Chapter 4

Configuring User Access with the C-Web Interface

This chapter contains information about how to configure user access to the SRC software and how to configure an announcement for users to see at login.

You can configure user access to the SRC software using the SRC CLI. See *SRC-PE Getting Started Guide, Chapter 24, Configuring User Access with the SRC CLI*.

Topics in this chapter include:

Overview of User Accounts

All users who can log in to the SRC software must be a member of a login class. With login classes, you define the following:

- Access privileges that users have when they are logged in to the SRC software
- Commands and statements that users can and cannot specify
- How long a login session can be idle before it times out and the user is logged out

You can define any number of login classes. You then apply one login class to an individual user account.

Login Classes for User Accounts with the C-Web Interface

The SRC software provides four predefined login classes to use for configuring user accounts. You can also configure login classes to precisely define access privileges for the user accounts in your SRC environment.

Access Privilege Level

In the SRC CLI, each top-level command-line interface (CLI) command and each configuration statement have an access privilege level associated with them. Similarly, each task and subtask in the C-Web interface have an access privilege level associated with them. Users can configure and view only those tasks for which they have access privileges. The access privileges for each login class are defined by one or more *permission options*.

Permission options specify which actions are allowed for users assigned to use a login class. More than one permission option can be configured for a login class. Table 2 lists the permission options available when you configure permissions with the SRC CLI and the C-Web interface.

You can use the SRC CLI or the C-Web interface to configure permission options for all commands, statements, tasks, and subtasks. For example, if you configure a user to have the system permission class using the C-Web interface, that user will have the same permission when accessing the SRC CLI.

The SRC software also provides a default set of system login classes that have permissions preset. Table 3 on page 29 lists the default system login classes.

Table 2: 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 **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).

Table 2: Login Class Permission Options (continued)

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

Table 2: Login Class Permission Options (continued)

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

Table 2: Login Class Permission Options (continued)

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

When you configure more than one permission with the SRC CLI or the C-Web interface, the resulting set of permissions is a combination of all of the permissions set. This does not apply when you include all and control with the SRC CLI.

When you configure permissions with the SRC CLI, 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.

When you configure permissions with the C-Web interface, click **Monitor** to display information and **Configure** to configure.

Predefined Login Classes

Table 3 lists the system login classes predefined in the SRC software.

Table 3: Default System Login Classes

Login Class	Permission Options Set
operator	clear, network, reset, view
read-only	view
super-user	all
unauthorized	None

NOTE: You cannot modify a predefined login class name. If you issue the set command on a predefined class name with the SRC CLI, the software will append -local to the login class name. The following message also appears:

```
warning: '<class-name>' is a predefined class name; changing to '<class-name>-local'
```

NOTE: You cannot issue the rename or copy command on a predefined login class with the SRC CLI. Doing so results in the following error message:

```
error: target '<classname>' is a predefined class
```

Access to Individual Commands and Configuration Statements with the C-Web Interface

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 Tasks

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.

In the C-Web interface, you specify these regular expressions for the following options in the Class pane (by clicking the user class in **Configure > System > Login**).

- Allow Commands
- Deny Commands
- Allow Configuration
- Deny Configuration

Command regular expressions implement the extended (modern) regular expressions as defined in POSIX 1003.2. Table 4 lists common regular expression operators.

Table 4: 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
  - In the C-Web interface, an extended regular expression that connects two or more terms with the pipe (|) symbol. For example, you could enter the following in the Deny Configuration box:

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

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

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

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

Configuring Login Classes with the C-Web Interface

Before you configure a login class:

- Review the predefined login classes to determine whether you can use one of these classes rather than creating a new one.

  See *Predefined Login Classes* on page 29.

- Make sure you are familiar with how to use regular expressions to specify which commands and configuration statements to allow or deny.

  Consider that you can issue one **allow** statement and one **deny** statement for operation mode commands, and one **allow** statement and one **deny** statement for configuration mode commands. Use regular expressions in a statement to specify more than one command in a statement.

  See *Regular Expressions for Allow and Deny Tasks* on page 30.

Configuring a Login Class

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**.

Configuring User Accounts with the C-Web Interface

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*.

Configuring a User Account

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**.

Configuring Authentication for User Accounts

You can configure the following types of authentication for user accounts:

- Plain text password—Prompt for a plain text (unencrypted) password. The requirements for plain text passwords are:
  - Can contain between 6 and 128 characters
  - Can include most character classes in a password (uppercase letters, lowercase letters, numbers, punctuation marks, and other special characters).

NOTE: We do not recommend that the password include control characters. We do recommend that the password include at least one change of case or character class.

If you configure a plain text password, you are prompted to enter and confirm the password.

- Encrypted password—Password encoded with crypt. The format of encrypted passwords is "{crypt}<13-characters in a-zA-Z0-9./>".

NOTE: We recommend that you *do not* enter the password in encrypted format.

- SSH—SSH authentication. For SSH authentication, you can copy the contents of an SSH keys file into a CLI session.

Configuring a Plain Text Password

To configure a plain text password for a user account:

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**.

Changing the root Password

You can change the root password only with the SRC CLI. For more information, see *SRC-PE Getting Started Guide, Chapter 24, Configuring User Access with the SRC CLI.*

Configuring a System Login Announcement with the 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**.