

About strong passwords

Strong passwords are passwords that are not easily guessed or broken. The use of strong passwords can help safeguard your system. This is important because data transmitted through the server may be of considerable value to your company or your client.

By default, the server is configured so that you must set a strong password when creating a user account. Your system administrator can change this setting to make strong passwords optional.

Guidelines for creating strong passwords

- Passwords should be at least 12 characters long.
- Passwords should contain a combination of different types of characters, and must contain at least one character from three of the following four groups:
 - Uppercase letters: A, B, C...Z
 - Lowercase letters: a, b, c...z
 - Numbers: 0, 1, 2...9
 - Special characters, such as punctuation or symbols: {, }, #, \$, %, and so on
- Passwords should not contain any part of the user's e-mail name, user account name, given names, or any other names by which the user is known.
- Passwords should not be everyday words. Avoid words from the dictionary, and avoid slang terms that are in common use.
- Passwords should be complex but relatively easy to remember. For example:

ihVsns(5]Ia1

(I have five sons in Alaska)

- Passwords should be kept private. If a password is shared or discovered, change it immediately.
- Passwords should be changed regularly (for example, every 90 days).