

Chapter 19

Configuring User Access

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. Topics include:

- Overview of User Accounts on page 161
- Login Classes for User Accounts on page 161
- Configuring Login Classes on page 167
- Configuring User Accounts on page 171
- Configuring a System Login Announcement on page 177

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 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

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

Each top-level command-line interface (CLI) command and each configuration statement has an access privilege level associated with it. Users can execute only those commands and configure and view only those statements 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 by users assigned to use a login class. More than one permission option can be configured for a login class. Table 12 lists the permission options available.

The privilege level for each command and statement is listed in *SRC-PE CLI Command Reference*.

The SRC software also provides a default set of system login classes that have permissions preset. Table 13 on page 164 lists the default system login classes.

Table 12: Login Class Permission Options

Permission	Description
admin	Can view user account information in configuration mode and with the show configuration command.
admin-control	Can view user accounts and configure them (at the [edit system login] hierarchy level).
all	Has all permissions.
clear	Can clear (delete) information learned from the network that is stored in various network databases (using the clear commands).
configure	Can enter configuration mode (using the configure command).
control	Can perform all control-level operations (all operations configured with the -control permission).
field	Reserved for field (debugging) support.
firewall	Can view the firewall filter configuration in configuration mode.
firewall-control	Can view and configure firewall filter information (at the [edit firewall] hierarchy level).
interface	Can view the interface configuration in configuration mode and with the show configuration operational mode command.
interface-control	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).
maintenance	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).
network	Can access the network by entering the SSH and telnet commands.
reset	Can restart software processes using the restart command, enable components using the enable command, and disable components using the disable command.
routing	Can view general routing, routing protocol, and routing policy configuration information in configuration and operational modes.

Table 12: Login Class Permission Options (continued)

Permission	Description
routing-control	Can view general routing, routing protocol, and routing policy configuration information and configure general routing (at the [edit routing-options] hierarchy level), routing protocols (at the [edit protocols] hierarchy level), and routing policy (at the [edit policy-options] hierarchy level).
secret	Can view passwords and other authentication keys in the configuration.
secret-control	Can view passwords and other authentication keys in the configuration and can modify them in configuration mode.
security	Can view security configuration in configuration mode and with the show configuration operational mode command.
security-control	Can view and configure security information (at the [edit security] hierarchy level).
service	Can view service and policy definitions.
service-control	Can view and modify service and policy definitions.
shell	Can start a local shell by entering the start shell command.
snmp	Can view Simple Network Management Protocol (SNMP) configuration information in configuration and operational modes.
snmp-control	Can view SNMP configuration information and configure SNMP (at the [edit snmp] hierarchy level).
subscriber	Can view information about subscriber definitions.
subscriber-control	Can view and control information about subscriber definitions.
system	Can view system-level information in configuration and operational modes.
system-control	Can view system-level configuration information and configure it (at the [edit system] hierarchy level).
view	Can use various commands to display current systemwide, routing table, and protocol-specific values and statistics.
view-configuration	Can view all system configuration, excluding any secret configuration.

When you configure more than one permission, the resulting set of permissions is a combination of all of the permissions set, except for **all** and **control**.

When you configure permissions, include **view** to display information and **configure** to enter configuration mode. Two forms for the permissions control the individual parts of the configuration:

- “Plain” form—Provides read-only capability for that permission type. An example is **interface**.
- Form that ends in **-control**—Provides read and write capability for that permission type. An example is **interface-control**.

Predefined Login Classes

Table 13 lists the system login classes predefined in the SRC software.

Table 13: Default System Login Classes

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



NOTE: You cannot modify a predefined login class name. If you issue the **set** command on a predefined class name, 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. Doing so results in the following error message:

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

Access to Individual Commands and Configuration Statements

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 8 lists common regular expression operators.

Table 14: Common Regular Expression Operators to Allow or Deny Operational Mode and Configuration Mode Commands

Operator	Match
Operation Mode and Configuration Mode	
	One of the two terms on either side of the pipe.
^	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, <code>allow-commands "show interfaces\$"</code> means that the user can issue the <code>show interfaces</code> command but cannot issue <code>show interfaces detail</code> or <code>show interfaces extensive</code> .
[]	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 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`.

Configuring 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* on page 164.

- 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 *Specifying Regular Expressions for Allow and Deny Statements* on page 65.

Configuration Statements for Login Classes

Use the following configuration statements to configure login classes at the [edit] hierarchy level:

```
system login class name {
  allow-commands allow-commands;
  allow-configuration allow-configuration;
  deny-commands deny-commands;
  deny-configuration deny-configuration;
  idle-timeout idle-timeout;
  permissions
  [(admin | admin-control | all | clear | configure | control | field | firewall |
  firewall-control | interface | interface-control | maintenance | network | reset |
  routing | routing-control | secret | secret-control security | security-control |
  shell | snmp | snmp-control | system | system-control | view | view-configuration
  | service | service-control | subscriber | subscriber-control)...];
}
```

Configuring a Login Class

To configure a login class:

1. From configuration mode, access the configuration statement that configures login classes, and assign a name to the login class.

```
[edit]
user@host# edit system login class name
```

2. Specify the permissions for the login class.

```
[edit system login class name]
user@host# set permissions permissions
```

For example, the following statement specifies that the user-account class can configure and view only user accounts:

```
[edit system login class user-accounts]
user@host# set permissions [configure admin admin-control]
```

The following statement specifies that the network-mgmt class can configure and view only SNMP parameters:

```
[edit system login class network-mgmt]
user@host# set permissions [configure snmp snmp-control]
```

3. (Optional) Configure access to specified operational mode commands that would otherwise be denied,

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

For example, the following statement specifies that the network-mgmt class can install system software:

```
[edit system login class network-mgmt]
user@host# set allow-commands "request system install"
```

4. (Optional) Deny access to specified operational mode commands that would otherwise be allowed.

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

For example, the following statement specifies that the remote class cannot connect to the SRC software through Telnet:

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


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

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

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

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

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

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

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

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

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

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

8. Display the results of the configuration.

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

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

Examples: Configuring Access Privileges for Operational Mode Commands

The following example allows access to the `request system reboot` command for the login class `operator-and-boot` that has operator privileges defined by the `clear`, `network`, `reset`, and `view` permissions.

```
[edit system login class operator-and-boot]
user@host# set permissions [ clear network reset view ]
user@host# set allow-commands "request system reboot"
```

The following example denies access to `set` commands for the login class `operator-no-set` that has operator privileges defined by the `clear`, `network`, `reset`, and `view` permissions.

```
[edit system login class operator-no-set]
user@host# set permissions [ clear network reset view ]
user@host# set deny-commands "set"
```

The following example allows software installation but denies access to the `show nic` command for the login class `operator-no-set` that has operator privileges defined by the `clear`, `network`, `reset`, and `view` permissions.

```
[edit system login class operator-and-install-no-nic]
user@host# set permissions [ clear network reset view ]
user@host# set allow-commands "request system install"
user@host# set deny-commands "show nic"
```

Examples: Defining Access Privileges for Configuration Mode Commands

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

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

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

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

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

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

Configuring User Accounts

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 platform, which is created the first time that the user logs in. Home directories that have the same name as the user ID are created in the */var/home* directory; for example, the home directory for a user with the user ID Chris_Bee is */var/home/Chris_Bee*.

Configuration Statements for User Accounts

Use the following configuration statements to configure user accounts at the [edit] hierarchy level.

```
system login user user-name {
  class class;
  full-name full-name;
  uid uid;
  prompt prompt;
  level (basic | normal | advanced | expert);
  complete-on-space (on | off);
}
```

```

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

```

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

Configuring a User Account

To configure a user account:

1. From configuration mode, access the configuration statement that configures a user account, and specify a username that identifies the user.

```

[edit]
user@host# edit system login user user-name

```

The username must be unique within the system. Do not include spaces, colons, or commas in the username. For example:

```

[edit]
user@host# edit system login user JASmith

```

```

[edit system login user JASmith]
user@host#

```

2. Specify the name of the login class that defines the user's access privilege. [edit system login user *user-name*]

```

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

```

The login class is one of the login classes that you defined in the **class** statement at the [edit system login] hierarchy level, or one of the default classes listed in Table 7 on page 64.

3. Specify the user's full name.

```

[edit system login user user-name]
user@host# set full-name full-name

```

If the full name contains spaces, enclose it in quotation marks. Do not include colons or commas. For example:

```

[edit system login user JASmith]
user@host# set full-name "John A. Smith"

```

4. (Optional) Specify a user identifier (UID) for the user.

```
[edit system login user user-name]
user@host# set uid uid
```

The identifier must be a number in the range 0 through 64,000 and must be unique within the system. If you do not assign a UID to a username, the software assigns one when you commit the configuration, preferring the lowest available number.

You must ensure that the UID is unique. However, it is possible to assign the same UID to different users.

5. (Optional) Specify a prompt that the user sees at the SRC CLI.

```
[edit system login user user-name]
user@host# set prompt prompt
```

6. (Optional) Specify the editing level available to the user. The level determines which configuration commands are visible to the user.

```
[edit system login user user-name]
user@host# set level (basic | normal | advanced | expert)
```

where:

- **basic**—Minimal set of configuration statements and commands— only the statements that must be configured are visible.
- **normal**—Normal set of configuration statements and commands— the common and basic statements are visible.
- **advanced**—All configuration statements and commands, including the common and basic ones, are visible.
- **expert**—All configuration statements, including common, basic, and internal statements and commands used for debugging, are visible.

7. (Optional) Specify whether entering a space completes a command.

```
[edit system login user user-name]
user@host# set complete-on-space (on | off)
```

If you do not enter a value, **complete-on-space** is enabled by default.

8. Define the authentication methods that a user can use to log in to a C-series platform.

See *Configuring Authentication for User Accounts* on page 174.

9. Display the results of the configuration.

```
[edit system login]
user@host# show
. . .
user JASmith {
  class network-mgmt;
  full-name "John A. Smith";
  uid 507;
  gid 100;
  authentication {
    encrypted-password "{crypt}caZEWDaE1au0c";
  }
  level normal;
  complete-on-space on;
}
```

Configuring Authentication for User Accounts

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

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



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

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

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



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

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

Configuring a Plain Text Password

To configure a plain text password for a user account:

- At the [edit system user *user-name*] hierarchy, enter the `set authentication plain-text-password` command. For example:

```
[edit system user JASmith]
user@host# set authentication plain-text-password
New password: type password here
Retype new password: retype password here
```

Configuring SSH Authentication

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

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

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

2. On the C-series platform enter the `set system login user testuser authentication ssh-authorized-key` command, and paste in the SSH key:

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

For example:

```
user@host# set system login user testuser authentication
ssh-authorized-key "ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAvSqAWNMTQJS9eqG1eq
RANI3ML4hH+u7WX/HP0W82gDSPpjhnt1e5de3D8UkuIIeUBf1obgy/7AK
c98FqAlvVp5onCiMg8ELD6
RYkgOgo7U6zERB25qy3sK1Rn9NzrB20qLzbvAcZW1NlePmf1R99d/Rge7k
B/5k6fq3NOG0fc= id@server" "ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxlwe9HfZ78vdbfq1+AYOuCF79yGPxGu
w
GZd9QVdT+dnwGh/4HwLITvKd8SYrhMJsyz5dWuZm94JSwQosm9BVhJw
REt39NYIkLWOjGIMkk8Cw4
TkpFfelz1cSbeFxtFBFVaBbo4YkEv5ltbuxwvbTWURkvsQa2VJXAqls7z8=
id2@server2
erian" "ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAwOUD4m+SazgzF2kRlq5Y2+lx2zQb
CxqBS
D1rmW92eLPOQIBv/sEy2d8UNeHpoKot9Px8q9ABriOyONc7vqNsSVnAMyi
cQB786uHoabSErVIYscapT
YvIGg+olbdhKySbSxOoXMehhgoQS0JZxHCbxsQJip7/7vJPCjRGU8Xq0=
id@server3" ];
```

Changing the root Password

An account for the user `root` is always present in the configuration. Only the `root` user can change the root password.

To change the `root` password:

1. Log into the SRC software as `root`.
2. From operational mode, change the `root` password.

```
root@host> set cli password
Changing password for user root.
New UNIX password:
```

You can also create a regular account for `root` and set the SSH key there. The class for `root` is always `super-user`—if you create an account for `root`, the class is ignored.

Example: User Accounts

The following example shows the configuration for user accounts for three system users and the template user “remote.” All users use one of the default system login classes.

```
system login user philip {
  class super-user;
  full-name "Philip of Macedonia";
  uid 1001;
  authentication {
    encrypted-password "{crypt}6YPqJe88Wz5fQ";
    ssh-authorized-keys [ "ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAvSqAWNMTQJS9eqG1eq
RANI3ML4hH+u7WX/HP0W82gDSPpjghnt1e5de3D8UkulIEUBf1obgy/7AK
c98FqAlvVp5onCiMg8ELD6
RYkgOgo7U6zERB25qy3sK1Rn9NzrB20qLzbvAcZW1NiePmf1R99d/Rge7k
B/5k6fq3NOG0fc= id@server" "ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxIwe9HfZ78vdbfq1+AY0uCF79yGPxgGu
w
GZd9QVdT+dniwGh/4HwLITvKd8SYrhmJsyhz5dWuZm94JSwQosm9BVhJw
REt39NYIkLW0jGIMkk8Cw4
TkpFfelz1cSbeFxtFBFVaBbo4YkEv5ltbuxwvbTWURkvsQa2VJXAqIs7z8=
id2@server2
eriand" "ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAwW0oUD4m+SazgzF2kRlq5Y2+lx2zQb
CxqBS
D1rmW92eLPOQIBv/sEy2d8UNeHpoKot9Px8q9ABriOyONc7vqNsSVnAMyi
cQB786uHoabSErVIYscapT
YvIGg+olbdhKySbSxOoXMehhgoQS0JZxHCbxsQJip7/7vJPCjRGU8Xq0=
id@server3" ];
  }
}
user alexander {
  full-name "Alexander the Great";
  uid 1002;
  class view;
  authentication {
    encrypted-password "{crypt}6ZSqJe75Tz5fN";
    ssh-authorized-keys [ "ssh-rsa
```



```

AAAAB3NzaC1yc2EAAAABlWAAAIEAvSqAWNMTQJS9eqG1eq
RANI3ML4hH+u7WX/HP0W82gDSPpjghnt1e5de3D8UkullEUBf1obgy
/7AKc98FqAlvVp5onCiMg8ELD6
RYkgOgo7U6zERB25qy3sK1Rn9NzrB20qLzbvAcZW1NlePmf1R99d
/Rge7kB/5k6fq3NOG0fc= id@server" "ssh-rsa
AAAAB3NzaC1yc2EAAAABlWAAAIEAxIwe9HfZ78vdbfq1+AY0uCF79y
GPxgGuw
GZd9QVdT+dniwGh/4HwLITvKd8SYrhMJsyhz5dWuZm94JSwQosm9
BVhJwREt39NYIkLW0jGIMkk8Cw4
TkPffelz1cSbeFxtFBFVaBbo4YkEv5ItbuxwvbTWURkvsQa2VJXA
qls7z8= id2@server2
erian" "ssh-rsa AAAAB3NzaC1yc2EAAAABlWAAAIEAwW0oUD4m+Sazgz
F2kRIq5Y2+lx2zQbCxqBS
D1rmW92eLPOQIBv/sEy2d8UNeHpoKot9Px8q9ABri0yONc7vqNsS
VnAMyicQB786uHoabSERVIYscapT
YvIGg+olbdhKySbSx0oXMehhgoQSOJZxHCbxsQJip7/7vJPCjRGU
8Xq0= id@server3" ];
}
}
user darius {
    full-name "Darius King of Persia";
    uid 1003;
    class operator;
    authentication {
        ssh "1024 37 12341234@ecbatana.per";
    }
}
user remote {
    full-name "All remote users";
    uid 9999;
    class read-only;
}
}

```

Configuring a System Login Announcement

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.

