

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 Topics

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

Published: 2009-09-25