Chapter 5

Authenticating Users on a C-series Controller with the C-Web Interface

This chapter describes how to configure RADIUS and TACACS+ authentication for users who access a C-series Controller with the C-Web interface.

You can also use the SRC CLI to configure RADIUS and TACACS+ authentication. See *SRC-PE Getting Started Guide, Chapter 25, Authenticating Users on a C-series Controller with the SRC CLI*.

Topics in this chapter include:

- Configuring RADIUS and TACACS+ Authentication on a C-series Controller with the C-Web Interface on page 37
- Configuring RADIUS Authentication with the C-Web Interface on page 38
- Configuring TACACS+ Authentication with the C-Web Interface on page 38
- *Configuring More Than One Authentication Method with the C-Web Interface* on page 39
- Configuring Template Accounts for RADIUS and TACACS+ Authentication with the C-Web Interface on page 40

Configuring RADIUS and TACACS+ Authentication on a C-series Controller with the 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 with the C-Web Interface* on page 38.

   See *Configuring TACACS+ Authentication with the C-Web Interface* on page 38.

2. Configure the authentication order.

   See *Configuring More Than One Authentication Method with the C-Web Interface* on page 39.

3. Configure template accounts.

   See *Configuring Template Accounts for RADIUS and TACACS+ Authentication with the C-Web Interface* on page 40.

4. (Optional) Configure individual user profiles.

   See *Chapter 3, Configuring User Access with the C-Web Interface*.

Configuring RADIUS Authentication with the 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. See *Configuring Template Accounts for RADIUS and TACACS+ Authentication with the C-Web Interface* on page 40.

Configuring TACACS+ Authentication with the 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. See *Configuring Template Accounts for RADIUS and TACACS+ Authentication with the C-Web Interface* on page 40.

Configuring More Than One Authentication Method with the C-Web Interface

On a C-series Controller, you can use more than one authentication method. You can configure the C-series Controller to be a RADIUS and TACACS+ client by:

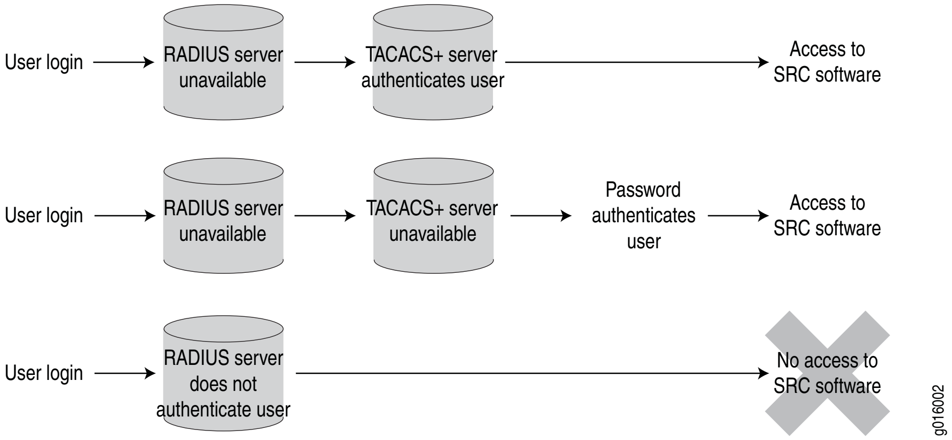
- Configuring RADIUS and TACACS+ authentication.
- Configuring the authentication order to prioritize the order in which the C-series Controller uses configured authentication methods.

For each login attempt, the SRC software tries the authentication methods in the order configured, until the password matches. If one of the authentication methods in the authentication order fails to authenticate a user, the user is denied access to the C-series Controller.

If password authentication does not appear in the prioritized list of authentication methods, the SRC software uses password authentication last. The SRC software always uses password authentication, whether or not it appears in the list of authentication methods to be used. As a result, users can log in to the C-series Controller through password authentication if configured authentication servers are unavailable.

Figure 1 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 an active server.

Figure 1: Authentication Order: RADIUS, TACACS+, Password


User login
RADIUS server unavailable
TACACS+ server authenticates user
Access to SRC software
User login
RADIUS server unavailable
TACACS+ server unavailable
Password authenticates user
Access to SRC software
User login
RADIUS server does not authenticate user
No access to SRC software
g016002

Configuring Authentication Order

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.

Removing an Authentication Method from the Authentication Order

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.

Configuring Template Accounts for RADIUS and TACACS+ Authentication with the C-Web Interface

When a user logs in to the CLI, the following authentication is performed:

- RADIUS and /or TACSACS+ server authentication
- Authentication through a user account configured under [system login user]

For authorization purposes, you can use a template account to create a single account that can be shared by a set of users at the same time.

Typically when you use RADIUS and/or TACACS+ authentication, the user account is shared among a group of users who have the same privileges. You create template accounts for sets of users. Template accounts can be named:

- remote—(Default) A single account that defines user permissions for all users that authenticate through RADIUS or TACACS+
- *name-of-your-choice*—Account for a group of users

Use a named template account when you need different types of templates. Each template can define a different set of permissions appropriate to a group of users who use that template. For example, you can configure a set of remote users to concurrently share a single user ID.

When a user is part of a group that uses a template account, the command-line interface (CLI) username is the login name; however, the privileges, file ownership, and effective username are inherited from the template account.

Using Named Template Accounts

Template accounts for which you define a name are defined on a C-series Controller and are referenced by the TACACS+ and RADIUS authentication servers through usernames. All users who share a local user template account have the same access privileges.

When a user who accesses the C-series Controller through a name template account logs in:

1. The SRC software issues a request to the authentication server to authenticate the user's login name.
2. If a user is authenticated, the server returns the username to the SRC software.
3. The SRC software determines whether a username is specified for that login name.
4. If there is a username, the SRC software selects the appropriate template.
5. If a user template does not exist for the authenticated user, the C-series Controller uses the remote template.

Using Remote Template Accounts

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

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**.

Configuring a Local User Template

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

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**.