Configure Password Strength and Complexity Settings on the Switch

Objective

The first time that you log in to the web-based utility of your switch, you have to use the default username and password which is: cisco/cisco. You are then required to enter and configure a new password for the cisco account. Password complexity is enabled by default. If the password that you choose is not complex enough, you are prompted to create another password.

Since passwords are used to authenticate users accessing the device, simple passwords are potential security hazards. Therefore, password complexity requirements are enforced by default and may be configured as necessary.

This article provides instructions on how to define password complexity rules on the user accounts on your switch.

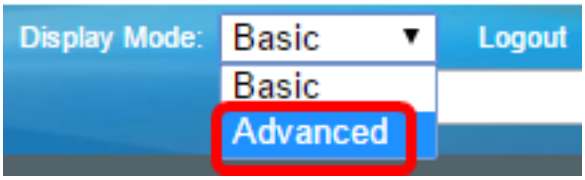
Applicable Devices | Software Version

- Sx250 | 2.2.5.68 (Download latest)
- Sx300 Series | 1.4.7.05 (Download latest)
- Sx350 Series | 2.2.5.68 (Download latest)
- SG350X Series | 2.2.5.68 (Download latest)
- Sx550X Series | 2.2.5.68 (Download latest)

Configure Password Strength and Complexity Settings on your Switch

Step 1. Log in to the web-based utility of your switch then choose **Advanced** in the Display Mode drop-down list.

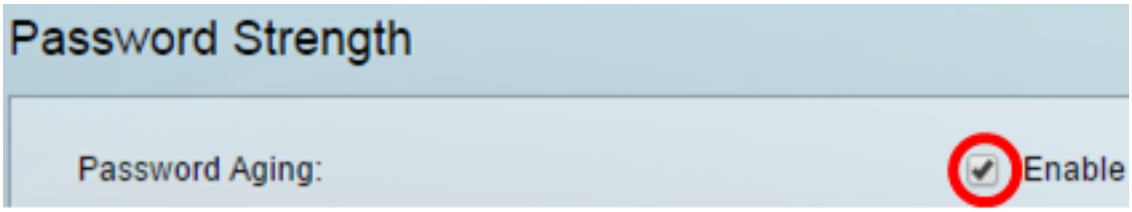
Note: In this example, SG350X-48MP switch is used.



Note: If you have an Sx300 Series switch, skip to Step 2.

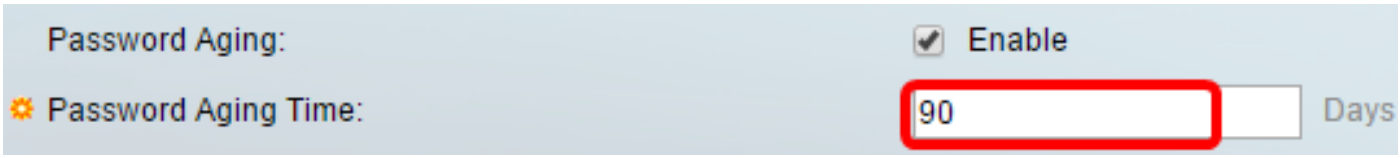
Step 2. Choose **Security > Password Strength**.

Step 3. (Optional) Uncheck the **Enable** Password Aging check box to disable the password aging feature. If this option is enabled, the user is prompted to change the password when the specified Password Aging Time expires. This feature is enabled by default.



Step 4. Enter the number of days that can elapse before the user is prompted to change the password. The default value is 180, and the range is 1 to 356 days. In this example, 90 is used.

Note: If you disabled this feature in Step 3, skip to Step 5.



Note: Password aging also applies to zero-length or no password.

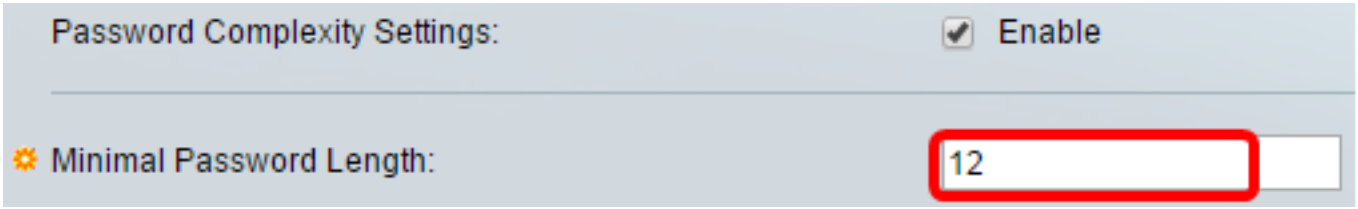
Step 5. (Optional) Check the **Password Complexity Settings** check box to enable complexity rules for passwords. If this feature is enabled, new passwords must conform to the following default settings:

- Have a minimum length of eight characters.
- Contain characters from at least three character classes (uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard).
- Are different from the current password.
- Contain no character that is repeated more than three times consecutively.
- Do not repeat or reverse the users name or any variant reached by changing the case of the characters.
- Do not repeat or reverse the manufacturers name or any variant reached by changing the case of the characters.

Note: If you do not want to enable Password Complexity Settings, skip to Step 10.

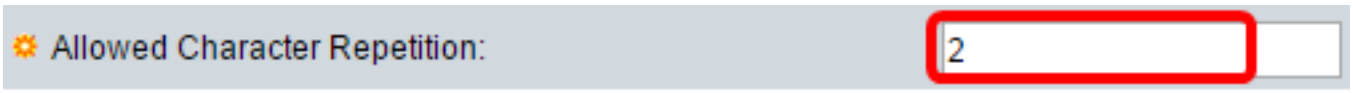
Step 6. (Optional) Enter the minimal number of characters required for passwords in the *Minimal Password Length* field. The default value is 8, and the range is 0 to 64 characters.

Note: A zero-length or no password is allowed, and can still have password aging assigned to it.



Note: In this example, 12 is used.

Step 7. Enter the number of times that a character can be repeated in the *Allowed Character Repetition* field. The default value is 3, and the range is 0 to 16 instances.



Note: In this example, 2 is used.

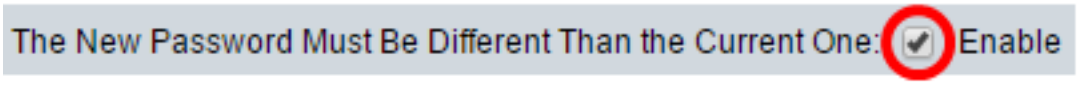
Step 8. Enter the number of character classes which must be present in a password. Up to four distinct character classes may be enforced for passwords. The default value is 3, and the range is 0 to 4 character classes.

The classes are:

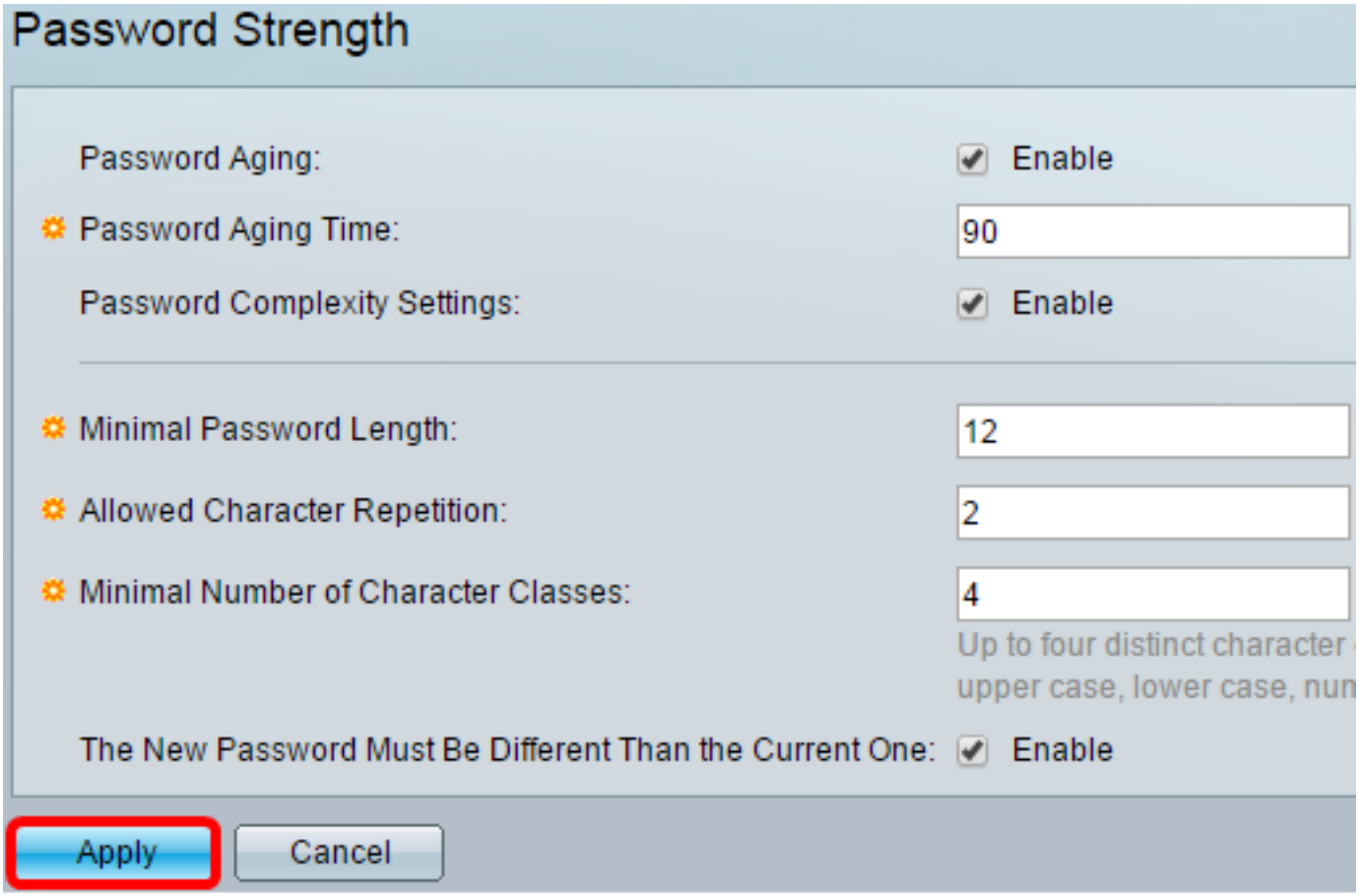
- 1 — Lower Case
- 2 — Upper Case
- 3 — Digits or Numbers
- 4 — Symbols or Special Characters

Note: In this example, 4 is used.

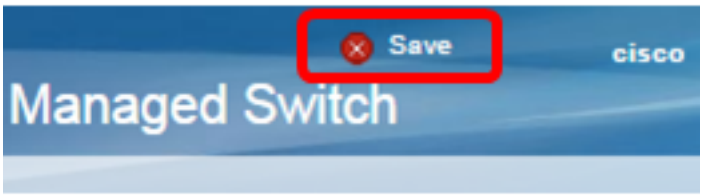
Step 9. (Optional) Check the **Enable** The New Password Must Be Different Than the Current One check box to require a unique password upon password change.



Step 10. Click **Apply**.



Step 11. (Optional) Click **Save** to save settings to the startup configuration file.



You should now have successfully configured the password strength and complexity settings of the switch.

For more information, including links to all articles related to your series of switch, check out the appropriate product page:

- 250 Series Switches Product Page
- 300 Series Switches Product Page
- 350 Series Switches Product Page
- 350X Series Switches Product Page
- 550 Series Switches Product Page
- 550X Series Switches Product Page