# Konfigurieren der Einstellungen für das Kennwort oder die WPA-PSK-Komplexität auf einem WAP125- oder WAP581-Access Point

## Ziel

Die Sicherheit von Kennwörtern nimmt mit zunehmender Komplexität von Kennwörtern zu. Es ist wichtig, dass Sie lange Kennwörter mit einer Kombination aus Groß- und Kleinbuchstaben, Zahlen und Symbolen verwenden, um die Sicherheit zu gewährleisten. Die Komplexität von Kennwörtern wird verwendet, um Anforderungen für Kennwörter festzulegen, um das Risiko einer Sicherheitsverletzung zu verringern.

Wi-Fi Protected Access (WPA) ist eines der Sicherheitsprotokolle für Wireless-Netzwerke. Im Vergleich zum Sicherheitsprotokoll Wired Equivalent Privacy (WEP) hat WPA die Authentifizierungs- und Verschlüsselungsfunktionen verbessert. Wenn WPA auf dem AP konfiguriert ist, wird ein WPA Pre-Shared Key (PSK) ausgewählt, um Clients sicher zu authentifizieren. Wenn die WPA-PSK-Komplexität aktiviert ist, können Komplexitätsanforderungen für den Schlüssel, der im Authentifizierungsprozess verwendet wird, konfiguriert werden. Komplexere Schlüssel erhöhen die Sicherheit.

In diesem Dokument wird erläutert, wie Sie die Einstellungen für die Kennwortkomplexität und die WPA-PSK-Komplexität auf Ihrem WAP125 oder WAP581 Access Point konfigurieren.

## Anwendbare Geräte

- WAP125
- WAP581

## Softwareversion

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

## Konfigurieren der Kennwortsicherheit

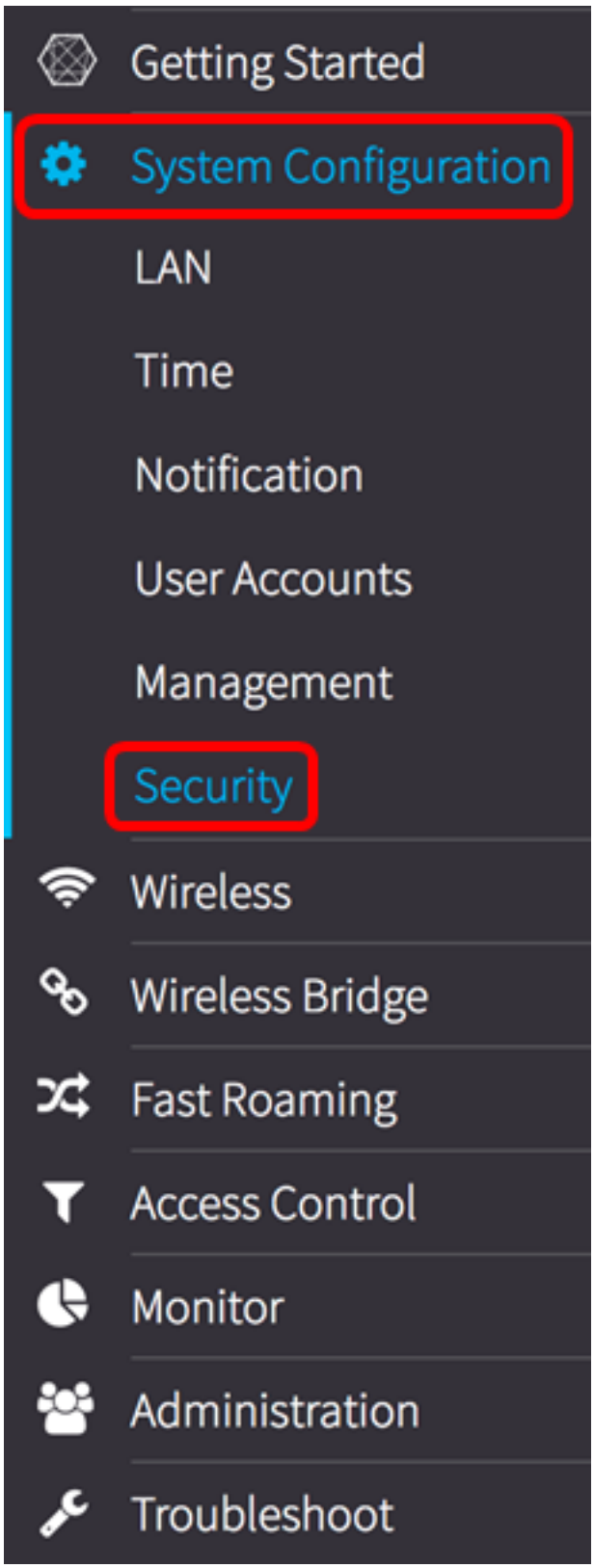
### Konfigurieren der Kennwortkomplexität

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm Ihres WAP an. Der Standard-Benutzername und das Kennwort lautet cisco/cisco.

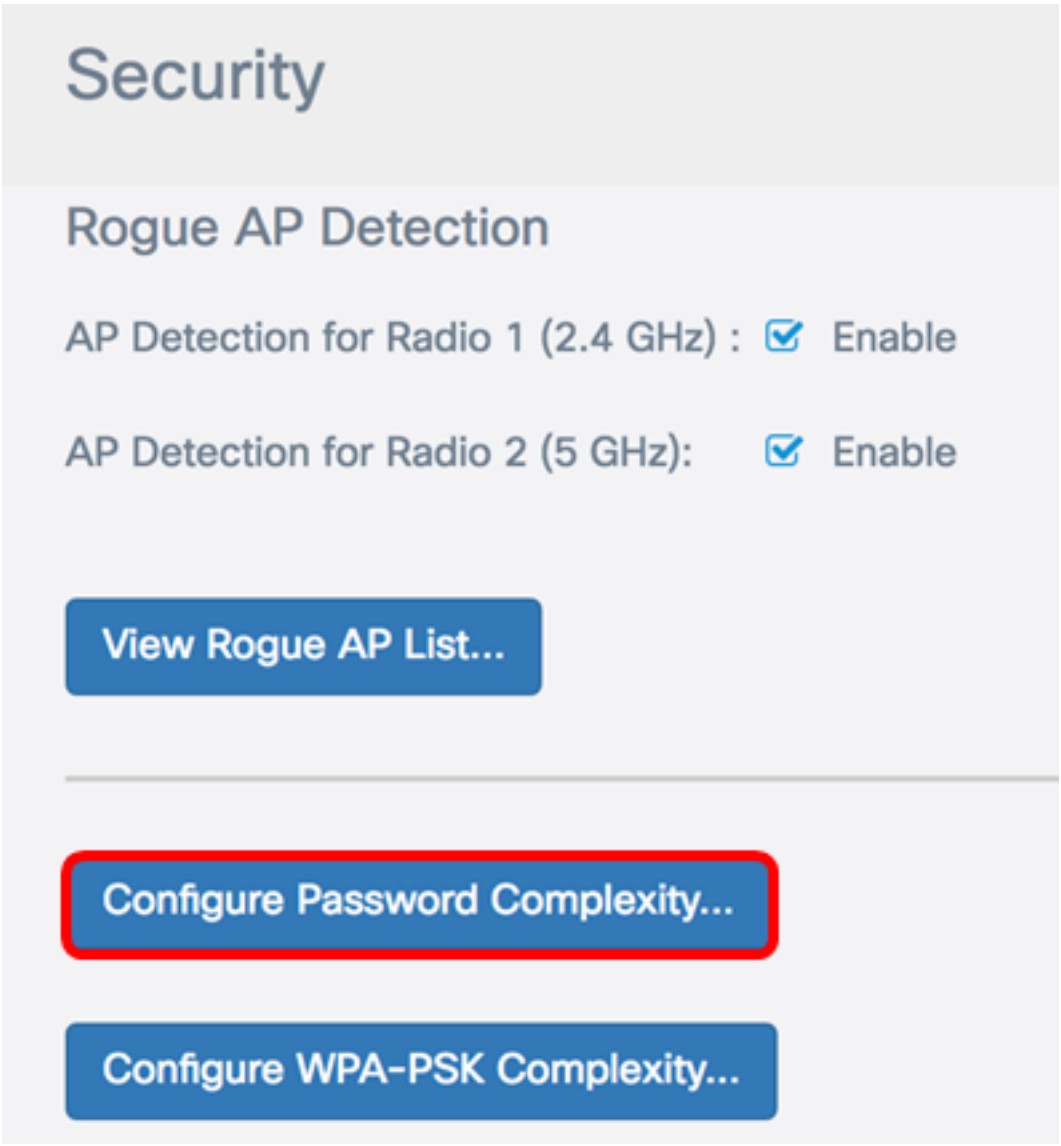

**Hinweis:** Wenn Sie das Kennwort bereits geändert oder ein neues Konto erstellt haben, geben Sie stattdessen Ihre neuen Anmeldeinformationen ein.

Schritt 2: Wählen Sie **Systemkonfiguration > Sicherheit aus**.

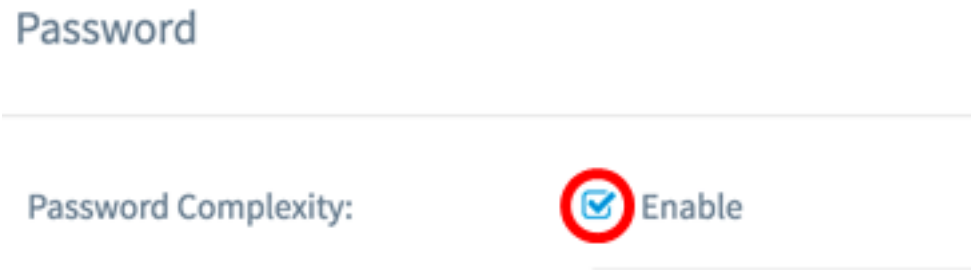
**Hinweis:** Die verfügbaren Optionen können je nach Gerät variieren. In diesem Beispiel wird WAP125 verwendet.




Schritt 3: Klicken Sie unter dem Bereich "Erkennung nicht autorisierter APs" auf die Schaltfläche **Kennwortkomplexität konfigurieren...**



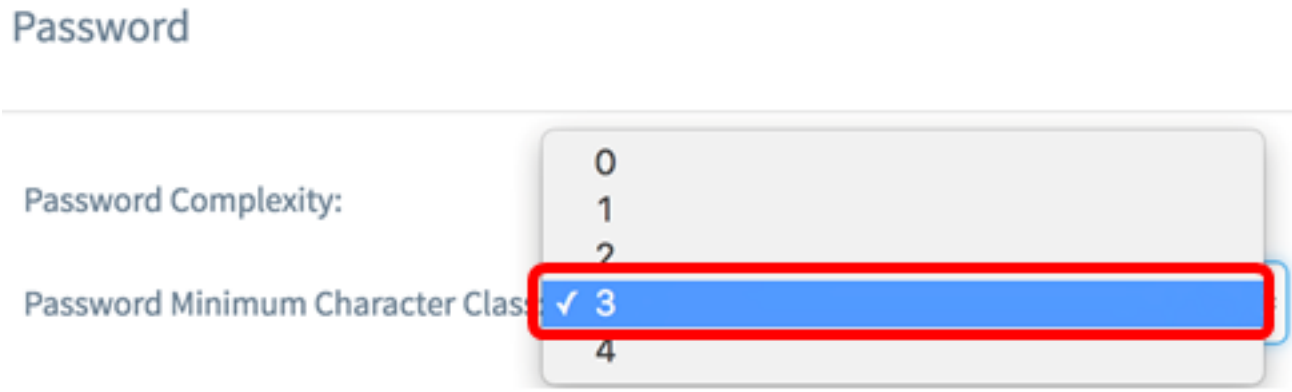

Schritt 4: Aktivieren Sie das Kontrollkästchen **Enable Password Complexity (Kennwortkomplexität aktivieren)**, um die Schritte zum Festlegen der Kennwortkomplexität zu aktivieren. Wenn diese Option nicht markiert ist, fahren Sie mit Schritt 8 fort.



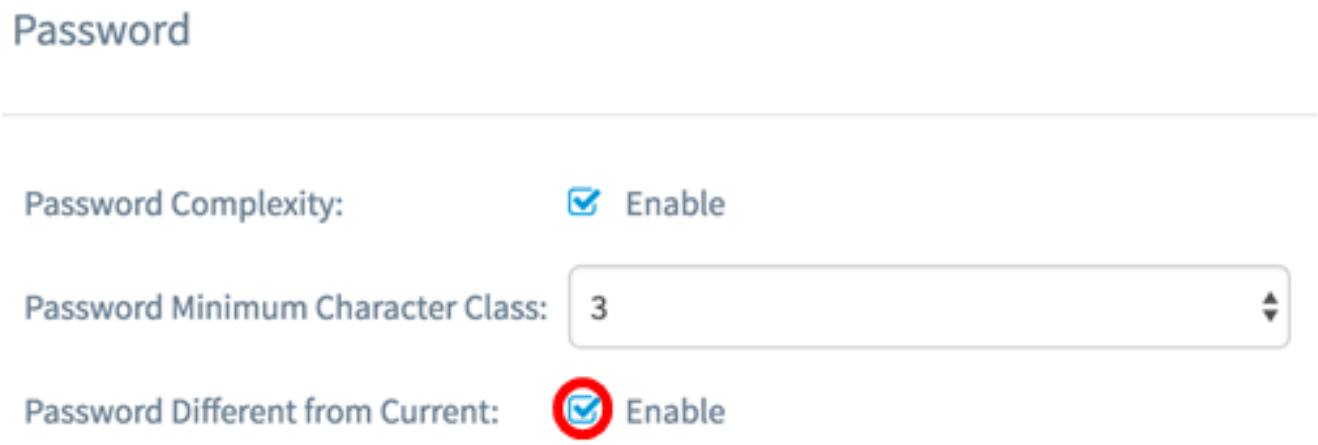

Schritt 5: Wählen Sie einen Wert aus der Dropdown-Liste Password Minimum Character Class (Minimale Zeichenklasse für Kennwort) aus. Die eingegebene Nummer stellt die Anzahl der Mindest- oder Höchstzeichen der verschiedenen Klassen dar:

- Das Passwort besteht aus Großbuchstaben (ABCD).
- Das Kennwort besteht aus Kleinbuchstaben (abcd).
- Das Kennwort besteht aus numerischen Zeichen (1234).
- Das Kennwort besteht aus Sonderzeichen (!@#$).

**Hinweis:** In diesem Beispiel wird 3 ausgewählt.

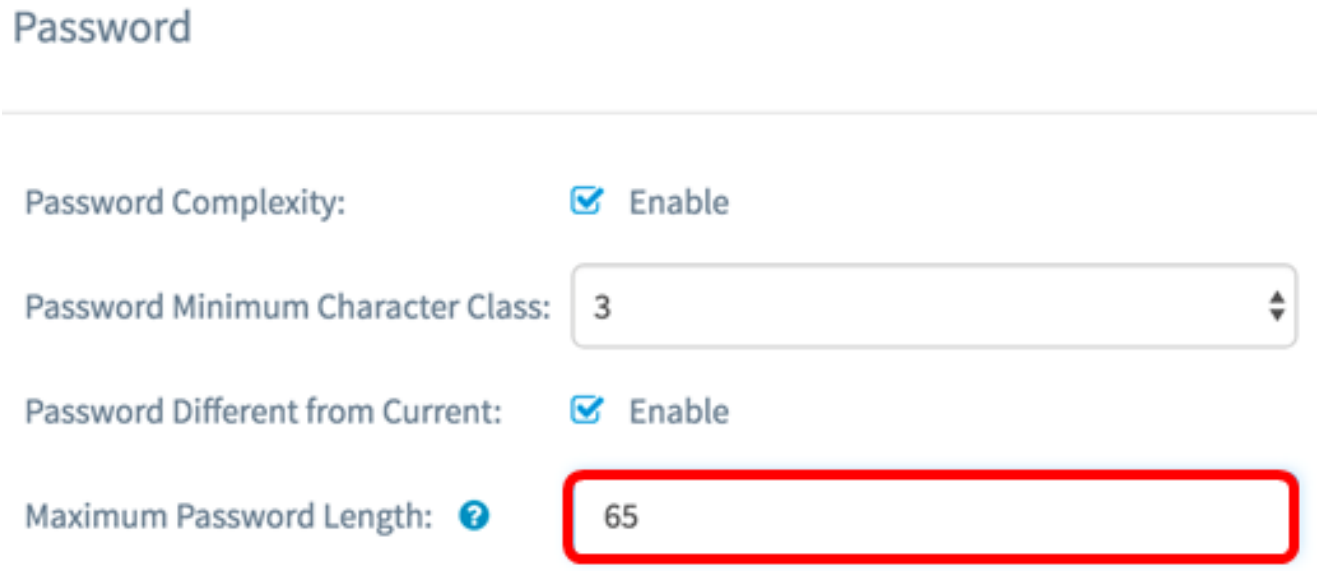



Schritt 6: Aktivieren Sie das Kontrollkästchen **Enable** Password Different from Current (Kennwortabweichung von Aktuell **aktivieren**), damit Benutzer ihr Kennwort nach Ablauf aktualisieren können. Wenn diese Option nicht markiert ist, können Benutzer nach Ablauf dieses Kennworts immer noch dasselbe Kennwort erneut eingeben.




Schritt 7: Geben Sie im Feld *Maximale Kennwortlänge* einen Wert zwischen 64 und 127 ein, um die Anzahl der Zeichen und die Länge des Kennworts festzulegen. Der Standardwert ist 64.

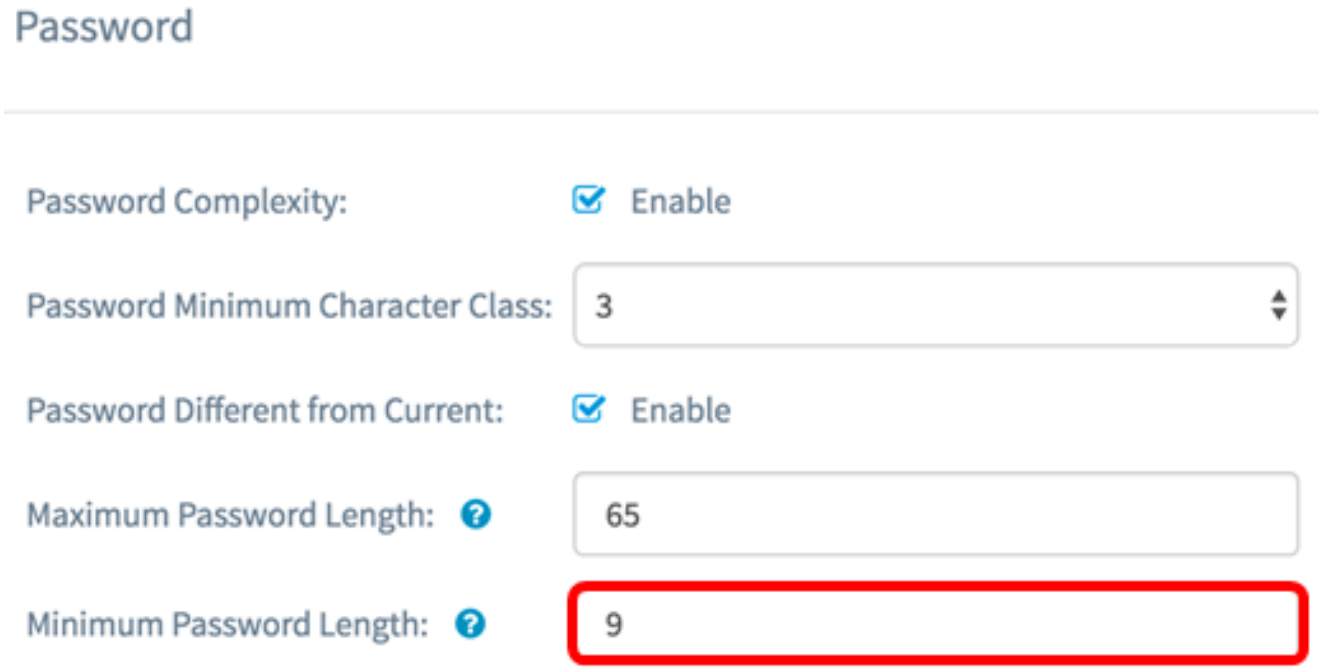
**Hinweis:** In diesem Beispiel wird 65 verwendet.



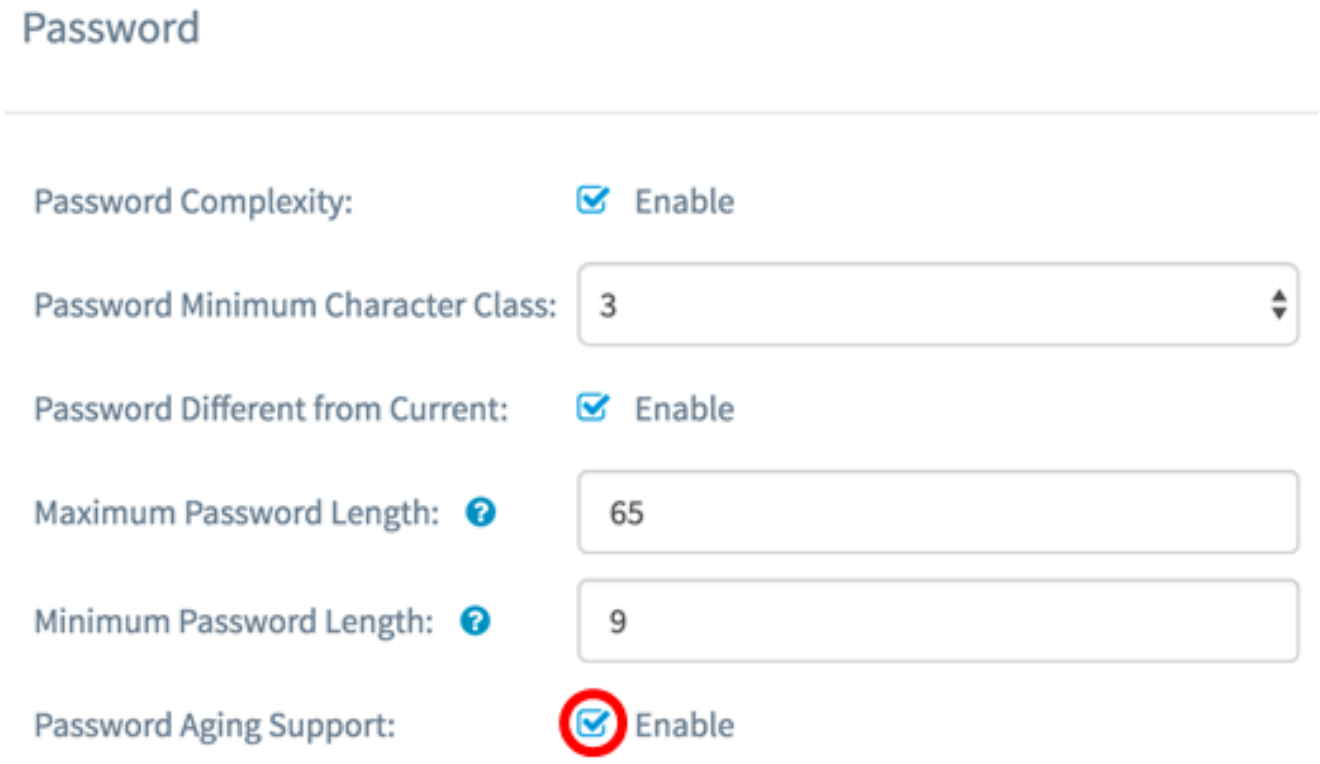

Schritt 8: Geben Sie im Feld *Minimale Kennwortlänge* einen Wert zwischen 0 und 32 ein, um die erforderliche Mindestanzahl von Zeichen für das Kennwort festzulegen. Der

Standardwert ist 8.

**Hinweis:** In diesem Beispiel ist die Mindestlänge für das Kennwort 9.

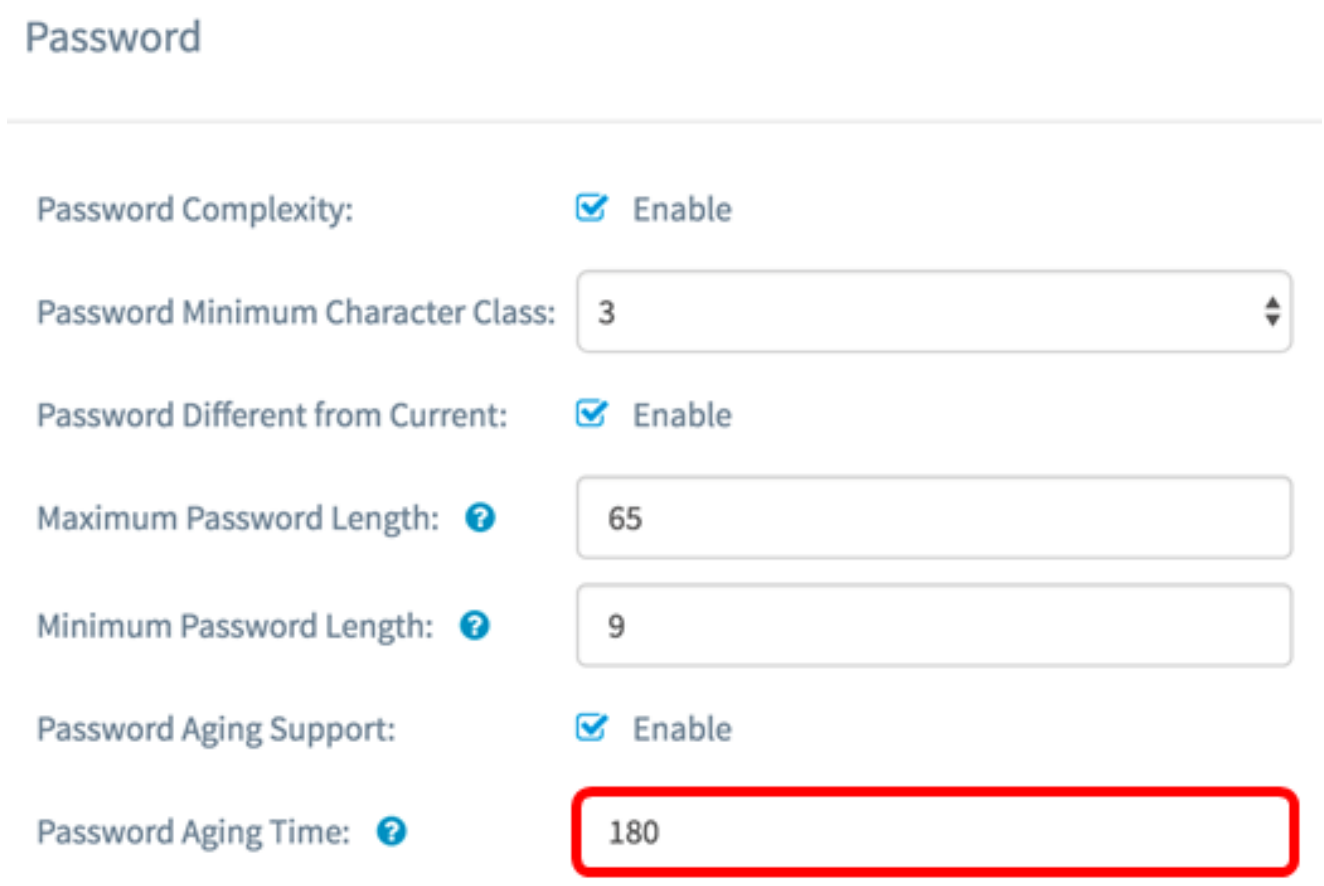



Schritt 9: Aktivieren Sie das Kontrollkästchen **Enable Password Aging Support (Unterstützung für Kennwortveralterung aktivieren)**, damit Kennwörter ablaufen. Wenn diese Option aktiviert ist, fahren Sie mit dem nächsten Schritt fort. Fahren Sie andernfalls mit fort.

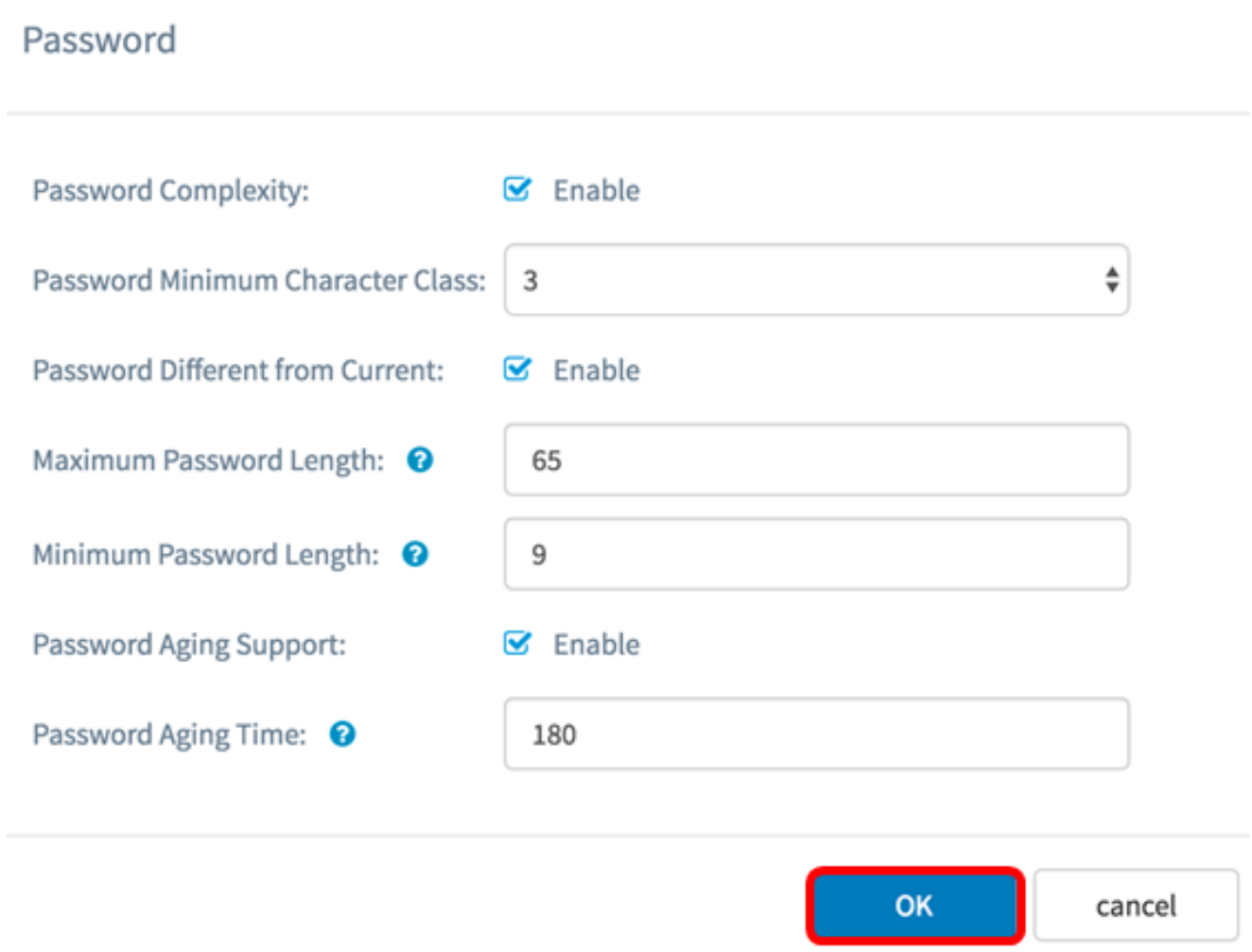



Schritt 10: Geben Sie im Feld *Password Aging Time (Kennwortalterung) einen Wert zwischen 1 und 365 ein, um die Anzahl der Tage festzulegen, bevor ein neu erstelltes Kennwort abläuft.* Der Standardwert ist 180 Tage.

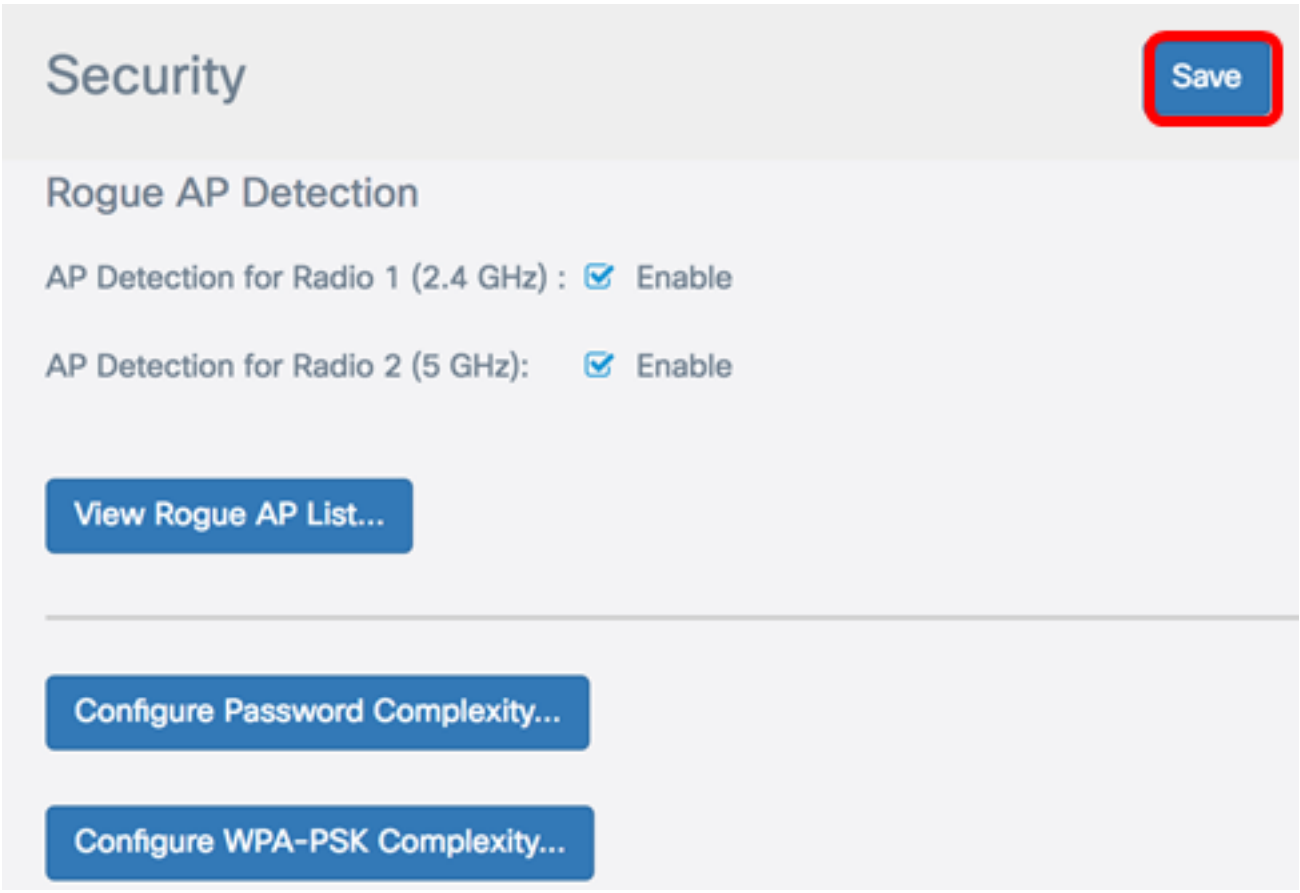
**Hinweis:** In diesem Beispiel wird 180 verwendet.




Schritt 11: Klicken Sie auf **OK**. Sie gelangen wieder zur Hauptseite für die Sicherheitskonfiguration.



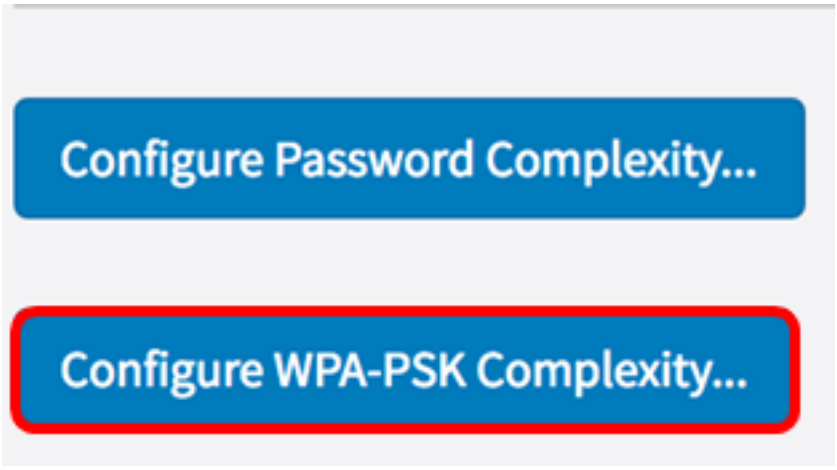

Schritt 12: Klicken Sie auf die Schaltfläche **Speichern**, um die konfigurierten Einstellungen zu speichern.



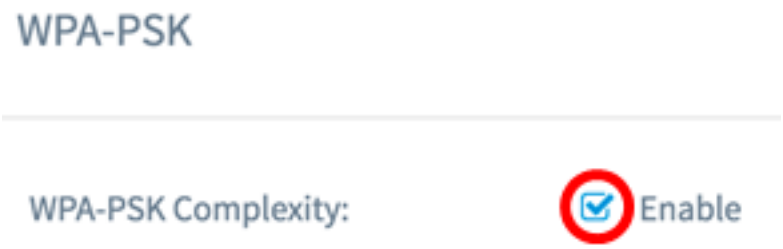

Sie sollten jetzt die Sicherheitseinstellungen für die Kennwortkomplexität erfolgreich auf Ihrem WAP konfiguriert haben.

## Konfigurieren der WPA-PSK-Komplexität

Schritt 1: Klicken Sie auf die Schaltfläche **WPA-PSK-Komplexität konfigurieren**.




Schritt 2: Aktivieren Sie das Kontrollkästchen **Enable** WPA-PSK Complexity (WPA-PSK-Komplexität aktivieren), um die Schritte zum Festlegen der Kennwortkomplexität zu aktivieren.

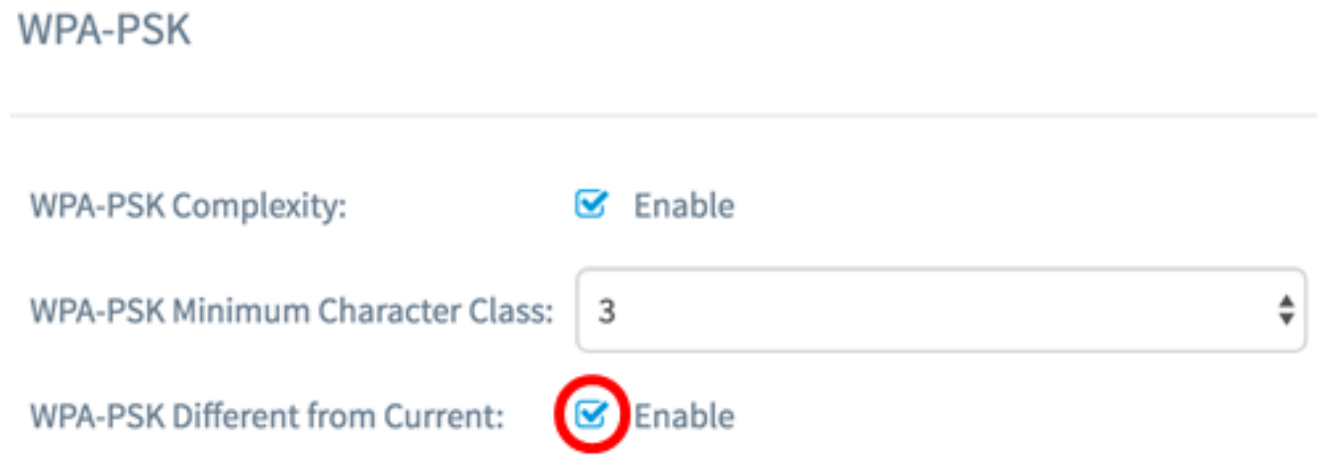



Schritt 3: Wählen Sie einen Wert aus der Dropdown-Liste "WPA-PSK Minimum Character Class" aus. Die eingegebene Nummer stellt die Anzahl der Mindest- oder Höchstzeichen der verschiedenen Klassen dar:

- Das Passwort besteht aus Großbuchstaben (ABCD).
- Das Kennwort besteht aus Kleinbuchstaben (abcd).
- Das Kennwort besteht aus numerischen Zeichen (1234).
- Das Kennwort besteht aus Sonderzeichen (!@#$).

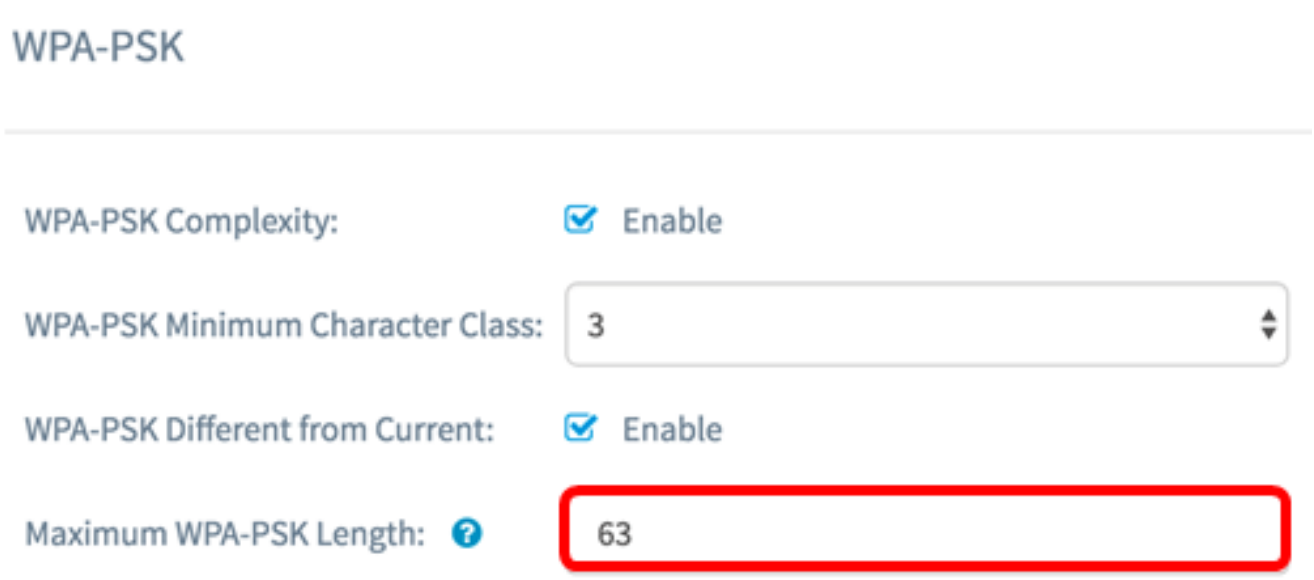
**Hinweis:** In diesem Beispiel wird 3 ausgewählt.


Schritt 4: Aktivieren Sie das Kontrollkästchen **Enable** WPA-PSK Different from Current (WPA-PSK anders als Aktuell aktivieren), um Benutzern zu ermöglichen, ihr Kennwort nach Ablauf zu aktualisieren. Wenn diese Option nicht markiert ist, können Benutzer nach Ablauf dieses Kennworts immer noch dasselbe Kennwort erneut eingeben.



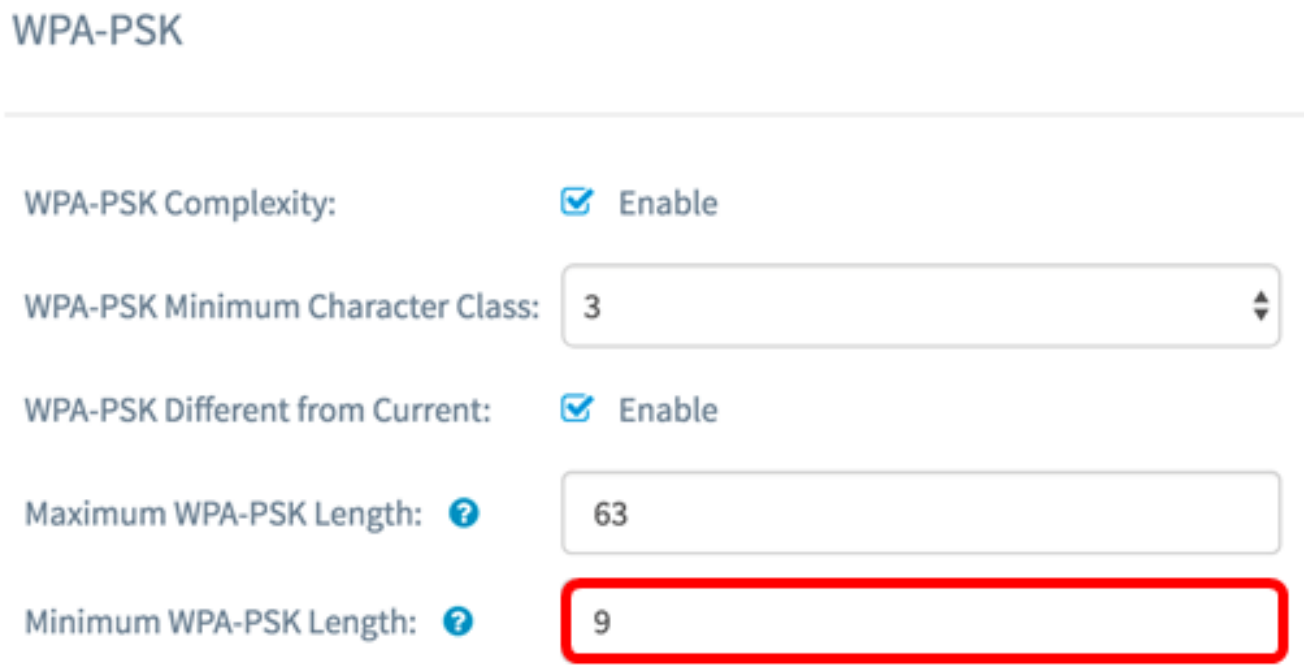

Schritt 5: Geben Sie im Feld *Maximale WPA-PSK-Länge* einen Wert zwischen 32 und 63 ein, um die Anzahl der Zeichen und die Länge des Kennworts zu definieren. Der Standardwert ist 63.

**Hinweis:** In diesem Beispiel wird 63 verwendet.

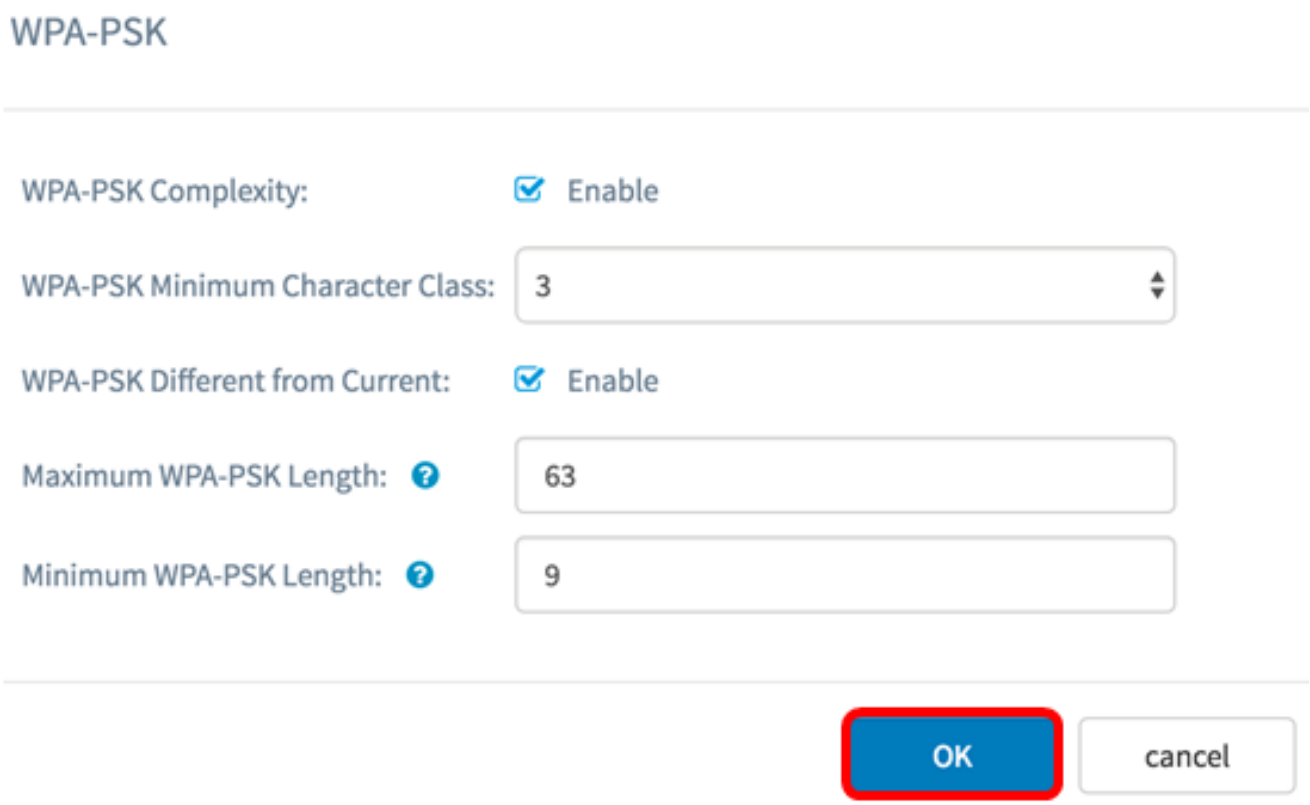



Schritt 6: Geben Sie im Feld *Minimum WPA-PSK Length* (Mindestlänge für WPA-PSK) einen Wert zwischen 0 und 32 ein, um die erforderliche Mindestanzahl von Zeichen für das Kennwort festzulegen. Der Standardwert ist 8.

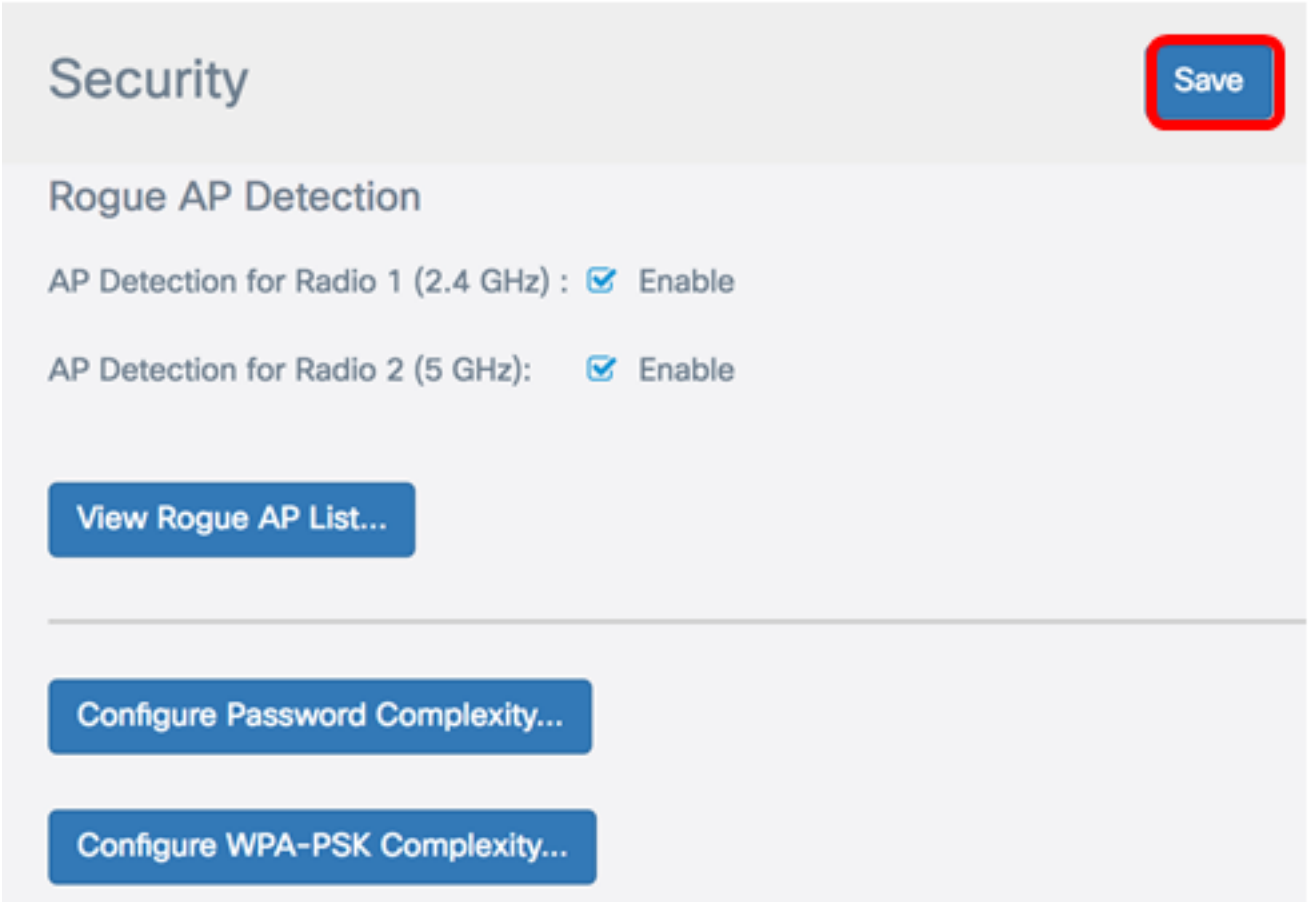
**Hinweis:** In diesem Beispiel ist die Mindestlänge für das Kennwort 9.




Schritt 7: Klicken Sie auf **OK**. Sie gelangen wieder zur Hauptseite für die Sicherheitskonfiguration.




Schritt 8: Klicken Sie auf die Schaltfläche **Speichern**, um die konfigurierten Einstellungen zu speichern.




Sie sollten jetzt die Sicherheitseinstellungen für die WPA-PSK-Komplexität erfolgreich auf Ihrem WAP konfiguriert haben.