Password Strength Settings on Sx500 Series Stackable Switches

Objective

Password strength is necessary to make the configured password more secure. The objective of this document is to help configure Password Strength Settings on Sx500 Series Stackable Switches.

Applicable Devices

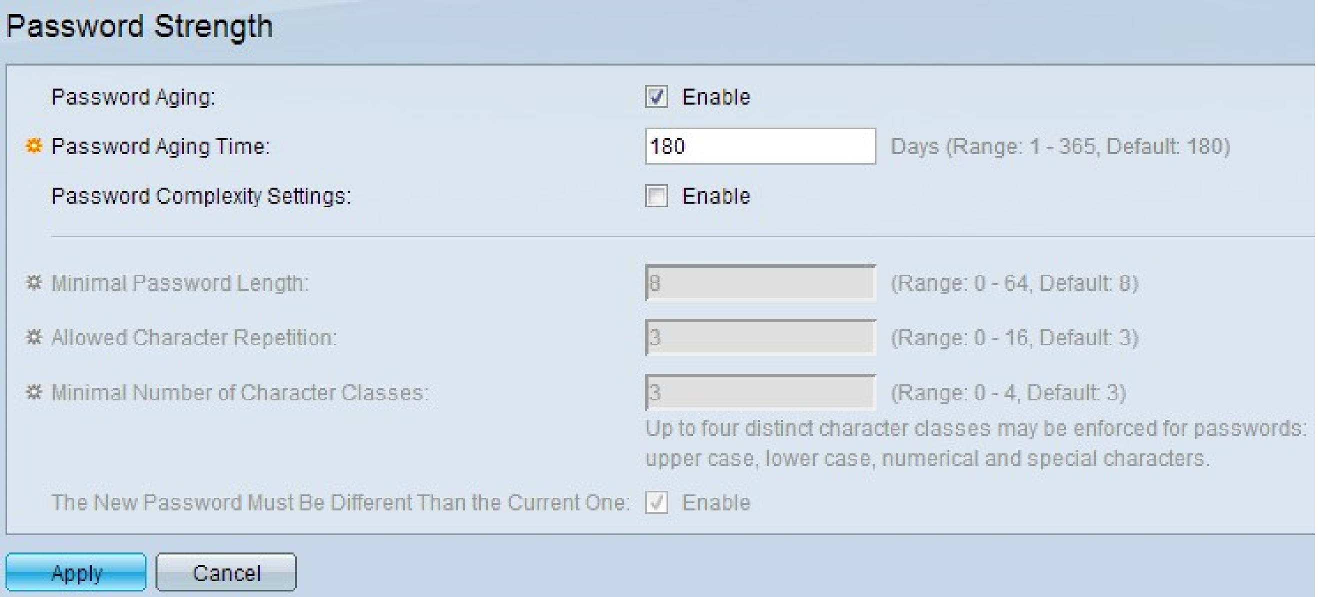
- Sx500 Series Stackable Switches

Software Version

- 1.3.0.62

Password Strength Settings

Step 1. Log in to the web based configuration utility and choose **Security > Password Strength.** The *Password Strength* page opens:



Password Strength

Password Aging: ☑ Enable

Password Aging Time: 180 Days (Range: 1 - 365, Default: 180)

Password Complexity Settings: □ Enable

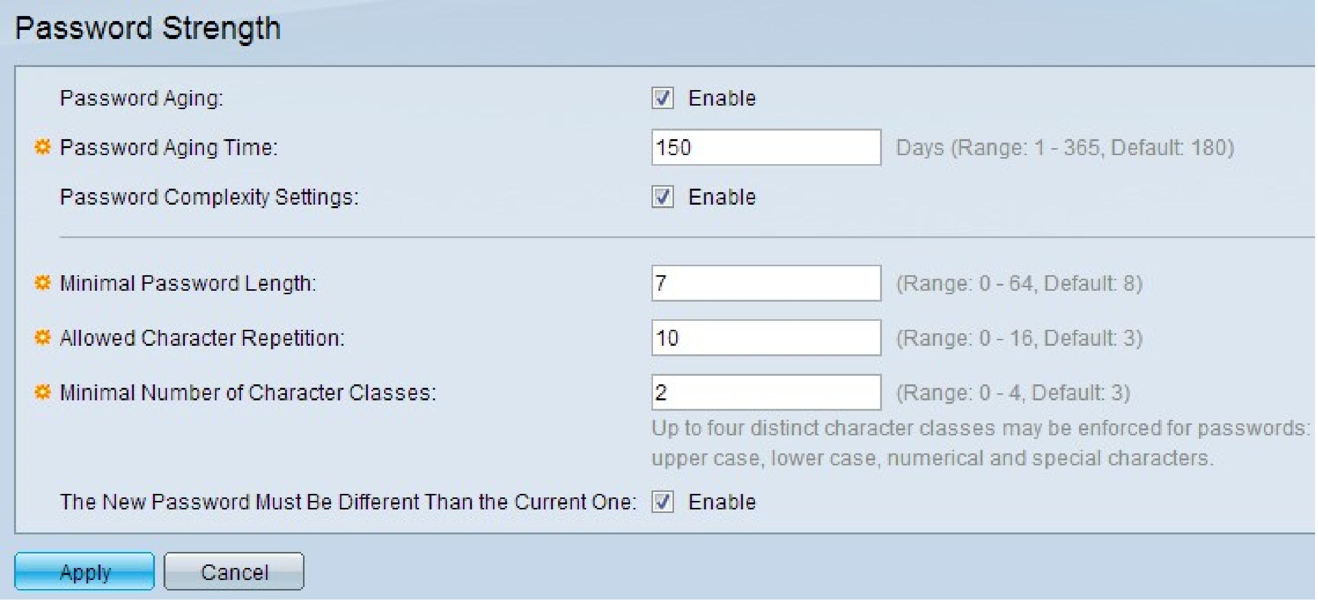
Minimal Password Length: 8 (Range: 0 - 64, Default: 8)

Allowed Character Repetition: 3 (Range: 0 - 16, Default: 3)

Minimal Number of Character Classes: 3 (Range: 0 - 4, Default: 3)

Up to four distinct character classes may be enforced for passwords: upper case, lower case, numerical and special characters.

The New Password Must Be Different Than the Current One: ☑ Enable



Password Strength

Password Aging:	☑ Enable	
Password Aging Time:	150	Days (Range: 1 - 365, Default: 180)
Password Complexity Settings:	☑ Enable	
Minimal Password Length:	7	(Range: 0 - 64, Default: 8)
Allowed Character Repetition:	10	(Range: 0 - 16, Default: 3)
Minimal Number of Character Classes:	2	(Range: 0 - 4, Default: 3)
	Up to four distinct character classes may be enforced for passwords: upper case, lower case, numerical and special characters.	
The New Password Must Be Different Than the Current One:	☑ Enable	

Step 2. In the Password Aging field, check the **Enable** check box to prompt the user to change the password when the password aging time expires.

Step 3. In the Password Aging Time field, enter the number of days that can elapse before the user is prompted to change the password.

Step 4. In the Password Complexity Settings field, check the **Enable** check box to enable complexity rules for passwords.

Step 5. In the Minimum Password Length field, enter a value for the minimum length of characters required in the password. It should be between 0 and 64, and it is set as 8 by default.

Step 6. In the Minimum Number of Character Classes field, assign a value for the minimum number of character classes required in a password. It is set as 3 by default. The classes are of four types: upper case, lower case, numerical, and special characters.

Step 7. (Optional) To require that the new password is different from the present password, check the **Enable** check box in the The New Password Must Be Different Than The Current One field.

Step 8. Click **Apply**.