User Access and Authentication

Modified: 2018-10-08

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

User Access and Authentication

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.

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.

Table of Contents

List of Figures

List of Tables

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at https://www.juniper.net/documentation/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at https://www.juniper.net/books.

Documentation Conventions

Table 1 on page x defines notice icons used in this guide.

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.

Documentation Conventions

Table 1 on page x defines the notice icons used in this guide. Table 3 on page xi defines text conventions used throughout this documentation.

Table 2: 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 3: Text Conventions

Convention	Description	Examples
Bold text like this	• Represents keywords, scripts, and tools in text. • Represents a GUI element that the user selects, clicks, checks, or clears.	• 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.	`nic-locators {`
		`  login {`
		`  resolution {`
		`  resolver-name /realms/`
		`  login/A1;`
		`  key-type LoginName;`
		`  value-type SaeId;`
		`  }`

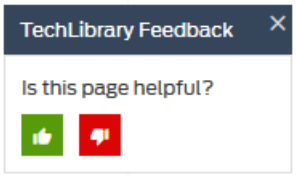
Table 3: Text Conventions (continued)

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

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use 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 https://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/
- Open a case online in the CSC Case Management tool: https://www.juniper.net/cm/

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

Opening a Case with JTAC

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

- Use the Case Management tool in the CSC at https://www.juniper.net/cm/.
- 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://www.juniper.net/support/requesting-support.html.

PART 1

Overview

CHAPTER 1

Software Features Overview

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 3 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)	• 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.
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.

Table 4: Descriptions of SRC Components (continued)

Component	Description
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	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. 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.
Repository	
Directory	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. For large subscriber databases, you must supply your own directory.
SRC Configuration and Management Tools	
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.

Table 4: Descriptions of SRC Components (continued)

Component	Description
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.
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	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. 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.
Demonstration Applications (available on the Juniper Networks Website)	

Table 4: Descriptions of SRC Components (continued)

Component	Description
Enterprise Audit Plug-In	Defines a callback interface, which receives events when IT managers complete specified operations.
Enterprise Manager Portal	Allows service providers to provision services for enterprise subscribers on routers running JunosE or Junos OS and allows IT managers to manage services. 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 all IT managers to make requests about public IP addresses through the Enterprise Manager Portal.
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*

CHAPTER 2

User Access

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 8
- Types of Authentication for SRC User Accounts on page 16
- Configuring Authentication for SRC User Accounts (SRC CLI) on page 30
- Configuring Authentication for SRC User Accounts (C-Web Interface) on page 31

- *Viewing Information About the Users on the System (C-Web Interface)*
- Example: SRC User Accounts on page 54

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 7
- Login Class Permission Options for the SRC Software on page 9
- Configuring a Login Class (SRC CLI) on page 24
- Predefined Login Classes for the SRC Software on page 12
- Before You Configure Login Classes on page 23

Login Class Permission Options for the SRC Software

Table 5 on page 9 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 5: Login Class Permission Options

Permission	Description
admin	SRC CLI—Can view user account information in configuration mode and with the **show configuration** command. C-Web interface—Can view user account information by accessing the **Monitor>CLI>Authorization**.
admin-control	SRC CLI—Can view user accounts and configure them at the **[edit system login]** hierarchy level. C-Web interface—Can view user accounts and configure them by accessing **Configure>System>Login**.
all	SRC CLI and C-Web interface—Has all permissions.
clear	SRC CLI—Can clear (delete) information learned from the network that is stored in various network databases using the **clear** commands. C-Web interface—Can clear (delete) information learned from the network that is stored in various network databases by accessing **Manage>Clear**.
configure	SRC CLI—Can enter configuration mode using the **configure** command. C-Web interface—Can access the **Configure** task and subtasks.
control	SRC CLI and C-Web interface—Can perform all control-level operations (all operations configured with the **-control** permission).
field	SRC CLI and C-Web interface—Reserved for field (debugging) support.
firewall	SRC CLI—Can view the firewall filter configuration in configuration mode. C-Web interface—Can view the firewall filter configuration by accessing **Monitor>SAE>Services**.
firewall-control	SRC CLI—Can view and configure firewall filter information at the **[edit firewall]** hierarchy level. C-Web interface—Can view and configure firewall filter information by accessing **Configure>Services**.

Table 5: Login Class Permission Options (continued)

Permission	Description
interface	SRC CLI—Can view the interface configuration in configuration mode and with the **show configuration** operational mode command. C-Web interface—Can view the interface configuration by accessing **Monitor>Interfaces**.
interface-control	SRC CLI—Can view chassis, class of service, groups, forwarding options, and interfaces configuration information. Can configure chassis, class of service, groups, forwarding options, and interfaces at the [edit] hierarchy level. C-Web interface—Can view chassis, class of service, groups, forwarding options, and interfaces configuration information. Can configure chassis, class of service, groups, forwarding options, and interfaces by accessing the **Configure** task and subtasks.
maintenance	SRC CLI—Can perform system maintenance, including starting a local shell on the system and becoming the superuser in the shell (by issuing the **su root** command), and can halt and reboot the system (using the **request system** commands). C-Web interface—Can perform system maintenance, including halting and reboot the system, by accessing **Manage>Request>System**.
network	SRC CLI and C-Web interface—Can access the network by entering the **SSH** and **telnet** commands.
reset	SRC CLI—Can restart software processes using the **restart** command, enable components using the **enable** command, and disable components using the **disable** command. C-Web interface—Can restart software processes by accessing **Manage>Restart**, enable components by accessing **Manage>Enable**, and disable components by accessing **Manage>Disable**.
routing	SRC CLI—Can view general routing information in configuration and operational modes. C-Web interface—Can view general routing information by accessing **Monitor>SAE>Route**.
routing-control	SRC CLI—Can view and configure general routing at the **[edit routing-options]** hierarchy level. C-Web interface—Can view general routing and configure general routing by accessing **Configure>Routing Options**.
secret	SRC CLI and C-Web interface—Can view passwords and other authentication keys in the configuration.

Table 5: Login Class Permission Options (continued)

Permission	Description
secret-control	SRC CLI—Can view passwords and other authentication keys in the configuration and can modify them in configuration mode. C-Web interface—Can view passwords and other authentication keys in the configuration and can modify them by accessing **Configure>System>Login**.
security	SRC CLI—Can view security configuration in configuration mode and with the **show configuration** operational mode command. C-Web interface—Can view security configuration by accessing **Monitor>Security>Certificate**.
security-control	SRC CLI—Can view and configure security information at the **[edit security]** hierarchy level. C-Web interface—Can view security information and configure security information by accessing **Manage>Request>Security**.
service	SRC CLI and C-Web interface—Can view service and policy definitions. C-Web interface—Can view service definitions by accessing **Monitor>SAE>Services** and policy definitions by accessing **Monitor>SAE>Policies**.
service-control	SRC CLI—Can view and modify service and policy definitions. C-Web interface—Can view and modify service and policy definitions by accessing **Configure>Services** and **Configure>Policies**.
shell	SRC CLI and C-Web interface—Can start a local shell by entering the **start shell** command.
snmp	SRC CLI—Can view Simple Network Management Protocol (SNMP) configuration information in configuration and operational modes. C-Web interface—Can view Simple Network Management Protocol (SNMP) configuration information by accessing **Monitor>SAE>Statistics**.
snmp-control	SRC CLI—Can view SNMP configuration information and configure SNMP (at the **[edit snmp**] hierarchy level). C-Web interface—Can view SNMP configuration information and configure SNMP by accessing **Configure>SNMP**.
subscriber	SRC CLI—Can view information about subscriber definitions. C-Web interface—Can view information about subscriber definitions by accessing **Monitor>SAE>Subscribers**.

Table 5: Login Class Permission Options (continued)

Permission	Description
subscriber-control	SRC CLI—Can view and control information about subscriber definitions. C-Web interface—Can view information about subscriber definitions and control information about subscriber definitions by accessing **Configure>Subscribers**.
system	SRC CLI—Can view system-level information in configuration and operational modes. C-Web interface—Can view system-level configuration information by accessing **Monitor>System**.
system-control	SRC CLI—Can view system-level configuration information and configure it at the **[edit system]** hierarchy level. C-Web interface—Can view system-level configuration and configure it by accessing **Configure>System**.
view	SRC CLI—Can use various commands to display current systemwide, routing table, and protocol-specific values and statistics. C-Web interface—Can access various **Monitor** subtasks to display current systemwide, routing table, and protocol-specific values and statistics.
view-configuration	SRC CLI and C-Web interface—Can view all system configurations, excluding any secret configuration.

To review the default system login classes, see "Predefined Login Classes for the SRC Software" on page 12.

Related Documentation

- Login Classes for SRC User Accounts on page 8
- SRC User Accounts Overview on page 7
- Access to Individual Commands and Configuration Statements (SRC CLI) on page 13
- Configuring a Login Class (SRC CLI) on page 24

Predefined Login Classes for the SRC Software

Table 6 on page 12 lists the system login classes predefined in the SRC software.

Table 6: Default System Login Classes

Login Class	Permission Options Set
operator	**clear**, **network**, **reset**, **view**
read-only	**view**

Table 6: Default System Login Classes (continued)

Login Class	Permission Options Set
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 8
- SRC User Accounts Overview on page 7
- Login Class Permission Options for the SRC Software on page 9
- Configuring a System Login Announcement (SRC CLI) on page 34
- Changing the root Password for the SRC Software (SRC CLI) on page 32

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 7 on page 14 lists common regular expression operators.

Table 7: Common Regular Expression Operators to Allow or Deny Operational Mode and Configuration Mode Commands

Operator	Match
Operation Mode and Configuration Mode	
|	One of the two terms on either side of the pipe.
^	Character at the beginning of an expression. Used to denote where the command begins, where there might be some ambiguity.
$	Character at the end of a command. Used to denote a command that must be matched exactly up to that point. For example, **allow-commands "show interfaces$"** means that the user can issue the **show interfaces** command but cannot issue **show interfaces detail** or **show interfaces extensive**.
[ ]	Range of letters or digits. To separate the start and end of a range, use a hyphen (-).
( )	A group of commands, indicating an expression to be evaluated; the result is then evaluated as part of the overall expression.
Configuration Mode Only	
*	0 or more terms.
+	One or more terms.
. (dot)	Any character except for a space.

Guidelines for Using Regular Expressions

Keep in mind the following considerations when using regular expressions to specify which statements or commands to allow or deny:

- Regular expressions are not case-sensitive.
- If a regular expression contains a syntax error, authentication fails and the user cannot log in.
- If a regular expression does not contain any operators, all varieties of the command are allowed.

Follow these guidelines when using regular expressions:

- Enclose the following in quotation marks:

- A command name or regular expression that contains:
  - Spaces
  - Operators
  - Wildcard characters
- An extended regular expression that connects two or more terms with the pipe (|) symbol. For example:

```
[edit system login class class-name ]
user@host# set deny-configuration "(system login class) | (system services)"
```

- Do not use spaces between regular expressions separated with parentheses and connected with the pipe (|) symbol.
- Specify the full paths in the extended regular expressions with the **allow-configuration** and **deny-configuration** options.

NOTE: You cannot define access to keywords such as set or edit.

Timeout Value for Idle Login Sessions

An idle login session is one in which the CLI operational mode prompt is displayed but there is no input from the keyboard. By default, a login session remains established until a user logs out of the system, even if that session is idle. To close idle sessions automatically, you configure a time limit for each login class. If a session established by a user in that class remains idle for the configured time limit, the session automatically closes.

For users who belong to a login class for which an idle timeout is configured, the CLI displays messages similar to the following when an idle user session times out.

```
user@host# Session will be closed in 5 minutes if there is no activity.
Warning: session will be closed in 1 minute if there is no activity
Warning: session will be closed in 10 seconds if there is no activity
Idle timeout exceeded: closing session
```

If you configure a timeout value, the session closes after the specified time has elapsed, except if the user is running commands such as **ssh**, **start shell**, or **telnet**.

The C-Web interface session closes after the specified time has elapsed with no message, and returns to the login window.

Related Documentation

- Login Classes for SRC User Accounts on page 8
- Login Class Permission Options for the SRC Software on page 9

- Predefined Login Classes for the SRC Software on page 12
- Configuring a Login Class (SRC CLI) on page 24

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 30
- Configuring User Accounts (C-Web Interface) on page 29
- Example: SRC User Accounts on page 54

CHAPTER 3

User Authentication

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.

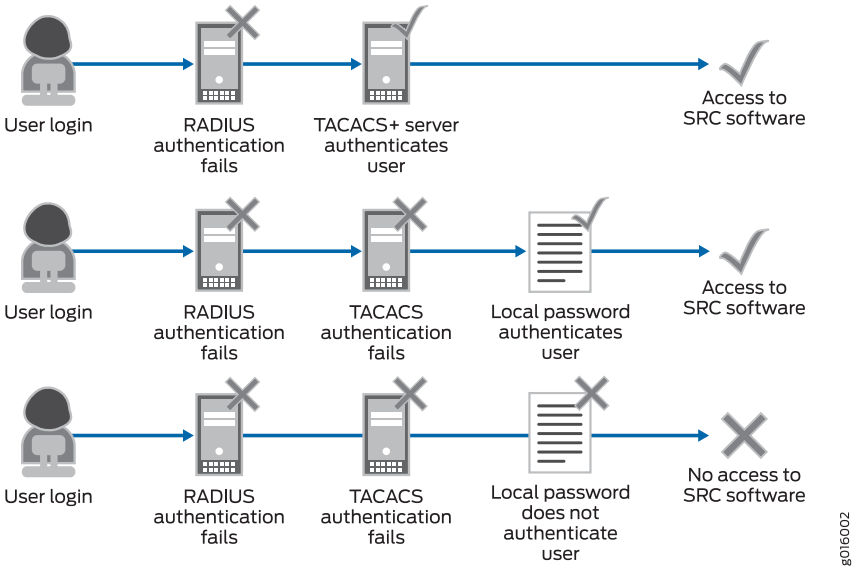
For each login attempt, the SRC software tries the authentication methods in the order configured, until the password matches. The SRC software fails to authenticate a user either because the authentication server (RADIUS or TACACS+ server) is unavailable or because the user entered wrong credentials (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 1 on page 18 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 1: Authentication Order: RADIUS, TACACS+, Local Password



Related Documentation

- Configuring RADIUS and TACACS+ Authentication on a C Series Controller (SRC CLI) on page 37
- Configuring RADIUS Authentication (SRC CLI) on page 39
- Configuring TACACS+ Authentication (C-Web Interface) on page 42

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 8 on page 18 describes the supported authentication/authorization attributes.

Table 8: 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

Table 8: Supported TACACS+ and RADIUS Authentication/Authorization Attributes (continued)

TACACS+ Authorization Attribute	RADIUS VSA	Description	Length	String
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
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 37
- Configuring RADIUS and TACACS+ Authentication on a C Series Controller (SRC CLI) on page 37
- A C Series Controller as a RADIUS Client and TACACS+ Client on page 17

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 42.
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.

PART 2

Configuration

CHAPTER 4

Configuration Tasks for User Access

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 12.

- 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 13.

Related Documentation

- Login Class Permission Options for the SRC Software on page 9
- *Viewing Information About the Users on the System (C-Web Interface)*

- Login Classes for SRC User Accounts on page 8

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 Telnet:

```
[edit system login class remote]
user@host# set deny-commands telnet
```

5. (Optional) Configure access to specified configuration mode commands that would otherwise be denied.

```
[edit system login class name ]
user@host# set allow-configuration allow-configuration
```

For example, the following statement specifies that the network-mgmt class can issue configuration mode commands at the **[routing-options]** hierarchy level:

```
[edit system login class network-mgmt]
user@host# set allow-configuration " routing options"
```

6. (Optional) Deny access to specified configuration mode commands that would otherwise be allowed.

```
[edit system login class name ]
user@host# set deny-configuration deny-configuration
```

For example, the following statement specifies that the network-mgmt class does not have access to the **[snmp address]** hierarchy level:

```
[edit system login class network-mgmt]
user@host# set deny-configuration " snmp address"
```

7. Specify the number of minutes that a session can be idle before it is automatically closed.


```
[edit system login class class-name]
user@host# set idle-timeout minutes
```

8. Display the results of the configuration.

```
[edit system login]
user@host# show
```

```
class network-mgmt {
 allow-commands "request system install";
  allow-configuration routing-options;
deny-configuration "snmp address";
}
class remote {
  deny-configuration "system services telnet";
  permissions all;
}
```

Related Documentation

- Configuring Login Classes (C-Web Interface) on page 26
- Configuring a System Login Announcement (SRC CLI) on page 34
- *Viewing Information About the Users on the System (C-Web Interface)*
- Configuring Authentication for SRC User Accounts (SRC CLI) on page 30
- Example: SRC User Accounts on page 54

Configuring Login Classes (C-Web Interface)

To configure a login class:

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

   The Login pane appears.

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

   The Class pane appears.

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

Related Documentation

- Configuring User Accounts (C-Web Interface) on page 29
- Configuring a System Login Announcement (C-Web Interface) on page 35
- Configuring a Login Class (SRC CLI) on page 24
- Login Classes for SRC User Accounts on page 8

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 5 on page 9.

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 16.

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;
}
```

Configuring User Accounts (C-Web Interface)

To configure a user account:

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

   The Login pane appears.

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

   The User pane appears.

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

Related Documentation

- Configuring Authentication for SRC User Accounts (C-Web Interface) on page 31
- Using Remote Template Accounts (C-Web Interface) on page 46
- *Viewing Information About the Users on the System (C-Web Interface)*
- SRC User Accounts Overview on page 7

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 30
- Configuring SSH Authentication on page 30

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)*
- SRC User Accounts Overview on page 7
- Configuring a Login Class (SRC CLI) on page 24
- Configuring User Accounts (SRC CLI) on page 27
- Types of Authentication for SRC User Accounts on page 16

Configuring SSH Authentication

Before you configure SSH authentication, obtain the contents of SSH key files. You can copy the contents of an SSH keys file into a CLI session:

1. On a management machine such as a PC or personal workstation, create an ssh-rsa key:

```
> ssh-keygen
(provide input)
> cat ~/.ssh/id_rsa.pub
```

2. On the C Series Controller enter the **set system login user testuser authentication ssh-authorized-key** command, and paste in the SSH key:

```
user@host# set system login user testuser authentication ssh-authorized-key " pasted
   content of id_rsa.pub "
```

For example:

```
user@host# set system login user testuser authentication ssh-authorized-key "ssh-rsa
   AAAAB3NzaC1yc2EAAAABIwAAAIEAvSqAWNdMTQJS9eqG1eq
RANI3ML4hH+u7WX/HP0W82gDSPpjghnt1e5de3D8U
   kuIIEUBf1obgy/7AKc98FqAIvVp5onCiMg8ELD6
RYkgOgo7U6zERB25qy3sK1Rn9NzrB20qLzbvAcZW1
   NIePmf1R99d/Rge7KB/5k6fq3NOG0fc= id@server" "ssh-rsa AAAA
   B3NzaC1yc2EAAAABIwAAAIEAxlwe9HfZ78vbdfq1+AY0uCF79yGPxgGuw
GZd9QVdT+dniwGh/4HwLITvKd8SYrhmJsyhz5dWuZm
   94JSwQosm9BVhJwREt39NYIkLWOjGIMkk8Cxw4
TkpFfeIz1cSbeFxtFBFVaBbo4YkEv5ItbuxwvbTWURkvsQa
   2VJXAqIs7z8= id2@server2
eriand" "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAwwOo
   UD4m+SazgzF2kRIq5Y2+Ix2zQbCxqBS
D1rmW92eLPOQIBv/sEy2d8UNeHpoKot9Px8q9ABriOyO
   Nc7vqNsSVnAMyicQB786uHoabSErVIYscapT
YvIGg+olbdhKySbSxOoXMehhgoQS0JZxHCbxsQJip7/7vJ
   PCjRGU8Xq0= id@server3" ];
```

See Also

- Configuration Statements for SRC User Accounts on page 59
- SRC User Accounts Overview on page 7
- Configuring User Accounts (SRC CLI) on page 27
- Types of Authentication for SRC User Accounts on page 16

Related Documentation

- Example: SRC User Accounts on page 54
- *Configuring User Accounts for Web Applications (SRC CLI)*
- Configuring a Login Class (SRC CLI) on page 24
- Configuration Statements for SRC User Accounts on page 59
- SRC User Accounts Overview on page 7
- Configuring User Accounts (SRC CLI) on page 27
- Types of Authentication for SRC User Accounts on page 16

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

You can configure user accounts by using the following methods:

1. Configuring a Plain Text Password on page 31
2. Configuring SSH Authentication on page 32

Configuring a Plain Text Password

To configure a plain text password for a user account:

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

   The Login pane appears.

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

Configuring SSH Authentication

Before you configure SSH authentication, obtain the contents of SSH key files. You can copy the contents of an SSH keys file into a CLI session:

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

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

See Also

- Configuring Authentication for SRC User Accounts (SRC CLI) on page 30
- Configuring User Accounts (C-Web Interface) on page 29
- Configuring Authentication Order (C-Web Interface) on page 45
- Removing an Authentication Method from the Authentication Order (C-Web Interface) on page 45
- SRC User Accounts Overview on page 7

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 34
- Predefined Login Classes for the SRC Software on page 12

- Login Class Permission Options for the SRC Software on page 9

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 32

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) on page 35
- Before You Configure Login Classes on page 23
- Configuring a Login Class (SRC CLI) on page 24
- Changing the root Password for the SRC Software (SRC CLI) on page 32

Configuring a System Login Announcement (C-Web Interface)

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

To configure a system login announcement:

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

   The Login pane appears.

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

Related Documentation

- Configuring a System Login Announcement (SRC CLI) on page 34
- Configuring Login Classes (C-Web Interface) on page 26
- SRC User Accounts Overview on page 7

CHAPTER 5

Configuration Tasks for User Authentication

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 39.

   See "Configuring TACACS+ Authentication (SRC CLI)" on page 41.

   See "Configuring TACACS+ Authentication (C-Web Interface)" on page 42.

2. Configure the authentication order.

   See "Configuring More Than One Authentication Method (SRC CLI)" on page 42.

3. Configure template accounts.

   See "SRC Template Accounts for RADIUS and TACACS+ Authentication Overview" on page 19.

4. (Optional) Configure individual user profiles.

   See "SRC User Accounts Overview" on page 7.

Related Documentation

- Configuring RADIUS and TACACS+ Authentication on a C Series Controller (C-Web Interface) on page 38
- Configuring TACACS+ Authentication (C-Web Interface) on page 42
- Removing an SRC Authentication Method from the Authentication Order (SRC CLI) on page 45
- Example: Configuring SRC Authentication on page 56

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

The SRC software always performs password authentication on a C Series Controller. You can configure RADIUS and/ or TACACS+ authentication to complement password authentication. In this case, the software performs RADIUS and/or TACACS+ authentication before password authentication.

To configure RADIUS and TACACS+ authentication for users who access a C Series Controller:

1. Configure the connection to the RADIUS or TACACS+ server.

   See "Configuring RADIUS Authentication (C-Web Interface)" on page 40.

   See "Configuring TACACS+ Authentication (C-Web Interface)" on page 42.

2. Configure the authentication order.

3. Configure template accounts.

   See "Using Remote Template Accounts (C-Web Interface)" on page 46 and "Configuring a Local SRC User Template (C-Web Interface)" on page 47.

4. (Optional) Configure individual user profiles.

   See "SRC User Accounts Overview" on page 7.

Related Documentation

- Configuring RADIUS and TACACS+ Authentication on a C Series Controller (SRC CLI) on page 37
- Configuring Authentication Order (C-Web Interface) on page 45
- Removing an Authentication Method from the Authentication Order (C-Web Interface) on page 45

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) on page 40
- Configuring RADIUS and TACACS+ Authentication on a C Series Controller (SRC CLI) on page 37
- Removing an SRC Authentication Method from the Authentication Order (SRC CLI) on page 45
- Example: Configuring SRC Authentication on page 56
- A C Series Controller as a RADIUS Client and TACACS+ Client on page 17

Configuring RADIUS Authentication (C-Web Interface)

To configure information about RADIUS servers for authentication:

1. Click **Configure>System.**

   The System pane appears.

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

   The RADIUS Server pane appears.

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

To configure a set of users that share a single account for authorization purposes, you create a template user.

Related Documentation

- Configuring RADIUS Authentication (SRC CLI) on page 39
- Configuring RADIUS and TACACS+ Authentication on a C Series Controller (C-Web Interface) on page 38
- Configuring Authentication Order (C-Web Interface) on page 45

- Removing an Authentication Method from the Authentication Order (C-Web Interface) on page 45

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 19.

Related Documentation

- Configuring TACACS+ Authentication (C-Web Interface) on page 42
- Configuring RADIUS and TACACS+ Authentication on a C Series Controller (SRC CLI) on page 37
- A C Series Controller as a RADIUS Client and TACACS+ Client on page 17
- Removing an SRC Authentication Method from the Authentication Order (SRC CLI) on page 45
- Example: Configuring SRC Authentication on page 56

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 37
- A C Series Controller as a RADIUS Client and TACACS+ Client on page 17
- Removing an SRC Authentication Method from the Authentication Order (SRC CLI) on page 45
- Example: Configuring SRC Authentication on page 56
- Configuring RADIUS Authentication (C-Web Interface) on page 40
- Configuring Authentication Order (C-Web Interface) on page 45

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 42
2. Configuring TACACS+ or RADIUS Authentication on page 43
3. Configuring TACACS+ and RADIUS Authentication on page 44

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 16
- Removing an SRC Authentication Method from the Authentication Order (SRC CLI) on page 45
- A C Series Controller as a RADIUS Client and TACACS+ Client on page 17
- Configuring RADIUS Authentication (SRC CLI) on page 39
- Example: Configuring SRC Authentication on page 56

Configuring Authentication Order (C-Web Interface)

To configure the order in which to use authentication servers:

1. Click **Configure>System**.

   The System pane appears.

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

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

Related Documentation

- Configuring More Than One Authentication Method (SRC CLI) on page 42
- Configuring More Than One Authentication Method (SRC CLI) on page 42
- Removing an Authentication Method from the Authentication Order (C-Web Interface) on page 45

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 16
- Configuring Authentication for SRC User Accounts (SRC CLI) on page 30
- Example: Configuring SRC Authentication on page 56

Removing an Authentication Method from the Authentication Order (C-Web Interface)

To delete an authentication method from the authentication order:

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

Related Documentation

- Removing an SRC Authentication Method from the Authentication Order (SRC CLI) on page 45
- Configuring Authentication Order (C-Web Interface) on page 45

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.

Related Documentation

- Using Remote Template Accounts (C-Web Interface) on page 46
- Configuring a Local SRC User Template (SRC CLI) on page 47

Using Remote Template Accounts (C-Web Interface)

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

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

   The Login pane appears.

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

The User pane appears.

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

Related Documentation

- Configuring a Local SRC User Template (C-Web Interface) on page 47

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 ;
}
```

Related Documentation

- Configuring a Local SRC User Template (C-Web Interface) on page 47
- Using Remote Template Accounts (SRC CLI) on page 46

Configuring a Local SRC User Template (C-Web Interface)

To configure a local user template and specify the privileges that you want to grant to the local users to whom the template applies:

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

   The Login pane appears.

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

   The User pane appears.

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

Related Documentation

- Using Remote Template Accounts (C-Web Interface) on page 46

CHAPTER 6

Configuration Tasks for TACACS+ Accounting

Configuring TACACS+ System Accounting (SRC CLI)

You can use TACACS+ sysetm 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 49
2. Configuring TACACS+ Server Accounting (SRC CLI) on page 50

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 9 on page 50.

Table 9: 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”)
		cmd_arg (for instance: “sae subscribers brief”)

See Also
- Configuring TACACS+ Server Accounting (SRC CLI) on page 50

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 42
- Configuring TACACS+ Authentication (SRC CLI) on page 41

CHAPTER 7

Examples

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 7
- Login Class Permission Options for the SRC Software on page 9
- Configuring a Login Class (SRC CLI) on page 24

Examples: Defining Access Privileges for SRC Configuration Mode Commands

The following example does not allow access the C Series Controller through a Telnet session for the login class remote that has permission set to **all**:

```
[edit system login class remote]
user@host# set permissions all
user@host# set deny-configuration "system services telnet"
```

The following example does not allow access to any login class whose name begins with " m" for the login class local that has permission set to **all**:

```
[edit system login class local]
user@host# set permissions all
user@host# set deny-configuration "system login class m.*"
```

The following example does not allow access to configuration mode commands at the [**system login class**] or [**system services hierarchy**] levels for the login class config-admin that has permission set to **all**:

```
[edit system login class config-admin]
user@host# set permissions all
user@host# set deny-configuration "(system login class) | (system services)"
```

Related Documentation

- Configuring a Login Class (SRC CLI) on page 24
- SRC User Accounts Overview on page 7
- Login Class Permission Options for the SRC Software on page 9

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
    IEAvSqAWNdMTQJS9eqG1eq
RANI3ML4hH+u7WX/HP0W82gDSPpjghnt1e5de3D8UkuIIEUB
    f1obgy/7AKc98FqAIvVp5onCiMg8ELD6
RYkgOgo7U6zERB25qy3sK1Rn9NzrB20qLzbvAcZW1NIePmf
    1R99d/Rge7KB/5k6fq3NOG0fc= id@server" "ssh-rsa AAAAB3NzaC1yc2EA
    AAABIwAAAIEAxlwe9HfZ78vbdfq1+AY0uCF79yGPxgGuw
GZd9QVdT+dniwGh/4HwLITvKd8SYrhmJsyhz5dWuZm94JSwQ
    osm9BVhJwREt39NYIkLWOjGIMkk8Cxw4
TkpFfeIz1cSbeFxtFBFVaBbo4YkEv5ItbuxwvbTWURkvsQa2VJXA
    qIs7z8= id2@server2
eriand" "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAwwOoUD4
    m+SazgzF2kRIq5Y2+Ix2zQbCxqBS
D1rmW92eLPOQIBv/sEy2d8UNeHpoKot9Px8q9ABriOyONc7v
    qNsSVnAMyicQB786uHoabSErVIYscapT
YvIGg+olbdhKySbSxOoXMehhgoQS0JZxHCbxsQJip7/7vJPCjRG
    U8Xq0= id@server3" ];
user alexander {
    full-name " Alexander the Great" ;
    uid 1002;
class view;
    authentication {
    }
ssh-authorized-keys [ "ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAvSqAWNdMTQJS9eqG1eq
RANI3ML4hH+u7WX/HP0W82gDSPpjghnt1e5de3D8UkuIIEUBf1obgy
/7AKc98FqAIvVp5onCiMg8ELD6
RYkgOgo7U6zERB25qy3sK1Rn9NzrB20qLzbvAcZW1NIePmf1R99d
/Rge7KB/5k6fq3NOG0fc= id@server" "ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxlwe9HfZ78vbdfq1+AY0uCF79y
GPxgGuw
GZd9QVdT+dniwGh/4HwLITvKd8SYrhmJsyhz5dWuZm94JSwQosm9
BVhJwREt39NYIkLWOjGIMkk8Cxw4
TkpFfeIz1cSbeFxtFBFVaBbo4YkEv5ItbuxwvbTWURkvsQa2VJXA
qIs7z8= id2@server2
eriand" "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAwwOoUD4m+Sazgz
F2kRIq5Y2+Ix2zQbCxqBS
D1rmW92eLPOQIBv/sEy2d8UNeHpoKot9Px8q9ABriOyONc7vqNsS
VnAMyicQB786uHoabSErVIYscapT
YvIGg+olbdhKySbSxOoXMehhgoQS0JZxHCbxsQJip7/7vJPCjRGU
8Xq0= id@server3" ];
user darius {
    full-name " Darius King of Persia" ;
    uid 1003;
    class operator;
    authentication {
        ssh " 1024 37 12341234@ecbatana.per" ;
    }
}
user remote {
```

```
    full-name “ All remote users” ;
    uid 9999;
    class read-only;
}
```

Related Documentation

- SRC User Accounts Overview on page 7
- Login Classes for SRC User Accounts on page 8
- Types of Authentication for SRC User Accounts on page 16
- Configuring Authentication for SRC User Accounts (SRC CLI) on page 30
- *Viewing Information About the Users on the System (C-Web Interface)*

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 16
- Configuring Authentication for SRC User Accounts (SRC CLI) on page 30
- Removing an SRC Authentication Method from the Authentication Order (SRC CLI) on page 45

CHAPTER 8

Configuration Statements and Commands

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 27
- Types of Authentication for SRC User Accounts on page 16
- Configuring Authentication for SRC User Accounts (SRC CLI) on page 30
- SRC User Accounts Overview on page 7
- Login Classes for SRC User Accounts on page 8
- Before You Configure Login Classes on page 23