From configuration mode, access the statement that configures the virtual host.

By default, SRC applications run on the virtual host **eth0**. You must configure **eth0** as a virtual host. The hostname must be unique.

```
user@host# edit slot 0 application-server virtual-host eth0
```

2. Specify the alternate DNS names or IP addresses for the virtual host.

```
[edit slot 0 application-server virtual-host eth0]
user@host# set alias [alias ...]
```

The alias must be unique. Specify the following alias for the **eth0** virtual host:

- The IP address assigned to **eth0**.
 - The name for the SRC host configured at the **[edit system host-name]** and **[edit system domain-name]** hierarchy levels.
3. Configure access to the virtual host. Specify the IP addresses for remote clients that are allowed access to the virtual host.

```
[edit slot 0 application-server virtual-host eth0]  
user@host# set allow-address [allow-address...]
```

4. Configure access to the virtual host. Specify the hostnames for remote clients that are allowed access to the virtual host.

```
[edit slot 0 application-server virtual-host eth0]  
user@host# set allow-host [allow-host...]
```

5. Deny access to the virtual host. Specify the IP addresses for remote clients that are denied access to the virtual host.

```
[edit slot 0 application-server virtual-host eth0]  
user@host# set deny-address [deny-address...]
```

6. Deny access to the virtual host. Specify the hostnames for remote clients that are denied access to the virtual host.

```
[edit slot 0 application-server virtual-host eth0]  
user@host# set deny-host [deny-host...]
```

- Related Documentation**
- [Configuring the Web Application Server \(SRC CLI\) on page 218](#)
 - [Web Application Server on C Series Controllers Overview on page 215](#)

Configuring User Accounts for Web Applications (SRC CLI)

User accounts provide one way for clients to authenticate with the application server. For each account, you define the login name for the user, authentication information, and role. You can configure plain-text password or encrypted password as the type of authentication for user accounts. When you delete user accounts, the software verifies that the user account is not referenced by another configuration.



NOTE: Client profiles can be cached by applications for 30 minutes. If you change the password or role of a client that has been used within the last 30 minutes, it can take up to 30 minutes before these changes take effect.

If you do not want to wait 30 minutes for the changes to take effect, restart the Web application server.

Use the following configuration statements to configure user accounts at the **[edit]** hierarchy level:

```
shared application-server user name
```



```
shared application-server user name authentication {
  encrypted-password encrypted-password;
  plain-text-password;
  role [DSA | PCMM | VTA-group name];
}
```

To configure a user account:

1. From configuration mode, access the configuration statement that configures a user account and specify a username that identifies the client.

```
user@host# edit shared application-server user name
```

The username must be unique within the system. Do not include spaces, colons, or commas in the username.

2. Configure authentication for the user account.

```
[edit shared application-server user name]
user@host# set authentication (plain-text-password | encrypted-password)
```

where:

- **plain-text-password**—Prompt for a plain-text (unencrypted) password.
- **encrypted-password**—Password encoded with crypt. The format of encrypted passwords is "{crypt}<13-characters in a-zA-Z0-9./>".

We recommend that you not enter the password in encrypted format.

For example:

```
user@host# set authentication plain-text-password
New password: type password here
Retype new password: retype password here
```

3. Configure the role for the user account.

```
[edit shared application-server user name]
user@host# set role VTA-Quota
```

Set the role to one of the following values:

- **DSA**—Role for clients accessing the DSA services: dsa-service and dsa2-service
- **PCMM**—Role for clients accessing the DSA service: pcmm-service
- **VTA-group name**—Role for clients accessing the SOAP API for the SRC VTA. The CLI returns all SRC VTA groups configured under the **[edit shared vta group]** hierarchy with the prefix "VTA". For example, set the role to VTA-Quota for clients accessing the SOAP API for the SRC VTA group called Quota.

- Related Documentation**
- [Configuring Remote Access to the Application Server \(SRC CLI\) on page 223](#)
 - [SRC VTA SOAP Interface](#)
 - [Enabling the SOAP Interface for an SRC VTA Group \(SRC CLI\)](#)
 - [Methods for the SRC Volume Tracking Application SOAP Interface](#)

Installing Web Applications in the SRC Web Application Server

The SRC software includes a Web application server component for deploying Web applications for lab tests and demonstrations.

Use the following procedure to deploy Web applications in the SRC Web application server.



NOTE: You can deploy a Web application in the Web application server for lab tests and demonstrations. However, running non-SRC Web applications in production environments is not supported.

To deploy a Web application in the SRC Web application server:

1. Start the Web application server.
2. Prepare the Web application archive (WAR) file on a machine other than the C Series Controller.
3. Deploy the WAR file on the C Series Controller. The SRC Web application server automatically starts the Web application when a new WAR file is deployed.

```
user@host> request appsvr deploy file name
```

For example:

```
user@host> request appsvr deploy file ftp://host/path/ssportal.war
```

- Related Documentation**
- [Removing Web Applications from the Application Server on page 228](#)
 - [Starting the Web Application Server on a C Series Controller on page 229](#)
 - [Restarting the Web Application Server on a C Series Controller on page 229](#)

Removing Web Applications from the Application Server

To undeploy a Web application from the Web application server:

```
user@host> request appsvr undeploy file name
```

For example:

```
user@host> request appsvr undeploy file dsa.war
```

- Related Documentation**
- [Installing Web Applications in the SRC Web Application Server on page 228](#)
 - [Stopping External Subscriber Monitor \(C-Web Interface\)](#)

Starting the Web Application Server on a C Series Controller

To start the Web application server on a C Series Controller:

```
user@host> enable component appsvr
```

- Related Documentation**
- [Restarting the Web Application Server on a C Series Controller on page 229](#)
 - [Stopping the Web Application Server on a C Series Controller on page 229](#)

Restarting the Web Application Server on a C Series Controller

To restart the Web application server on a C Series Controller:

```
user@host> restart component appsvr
```

- Related Documentation**
- [Starting the Web Application Server on a C Series Controller on page 229](#)
 - [Stopping the Web Application Server on a C Series Controller on page 229](#)

Stopping the Web Application Server on a C Series Controller

To stop the Web application server on a C Series Controller:

```
user@host> disable component appsvr
```

- Related Documentation**
- [Starting the Web Application Server on a C Series Controller on page 229](#)
 - [Restarting the Web Application Server on a C Series Controller on page 229](#)

Viewing Statistics for the Web Application Server (SRC CLI)

Purpose View statistics for the Web application server.

Action user@host> show application-server statistics

```
Appsrv Process Statistics
JBoss Server Process
JBoss server up time(seconds) 4673
JBoss server up since        Thu Mar 13 11:07:30 EDT 2008
JBoss server thread(s)       63
Heap used(byte)              47316168 (9%)
Heap limit(byte)             520749056
```

- Related Documentation**
- [Web Application Server on C Series Controllers Overview on page 215](#)
 - [Configuration Statements for the Web Application Server on page 217](#)
 - [Configuring the Web Application Server \(SRC CLI\) on page 218](#)
 - [Configuring Local Properties for the Web Application Server \(SRC CLI\) on page 219](#)

Viewing Statistics for the Web Application Server (C-Web Interface)

Purpose View statistics for the Web application server.

Action Click **Monitor>Application Server>Statistics**.

The Statistics pane displays the application server process statistics.

- Related Documentation**
- [Configuring the Web Application Server \(SRC CLI\) on page 218](#)

Viewing the Web Application Server Cluster Status (SRC CLI)

Purpose View the status of the Web application server.

Action user@host> show application-server cluster status *cluster-name*

```
Appsvr Cluster Status
JBoss Cluster Info
Cluster name  example
Cluster state Started
Channel stack udp
Cluster view  [exp1:1099, exp2:1099]
```

- Related Documentation**
- [Configuring the Web Application Server \(SRC CLI\) on page 218](#)
 - [Viewing the Web Application Server Cluster History \(SRC CLI\) on page 231](#)
 - [Configuring the Nodes in the Web Application Server Cluster \(SRC CLI\) on page 222](#)

- [Configuring the Web Application Server Shared Cluster Configuration \(SRC CLI\) on page 221](#)

Viewing the Web Application Server Cluster History (SRC CLI)

Purpose View the Web application server history. If you restart a node, the history shows the node as being removed from the cluster during the restart period.

Action `user@host> show application-server cluster history cluster-name`

```
6/30/11 2:06 PM : Partition object created
6/30/11 2:06 PM : Partition object created
6/30/11 2:06 PM : Initializing partition example
6/30/11 2:06 PM : Starting partition kanata
6/30/11 2:06 PM : New view: [exp2:1099, exp1:1099] with viewId: 3 (old
view:[exp2:1099, exp1:1099] )
```

**Related
Documentation**

- [Configuring the Web Application Server \(SRC CLI\) on page 218](#)
- [Viewing the Web Application Server Cluster Status \(SRC CLI\) on page 230](#)
- [Configuring the Nodes in the Web Application Server Cluster \(SRC CLI\) on page 222](#)
- [Configuring the Web Application Server Shared Cluster Configuration \(SRC CLI\) on page 221](#)

PART 6

Managing SRC Access and Security (SRC CLI)

- [Configuring User Access \(SRC CLI\) on page 235](#)
- [Authenticating Users on a C Series Controller \(SRC CLI\) on page 259](#)
- [Managing Security Digital Certificates on page 275](#)
- [Connecting to Remote Hosts from the SRC Software on page 283](#)
- [Configuring and Starting the SRC SNMP Agent \(SRC CLI\) on page 285](#)

CHAPTER 24

Configuring User Access (SRC CLI)

- [SRC User Accounts Overview on page 235](#)
- [Login Classes for SRC User Accounts on page 236](#)
- [Login Class Permission Options for the SRC Software on page 237](#)
- [Predefined Login Classes for the SRC Software on page 241](#)
- [Access to Individual Commands and Configuration Statements \(SRC CLI\) on page 241](#)
- [Before You Configure Login Classes on page 244](#)
- [Configuring a Login Class \(SRC CLI\) on page 244](#)
- [Examples: Configuring Access Privileges for SRC Operational Mode Commands on page 247](#)
- [Examples: Defining Access Privileges for SRC Configuration Mode Commands on page 248](#)
- [Configuration Statements for SRC User Accounts on page 248](#)
- [Configuring User Accounts \(SRC CLI\) on page 249](#)
- [Types of Authentication for SRC User Accounts on page 251](#)
- [Configuring Authentication for SRC User Accounts \(SRC CLI\) on page 252](#)
- [Example: SRC User Accounts on page 254](#)
- [Changing the root Password for the SRC Software \(SRC CLI\) on page 255](#)
- [Recovering the root Password \(SRC CLI\) on page 256](#)
- [Configuring a System Login Announcement \(SRC CLI\) on page 257](#)

SRC User Accounts Overview

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`.

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.

**Related
Documentation**

- [Login Classes for SRC User Accounts on page 236](#)
- [Types of Authentication for SRC User Accounts on page 251](#)
- [Configuring Authentication for SRC User Accounts \(SRC CLI\) on page 252](#)
- [Configuring Authentication for SRC User Accounts \(C-Web Interface\)](#)
- [Viewing Information About the Users on the System \(C-Web Interface\)](#)
- [Example: SRC User Accounts on page 254](#)

Login Classes for SRC User Accounts

The SRC software provides four predefined login classes to use for configuring user accounts. A login class defines the access privilege levels to the SRC software. You can also configure login classes to precisely define access privileges for the user accounts in your SRC environment.

In the SRC CLI, each top-level command-line interface (CLI) command and each configuration statement have an access privilege level associated with them. Similarly, each task and subtask in the C-Web interface have an access privilege level associated with them. Users can configure and view only those tasks for which they have access privileges. The access privileges for each login class are defined by one or more *permission options*.

Permission options specify which actions are allowed for users assigned to use a login class. More than one permission option can be configured for a login class. You can use the SRC CLI or the C-Web interface to configure permission options for all commands, statements, tasks, and subtasks. For example, if you configure a user to have the **system** permission class using the C-Web interface, that user will have the same permission when accessing the SRC CLI. The privilege level for each command and statement is listed in *SRC PE CLI Command Reference*.

When you configure more than one permission, the resulting set of permissions is a combination of all of the permissions set, except for **all** and **control**.

When you configure permissions, include **view** to display information and **configure** to enter configuration mode. Two forms for the permissions control the individual parts of the configuration:

- “Plain” form—Provides read-only capability for that permission type. An example is **interface**.
- Form that ends in **-control**—Provides read and write capability for that permission type. An example is **interface-control**.

Related Documentation

- [SRC User Accounts Overview on page 235](#)
- [Login Class Permission Options for the SRC Software on page 237](#)
- [Configuring a Login Class \(SRC CLI\) on page 244](#)
- [Predefined Login Classes for the SRC Software on page 241](#)
- [Before You Configure Login Classes on page 244](#)

Login Class Permission Options for the SRC Software

Table 17 on page 237 lists the permission options available when you configure permissions with the SRC CLI and the C-Web interface. The SRC software also provides a default set of system login classes that have permissions preset.

Table 17: Login Class Permission Options

Permission	Description
admin	<p>SRC CLI—Can view user account information in configuration mode and with the show configuration command.</p> <p>C-Web interface—Can view user account information by accessing the Monitor>CLI>Authorization.</p>
admin-control	<p>SRC CLI—Can view user accounts and configure them at the [edit system login] hierarchy level.</p> <p>C-Web interface—Can view user accounts and configure them by accessing Configure>System>Login.</p>
all	SRC CLI and C-Web interface—Has all permissions.
clear	<p>SRC CLI—Can clear (delete) information learned from the network that is stored in various network databases using the clear commands.</p> <p>C-Web interface—Can clear (delete) information learned from the network that is stored in various network databases by accessing Manage>Clear.</p>
configure	<p>SRC CLI—Can enter configuration mode using the configure command.</p> <p>C-Web interface—Can access the Configure task and subtasks.</p>
control	SRC CLI and C-Web interface—Can perform all control-level operations (all operations configured with the -control permission).

Table 17: Login Class Permission Options (continued)

Permission	Description
field	SRC CLI and C-Web interface—Reserved for field (debugging) support.
firewall	<p>SRC CLI—Can view the firewall filter configuration in configuration mode.</p> <p>C-Web interface—Can view the firewall filter configuration by accessing Monitor>SAE>Services.</p>
firewall-control	<p>SRC CLI—Can view and configure firewall filter information at the [edit firewall] hierarchy level.</p> <p>C-Web interface—Can view and configure firewall filter information by accessing Configure>Services.</p>
interface	<p>SRC CLI—Can view the interface configuration in configuration mode and with the show configuration operational mode command.</p> <p>C-Web interface—Can view the interface configuration by accessing Monitor>Interfaces.</p>
interface-control	<p>SRC CLI—Can view chassis, class of service, groups, forwarding options, and interfaces configuration information. Can configure chassis, class of service, groups, forwarding options, and interfaces at the [edit] hierarchy level.</p> <p>C-Web interface—Can view chassis, class of service, groups, forwarding options, and interfaces configuration information. Can configure chassis, class of service, groups, forwarding options, and interfaces by accessing the Configure task and subtasks.</p>
maintenance	<p>SRC CLI—Can perform system maintenance, including starting a local shell on the system and becoming the superuser in the shell (by issuing the su root command), and can halt and reboot the system (using the request system commands).</p> <p>C-Web interface—Can perform system maintenance, including halting and reboot the system, by accessing Manage>Request>System.</p>
network	SRC CLI and C-Web interface—Can access the network by entering the SSH command.
reset	<p>SRC CLI—Can restart software processes using the restart command, enable components using the enable command, and disable components using the disable command.</p> <p>C-Web interface—Can restart software processes by accessing Manage>Restart, enable components by accessing Manage>Enable, and disable components by accessing Manage>Disable.</p>

Table 17: Login Class Permission Options (continued)

Permission	Description
routing	<p>SRC CLI—Can view general routing information in configuration and operational modes.</p> <p>C-Web interface—Can view general routing information by accessing Monitor>SAE>Route.</p>
routing-control	<p>SRC CLI—Can view and configure general routing at the [edit routing-options] hierarchy level.</p> <p>C-Web interface—Can view general routing and configure general routing by accessing Configure>Routing Options.</p>
secret	<p>SRC CLI and C-Web interface—Can view passwords and other authentication keys in the configuration.</p>
secret-control	<p>SRC CLI—Can view passwords and other authentication keys in the configuration and can modify them in configuration mode.</p> <p>C-Web interface—Can view passwords and other authentication keys in the configuration and can modify them by accessing Configure>System>Login.</p>
security	<p>SRC CLI—Can view security configuration in configuration mode and with the show configuration operational mode command.</p> <p>C-Web interface—Can view security configuration by accessing Monitor>Security>Certificate.</p>
security-control	<p>SRC CLI—Can view and configure security information at the [edit security] hierarchy level.</p> <p>C-Web interface—Can view security information and configure security information by accessing Manage>Request>Security.</p>
service	<p>SRC CLI and C-Web interface—Can view service and policy definitions.</p> <p>C-Web interface—Can view service definitions by accessing Monitor>SAE>Services and policy definitions by accessing Monitor>SAE>Policies.</p>
service-control	<p>SRC CLI—Can view and modify service and policy definitions.</p> <p>C-Web interface—Can view and modify service and policy definitions by accessing Configure>Services and Configure>Policies.</p>
shell	<p>SRC CLI and C-Web interface—Can start a local shell by entering the start shell command.</p>

Table 17: Login Class Permission Options (continued)

Permission	Description
snmp	<p>SRC CLI—Can view Simple Network Management Protocol (SNMP) configuration information in configuration and operational modes.</p> <p>C-Web interface—Can view Simple Network Management Protocol (SNMP) configuration information by accessing Monitor>SAE>Statistics.</p>
snmp-control	<p>SRC CLI—Can view SNMP configuration information and configure SNMP (at the [edit snmp] hierarchy level).</p> <p>C-Web interface—Can view SNMP configuration information and configure SNMP by accessing Configure>SNMP.</p>
subscriber	<p>SRC CLI—Can view information about subscriber definitions.</p> <p>C-Web interface—Can view information about subscriber definitions by accessing Monitor>SAE>Subscribers.</p>
subscriber-control	<p>SRC CLI—Can view and control information about subscriber definitions.</p> <p>C-Web interface—Can view information about subscriber definitions and control information about subscriber definitions by accessing Configure>Subscribers.</p>
system	<p>SRC CLI—Can view system-level information in configuration and operational modes.</p> <p>C-Web interface—Can view system-level configuration information by accessing Monitor>System.</p>
system-control	<p>SRC CLI—Can view system-level configuration information and configure it at the [edit system] hierarchy level.</p> <p>C-Web interface—Can view system-level configuration and configure it by accessing Configure>System.</p>
view	<p>SRC CLI—Can use various commands to display current systemwide, routing table, and protocol-specific values and statistics.</p> <p>C-Web interface—Can access various Monitor subtasks to display current systemwide, routing table, and protocol-specific values and statistics.</p>
view-configuration	<p>SRC CLI and C-Web interface—Can view all system configurations, excluding any secret configuration.</p>

To review the default system login classes, see [“Predefined Login Classes for the SRC Software” on page 241](#).

Related Documentation

- [Login Classes for SRC User Accounts on page 236](#)
- [SRC User Accounts Overview on page 235](#)

- [Access to Individual Commands and Configuration Statements \(SRC CLI\) on page 241](#)
- [Configuring a Login Class \(SRC CLI\) on page 244](#)

Predefined Login Classes for the SRC Software

Table 18 on page 241 lists the system login classes predefined in the SRC software.

Table 18: 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'
```

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
```

Related Documentation

- [Login Classes for SRC User Accounts on page 236](#)
- [SRC User Accounts Overview on page 235](#)
- [Login Class Permission Options for the SRC Software on page 237](#)
- [Configuring a System Login Announcement \(SRC CLI\) on page 257](#)
- [Changing the root Password for the SRC Software \(SRC CLI\) on page 255](#)

Access to Individual Commands and Configuration Statements (SRC CLI)

By default, all top-level CLI commands have associated access privilege levels. Users can execute only those commands and view only those statements for which they have access privileges. For each login class, you can deny or allow the use of specified

operational and configuration mode commands that would otherwise be permitted or not allowed by a specified privilege level.

Regular Expressions for Allow and Deny Statements

You can use extended regular expressions to specify which commands to allow or deny. By using extended regular expressions, you can list a number of commands in each statement.

You specify these regular expressions in the following statements at the **[edit system login class]** hierarchy level:

- **allow-commands**
- **deny-commands**
- **allow-configuration**
- **deny-configuration**

Command regular expressions implement the extended (modern) regular expressions as defined in POSIX 1003.2. [Table 19 on page 242](#) lists common regular expression operators.

Table 19: 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** or **start shell**.

The C-Web interface session closes after the specified time has elapsed with no message, and returns to the login window.

- Related Documentation**
- [Login Classes for SRC User Accounts on page 236](#)
 - [Login Class Permission Options for the SRC Software on page 237](#)
 - [Predefined Login Classes for the SRC Software on page 241](#)
 - [Configuring a Login Class \(SRC CLI\) on page 244](#)

Before You Configure Login Classes

Before you configure a login class:

- Review the predefined login classes to determine whether you can use one of these classes rather than creating a new one.

See [“Predefined Login Classes for the SRC Software” on page 241](#).

- Make sure you are familiar with how to use regular expressions to specify which commands and configuration statements to allow or deny.

Consider that you can issue one **allow** statement and one **deny** statement for operation mode commands, and one **allow** statement and one **deny** statement for configuration mode commands. Use regular expressions in a statement to specify more than one command in a statement.

See [“Access to Individual Commands and Configuration Statements \(SRC CLI\)” on page 241](#).

- Related Documentation**
- [Login Class Permission Options for the SRC Software on page 237](#)
 - [Viewing Information About the Users on the System \(C-Web Interface\)](#)
 - [Login Classes for SRC User Accounts on page 236](#)

Configuring a Login Class (SRC CLI)

Use the following configuration statements to configure login classes at the **[edit]** hierarchy level:

```

system login class name {
  allow-commands allow-commands;
  allow-configuration allow-configuration;
  deny-commands deny-commands;
  deny-configuration deny-configuration;
  idle-timeout idle-timeout;
  permissions
}

```

To configure a login class:

1. From configuration mode, access the configuration statement that configures login classes, and assign a name to the login class.

```

[edit]
user@host# edit system login class name

```

2. Specify the permissions for the login class.

```

[edit system login class name ]
user@host# set permissions permissions

```

For example, the following statement specifies that the user-account class can configure and view only user accounts:

```

[edit system login class user-accounts]
user@host# set permissions [configure admin admin-control]

```

The following statement specifies that the network-mgmt class can configure and view only SNMP parameters:

```

[edit system login class network-mgmt]
user@host# set permissions [configure snmp snmp-control]

```

3. (Optional) Configure access to specified operational mode commands that would otherwise be denied.

```

[edit system login class name ]
user@host# set allow-commands allow-commands

```

For example, the following statement specifies that the network-mgmt class can install system software:

```

[edit system login class network-mgmt]
user@host# set allow-commands "request system install"

```

4. (Optional) Deny access to specified operational mode commands that would otherwise be allowed.

```
[edit system login class class-name ]  
user@host# set deny-commands deny-commands
```

For example, the following statement specifies that the remote class cannot connect to the SRC software through SFTP:

```
[edit system login class remote]  
user@host# set deny-commands sftp
```

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 sftp";
  permissions all;
}
```

- Related Documentation**
- *Configuring Login Classes (C-Web Interface)*
 - [Configuring a System Login Announcement \(SRC CLI\) on page 257](#)
 - *Viewing Information About the Users on the System (C-Web Interface)*
 - [Configuring Authentication for SRC User Accounts \(SRC CLI\) on page 252](#)
 - [Example: SRC User Accounts on page 254](#)

Examples: Configuring Access Privileges for SRC Operational Mode Commands

The following example allows access to the **request system reboot** command for the login class **operator-and-boot** that has operator privileges defined by the **clear**, **network**, **reset**, and **view** permissions.

```
[edit system login class operator-and-boot]
user@host# set permissions [ clear network reset view ]
user@host# set allow-commands "request system reboot"
```

The following example denies access to **set** commands for the login class **operator-no-set** that has operator privileges defined by the **clear**, **network**, **reset**, and **view** permissions.

```
[edit system login class operator-no-set]
user@host# set permissions [ clear network reset view ]
user@host# set deny-commands "set"
```

The following example allows software installation but denies access to the **show nic** command for the login class **operator-no-set** that has operator privileges defined by the **clear**, **network**, **reset**, and **view** permissions.

```
[edit system login class operator-and-install-no-nic]
user@host# set permissions [ clear network reset view ]
```

```
user@host# set allow-commands "request system install"
user@host# set deny-commands "show nic"
```

**Related
Documentation**

- [Rebooting the SRC Software](#)
- [SRC User Accounts Overview on page 235](#)
- [Login Class Permission Options for the SRC Software on page 237](#)
- [Configuring a Login Class \(SRC CLI\) on page 244](#)

Examples: Defining Access Privileges for SRC Configuration Mode Commands

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)"
```

**Related
Documentation**

- [Configuring a Login Class \(SRC CLI\) on page 244](#)
- [SRC User Accounts Overview on page 235](#)
- [Login Class Permission Options for the SRC Software on page 237](#)

Configuration Statements for SRC User Accounts

Use the following configuration statements to configure user accounts at the **[edit]** hierarchy level.

```
system login user user-name {
  class class;
  full-name full-name;
  uid uid;
  prompt prompt;
  level (basic | normal | advanced | expert);
  complete-on-space (on | off);
```

```

}
system login user user-name authentication {
  plain-text-password;
  encrypted-password "password";
  ssh-authorized-keys [ssh-authorized-keys ...];
}

```

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

Related Documentation

- [Configuring User Accounts \(SRC CLI\) on page 249](#)
- [Types of Authentication for SRC User Accounts on page 251](#)
- [Configuring Authentication for SRC User Accounts \(SRC CLI\) on page 252](#)
- [SRC User Accounts Overview on page 235](#)
- [Login Classes for SRC User Accounts on page 236](#)
- [Before You Configure Login Classes on page 244](#)

Configuring User Accounts (SRC CLI)

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 17 on page 237](#).

3. Specify the user's full name.

```
[edit system login user user-name ]  
user@host# set full-name full-name
```

If the full name contains spaces, enclose it in quotation marks. Do not include colons or commas. For example:

```
[edit system login user JASmith]  
user@host# set full-name " John A. Smith"
```

4. (Optional) Specify a user identifier (UID) for the user.

```
[edit system login user user-name ]  
user@host# set uid uid
```

The identifier must be a number in the range 0 through 64,000 and must be unique within the system. If you do not assign a UID to a username, the software assigns one when you commit the configuration, preferring the lowest available number.

You must ensure that the UID is unique. However, it is possible to assign the same UID to different users.

5. (Optional) Specify a prompt that the user sees at the SRC CLI

```
[edit system login user user-name ]  
user@host# set prompt prompt
```

6. (Optional) Specify the editing level available to the user. The level determines which configuration commands are visible to the user.

```
[edit system login user user-name ]  
user@host# set level (basic | normal | advanced | expert)
```

where:

- basic—Minimal set of configuration statements and commands—only the statements that must be configured are visible.
 - normal—Normal set of configuration statements and commands—the common and basic statements are visible.
 - advanced—All configuration statements and commands, including the common and basic ones, are visible.
 - expert—All configuration statements, including common, basic, and internal statements and commands used for debugging, are visible.
7. (Optional) Specify whether entering a space completes a command.


```
[edit system login user user-name ]
user@host# set complete-on-space (on | off)
```

If you do not enter a value, **complete-on-space** is enabled by default.

8. Define the authentication methods that a user can use to log in to a C Series Controller.

See [“Types of Authentication for SRC User Accounts” on page 251](#).

9. Display the results of the configuration.

```
[edit system login]
user@host# show
. . .
user JASmith {
  class network-mgmt;
  full-name "John A. Smith";
  uid 507;
  gid 100;
  authentication {
    encrypted-password "{crypt}caZEWdaE1au0c";
  }
  level normal;
  complete-on-space on;
}
```

- Display the results of the configuration.

```
[edit system login]
user@host# show
. . .
user JASmith {
  class network-mgmt;
  full-name "John A. Smith";
  uid 507;
  gid 100;
  authentication {
    encrypted-password "{crypt}caZEWdaE1au0c";
  }
  level normal;
  complete-on-space on;
}
```

Types of Authentication for SRC User Accounts

You can configure the following types of authentication for user accounts:

- Plain text password—Prompt for a plain text (unencrypted) password. The requirements for plain text passwords are:
 - Can contain between 6 and 128 characters
 - Can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters).



NOTE: We do not recommend that the password include control characters. We do recommend that the password include at least one change of case or character class.

If you configure a plain text password, you are prompted to enter and confirm the password.

- Encrypted password—Password encoded with crypt. The format of encrypted passwords is "{crypt}<13-characters in a-zA-Z0-9./>".



NOTE: We recommend that you *do not* enter the password in encrypted format.

- SSH—SSH authentication. For SSH authentication, you can copy the contents of an SSH keys file into a CLI session.

Do not configure a plain text password and an encrypted password at the same time because one value will overwrite the other.

Related Documentation

- [Configuring Authentication for SRC User Accounts \(SRC CLI\) on page 252](#)
- [Configuring User Accounts \(C-Web Interface\)](#)
- [Example: SRC User Accounts on page 254](#)

Configuring Authentication for SRC User Accounts (SRC CLI)

You can configure user accounts by using the following methods:

- [Configuring a Plain Text Password on page 252](#)
- [Configuring SSH Authentication on page 253](#)

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
```

- See Also**
- [Configuring User Accounts for Web Applications \(SRC CLI\) on page 226](#)
 - [SRC User Accounts Overview on page 235](#)

- [Configuring a Login Class \(SRC CLI\) on page 244](#)
- [Configuring User Accounts \(SRC CLI\) on page 249](#)
- [Types of Authentication for SRC User Accounts on page 251](#)

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
AAAAB3NzaC1yc2EAAAABIwAAAIEAvSqAWNMTQJS9eqG1eq
RANI3ML4hH+u7WX/HP0W82gDSPjghnt1e5de3D8U
kuIIeUBflobgy/7AKc98FqAlvVp5onCiMg8ELD6
RYkgOgo7U6zERB25qy3sK1Rn9NzrB20qLzbvAcZW1
NiePmf1R99d/Rge7KB/5k6fq3NOG0fc= id@server" "ssh-rsa AAAA
B3NzaC1yc2EAAAABIwAAAIEAxIwe9HfZ78vbdq1+AY0uCF79yGPxgGuw
GZd9QVdT+dnwGh/4HwLITvKd8SYrhMJsyz5dWuZm
94JswQosm9BVhJwREt39NYIkLWOjGIMkk8Cxx4
TkpfFelz1cSbeFxtFBFVaBbo4YkEv5ltbuxwvbTWURkvsQa
2VJXAqls7z8= id2@server2
eriand" "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAwWoo
UD4m+SazgzF2kRIq5Y2+lx2zQbCxxqBS
D1rmW92eLPOQIBv/sEy2d8UNeHpoKot9Px8q9ABriOyO
Nc7vqNsSVnAMyicQB786uHoabSERVIYscapT
YvIGg+olbdhKySbSxOoXMehhgoQSOJZxHCbxsQJip7/7vJ
PCjRGU8Xq0= id@server3" ];
```

- See Also**
- [Configuration Statements for SRC User Accounts on page 248](#)
 - [SRC User Accounts Overview on page 235](#)
 - [Configuring User Accounts \(SRC CLI\) on page 249](#)
 - [Types of Authentication for SRC User Accounts on page 251](#)

**Related
Documentation**

- [Example: SRC User Accounts on page 254](#)
- [Configuring User Accounts for Web Applications \(SRC CLI\) on page 226](#)
- [Configuring a Login Class \(SRC CLI\) on page 244](#)
- [Configuration Statements for SRC User Accounts on page 248](#)
- [SRC User Accounts Overview on page 235](#)
- [Configuring User Accounts \(SRC CLI\) on page 249](#)
- [Types of Authentication for SRC User Accounts on page 251](#)

Example: SRC User Accounts

The following example shows the configuration for user accounts for three system users and the template user "remote." All users use one of the default system login classes.

```
system login user philip {
  class super-user;
  full-name " Philip of Macedonia" ;
  uid 1001;
  authentication {
  }
  ssh-authorized-keys [ "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAA
    IEAvSqAWNndMTQJS9eqG1eq
    RANi3ML4hH+u7WX/HP0W82gDSPpjhnt1e5de3D8UkullEUB
    flobgy/7AKc98FqAlvVp5onCiMg8ELD6
    RYkgOgo7U6zERB25qy3sK1Rn9NzrB20qLzbvAcZW1NlePmf
    1R99d/Rge7KB/5k6fq3NOG0fc= id@server" "ssh-rsa AAAAB3NzaC1yc2EA
    AAABlwAAAIEAxIwe9HfZ78vdbfq1+AY0uCF79yGPxgGuw
    GZd9QVdT+dnwGh/4HwLITvKd8SYrhMJsyz5dWuZm94JSwQ
    osm9BVhJwREt39NYIkLWOjGIMkk8Cw4
    TkpFfelz1cSbeFxtFBFVaBbo4YkEv5ltbuxwvbTWURkvsQa2VJXA
    qls7z8= id2@server2
    erian" "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAwW0oUD4
    m+SazgzF2kRlq5Y2+lx2zQbCqxBS
    D1rmW92eLPOQIBv/sEy2d8UNeHpoKot9Px8q9ABriOyONc7v
    qNsSVnAMyicQB786uHoabSERVIYscapT
    YvIGg+olbdhKySbSxOoXMehgoQSOJZxHCbxsQJip7/7vJPCjRG
    U8Xq0= id@server3" ];
  user alexander {
    full-name " Alexander the Great" ;
    uid 1002;
    class view;
    authentication {
    }
    ssh-authorized-keys [ "ssh-rsa
      AAAAB3NzaC1yc2EAAAABIwAAAIEAvSqAWNndMTQJS9eqG1eq
      RANi3ML4hH+u7WX/HP0W82gDSPpjhnt1e5de3D8UkullEUBflobgy
      /7AKc98FqAlvVp5onCiMg8ELD6
      RYkgOgo7U6zERB25qy3sK1Rn9NzrB20qLzbvAcZW1NlePmf1R99d
      /Rge7KB/5k6fq3NOG0fc= id@server" "ssh-rsa
      AAAAB3NzaC1yc2EAAAABIwAAAIEAxIwe9HfZ78vdbfq1+AY0uCF79y
```

```

GPxgGuw
GZd9QVdT+dniwGh/4HwLITvKd8SYrhMJsyz5dWuZm94JSwQosm9
BVhJwREt39NYIkLWOjGIMkk8Cw4
TkpfFelz1cSbeFxtFBFVaBbo4YkEv5ltbuxwvbTWURkvsQa2VJXA
qls7z8= id2@server2
erand" "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAwW0oUD4m+Sazgz
F2kRIq5Y2+lx2zQbCxqBS
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;
}

```

Related Documentation

- [SRC User Accounts Overview on page 235](#)
- [Login Classes for SRC User Accounts on page 236](#)
- [Types of Authentication for SRC User Accounts on page 251](#)
- [Configuring Authentication for SRC User Accounts \(SRC CLI\) on page 252](#)
- [Viewing Information About the Users on the System \(C-Web Interface\)](#)

Changing the root Password for the SRC Software (SRC CLI)

An account for the user **root** is always present in the configuration. Only the root user can change the root password. You can change the **root** password with the SRC CLI, but not with the C-Web Interface.

To change the root password:

1. Log into the SRC software as root.
2. From operational mode, change the root password.

```

root@host> set cli password
Changing password for user root.
New UNIX password:

```

You can also create a regular account for root and set the SSH key there. The class for root is always super-user—if you create an account for root, the class is ignored.

**Related
Documentation**

- [Configuring a System Login Announcement \(SRC CLI\) on page 257](#)
- [Predefined Login Classes for the SRC Software on page 241](#)
- [Login Class Permission Options for the SRC Software on page 237](#)

Recovering the root Password (SRC CLI)

If you lose the root password, you will not be able to log in as the root user unless you perform one of these tasks:

- Reset the password with the supplied USB storage device.
- Restore the default configuration from the console.



NOTE: Restoring the default configuration replaces the existing configuration with the basic default configuration supplied with the SRC software.

To reset the password with the supplied USB storage device:



NOTE: This procedure installs all system software, including the operating system, and partitions the system hard drives. As a result, any data, including data previously in the snapshot partition (if you do not select the **retainsnapshot** option at the boot prompt during the installation), is lost. To retain a copy of your configuration, save the configuration to a file in XML format and copy that file to an external system before installing the SRC software from the USB storage device.

1. Plug the USB storage device into the USB port on the C Series Controller.
2. Connect a console terminal to the C Series Controller.
See your C Series Controller Hardware Guide.
3. Power on the system.
4. At the boot prompt, enter **rescue**, and follow the instructions on the display to mount the existing system image and go into the shell.
5. In the shell, use the **chroot** command to change the root directory to the attached system image.
6. In the shell, use the **passwd** command to reset the password.

7. Exit the shell.
8. After the C Series Controller reboots and returns to the boot prompt, power off the system and remove the USB storage device before powering on the system.

The root password should be set to the password you specified in Step 6.



NOTE: After you complete this procedure, remember to disconnect the supplied USB storage device. Failure to do so can result in the loss of configuration and data if the system loses power or is rebooted.

To restore the default password from the console by loading the default configuration:

1. Connect to the console for the C Series Controller.
2. When the boot menu appears, press **a** to get to the boot command line.
3. Enter **4** as the argument at the end of the boot command line to run level 4, which will load the default configuration (including the password) that was supplied with the SRC software.

The default configuration replaces the existing configuration.

**Related
Documentation**

- [Changing the root Password for the SRC Software \(SRC CLI\) on page 255](#)

Configuring a System Login Announcement (SRC CLI)

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

To configure a system login announcement:

- At the **[edit system login]** hierarchy level, add the **announcement** statement.

```
[edit system login]
user@host# set announcement text
```

If the announcement text contains any spaces, enclose it in quotation marks.

**Related
Documentation**

- [Configuring a System Login Announcement \(C-Web Interface\)](#)
- [Before You Configure Login Classes on page 244](#)
- [Configuring a Login Class \(SRC CLI\) on page 244](#)

- [Changing the root Password for the SRC Software \(SRC CLI\) on page 255](#)

CHAPTER 25

Authenticating Users on a C Series Controller (SRC CLI)

- [Configuring RADIUS and TACACS+ Authentication on a C Series Controller \(SRC CLI\) on page 259](#)
- [TACACS+ and RADIUS Authentication/Authorization Attributes on page 260](#)
- [Configuring RADIUS Authentication \(SRC CLI\) on page 261](#)
- [Configuring TACACS+ Authentication \(SRC CLI\) on page 263](#)
- [Configuring TACACS+ Authentication \(C-Web Interface\) on page 264](#)
- [A C Series Controller as a RADIUS Client and TACACS+ Client on page 264](#)
- [Configuring More Than One Authentication Method \(SRC CLI\) on page 266](#)
- [Removing an SRC Authentication Method from the Authentication Order \(SRC CLI\) on page 268](#)
- [SRC Template Accounts for RADIUS and TACACS+ Authentication on page 268](#)
- [Example: Configuring SRC Authentication on page 270](#)
- [Configuring TACACS+ System Accounting \(SRC CLI\) on page 271](#)

Configuring RADIUS and TACACS+ Authentication on a C Series Controller (SRC CLI)

The SRC software always performs password authentication on a C Series Controller. You can configure RADIUS or TACACS+ (or both) authentication to complement password authentication. In this case, the software performs RADIUS or TACACS+ (or both) authentication before password authentication.

To configure RADIUS and TACACS+ authentication for users who access a C Series Controller:

1. Configure the connection to the RADIUS or TACACS+ server.
 - See [“Configuring RADIUS Authentication \(SRC CLI\)” on page 261](#).
 - See [“Configuring TACACS+ Authentication \(SRC CLI\)” on page 263](#).
 - See [“Configuring TACACS+ Authentication \(C-Web Interface\)” on page 264](#).
2. Configure the authentication order.
 - See [“Configuring More Than One Authentication Method \(SRC CLI\)” on page 266](#).

3. Configure template accounts.

See [“SRC Template Accounts for RADIUS and TACACS+ Authentication Overview”](#) on page 268.

4. (Optional) Configure individual user profiles.

See [“SRC User Accounts Overview”](#) on page 235.

Related Documentation

- [Configuring RADIUS and TACACS+ Authentication on a C Series Controller \(C-Web Interface\)](#)
- [Configuring TACACS+ Authentication \(C-Web Interface\)](#) on page 264
- [Removing an SRC Authentication Method from the Authentication Order \(SRC CLI\)](#) on page 268
- [Example: Configuring SRC Authentication](#) on page 270

TACACS+ and RADIUS Authentication/Authorization Attributes

Both the TACACS+ and RADIUS authentication/authorization modules support attributes returned by the authorization server. In the case of TACACS+, the attributes are encoded as strings. In the case of RADIUS, Juniper Networks RADIUS vendor-specific attributes (VSAs) are used. These VSAs are encapsulated in a RADIUS vendor-specific attribute with the vendor ID set to the Juniper Networks ID number, 2636. [Table 20 on page 260](#) describes the supported authentication/authorization attributes.

Table 20: Supported TACACS+ and RADIUS Authentication/Authorization Attributes

TACACS+ Authorization Attribute	RADIUS VSA	Description	Length	String
local-user-name	Juniper-Local-User-Name (2636.1)	Indicates the name of the user template used by this user when logging in to a device. This attribute is used only in Access-Accept packets.	≥3	One or more octets containing printable ASCII characters
allow-commands	Juniper-Allow-Commands (2636.2)	Contains an extended regular expression that enables the user to run operational mode commands in addition to the commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression

Table 20: Supported TACACS+ and RADIUS Authentication/Authorization Attributes (continued)

TACACS+ Authorization Attribute	RADIUS VSA	Description	Length	String
deny-commands	Juniper-Deny-Commands (2636.3)	Contains an extended regular expression that denies the user permission to run operation mode commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression
allow-configuration	Juniper-Allow-Configuration (2636.4)	Contains an extended regular expression that enables the user to run configuration mode commands in addition to the commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression
deny-configuration	Juniper-Deny-Configuration (2636.5)	Contains an extended regular expression that denies the user permission to run configuration commands authorized by the user's login class permission bits. This attribute is used only in Access-Accept packets.	≥3	One or more octets containing printable ASCII characters, in the form of an extended regular expression

- Related Documentation**
- [Configuring RADIUS and TACACS+ Authentication on a C Series Controller \(SRC CLI\) on page 259](#)
 - [Configuring RADIUS and TACACS+ Authentication on a C Series Controller \(SRC CLI\) on page 259](#)
 - [A C Series Controller as a RADIUS Client and TACACS+ Client on page 264](#)

Configuring RADIUS Authentication (SRC CLI)

Use the following configuration statements to configure information about one or more RADIUS servers on the network at the **[edit]** hierarchy level:

```
system radius-server address {
  port port ;
  secret secret ;
  timeout timeout;
  retry retry ;
}
```

To configure information about RADIUS servers for authentication:

1. From configuration mode, access the configuration statement that adds a RADIUS server.

```
[edit]
user@host# edit system radius-server address
```

2. Specify a port number on which to contact the RADIUS server.

```
[edit system radius-server address ]
user@host# set port port
```

By default, port number **1812** is used.

3. Specify a password. Passwords can contain spaces. The secret used by the C Series Controller must match that used by the server.

```
[edit system radius-server address ]
user@host# set secret secret
```

4. (Optional) Specify the amount of time that the C Series Controller waits to receive a response from a RADIUS server.

```
[edit system radius-server address ]
user@host# set timeout timeout
```

By default, the C Series Controller waits 3 seconds. You can change the timeout to a value from 1 through 90 seconds.

5. Specify the number of times that the C Series Controller attempts to contact a RADIUS authentication server.

```
[edit system radius-server address ]
user@host# set retry retry
```

By default, the C Series Controller retry property is set to 3 times. You can change the retry value to a number from 1 through 10 times.

To configure a set of users that share a single account for authorization purposes, you create a template user.

Related Documentation

- [Configuring RADIUS Authentication \(C-Web Interface\)](#)
- [Configuring RADIUS and TACACS+ Authentication on a C Series Controller \(SRC CLI\) on page 259](#)
- [Removing an SRC Authentication Method from the Authentication Order \(SRC CLI\) on page 268](#)

- [Example: Configuring SRC Authentication on page 270](#)
- [A C Series Controller as a RADIUS Client and TACACS+ Client on page 264](#)

Configuring TACACS+ Authentication (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;
  source-address source-address;
  secret secret;
}
```

To configure information about TACACS+ servers for authentication:

1. From configuration mode, access the configuration statement that adds a TACACS+ 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. (Optional) Specify the source address used when communicating with the TACACS+ server.

```
[edit system tacplus-server]
user@host# set source-address source-address
```

4. 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 [“SRC Template Accounts for RADIUS and TACACS+ Authentication Overview” on page 268](#).

- Related Documentation**
- [Configuring TACACS+ Authentication \(C-Web Interface\) on page 264](#)
 - [Configuring RADIUS and TACACS+ Authentication on a C Series Controller \(SRC CLI\) on page 259](#)
 - [A C Series Controller as a RADIUS Client and TACACS+ Client on page 264](#)
 - [Removing an SRC Authentication Method from the Authentication Order \(SRC CLI\) on page 268](#)
 - [Example: Configuring SRC Authentication on page 270](#)

Configuring TACACS+ Authentication (C-Web Interface)

To configure information about TACACS+ servers for authentication:

1. Click **Configure**, expand **System**, and then click **Tacplus Server**.
The Tacplus Server pane appears.
2. Click **Create**, enter information as described in the Help text in the main pane, and then click **Apply**.

To configure a set of users that share a single account for authorization purposes, you create a template user.

- Related Documentation**
- [Configuring RADIUS and TACACS+ Authentication on a C Series Controller \(SRC CLI\) on page 259](#)
 - [A C Series Controller as a RADIUS Client and TACACS+ Client on page 264](#)
 - [Removing an SRC Authentication Method from the Authentication Order \(SRC CLI\) on page 268](#)
 - [Example: Configuring SRC Authentication on page 270](#)
 - [Configuring RADIUS Authentication \(C-Web Interface\)](#)
 - [Configuring Authentication Order \(C-Web Interface\)](#)

A C Series Controller as a RADIUS Client and TACACS+ Client

On a C Series Controller, you can use more than one authentication method. You can configure the C Series Controller to be a RADIUS and TACACS+ client by:

- Configuring RADIUS and TACACS+ authentication.
- Configuring the authentication order to prioritize the order in which the C Series Controller uses configured authentication methods.

For each login attempt, the SRC software tries the authentication methods in the order configured, until the password matches. The SRC software fails to authenticate a user either because the authentication server (RADIUS or TACACS+ server) is unavailable or because the user entered wrong credentials (username or password). If one of the

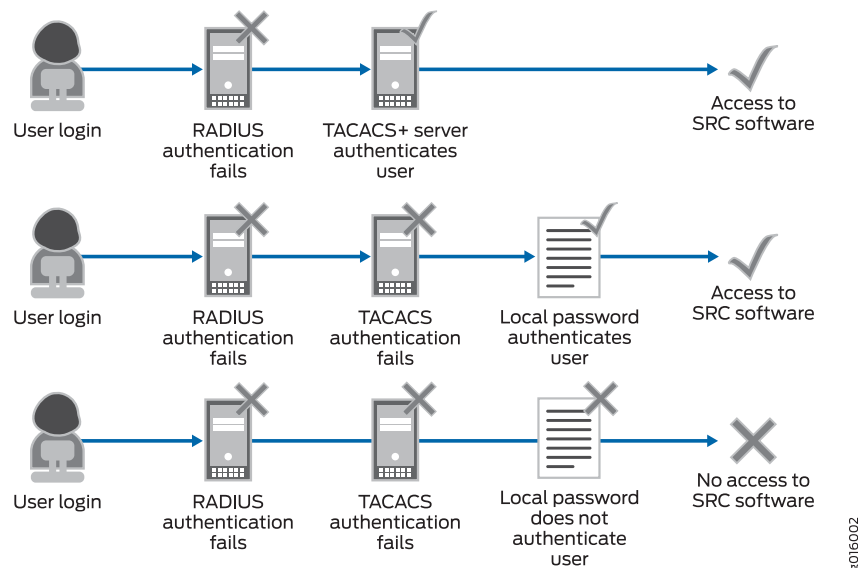
authentication methods in the authentication order fails to authenticate a user, then the SRC software tries to authenticate the user through other available authentication methods in the configured order. For example, if the SRC software tries to authenticate users through TACACS+ server, and if the TACACS+ authentication fails, the SRC software tries to authenticate users through RADIUS server; and then, if the RADIUS authentication fails, the SRC software uses local password authentication. When all the three authentication methods fail, the user is denied access to the C Series Controller.

If one of the RADIUS or TACACS+ servers among multiple configured servers is unavailable or the server fails to authenticate the user because of the invalid credentials, the SRC software tries to authenticate the user by sending requests to each of the RADIUS or TACACS+ servers in the configured order.

If local password authentication does not appear in the prioritized list of authentication methods, the SRC software uses local password authentication last. The SRC software always uses password configured locally, 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 local password authentication if RADIUS and TACACS+ authentication fails.

Figure 18 on page 265 shows three authentication scenarios. In the first two, a user is authenticated while authentication servers are unavailable. In the third scenario, a user is not authenticated by any of the three authentication methods.

Figure 18: Authentication Order: RADIUS, TACACS+, Local Password



Related Documentation

- [Configuring RADIUS and TACACS+ Authentication on a C Series Controller \(SRC CLI\) on page 259](#)
- [Configuring RADIUS Authentication \(SRC CLI\) on page 261](#)
- [Configuring TACACS+ Authentication \(C-Web Interface\) on page 264](#)

Configuring More Than One Authentication Method (SRC CLI)

Tasks to configure more than one authentication method at the SRC CLI are:

1. [Configuring Authentication Order on page 266](#)
2. [Configuring TACACS+ or RADIUS Authentication on page 266](#)
3. [Configuring TACACS+ and RADIUS Authentication on page 267](#)

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.



NOTE: The SRC software looks at the local password file even if the RADIUS server sends an Access-Reject.

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]
```

- Related Documentation**
- [Types of Authentication for SRC User Accounts on page 251](#)
 - [Removing an SRC Authentication Method from the Authentication Order \(SRC CLI\) on page 268](#)
 - [A C Series Controller as a RADIUS Client and TACACS+ Client on page 264](#)
 - [Configuring RADIUS Authentication \(SRC CLI\) on page 261](#)
 - [Example: Configuring SRC Authentication on page 270](#)

Removing an SRC Authentication Method from the Authentication Order (SRC CLI)

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
```

- Related Documentation**
- [Types of Authentication for SRC User Accounts on page 251](#)
 - [Configuring Authentication for SRC User Accounts \(SRC CLI\) on page 252](#)
 - [Example: Configuring SRC Authentication on page 270](#)

SRC Template Accounts for RADIUS and TACACS+ Authentication

1. [SRC Template Accounts for RADIUS and TACACS+ Authentication Overview on page 268](#)
2. [Using Remote Template Accounts \(SRC CLI\) on page 269](#)
3. [Configuring a Local SRC User Template \(SRC CLI\) on page 270](#)

SRC Template Accounts for RADIUS and TACACS+ Authentication Overview

When a user logs in to the CLI, the following authentication is performed:

- RADIUS or TACACS+ (or both) server authentication
- Authentication through a user account configured under **[system login user]**

For authorization purposes, you can use a template account to create a single account that can be shared by a set of users at the same time.

Typically when you use RADIUS and/or TACACS+ authentication, the user account is shared among a group of users who have the same privileges. You create template accounts for sets of users. Template accounts can be named:

- **remote**—(Default) A single account that defines user permissions for all users that authenticate through RADIUS or TACACS+
- *name-of-your-choice*—Account for a group of users

Use a named template account when you need different types of templates. Each template can define a different set of permissions appropriate to a group of users who use that template. For example, you can configure a set of remote users to concurrently share a single UID.

When a user is part of a group that uses a template account, the command-line interface (CLI) username is the login name; however, the privileges, file ownership, and effective username are inherited from the template account.

Named Template Accounts

Template accounts for which you define a name are defined on a C Series Controller and are referenced by the TACACS+ and RADIUS authentication servers through usernames. All users who share a local user template account have the same access privileges.

When a user who accesses the C Series Controller through a named template account logs in:

1. The user provides a login name and password at the system login prompts.
2. The system authenticates the user as configured based on the login name and password.

See “[Configuring Authentication Order](#)” on page 266.

3. If the authentication succeeds, the system loads the user profile as configured by the **system login user login-name** statement. If a profile is not configured through the **system login user login-name** statement, the system uses the profile configured through the **system login user remote** statement.

If authentication fails, or a profile could not be loaded, the login attempt fails.



NOTE: To ensure that remote users have a unique uid, we require a named template for each remote user.

Using Remote Template Accounts (SRC CLI)

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 ;
}
```



NOTE: To ensure that remote users have a unique `uid`, we require a named template for each remote user.

All users who share the remote template account have the same access privileges.

- See Also**
- [Using Remote Template Accounts \(C-Web Interface\)](#)
 - [Configuring a Local SRC User Template \(SRC CLI\) on page 270](#)

Configuring a Local SRC User Template (SRC CLI)

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 ;
}
```

- See Also**
- [Configuring a Local SRC User Template \(C-Web Interface\)](#)
 - [Using Remote Template Accounts \(SRC CLI\) on page 269](#)

Example: Configuring SRC Authentication

The following example allows login only by:

- Individual user Philip
- Users who have been authenticated by a remote RADIUS server

If a user logs in and is not authenticated by the RADIUS server, the user is denied access to the C Series Controller. However, if the RADIUS server is not available, the user can be authenticated through an SRC password.

In this example, user configuration includes:

- An individual user account for Philip that provides privileges for the **super-user** class after RADIUS authentication.
- A remote user template account for all other users to share the same class and user ID (UID) after RADIUS authentication.

Individual SRC accounts are not configured for other users. When they log in to the system and the RADIUS server authenticates them, they are given access using the same UID 9999 and the same privileges for the **operator** class.

```
[edit]
system {
  authentication-order radius;
  login {
    user philip {
      full-name "Philip";
      uid 1001;
      class super-user;
    }
    user remote {
      full-name "All remote users";
      uid 9999;
      class operator;
    }
  }
}
```

Related Documentation

- [Types of Authentication for SRC User Accounts on page 251](#)
- [Configuring Authentication for SRC User Accounts \(SRC CLI\) on page 252](#)
- [Removing an SRC Authentication Method from the Authentication Order \(SRC CLI\) on page 268](#)

Configuring TACACS+ System Accounting (SRC CLI)

You can use TACACS+ `system accounting` to track and log software logins, configuration changes, and interactive commands. To audit these events, include the following statements at the `[edit]` hierarchy level:

```
system accounting events [events....] {
}
system accounting destination tacplus server server-address{
  secret secret;
  source-address source-address;
  timeout timeout;
  port port-number;
```

```
}
```

1. [Specifying TACACS+ Auditing and Accounting Events \(SRC CLI\) on page 272](#)
2. [Configuring TACACS+ Server Accounting \(SRC CLI\) on page 273](#)

Specifying TACACS+ Auditing and Accounting Events (SRC CLI)

You can specify the types of events you want to audit when using a TACACS+ accounting server.

To configure the types of events you want to audit:

1. From configuration mode, access the configuration statement used to specify TACACS+ events.

```
[edit]
user@host# edit system accounting events events
```

events is one or more of the following:

- **login**—Audit logins.
- **change-log**—Audit configuration changes (copy, delete, edit, exit, help, history, insert, load, quit, rename, rollback, run, save, set, show, top, up).
- **interactive-commands**—Audit interactive commands (any command-line input).

Events are published to the accounting server with the information described in [Table 21 on page 272](#).

Table 21: Information Published for Events

Start Event	Stop Event	Update Event
username (for instance: root)	username (for instance: root)	username (for instance: root)
task_id: pid (for instance: 22956)	task_id: pid (for instance: 22956)	task_id: pid (for instance: 22956)
startTime in seconds. The time the CLI session was created, measured in seconds, between the time it was created and midnight, January 1, 1970 UTC.	startTime in seconds. The time the CLI session was created, measured in seconds, between the time it was created and midnight, January 1, 1970 UTC.	executedTime in seconds. The time the CLI command was executed, measured in seconds, between the time it was executed and midnight, January 1, 1970 UTC.
	stopTime in seconds. The time the CLI session was destroyed, measured in seconds, between the time it was destroyed and midnight, January 1, 1970 UTC.	cmd (for instance: "show")

Table 21: Information Published for Events (continued)

Start Event	Stop Event	Update Event
		cmd_arg (for instance: "sae subscribers brief")

See Also • [Configuring TACACS+ Server Accounting \(SRC CLI\) on page 273](#)

Configuring TACACS+ Server Accounting (SRC CLI)

To configure TACACS+ server accounting:

1. From configuration mode, access the configuration statement used to specify the TACACS+ server address.

```
[edit]
user@host# edit system accounting destination tacplus server server-address.
```

In the *server-address*, specify the address or hostname of the TACACS+ server. To configure multiple TACACS+ servers, include multiple server statements.



NOTE: If no TACACS+ servers are configured at the [edit system accounting destination tacplus] statement hierarchy level, the SRC software uses the TACACS+ servers configured at the [edit system tacplus-server] hierarchy level.

2. Specify the source address used when communicating with the TACACS+ server.

```
[edit system accounting destination tacplus server server-address]
user@host# set source-address source-address
```

3. Specify the secret (password) the TACACS+ client uses to connect to the TACACS+ server. This password must match the password used by the server.

```
[edit system accounting destination tacplus server server-address]
user@host# set secret secret
```

4. (Optional) Specify the length of time (in seconds) that the SRC software waits to receive a response from the TACACS+ server.

```
[edit system accounting destination tacplus server server-address]
user@host# set timeout timeout
```

By default, the SRC software waits 3 seconds. You can configure this to be a value in the range 1 through 90 seconds.

5. Specify the TACACS+ server port number.

```
[edit system accounting destination tacplus server server-address]  
user@host# set port port-number
```

**Related
Documentation**

- [Configuring TACACS+ Authentication \(C-Web Interface\) on page 264](#)
- [Configuring TACACS+ Authentication \(SRC CLI\) on page 263](#)

CHAPTER 26

Managing Security Digital Certificates

- [Digital Certificates Overview on page 275](#)
- [Before You Use Digital Certificates on page 276](#)
- [Commands to Manage Digital Certificates on page 276](#)
- [Manually Obtaining Digital Certificates \(SRC CLI\) on page 277](#)
- [Obtaining Digital Certificates through SCEP \(SRC CLI\) on page 278](#)
- [Removing a Certificate Request on page 280](#)
- [Removing a Certificate on page 280](#)

Digital Certificates Overview

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 routers running Junos OS.

You can use SRC CLI commands to manage certificates manually, or through the Simple Certificate Enrollment Protocol (SCEP).

Certificates are in the format defined in the X.509 standard for public key infrastructure. The certificate requests are in the Public Key Cryptology Standard (PKCS) #10 format.

Related Documentation

- [Before You Use Digital Certificates on page 276](#)
- [Commands to Manage Digital Certificates on page 276](#)
- [Manually Obtaining Digital Certificates \(SRC CLI\) on page 277](#)
- [Obtaining Digital Certificates through SCEP \(SRC CLI\) on page 278](#)
- [*Viewing Information About Security Certificates \(SRC CLI\)*](#)

Before You Use Digital Certificates

Before you use digital certificates, you should:

- Have a working relationship with a certificate authority (CA).
- Have a good working knowledge of how to work with certificates.
- Decide whether or not to use SCEP to assist with certificate management.
- Identify which connections should be secured by a protocol that requires digital certificates.
- Know how to use the file management commands in the CLI.

Related Documentation

- [Digital Certificates Overview on page 275](#)
- [Commands to Manage Digital Certificates on page 276](#)
- [Manually Obtaining Digital Certificates \(SRC CLI\) on page 277](#)
- [Obtaining Digital Certificates through SCEP \(SRC CLI\) on page 278](#)
- [Viewing Information About Security Certificates \(SRC CLI\)](#)

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**
- **request security generate-self-signed-certificate**
- **show security certificate**

For detailed information about each command, see the *SRC PE CLI Command Reference*.

Related Documentation

- [Manually Obtaining Digital Certificates \(SRC CLI\) on page 277](#)
- [Obtaining Digital Certificates through SCEP \(SRC CLI\) on page 278](#)

Manually Obtaining Digital Certificates (SRC CLI)

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 \(SRC CLI\)” on page 278](#).

To manually add a signed certificate:

1. Create a certificate signing request.

```
user@host> request security generate-certificate-request subject subject password
password
```

where:

- **subject** is the distinguished name of the SRC host; for example **cn=cseries1,ou=pop,o=Juniper,l=kanata,st=Ontario,c=Canada**.
- **password** is the password received from the certificate authority for the specified subject.

By default, this request creates the file **/tmp/certreq.csr** and encodes the file by using Privacy-Enhanced Mail (pem) encoding.

2. Copy the file generated to another system, and submit the certificate signing request file generated to the certificate authority.

You can transfer the file through FTP by using the **file copy** command.

```
user@host> file copy source_file ftp://username@server [:port ]/destination_file
```

The remote system prompts you for your password.

3. When you receive the signed certificate, copy the file back to the system to the **/tmp** directory.

You can transfer the file through FTP, as shown in Step 2.

4. Add the certificate to the SRC configuration.

```
user@host> request security import-certificate file-name file-name identifier identifier
```

where

- **file-name** is the name of the certificate file in the **/tmp** folder. The file has one of the following extensions:
 - CER—Windows extension
 - PEM—Privacy-Enhanced Mail encoding

- DER—Binary encoding
- BER—Binary encoding
- **identifier** is the name of the certificate.

For example, to import the file **sdx.cer** that is identified as **web**:

```
user@host> request security import-certificate file-name sdx.cer identifier web
```



NOTE: You can use the **request security generate-self-signed-certificate** command to create a self-signed certificate.

5. Verify that the certificate is part of the SRC configuration.

```
user@host> show security certificate
web  subject:CN=host
```

If there are no certificates on the system, the CLI displays the following message:

```
user@host> show security certificate
No entity certificates in key store
```

Related Documentation

- [Before You Use Digital Certificates on page 276](#)
- [Removing a Certificate Request on page 280](#)
- [Digital Certificates Overview on page 275](#)
- [Commands to Manage Digital Certificates on page 276](#)

Obtaining Digital Certificates through SCEP (SRC CLI)

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 \(SRC CLI\)” on page 277](#).

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 subjectsubjectpassword password
```

where:

- **subject** is the distinguished name of the SRC host; for example **cn=myhost**.
- **password** is the password received from the certificate authority for the specified subject.

For example, to request a certificate from the CA authority SdxCA at a specified URL on the server security_server:

```
user@host> request security enroll url
http://security_server:8080/ejbca/publicweb/apply/scep/pkiclient.exe identifier
web ca-identifier SdxCA subject cn=myhost password mypassword
```

```
Received certificate:
Version: 3
Serial Number: 6822890691617224432
Signature Algorithm: SHA1withRSA
Issuer: CN=SdxCA
```

```
Valid From: Tue Sep 19 16:33:11 EDT 2006
Valid Until: Thu Sep 18 16:43:11 EDT 2008
Subject: CN=myhost
Public key: RSA
Do you want to install the above certificate [yes,no] ? (no) y
```

3. Verify that the certificate is part of the SRC configuration.

```
user@host> show security certificate
web subject:CN=myhost
```

If there are no certificates on the system, the CLI displays the following message:

```
No entity certificates in key store
```

- Related Documentation**
- [Before You Use Digital Certificates on page 276](#)
 - [Removing a Certificate Request on page 280](#)
 - [Digital Certificates Overview on page 275](#)
 - [Commands to Manage Digital Certificates on page 276](#)

Removing a Certificate Request

To remove a certificate request:

1. Review the certificate request files on the system. These files are in the **/tmp** directory and have the file extension **.csr**.
2. Issue the **clear security certificate-request** command to remove a file. For example:

```
user@host> clear security certificate-request certreq.csr
```

- Related Documentation**
- [Manually Obtaining Digital Certificates \(SRC CLI\) on page 277](#)
 - [Obtaining Digital Certificates through SCEP \(SRC CLI\) on page 278](#)

Removing a Certificate

To remove a certificate:

1. Issue the **show security certificate** command to view information about the local certificates. For example:

```
user@host> show security certificate
web  subject:CN=myhost
CAcert1 subject:CN=myhost
```

2. Issue the **clear security certificate** command to remove a certificate. Use the **trusted** option if the certificate is a CA certificate.

```
clear security certificate <trusted> <identifier identifier>
```

For example:

- To remove the certificate **web** (that is not a trusted certificate) from myhost:

```
user@host>clear security certificate web
```

- To remove a trusted (CA) certificate from myhost:

```
user@host>clear security certificate trusted CAcert 1
```

**Related
Documentation**

- [Removing a Certificate Request on page 280](#)
- [Manually Obtaining Digital Certificates \(SRC CLI\) on page 277](#)
- [Obtaining Digital Certificates through SCEP \(SRC CLI\) on page 278](#)

CHAPTER 27

Connecting to Remote Hosts from the SRC Software

- [Connecting to a Remote Host Through SSH on page 283](#)
- [Connecting to a Remote Host Through Telnet on page 283](#)

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.

Related Documentation

- [Connecting to a Remote Host Through Telnet on page 283](#)
- [Configuring a C Series Controller to Accept SSH Connections \(SRC CLI\) on page 97](#)
- [Securing Connections Between a C Series Controller and Remote Hosts on page 96](#)

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.

**Related
Documentation**

- [Connecting to a Remote Host Through SSH on page 283](#)
- [Securing Connections Between a C Series Controller and Remote Hosts on page 96](#)

CHAPTER 28

Configuring and Starting the SRC SNMP Agent (SRC CLI)

- Configuration Statements for the SRC SNMP Agent on page 286
- Configuring the SRC SNMP Agent (SRC CLI) on page 287
- Configuring General Properties for the SRC SNMP Agent (SRC CLI) on page 287
- Configuring Initial Properties for the SRC SNMP Agent (SRC CLI) on page 288
- Configuring Directory Connection Properties for the SRC SNMP Agent (SRC CLI) on page 290
- Configuring Directory Monitoring Properties for the SRC SNMP Agent (SRC CLI) on page 291
- Configuring Logging Destinations for the SRC SNMP Agent (SRC CLI) on page 292
- Configuring JRE Properties (SRC CLI) on page 292
- Configuration Statements for the SRC SNMP Agent on page 293
- Configuring the SRC SNMP Agent (SRC CLI) on page 294
- Configuring System Information for the SRC SNMP Agent (SRC CLI) on page 295
- Configuring Access Control for SNMPv3 Users (C-Web Interface) on page 296
- Creating SNMPv3 Users on page 297
- Configuring Access Privileges for SNMPv3 Users (SRC CLI) on page 297
- Configuring Authentication for SNMPv3 Users (SRC CLI) on page 298
- Configuring Encryption for SNMPv3 Users (SRC CLI) on page 299
- Configuring Access Control for Communities (SRC CLI) on page 300
- Configuring Access Control for the VACM (SRC CLI) on page 301
- Associating Security Names with a Community (SRC CLI) on page 303
- Defining Named Views (SRC CLI) on page 304
- Defining Access Privileges for an SNMP Group (SRC CLI) on page 305
- Assigning Security Names to Groups (SRC CLI) on page 307
- Configuring Notification Targets (SRC CLI) on page 308
- Operating the SRC SNMP Agent on page 310
- Starting the SRC SNMP Agent (SRC CLI) on page 310

- [Stopping the SRC SNMP Agent \(SRC CLI\) on page 311](#)
- [Monitoring the SRC SNMP Agent \(SRC CLI\) on page 311](#)

Configuration Statements for the SRC SNMP Agent

Use the following configuration statements to configure the SRC 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*.

- Related Documentation**
- [Configuring the SRC SNMP Agent \(SRC CLI\) on page 287](#)

Configuring the SRC SNMP Agent (SRC CLI)

The SRC 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 SRC SNMP agent:

1. Configure general properties for the SRC SNMP agent, including trap history limit, component polling interval, and protocol log level.
See [“Configuring General Properties for the SRC SNMP Agent \(SRC CLI\)” on page 287](#).
2. Configure initial properties for the SRC SNMP agent, including the connection from the SRC SNMP agent to the directory and directory monitoring properties.
See [“Configuring Initial Properties for the SRC SNMP Agent \(SRC CLI\)” on page 288](#).
See [“Configuring Directory Connection Properties for the SRC SNMP Agent \(SRC CLI\)” on page 290](#).
See [“Configuring Directory Monitoring Properties for the SRC SNMP Agent \(SRC CLI\)” on page 291](#).
3. Configure logging destinations for the SRC SNMP agent.
See [“Configuring Logging Destinations for the SRC SNMP Agent \(SRC CLI\)” on page 292](#).
4. (Optional) Configure the Java heap memory for the SRC SNMP agent.
See [“Configuring JRE Properties \(SRC CLI\)” on page 292](#).

After you configure the local properties for the SRC SNMP agent, you can configure the SNMP agent. See [“Configuring the SRC SNMP Agent \(SRC CLI\)” on page 294](#).

- Related Documentation**
- [Starting the SRC SNMP Agent \(SRC CLI\) on page 310](#)
 - [Stopping the SRC SNMP Agent \(SRC CLI\) on page 311](#)
 - [Monitoring the SRC SNMP Agent \(SRC CLI\) on page 311](#)

Configuring General Properties for the SRC SNMP Agent (SRC CLI)

Use the following configuration statements to configure general properties for the SRC 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 SRC SNMP agent:

1. From configuration mode, access the configuration statement that configures the SRC SNMP agent.

```
[edit]
user@host# edit snmp agent
```

2. (Optional) Specify the maximum number of elements stored in the SNMP trap history table.

```
[edit snmp agent]
user@host# set trap-history-limit trap-history-limit
```

3. (Optional) Specify the interval at which an SRC component is polled.

```
[edit snmp agent]
user@host# set component-polling-interval component-polling-interval
```

4. (Optional) Specify the log level for SNMP requests and responses received from the master agent.

```
[edit snmp agent]
user@host# set protocol-log-level protocol-log-level
```

To enable packet-level logging, set the **protocol-log-level** option to 9 or less.

5. (Optional) Verify your configuration.

```
[edit snmp agent]
user@host# show
```

The output indicates the trap history limit, the component polling interval, the protocol log level, the initial properties, the logging destinations, and the Java heap size.

Related Documentation

- [Configuring the SRC SNMP Agent \(SRC CLI\) on page 287](#)
- [Configuring General Properties for the SRC SNMP Agent \(C-Web Interface\)](#)
- [Monitoring the SRC SNMP Agent \(SRC CLI\) on page 311](#)

Configuring Initial Properties for the SRC SNMP Agent (SRC CLI)

Use the following configuration statements to configure initial properties for the SRC SNMP agent:

```
snmp agent initial {
  base-dn base-dn;
  host-id host-id;
}
```

To configure properties for the SRC SNMP agent:

1. From configuration mode, access the configuration statement that configures the SRC SNMP agent.

```
[edit]
user@host# edit snmp agent initial
```

2. Specify the DN of the directory used for the SRC 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 SRC SNMP agent.

```
[edit snmp agent initial]
user@host# set host-id host-id
```

If the entry does not exist, the entry and the subentries for the components and traps is automatically created in the system management configuration.

4. (Optional) Verify your configuration.

```
[edit snmp agent initial]
user@host# show
base-dn o=UMC;
host-id POP-ID;
directory-connection {
  url ldap://127.0.0.1:389/;
  principal cn=sysman,ou=components,o=operators,<base>;
  credentials *****;
}
directory-eventing {
  eventing;
}
```

Related Documentation

- [Configuring the SRC SNMP Agent \(SRC CLI\) on page 287](#)
- [Configuring Initial Properties for the SRC SNMP Agent \(C-Web Interface\)](#)
- [Configuring General Properties for the SRC SNMP Agent \(SRC CLI\) on page 287](#)
- [Monitoring the SRC SNMP Agent \(SRC CLI\) on page 311](#)

Configuring Directory Connection Properties for the SRC SNMP Agent (SRC CLI)

Use the following configuration statements to configure directory connection properties for the SRC 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 SRC SNMP agent.

```
[edit]  
user@host# edit snmp agent initial directory-connection
```

2. Specify the directory connection properties.

```
[edit snmp agent initial directory-connection]  
user@host# set ?
```

For more information about the directory connection properties, see [“Configuring Directory Connection Properties” on page 321](#).

3. (Optional) Verify your configuration.

```
[edit snmp agent initial directory-connection]  
user@host# show  
url ldap://127.0.0.1:389/  
principal cn=sysman,ou=components,o=operators,<base>;  
credentials *****;
```

Related Documentation

- [Configuring the SRC SNMP Agent \(SRC CLI\) on page 287](#)
- [Configuring Directory Connection Properties for the SRC SNMP Agent \(C-Web Interface\)](#)
- [Configuring Directory Monitoring Properties for the SRC SNMP Agent \(SRC CLI\) on page 291](#)

- [Monitoring the SRC SNMP Agent \(SRC CLI\) on page 311](#)

Configuring Directory Monitoring Properties for the SRC SNMP Agent (SRC CLI)

Use the following configuration statements to configure directory monitoring properties for the SRC 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 SRC SNMP agent:

1. From configuration mode, access the configuration statement that configures the SRC SNMP agent.

```
[edit]
user@host# edit snmp agent initial directory-eventing
```

2. Specify the properties for the SRC SNMP agent.

```
[edit snmp agent initial eventing]
user@host# set ?
```

3. (Optional) Verify your configuration.

```
[edit snmp agent initial directory-eventing]
user@host# show
eventing;
```

Related Documentation

- [Configuring the SRC SNMP Agent \(SRC CLI\) on page 287](#)
- [Configuring Directory Monitoring Properties for the SRC SNMP Agent \(C-Web Interface\)](#)
- [Configuring Directory Connection Properties for the SRC SNMP Agent \(SRC CLI\) on page 290](#)
- [Monitoring the SRC SNMP Agent \(SRC CLI\) on page 311](#)

Configuring Logging Destinations for the SRC SNMP Agent (SRC CLI)

Use the following configuration statement to configure logging destinations for the SRC SNMP agent:

```
snmp agent logger name ...
```

To configure logging destinations:

1. From configuration mode, access the configuration statement that configures the SRC 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 system log-based logging:

```
[edit snmp agent]  
user@host# set logger name syslog
```

Related Documentation

- [Configuring the SRC SNMP Agent \(SRC CLI\) on page 287](#)
- [Configuring System Logging \(SRC CLI\)](#)
- [Configuring an SRC Component to Store Log Messages in a File \(SRC CLI\)](#)
- [Configuring the SAE to Store Log Messages in a File \(C-Web Interface\)](#)
- [Configuring Logging Destinations for the SRC SNMP Agent \(C-Web Interface\)](#)

Configuring JRE Properties (SRC CLI)

Use the following configuration statements to configure Java Runtime Environment (JRE) properties for the SRC SNMP agent:

```
snmp agent java {  
    heap-size heap-size;  
}
```

To configure properties for the SRC SNMP agent:

1. From configuration mode, access the configuration statement that configures the SRC 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;
```

Related Documentation • [Configuring JRE Properties \(C-Web Interface\)](#)

Configuration Statements for the SRC SNMP Agent

Use the following configuration statements to configure the SRC 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 access {
```

```
    authorization (read-only | read-write);
    oid oid;
}
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*.

Related Documentation • [Configuring the SRC SNMP Agent \(SRC CLI\) on page 294](#)

Configuring the SRC SNMP Agent (SRC CLI)

To configure the SRC SNMP agent to control its operation:

1. Configure information supplied by the SRC SNMP agent, including the listening address and system information.
[See “Configuring System Information for the SRC SNMP Agent \(SRC CLI\)” on page 295.](#)
2. Configure access control for the SRC 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 \(C-Web Interface\)” on page 296.](#)
[See “Configuring Access Control for Communities \(SRC CLI\)” on page 300.](#)

See “Configuring Access Control for the VACM (SRC CLI)” on page 301.

3. Configure active monitoring.

See “Configuring Notification Targets (SRC CLI)” on page 308.

**Related
Documentation**

- [Configuration Statements for the SRC SNMP Agent on page 293](#)
- [Operating the SRC SNMP Agent on page 310](#)

Configuring System Information for the SRC SNMP Agent (SRC CLI)

Use the following configuration statements to configure information supplied by the SRC SNMP agent:

```
snmp {
  contact contact;
  name name;
  location location;
  description description;
  address [address...];
}
```

To configure properties for the SRC SNMP agent:

1. From configuration mode, access the configuration statement that configures the SRC 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 SRC 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 SRC SNMP agent configuration.

**Related
Documentation**

- [Configuring the SRC SNMP Agent \(SRC CLI\) on page 294](#)
- [Configuring System Information for the SNMP Agent \(C-Web Interface\)](#)
- [Operating the SRC SNMP Agent on page 310](#)
- [Configuration Statements for the SRC SNMP Agent on page 293](#)

Configuring Access Control for SNMPv3 Users (C-Web Interface)

To configure access control for SNMPv3 users:

1. Click **Configure**, and expand **SNMP>V3>USM>Local Engine**.
2. From the Create new list, select **User**.
3. Enter a name for the new User in the dialog box, and click **OK**.
4. From the side pane, expand the name of the user, and (optional) specify the authentication type and (optional) the encryption.



NOTE: Before you configure encryption, you must configure the authentication type.

**Related
Documentation**

- [Configuring an SNMPv3 Security Name for SNMP Monitoring \(SRC CLI\)](#)
- [Configuring Authentication for SNMPv3 Users \(SRC CLI\) on page 298](#)

- [Configuring Access Control for Communities \(SRC CLI\) on page 300](#)

Creating SNMPv3 Users

You can create a user associated with an SNMPv3 group. For each SNMPv3 user, you specify the authentication type, encryption, and access privileges. The username functions as a security name when the SNMPv3 security model is a user-based security model (USM). This provides a level of security for SNMPv3.

To create an SNMPv3 user:

- From configuration mode, enter the following configuration statement.

```
[edit]
user@host# edit snmp v3 usm local-engine user username
```

Related Documentation

- [Configuring Authentication \(C-Web Interface\)](#)
- [Configuring Authentication for SNMPv3 Users \(SRC CLI\) on page 298](#)
- [Configuring Encryption for SNMPv3 Users \(SRC CLI\) on page 299](#)
- [Configuring Access Privileges for SNMPv3 Users \(SRC CLI\) on page 297](#)

Configuring Access Privileges for SNMPv3 Users (SRC CLI)

In a user-based security model (USM), you can define access privileges for SNMPv3 users. But you cannot assign the security name to an SNMP group. Here, the security name is the username configured at the **[edit snmp v3 usm local-engine user]** hierarchy level.

Use the following configuration statements to define access privileges for an SNMPv3 user at the **[edit snmp v3 usm local-engine user *username* access]** hierarchy level:

```
snmp v3 usm local-engine user username access {
  authorization (read-only | read-write);
  oid oid;
}
```

To define access privileges for an SNMPv3 user in a USM:

1. From configuration mode, enter the following configuration statement.

```
[edit]
user@host# edit snmp v3 usm local-engine user username access
```

2. (Optional) Specify the authorization level.

To specify read-only access:

```
[edit snmp v3 usm local-engine user username access]
user@host# set authorization read-only
```

To specify read-and-write access:

```
[edit snmp v3 usm local-engine user username access]
user@host# set authorization read-write
```

3. (Optional) Specify the object identifier used to represent the subtree of MIB objects to which access is allowed.

```
[edit snmp v3 usm local-engine user username access]
user@host# set oid oid
```



NOTE: By default, all clients are allowed to access the complete OID tree.

4. (Optional) Verify your configuration.

```
root@c3bng-src4# show
authorization read-only;
oid 1;
```

Related Documentation

- [Creating SNMPv3 Users on page 297](#)
- [Configuring an SNMPv3 Security Name for SNMP Monitoring \(SRC CLI\)](#)
- [Configuring Authentication for SNMPv3 Users \(SRC CLI\) on page 298](#)
- [Configuring Access Control for Communities \(SRC CLI\) on page 300](#)
- [Configuring Access Control for SNMPv3 Users \(C-Web Interface\) on page 296](#)

Configuring Authentication for SNMPv3 Users (SRC CLI)

For SNMPv3 users, you can configure the authentication type and the password used for authentication. The type of authentication can be Message Digest 5 (MD5) or Secure Hash Algorithm (SHA). By default, authentication is not configured for SNMPv3 users.

To configure authentication for SNMPv3 users:

1. From configuration mode, access the configuration statement that configures the authentication type.

To configure MD5 authentication:


```
[edit]
user@host# set snmp v3 usm local-engine user username authentication-md5
```

To configure SHA authentication:

```
[edit]
user@host# set snmp v3 usm local-engine user username authentication-sha
```

2. Specify the authentication password.

To configure authentication password for MD5:

```
[edit]
user@host# set snmp v3 usm local-engine user username authentication-md5
authentication-password
```

To configure authentication password for SHA:

```
[edit]
user@host# set snmp v3 usm local-engine user username authentication-sha
authentication-password
```

The password must contain at least eight characters.

- Related Documentation**
- [Creating SNMPv3 Users on page 297](#)
 - [Configuring the SRC SNMP Agent \(SRC CLI\) on page 294](#)
 - [Configuring Authentication \(C-Web Interface\)](#)
 - [Configuring Encryption for SNMPv3 Users \(SRC CLI\) on page 299](#)
 - [Configuration Statements for the SRC SNMP Agent on page 293](#)

Configuring Encryption for SNMPv3 Users (SRC CLI)

Before you configure encryption, you must configure the authentication type. See [“Configuring Authentication for SNMPv3 Users \(SRC CLI\)” on page 298](#). You need to use the authentication type and encryption when you query MIB values. By default, if you do not configure encryption for an SNMPv3 user, all clients are allowed access to all MIB values. To restrict access to MIB values and thereby increase security, you need to configure encryption.

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 contain at least eight characters.

**Related
Documentation**

- [Creating SNMPv3 Users on page 297](#)
- [Configuring the SRC SNMP Agent \(SRC CLI\) on page 294](#)
- [Configuration Statements for the SRC SNMP Agent on page 293](#)

Configuring Access Control for Communities (SRC CLI)

An SNMP community string is a text string that functions as a password. SNMP uses the community string to authenticate messages that are transmitted between the SNMP manager and the SNMP agent. The community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent. You can configure SNMP community strings for SNMPv1 and SNMPv2c users only. SNMPv3 users do not use community strings.

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 objects to which access is allowed.

```
[edit snmp community community]  
user@host# set oid oid
```

5. (Optional) Verify your configuration.

```
[edit snmp community community]  
user@host# show
```

Related Documentation

- [Configuring the SRC SNMP Agent \(SRC CLI\) on page 294](#)
- [Configuration Statements for the SRC SNMP Agent on page 293](#)

Configuring Access Control for the VACM (SRC CLI)

Use the view-based access control model (VACM) to restrict access to particular branches of a subtree of MIB objects by excluding or including a MIB variable. If you want to include system-related MIB values but not the system name and system contact MIB OID, then create a view by excluding the system name and system contact MIB OID. Then the system name and system contact MIB OID are not displayed.

To configure access control for a view-based access control model (VACM):



NOTE: You can also associate an SNMP view with a community by using this configuration.

1. Define a named view.
See [“Defining Named Views \(SRC CLI\)” on page 304.](#)
2. Map an SNMPv1 or SNMPv2c community name to a security name.
See [“Associating Security Names with a Community \(SRC CLI\)” on page 303.](#)
3. Create an SNMPv3 user.
See [“Creating SNMPv3 Users” on page 297.](#)
4. Map from a group of users or communities to a view.
See [“Defining Access Privileges for an SNMP Group \(SRC CLI\)” on page 305.](#)
5. Map a security name into a named group.
See [“Assigning Security Names to Groups \(SRC CLI\)” on page 307.](#)
6. (Optional) Verify your configuration.

```
[edit snmp v3]
```

```
snmp-community 123 {
  address 10.212.10.2;
  community-name TEST-Community;
  security-name testSecurity;
}
usm {
  local-engine {
    user testUser;
  }
}
vacm {
  access {
    group testGroup {
      default-context-prefix {
        security-model usm {
          security-level none {
            read-view testView;
            write-view none;
          }
        }
      }
    }
  }
}
security-to-group {
  security-model usm {
    security-name testUser {
      group-name testGroup;
    }
  }
}
```

```

    }
    security-model v2c {
        security-name testSecurity {
            group-name testGroup;
        }
    }
}

```

- Related Documentation**
- [Configuring the SRC SNMP Agent \(SRC CLI\) on page 294](#)
 - [Configuration Statements for the SRC SNMP Agent on page 293](#)

Associating Security Names with a Community (SRC CLI)

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

```

Use a 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
```

Related Documentation

- [Configuring Access Control for Communities \(SRC CLI\) on page 300](#)
- [Defining Access Privileges for an SNMP Group \(SRC CLI\) on page 305](#)
- [Associating Security Names with a Community \(C-Web Interface\)](#)

Defining Named Views (SRC CLI)

A named view identifies a group of MIB objects to which access is enabled. Each MIB object in a named view contains a common object identifier (OID) prefix that represents a subtree of MIB objects for the view.

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
```

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
```

```
test_view {
  oid 1.3.6.1.2.1.1.4 {
    exclude;
  }
  oid 1.3.6.1.2.1.1.5 {
    exclude;
  }
  oid system {
    include;
  }
}
```

Related Documentation

- [Defining Named Views \(C-Web Interface\)](#)
- [Creating SNMPv3 Users on page 297](#)
- [Configuring Access Control for the VACM \(SRC CLI\) on page 301](#)

Defining Access Privileges for an SNMP Group (SRC CLI)

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
```

Related Documentation

- [Configuring Access Control for Communities \(SRC CLI\) on page 300](#)
- [Configuring Access Control for the VACM \(SRC CLI\) on page 301](#)
- [Defining Access Privileges for an SNMP Group \(C-Web Interface\)](#)

Assigning Security Names to Groups (SRC CLI)

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
```

- Related Documentation**
- [Creating SNMPv3 Users on page 297](#)
 - [Associating Security Names with a Community \(SRC CLI\) on page 303](#)

Configuring Notification Targets (SRC CLI)

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
```

- Related Documentation**
- [Configuring Notification Targets \(C-Web Interface\)](#)
 - [SNMP Traps Overview](#)

Operating the SRC SNMP Agent

You must configure the SRC SNMP agent and then manually start the agent. If you attempt to manually start the SRC SNMP agent before it is configured, the software displays a message that the agent has not been configured and cannot start.

The SRC SNMP agent automatically restarts in the event of a host reboot or process failure that stops the agent.

- Related Documentation**
- [Configuring the SRC SNMP Agent \(SRC CLI\) on page 294](#)
 - [Configuration Statements for the SRC SNMP Agent on page 293](#)

Starting the SRC SNMP Agent (SRC CLI)

Before you start the SRC SNMP agent:

1. Perform the initial configuration tasks.
[See “Configuring the SRC Software” on page 46.](#)
2. Configure the SRC SNMP agent.
[See “Configuring the SRC SNMP Agent \(SRC CLI\)” on page 287.](#)

Manually start the SRC SNMP agent the first time it runs. Thereafter, the agent automatically restarts.

To start the SRC SNMP agent:

```
user@host> enable component agent
```

The system responds with a start message. If the SRC SNMP agent is already running, the system responds with a warning message indicating that fact.

- Related Documentation**
- [Starting the SRC SNMP Agent \(C-Web Interface\)](#)
 - [Stopping the SRC SNMP Agent \(SRC CLI\) on page 311](#)
 - [Monitoring the SRC SNMP Agent \(SRC CLI\) on page 311](#)

Stopping the SRC SNMP Agent (SRC CLI)

To stop the SRC SNMP agent:

```
user@host> disable component agent
```

The system responds with a stop message. If the SRC SNMP agent is not running when you issue the command, the software responds with a warning message indicating that fact.

**Related
Documentation**

- [Stopping the SRC SNMP Agent \(C-Web Interface\)](#)
- [Starting the SRC SNMP Agent \(SRC CLI\) on page 310](#)
- [Configuring the SRC SNMP Agent \(SRC CLI\) on page 287](#)

Monitoring the SRC SNMP Agent (SRC CLI)

Purpose Display the SRC SNMP agent status.

Action user@host> show component

The system responds with a status message.

**Related
Documentation**

- [Monitoring the SRC SNMP Agent \(C-Web Interface\)](#)
- [Configuring the SRC SNMP Agent \(SRC CLI\) on page 287](#)

PART 7

Configuring Operating Properties for Components

- [Distributing Directory Changes to SRC Components on page 315](#)
- [Configuring Local Properties \(SRC CLI\) on page 317](#)

Distributing Directory Changes to SRC Components

- [Directory Eventing System Overview on page 315](#)
- [Managing Directory Communication on page 316](#)

Directory Eventing System Overview

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/>.

Related Documentation

- [Managing Directory Communication on page 316](#)
- [Local Properties for SRC Components on page 317](#)
- [Configuring Initial Directory Eventing Properties for SRC Components on page 323](#)
- [Configuring Directory Connection Properties for the SRC SNMP Agent \(SRC CLI\) on page 290](#)
- [Viewing Information About Components Installed \(SRC CLI\)](#)

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 2.
4. If a directory fails to respond 10 times, DES prevents further communication with the directory.

For information about managing SRC components with the SRC CLI, see the *SRC PE CLI User Guide*.

Related Documentation

- [Directory Eventing System Overview on page 315](#)
- [Changing the Location of Data in the Directory on page 320](#)

CHAPTER 30

Configuring Local Properties (SRC CLI)

- [Local Properties for SRC Components on page 317](#)
- [Configuration Statements for Local Configuration on page 317](#)
- [Configuring Basic Local Properties on page 318](#)
- [Changing the Location of Data in the Directory on page 320](#)
- [Configuring Directory Connection Properties on page 321](#)
- [Configuring Initial Directory Eventing Properties for SRC Components on page 323](#)
- [Verifying the Local Configuration for a Component on page 324](#)

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.

For information about managing SRC components with the SRC CLI, see the *SRC PE CLI User Guide*.

Related Documentation

- [SRC Component Overview on page 9](#)
- [Configuring SRC Components on page 47](#)
- [Configuring Basic Local Properties on page 318](#)
- [Viewing Information About Components Installed \(SRC CLI\)](#)

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*.

- Related Documentation**
- [Configuring Basic Local Properties on page 318](#)
 - [Local Properties for SRC Components on page 317](#)

Configuring Basic Local Properties

In most cases you can use the default operating properties. Change the default properties if needed for your environment.

Use the following configuration statements to configure basic local properties for a component:

```
slot number component-name {
    base-dn base-dn ;
    java-runtime-environment java-runtime-environment ;
    java-heap-size java-heap-size ;
    snmp-agent;
}
```

To review the default local configuration and then change values:

1. From configuration mode, access the configuration statement that specifies the slot configuration for a component.

```
[edit]
user@host# edit slot number nic
```

For example:

```
[edit]
user@host# edit slot 0 nic
```

2. To view the default configuration, run the **show** command. For example:

```
[edit slot 0 nic]
user@host# show
base-dn o=umc;
java-runtime-environment ../jre/bin/java;
java-heap-size 128m;
hostname DemoHost;
initial {
```



NOTE: The **hostname** statement is specific to the NIC.

3. (Optional) If you store data in the directory in a location other than the default, *o=umc*, change this value.

```
[edit slot 0 nic]
user@host> set base-dn base-dn
```

4. (Optional) If you encounter problems caused by lack of memory, change the maximum memory size available to the JRE.

```
[edit slot 0 nic]
user@host> set java-heap-size java-heap-size
```

5. (Optional) Enable viewing of SNMP counters through an SNMP browser.

```
[edit slot 0 nic]
user@host> set snmp-agent
```

Related Documentation

- [Local Properties for SRC Components on page 317](#)
- [Verifying the Local Configuration for a Component on page 324](#)
- [Configuration Statements for Local Configuration on page 317](#)

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
```

- Related Documentation**
- [Configuring Initial Directory Eventing Properties for SRC Components on page 323](#)
 - [Configuring Basic Local Properties on page 318](#)
 - [Configuration Statements for Local Configuration on page 317](#)
 - [Managing Directory Communication on page 316](#)

Configuring Directory Connection Properties

Use the following configuration statements to configure directory properties for a component:

```
slot number component-name initial directory-connection {
    url url ;
    backup-urls [ backup-urls ...];
    principal principal ;
    credentials credentials ;
    protocol (ldaps);
    timeout timeout ;
    check-interval check-interval ;
    blacklist;
    snmp-agent;
}
```

To configure directory connection properties for a component:

1. From configuration mode, access the configuration statement that specifies the directory configuration for a component on a slot.

```
user@host# edit slot number component initial directory-connection
```

For example:

```
user@host# edit slot 0 nic initial directory-connection
```

2. Specify the URL that identifies the location of the primary directory server.

```
[edit slot 0 nic initial directory-connection]
user@host# set url url
```

On a C Series Controller, this value is ldap://127.0.0.1:389.

3. (Optional) Specify URLs that identify the locations of backup directory servers. Backup servers are used if the primary directory server is not accessible.

```
[edit slot 0 nic initial directory-connection]
user@host# set backup-urls directory-backup-url1 directory-backup-url2
```

4. Specify the DN that the SRC component uses for authentication to access the directory.

```
[edit slot 0 nic initial directory-connection]  
user@host# set principal principal
```

5. Specify the password with which the SRC component accesses the directory.

```
[edit slot 0 nic initial directory-connection]  
user@host# set credentials credentials
```

6. (Optional) Specify whether the connection to the directory uses secure LDAP. If you do not configure a security protocol, plain socket is used.

```
[edit slot 0 nic initial directory-connection]  
user@host# set protocol ldaps
```

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

```
[edit slot 0 nic initial directory-connection]  
user@host# set timeout timeout
```

8. (Optional) Specify the time interval at which the software attempts to connect to the directory.

```
[edit slot 0 nic initial directory-connection]  
user@host# set check-interval check-interval
```

9. (Optional) Enable the directory eventing system to prevent a connection to a directory after the directory fails to respond during an interval in which the directory was polled 10 times.

```
[edit slot 0 nic initial directory-connection]  
user@host# set blacklist
```

10. Specify that the SRC SNMP agent exports MIBs for this directory connection.

```
[edit slot 0 nic initial directory-connection]  
user@host# set snmp-agent
```

Related Documentation

- [Configuring Basic Local Properties on page 318](#)
- [Configuring Initial Directory Eventing Properties for SRC Components on page 323](#)
- [Configuration Statements for Local Configuration on page 317](#)
- [Verifying the Local Configuration for a Component on page 324](#)

Configuring Initial Directory Eventing Properties for SRC Components

You can use the default configuration for directory eventing properties, or you can change the configuration to comply with your environment.

The following configuration statements configure initial directory eventing properties for a component:

```
slot number sae initial directory-eventing {
    eventing;
    signature-dn signature-dn ;
    polling-interval polling-interval ;
    event-base-dn event-base-dn ;
    dispatcher-pool-size dispatcher-pool-size ;
}
```

To change directory eventing configuration:

1. From configuration mode, access the configuration statement that specifies the initial eventing configuration for a component on a slot.

```
[edit]
user@host# edit slot number component initial directory-eventing
```

For example:

```
[edit]
user@host# edit slot 0 nic initial directory-eventing
```

2. (Optional) Specify an interval at which an SRC component polls the directory to check for directory changes.

```
[edit slot 0 nic initial directory-eventing]
user@host# set polling-interval polling-interval
```

3. (Optional) Specify the DN of an entry superior to the data associated with an SRC component in the directory.

```
[edit slot 0 nic initial directory-eventing]
user@host# set event-base-dn event-base-dn
```

4. (Optional) Specify the number of events that an SRC component can receive simultaneously from the directory.

```
[edit slot 0 nic initial directory-eventing]
user@host# set dispatcher-pool-size dispatcher-pool-size
```

For information about the default setting for the directory eventing properties, see the *SRC PE CLI Command Reference*.

- Related Documentation**
- [Changing the Location of Data in the Directory on page 320](#)
 - [Directory Eventing System Overview on page 315](#)

Verifying the Local Configuration for a Component

Purpose Verify the local configuration for a component.

- Action**
1. From configuration mode, access the configuration statement that configures the slot connection. For example, to verify the slot configuration for the NIC:

```
user@host# edit slot 0 nic
```

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

```
[edit slot 0 nic ]
user@host# show
base-dn o=umc;
java-runtime-environment ../jre/bin/java;
java-heap-size 128m;
snmp-agent;
hostname DemoHost;
initial {
  dynamic-dn "ou=dynamicConfiguration, ou=Configuration, o=Management,<base>";

  directory-connection {
    url ldap://127.0.0.1:389/;
    backup-urls ;
    principal cn=nic,ou=Components,o=Operators,<base>;
    credentials *****;
    timeout 10;
    check-interval 60;
  }
  directory-eventing {
    eventing;
    signature-dn <base>;
    polling-interval 15;
    event-base-dn <base>;
    dispatcher-pool-size 1;
  }
  static-dn "l=OnePop,l=NIC, ou=staticConfiguration, ou=Configuration,
o=Management,<base>";
}
```

- Related Documentation**
- [Configuring Basic Local Properties on page 318](#)
 - *Viewing Information About Components Installed (SRC CLI)*
 - [Local Properties for SRC Components on page 317](#)

PART 8

Reference Material

- [SRC-Related Abbreviations on page 329](#)
- [SRC-Related References on page 339](#)

SRC-Related Abbreviations

- [SRC-Related Abbreviations on page 329](#)

SRC-Related Abbreviations

The following table includes the abbreviations used throughout the SRC documentation.

Table 22: SRC Software-Related Abbreviations

Abbreviation	Description
3GPP	Third-Generation Partnership Project
AAA	authentication, authorization, and accounting
AATV	authentication/authorization transfer vector
ACI	access control information
ADSL	asymmetric digital subscriber line
AES	Advanced Encryption Standard
AH	authentication header
API	application programming interface
A-RACF	access-resource and admission control function
ASCII	American Standard Code for Information Interchange
ASP	<ul style="list-style-type: none">• application service provider• Adaptive Services PIC
ATM	Asynchronous Transfer Mode
AVP	attribute value pair
BCID	billing correlation identifier

Table 22: SRC Software-Related Abbreviations (continued)

Abbreviation	Description
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
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

Table 22: SRC Software-Related Abbreviations (continued)

Abbreviation	Description
DISP	Directory Information Shadowing Protocol
DIT	directory information tree
DMI	Device Management Interface
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

Table 22: SRC Software-Related Abbreviations (continued)

Abbreviation	Description
GMT	Greenwich Mean Time
GRE	generic routing encapsulation
GUI	graphical user interface
HFC	hybrid fiber coaxial
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	Secure HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
ID	identification (identifying; identifier)
IDE	integrated development environment
IDL	interface definition language
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

Table 22: SRC Software-Related Abbreviations (continued)

Abbreviation	Description
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
LNS	L2TP network server
LSA	link-state advertisement
MAC	Media Access Control
Mb	megabit(s)
MB	megabyte(s)
MBeans	manageable JavaBeans

Table 22: SRC Software-Related Abbreviations (continued)

Abbreviation	Description
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

Table 22: SRC Software-Related Abbreviations (continued)

Abbreviation	Description
PFS	Perfect Forward Secrecy
PIB	Policy Information Base
PIM	Protocol Independent Multicast
PKCS	Public Key Cryptology Standard
PLP	packet loss priority
POP	point of presence
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PTA	PPP Terminated Aggregation
QoS	quality of service
QTP	QoS-tracking plug-in
RACS	resource and admission control subsystem
RADIUS	Remote Authentication Dial-In User Service
RAS	Remote Access Server
RCEF	resource control enforcement function
RDBMS	relational database management system
RDN	relative distinguished name
RED	random early detection
RF	radio frequency
RKS	record-keeping server
RPC	remote procedure call
RSpec	service request specification
RSVP	Resource Reservation Protocol
RTPS	real-time polling service

Table 22: SRC Software-Related Abbreviations (continued)

Abbreviation	Description
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	<ul style="list-style-type: none"> • security parameter index • service provider interface
SRC	Session and Resource Control (formerly SDX—Service Deployment System)
SRC ACP	SRC Admission Control Plug-In
SRC CLI	SRC command-line interface
SRC PE	SRC Policy Engine
SRC VTA	SRC Volume Tracking Application
SSL	Secure Sockets Layer

Table 22: SRC Software-Related Abbreviations (continued)

Abbreviation	Description
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	<ul style="list-style-type: none"> time to live time-to-live
UDP	User Datagram Protocol
UGS	unsolicited grant service
UGS-AD	unsolicited grant service with activity detection
UML	Unified Modeling Language
URI	Uniform Resource Indicator
URL	Uniform Resource Locator
UTF-8	Unicode Transformation Format-8
UUID	universal unique identifier
VACM	view-based access control model
VLAN	virtual local area network
VoIP	voice over Internet Protocol
VPN	virtual private network
VR	virtual router
VSA	vendor-specific attribute (RADIUS)

Table 22: SRC Software-Related Abbreviations (continued)

Abbreviation	Description
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

SRC-Related References

- SRC-Related References on page 339

SRC-Related References

This topic lists RFCs, draft RFCs, other software standards, hardware standards, and other references that provide information about the protocols and features supported by the SRC software. Topics include:

- Draft RFCs on page 339
- RFCs on page 339
- Other Software Standards on page 341
- URLs on page 341

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 website at <http://www.ietf.org> for the latest drafts.

Table 23: Draft RFCs

Reference	Protocol or Feature
LDAP Extensions for Scrolling View Browsing of Search Results— http://tools.ietf.org/id/draft-ietf-ldapext-ldapv3-vlv-09.txt (June 2003 expiration)	LDAP

RFCs

Table 24: RFCs

Reference	Protocol or Feature
RFC 3494—Lightweight Directory Access Protocol version 2 (LDAPv2) to Historic Status (March 2003)	LDAP

Table 24: RFCs (continued)

Reference	Protocol or Feature
RFC 3084—COPS Usage for Policy Provisioning (COPS-PR) (March 2001)	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 (January 2000)	COPS
RFC 2388—Returning Values from Forms: multipart/form-data (August 1998)	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
RFC 2131—Dynamic Host Configuration Protocol (March 1997)	DHCP
RFC 1588—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

Table 24: RFCs (continued)

Reference	Protocol or Feature
RFC 791—Internet Protocol (September 1981)	IP
RFC 5424—The Syslog Protocol (March 2009)	System Logging

Other Software Standards

Table 25: 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 26: Juniper Networks URLs

Reference	Description
https://www.juniper.net	Juniper Networks
https://www.juniper.net/us/en/partners	J-Partner Program
https://www.juniper.net/support	Customer Support Organization
https://www.juniper.net/documentation	Technical documentation
https://www.juniper.net/documentation/feedback/	Technical Documentation Feedback Form
https://www.juniper.net/documentation/software/junos/index.html	Junos OS technical documentation
https://www.juniper.net/documentation/software/erx/index.html	JunosE Software technical documentation
https://www.juniper.net/documentation/software/management/idp/	Technical documentation for Juniper Networks Intrusion Detection and Prevention (IDP) software

Table 26: Juniper Networks URLs (continued)

Reference	Description
https://www.juniper.net/documentation/software/management/src	Technical documentation for the SRC software
https://www.juniper.net/documentation/software/management/src/api-index.html	Technical documentation for the SRC application programming Interfaces
https://www.juniper.net/documentation/software/management/security-manager/index.html	Technical documentation for Juniper Networks NetScreen-Security Manager software

Table 27: Third-Party URLs

Reference	Protocol or Feature
ftp://ftp.gtk.org/pub/gtk/python	GTK library for use with Python programs
http://cui.unige.ch/db-research/Enseignement/analyseinfo/AboutBNF.html	BNF notation
http://openjdk.java.net/	OpenJDK
http://jakarta.apache.org/tomcat	Servlet container
http://attic.apache.org/projects/jakarta-regexp.html	Java regular expression documentation
http://docs.oracle.com/javase/6/docs/api/java/text/MessageFormat.html	Java message formats
http://docs.oracle.com/javase/6/docs/api/java/text/SimpleDateFormat.html	Java date and time format
http://docs.oracle.com/javase/6/docs/api/java/util/logging/FileHandler.html	Java logger
http://docs.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html	Java regular expression documentation
http://docs.oracle.com/javase/6/docs/technotes/guides/intl/encoding.doc.html	Character encoding that a compiler uses when loading Java source files
http://java.sun.com/j2ee/1.4/docs/tutorial/doc/index.html	Web application
http://docs.oracle.com/javase/6/docs/api/index.html	Java documentation
http://docs.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.html	Java keytool documentation

Table 27: Third-Party URLs (continued)

Reference	Protocol or Feature
http://docs.oracle.com/javase/tutorial/jndi/overview/index.html	Java Naming and Directory Interface (JNDI)
http://net-snmp.sourceforge.net/	Net-SNMP agent
http://gnuprologjava.sourceforge.net	GNUPROLOG
http://pysnmp.sourceforge.net	pysnmp
http://python-ldap.sourceforge.net	LDAP client API for Python
http://www.apache.org	Apache Web server and extensions
https://developer.mozilla.org/en-US/docs/Web/JavaScript/Guide	JavaScript scripting language
http://www.eclipse.org	Portal development
http://www.entrust.net	Certificate authority
https://www.juniper.net/documentation/en_US/release-independent/sbr/information-products/pathway-pages/sbr-carrier/product/index.html	Juniper SBR-Carrier RADIUS server
http://www.jacorb.org/documentation.html	JacORB documentation
http://www.jboss.org/	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

Table 27: Third-Party URLs (continued)

Reference	Protocol or Feature
http://www.packetcable.com/specifications/multimedia.html	PacketCable Multimedia Specification
http://www.python.org	Python programming language
https://docs.python.org/2/howto/regex.html	Python regular expression syntax
https://docs.python.org/2/library/	Python keywords
http://www.eclipsetotale.com/tomcatPlugin.html	Portal development
http://www.verisign.com	Certificate authority
http://www.w3.org/TR/SOAP/	Simple Object Access Protocol (SOAP)
http://marcelotoledo.wpengine.com/wp-content/uploads/2007/12/wispr_v10.pdf	WiFi Alliance WISPr version 1