



Password Security

Home > [SMB Support Assistant Configuration Overview](#) > Password Security

Password Security

[Introduction](#)

[Requirements](#)

[Strong Passwords](#)

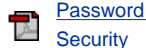
[Password-Generation Utilities](#)

[Password Audits](#)

[Username Policies](#)

[Related Information](#)

Download PDF



Service Requests

[Open a service request](#)

[Update a service request](#)

Feedback

Please rate this site:

++ + +/- - --

Suggestions for improvement:

If Cisco may contact you for more details or for future feedback opportunities, please enter your contact information:

Full Name:

Email:

Introduction

This document describes Cisco's recommendations for how to implement a strong password policy on Cisco devices that require a password.

[Back to Top](#)

Requirements

You do not need to provide any additional equipment to complete this procedure.

[Back to Top](#)

Strong Passwords

Password-based authentication systems that do not use strong passwords are vulnerable to dictionary attacks. A policy that requires users to select strong passwords is one of the most effective means to mitigate against potential dictionary attacks. A strong password policy should expire user passwords periodically, such as every three months. Give users advanced notice to change passwords before they expire.

Some characteristics of strong passwords include:

- A minimum of 10 characters
- A mixture of uppercase and lowercase letters
- At least one numeric character (0-9) or one non-alphanumeric character, such as !#\$%&
- No form of your username or user ID
- No domestic or foreign dictionary words
- Randomly generated passwords

Password-Generation Utilities

Password generation utilities are tools that help administrators and users generate strong passwords. These tools can be used by companies to enforce a password policy. In general, it is better if users select strong passwords with guidelines such as those described in this document. When users generate their own passwords, they are less likely to write the password down or document it anywhere but in their memory.

Password Audits

A strong password policy should periodically check for weak passwords. A common way to check for password weakness is to use a password-cracker utility. Password audits can be run regularly with these tools:

- [LC4](#) 
- [John the Ripper](#) 

Note: Cisco does not endorse these tools, but provides these links as examples of technology to enforce strong passwords.

Username Policies

In addition to a strong password policy, you should ensure that usernames do not create security vulnerabilities.

- All users should have unique usernames and passwords.
- Do not allow users to use the admin login and password.

[Back to Top](#)

Related Information

- [Cisco Security Vulnerability Policy](#)
- [Dictionary Attacks on Cisco LEAP](#)