

Einstellungen für die Kennwortstärke bei Stackable Switches der Serie Sx500

Ziel

Die Kennwortstärke ist erforderlich, um die Sicherheit des konfigurierten Kennworts zu erhöhen. Dieses Dokument soll Ihnen bei der Konfiguration der Einstellungen für die Kennwortstärke auf stapelbaren Switches der Serie Sx500 helfen.

Anwendbare Geräte

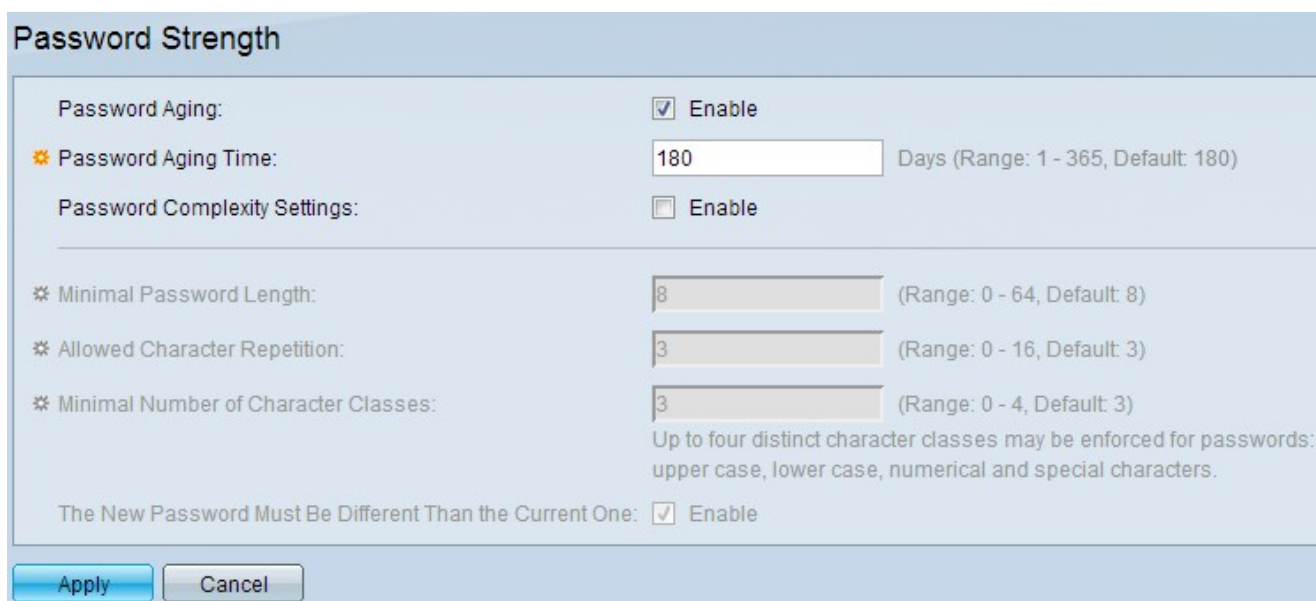
· Stackable Switches der Serie Sx500

Softwareversion

· 1.3.0.62

Einstellungen für Kennwortstärke

Schritt 1: Melden Sie sich beim webbasierten Konfigurationsprogramm an, und wählen Sie **Security > Password Strength** aus. Die Seite *Kennwortstärke* wird geöffnet:



The screenshot shows a configuration window titled "Password Strength" with the following settings:

- 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

At the bottom of the window are two buttons: "Apply" and "Cancel".

Password Strength

Password Aging:	<input checked="" type="checkbox"/> Enable
✳ Password Aging Time:	<input type="text" value="150"/> Days (Range: 1 - 365, Default: 180)
Password Complexity Settings:	<input checked="" type="checkbox"/> Enable
<hr/>	
✳ Minimal Password Length:	<input type="text" value="7"/> (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="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:	<input checked="" type="checkbox"/> Enable

Schritt 2: Aktivieren Sie im Feld Kennwortalterung das Kontrollkästchen **Aktivieren**, um den Benutzer aufzufordern, das Kennwort zu ändern, wenn die Kennwortalterung abläuft.

Schritt 3: Geben Sie im Feld Password Aging Time (Passwortalterzeit) die Anzahl der Tage ein, die vergehen können, bevor der Benutzer aufgefordert wird, das Kennwort zu ändern.

Schritt 4: Aktivieren Sie im Feld Password Complexity Settings (Einstellungen für die Kennwortkomplexität) das Kontrollkästchen **Enable (Aktivieren)**, um Komplexitätsregeln für Kennwörter zu aktivieren.

Schritt 5: Geben Sie im Feld Minimale Kennwortlänge einen Wert für die Mindestlänge von Zeichen ein, die im Kennwort erforderlich ist. Der Wert muss zwischen 0 und 64 liegen und standardmäßig auf 8 festgelegt sein.

Schritt 6: Weisen Sie im Feld Mindestanzahl von Zeichenklassen einen Wert für die Mindestanzahl von Zeichenklassen zu, die in einem Kennwort erforderlich sind. Er ist standardmäßig auf 3 festgelegt. Es gibt vier Klassen: Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen.

Schritt 7: (Optional) Um zu verlangen, dass sich das neue Kennwort vom aktuellen Kennwort unterscheidet, aktivieren Sie das Kontrollkästchen **Aktivieren** im Feld Neues Kennwort muss sich von dem Kontrollkästchen Aktuelles unterscheiden.

Schritt 8: Klicken Sie auf **Übernehmen**.