

Real-World Scenario 9-1: Password Policies

Scenario: In the figure we see that we are working on a Cisco SG200 switch. Examine the figure carefully. What security issues can you see that are related to passwords?

Password Strength

Password Aging:	<input checked="" type="checkbox"/> Enable
✱ Password Aging Time:	<input type="text" value="180"/> Days (Range: 1 - 365, Default: 90)
Password Complexity Settings:	<input type="checkbox"/> Enable
<hr/>	
✱ Minimal Password Length:	<input type="text" value="4"/> (Range: 0 - 64, Default: 8)
✱ Allowed Character Repetition:	<input type="text" value="10"/> (Range: 0 - 16, Default: 3)
✱ Minimal Number of Character Classes:	<input type="text" value="1"/> (Range: 0 - 4, Default: 3) Up to four distinct character classes may be enforced for password complexity: upper case, lower case, numerical and special characters
The New Password Must Be Different Than the Current One: <input checked="" type="checkbox"/> Enable	

Real-World Scenario 9-1 Solution

The most glaring problem is that the Password Complexity Settings checkbox is not enabled. By default, on a switch such as this it would be enabled, but you should always check just in case. Without complexity, a person could set very weak passwords for a user account allowed to log in to this switch. This doesn't affect other computers but it does affect all user accounts on this switch.

Once that is enabled, the options below it become configurable. Note that the current minimum password length of 4 characters is not nearly enough. Cisco recommends 8, but you might find 10 or even 15 characters as your organization's minimum. In addition, the allowed character repetition is much too high, and the minimal number of character classes is too low. You should opt for either 3 (the default here) or all 4.

Finally, your organization might decide that 180 days is too long for password aging time, and that passwords should be changed more frequently. In fact, this might be necessary for compliance with various third-party auditing organizations.

Video Solution: Watch the video solution "9-1: Password Policies."