WAP125 또는 WAP581 액세스 포인트에서 비밀번호 또는 WPA-PSK 복잡성 설정 구성

목표

비밀번호 보안은 비밀번호 복잡성이 증가하면서 증가합니다.강력한 보안을 유지하려면 대문자와 소문자, 숫자, 기호를 조합하여 긴 비밀번호를 사용해야 합니다.비밀번호 복잡성은 보안 침해 위험을 줄이기 위해 비밀번호에 대한 요구 사항을 설정하는 데 사용됩니다.

WPA(Wi-Fi Protected Access)는 무선 네트워크에 사용되는 보안 프로토콜 중 하나입니다 .WEP(Wired Equivalent Privacy) 보안 프로토콜과 비교할 때 WPA는 인증 및 암호화 기능을 개선했습니다.WPA가 AP에 구성된 경우 클라이언트를 안전하게 인증하도록 WPA PSK(Pre-Shared Key)가 선택됩니다.WPA-PSK 복잡성이 활성화된 경우 인증 프로세스에 사용되는 키에 대한 복잡성 요구 사항을 구성할 수 있습니다.더 복잡한 키는 보안을 강화합니다.

이 문서의 목적은 WAP125 또는 WAP581 액세스 포인트에서 비밀번호 복잡성 및 WPA-PSK 복잡성 설정을 구성하는 방법을 보여 주는 것입니다.

적용 가능한 디바이스

- WAP125
- WAP581

소프트웨어 버전

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

비밀번호 보안 구성

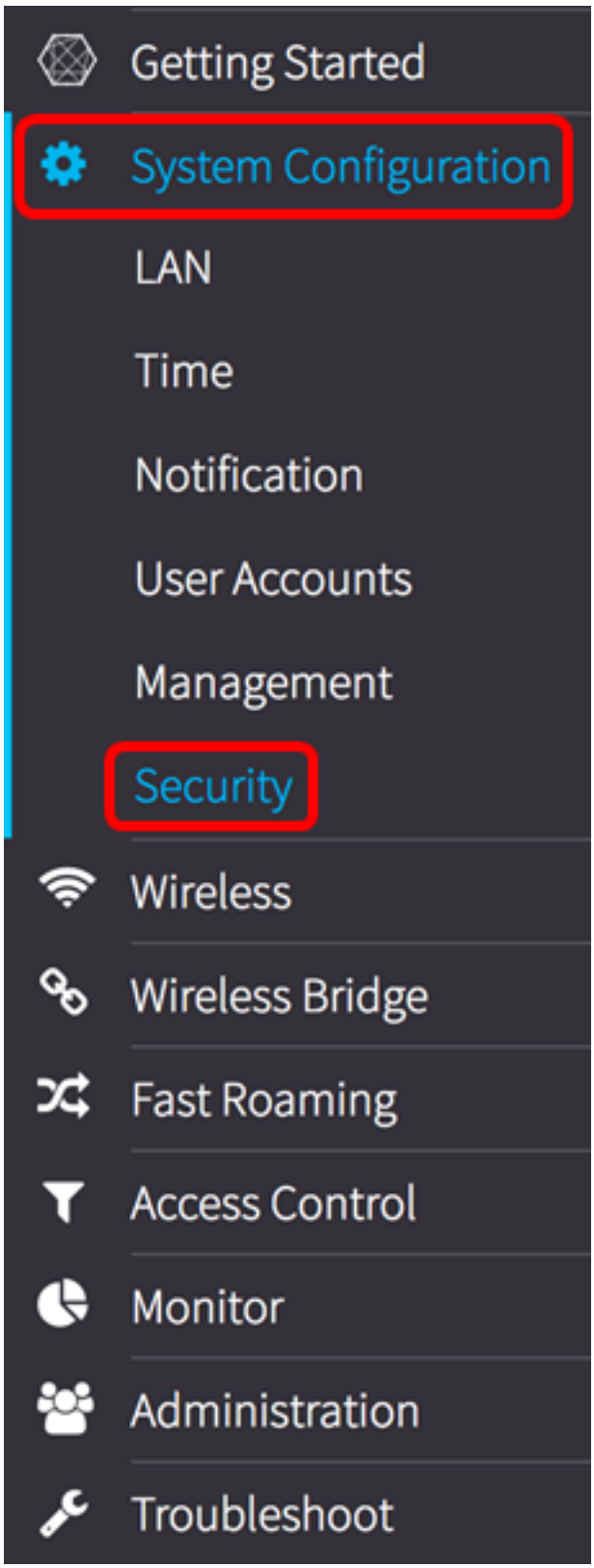
비밀번호 복잡성 구성

1단계. WAP의 웹 기반 유틸리티에 로그인합니다.기본 사용자 이름 및 비밀번호는 cisco/cisco입니다.

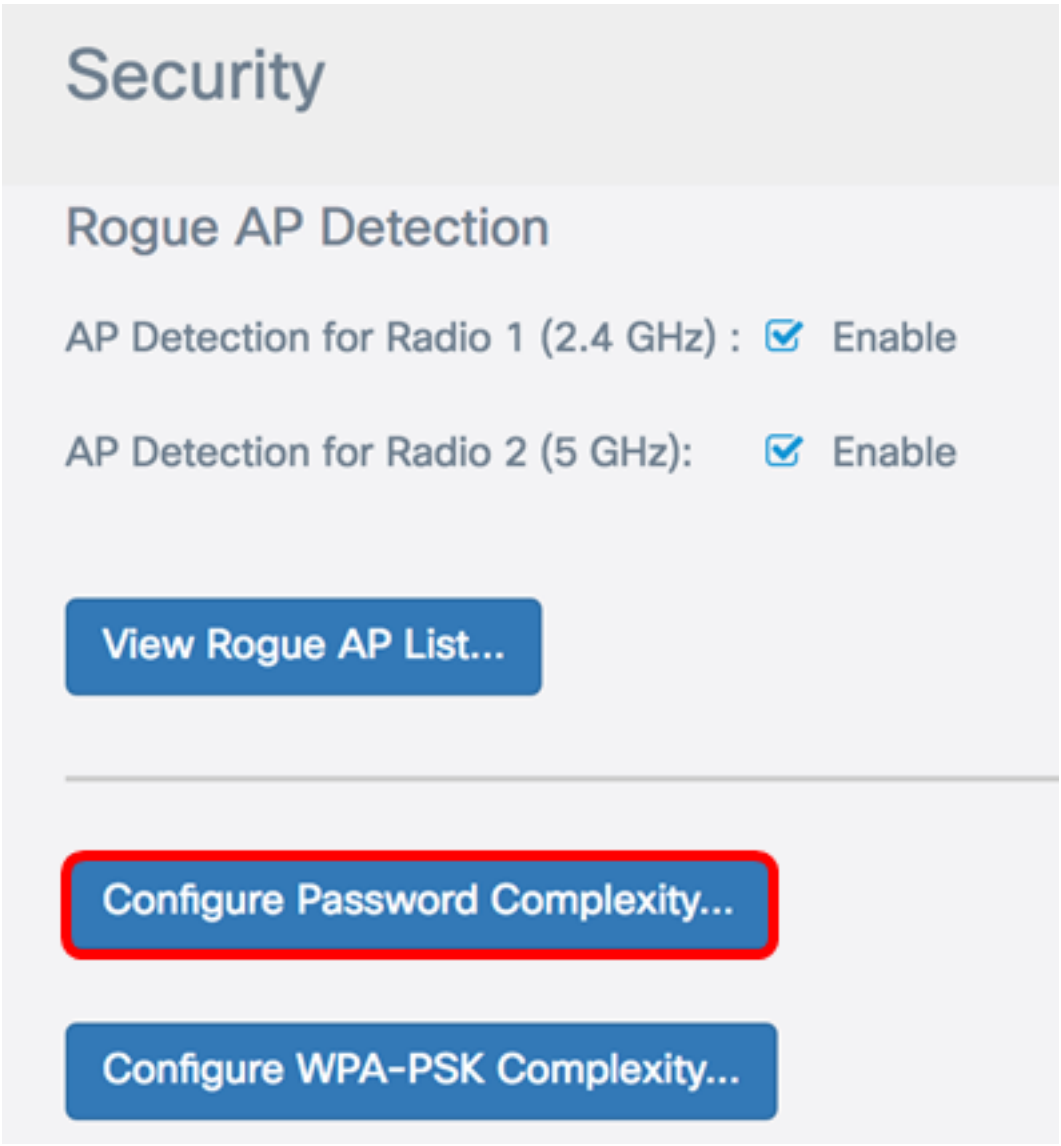
참고:이미 비밀번호를 변경하거나 새 계정을 생성한 경우 대신 새 자격 증명을 입력합니다.

2단계. System **Configuration(시스템 컨피그레이션) > Security(보안)를 선택합니다**.

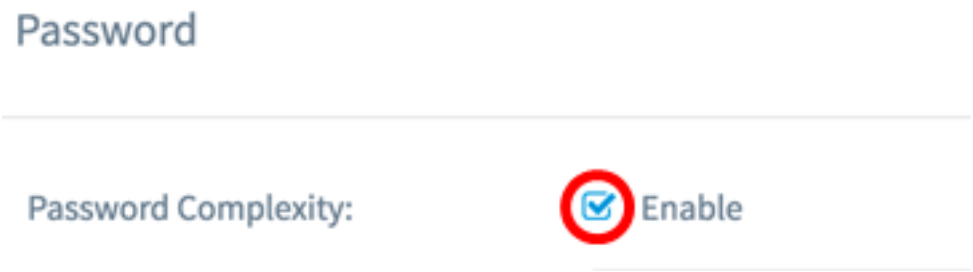
참고:사용 가능한 옵션은 디바이스의 정확한 모델에 따라 달라질 수 있습니다.이 예에서는 WAP125가 사용됩니다.



3단계. Rogue AP Detection(비인가 AP 탐지) 영역 아래에서 **Configure Password Complexity(비밀번호 복잡성 구성)..** 버튼을 클릭합니다.



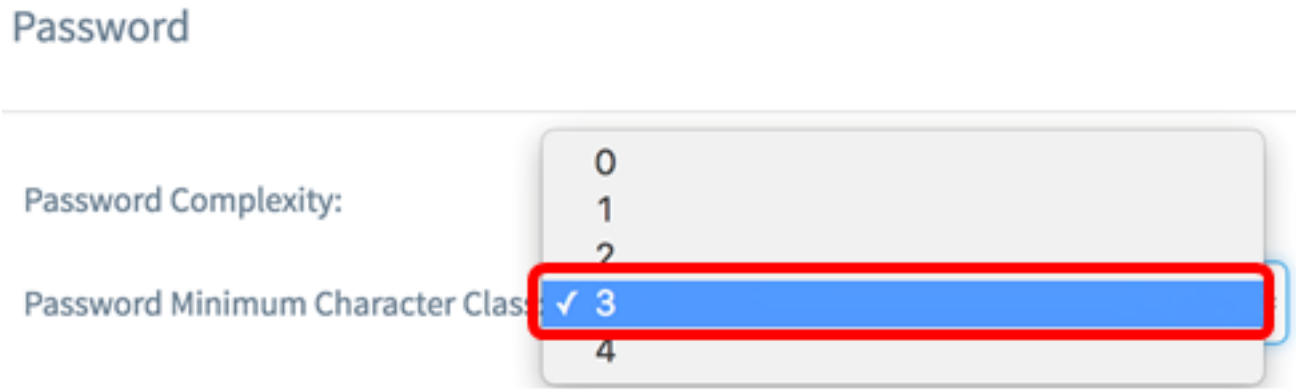
4단계. 비밀번호 복잡성 설정 단계를 활성화하려면 비밀번호 복잡성 사용 확인란을 선택합니다.이 옵션을 선택하지 않은 상태이면 8단계로 건너뜁니다.



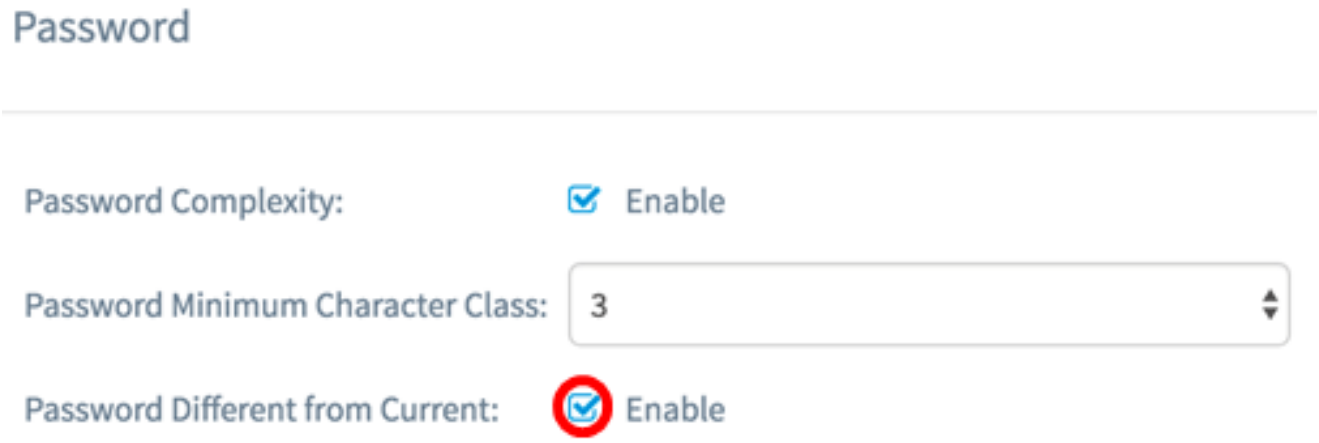
5단계. 비밀번호 최소 문자 클래스 드롭다운 목록에서 값을 선택합니다.입력한 숫자는 다른 클래스의 최소 또는 최대 문자 수를 나타냅니다.

- 비밀번호는 대문자(ABCD)로 구성됩니다.
- 비밀번호는 소문자(abcd)로 구성됩니다.
- 암호는 숫자 문자(1234)로 구성됩니다.
- 암호는 특수 문자(!@#$)로 구성됩니다.

참고:이 예에서는 3이 선택됩니다.

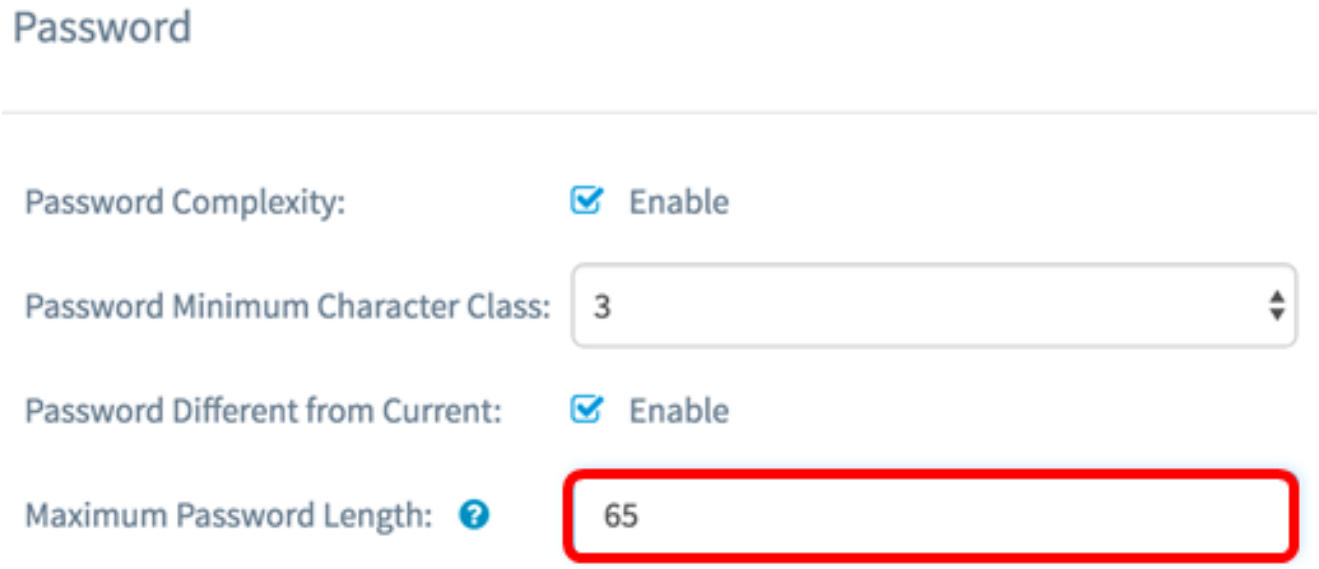


6단계. **Enable Password Different** from Current 확인란을 선택하여 사용자가 비밀번호 만료 시 비밀번호를 업데이트할 수 있도록 합니다.이 옵션을 선택하지 않으면 만료될 때 동일한 비밀번호를 다시 입력할 수 있습니다.



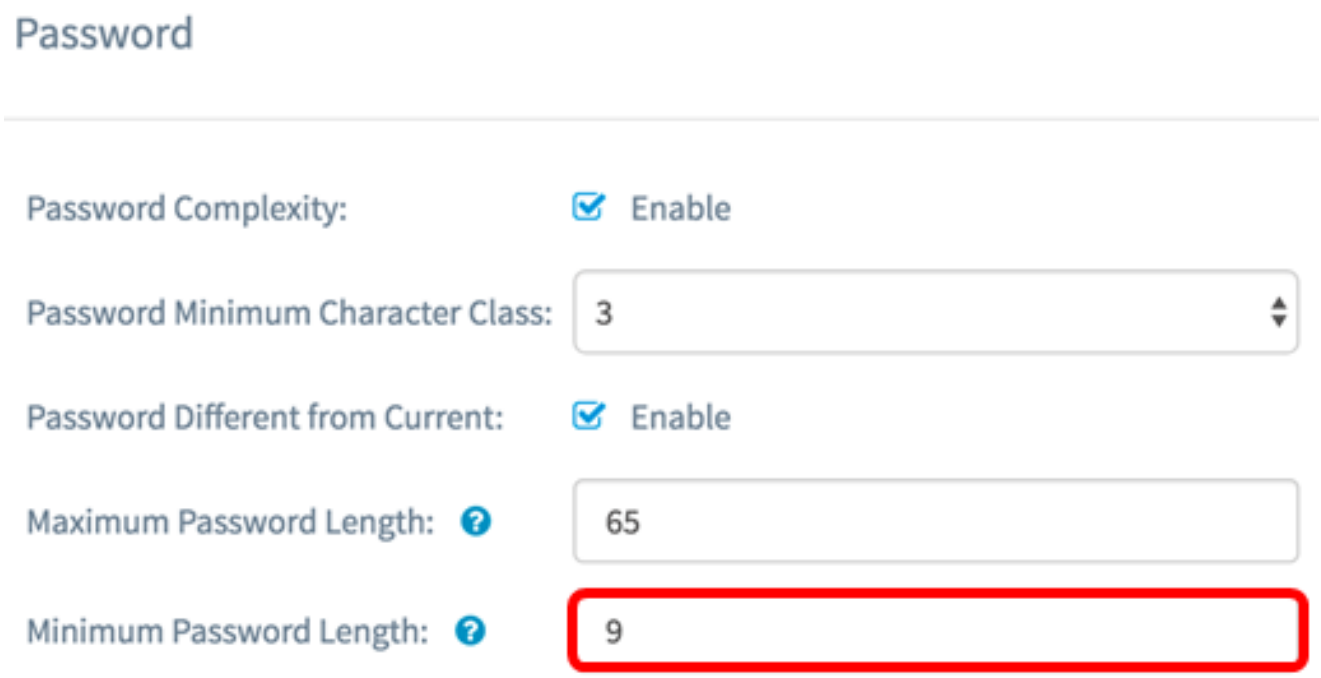
7단계. *최대 비밀번호 길이* 필드에 64~127의 값을 입력하여 비밀번호 문자 수와 길이를 정의합니다.기본값은 64입니다.

참고:이 예에서는 65가 사용됩니다.

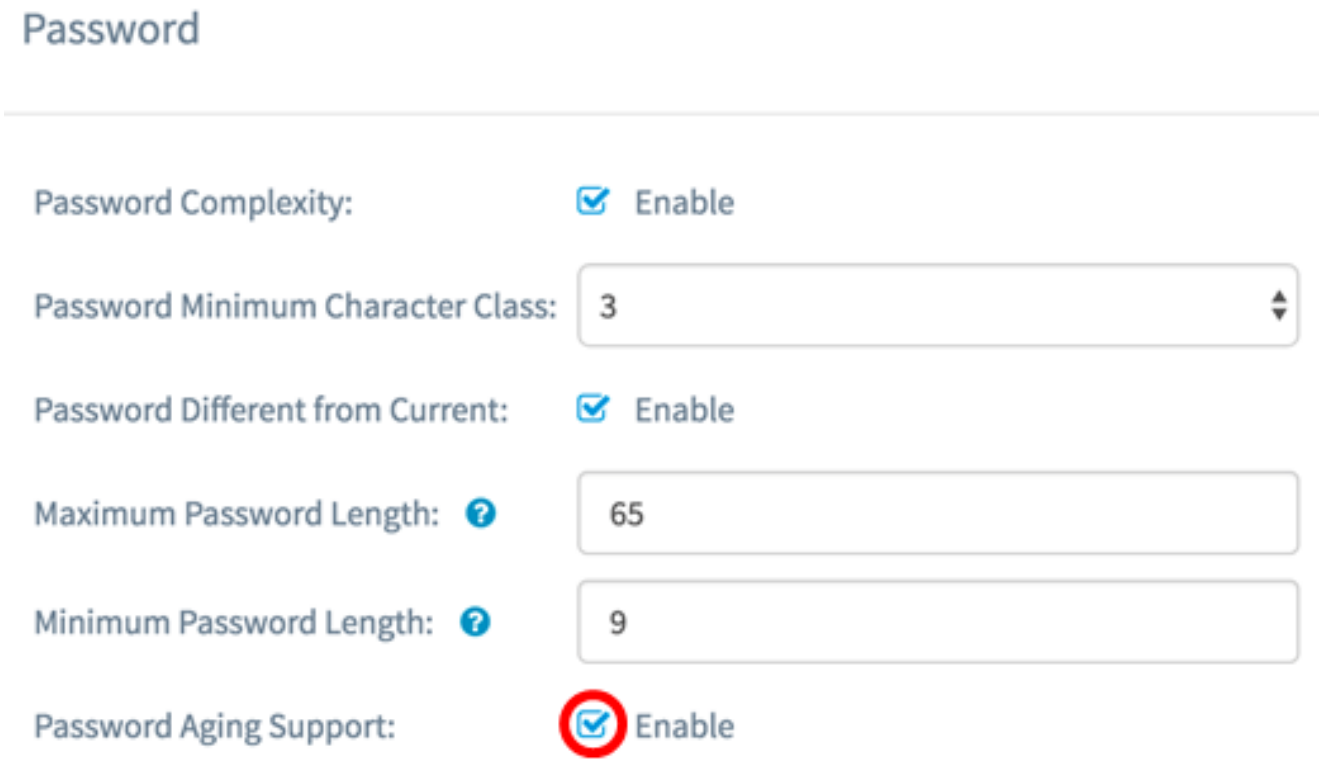


8단계. *최소 비밀번호 길이* 필드에 0~32의 값을 입력하여 비밀번호에 필요한 최소 문자 수를 설정합니다.기본값은 8입니다.

참고:이 예에서 최소 비밀번호 길이는 9입니다.

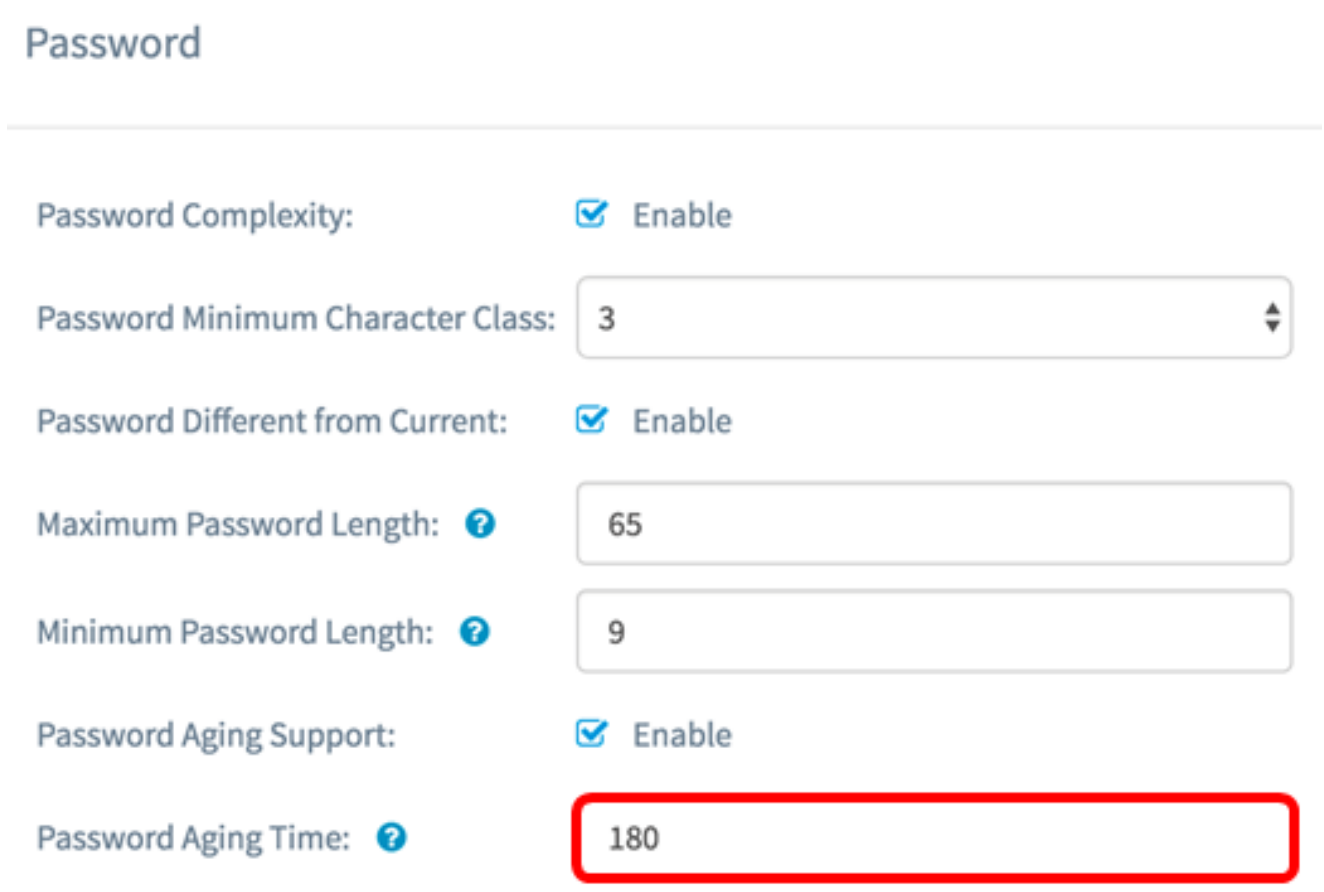


9단계. 비밀번호가 만료되도록 하려면 Enable Password Aging Support 확인란을 선택합니다 .이 옵션이 활성화된 경우 다음 단계로 진행하거나, 그렇지 않으면 로 건너뜁니다.

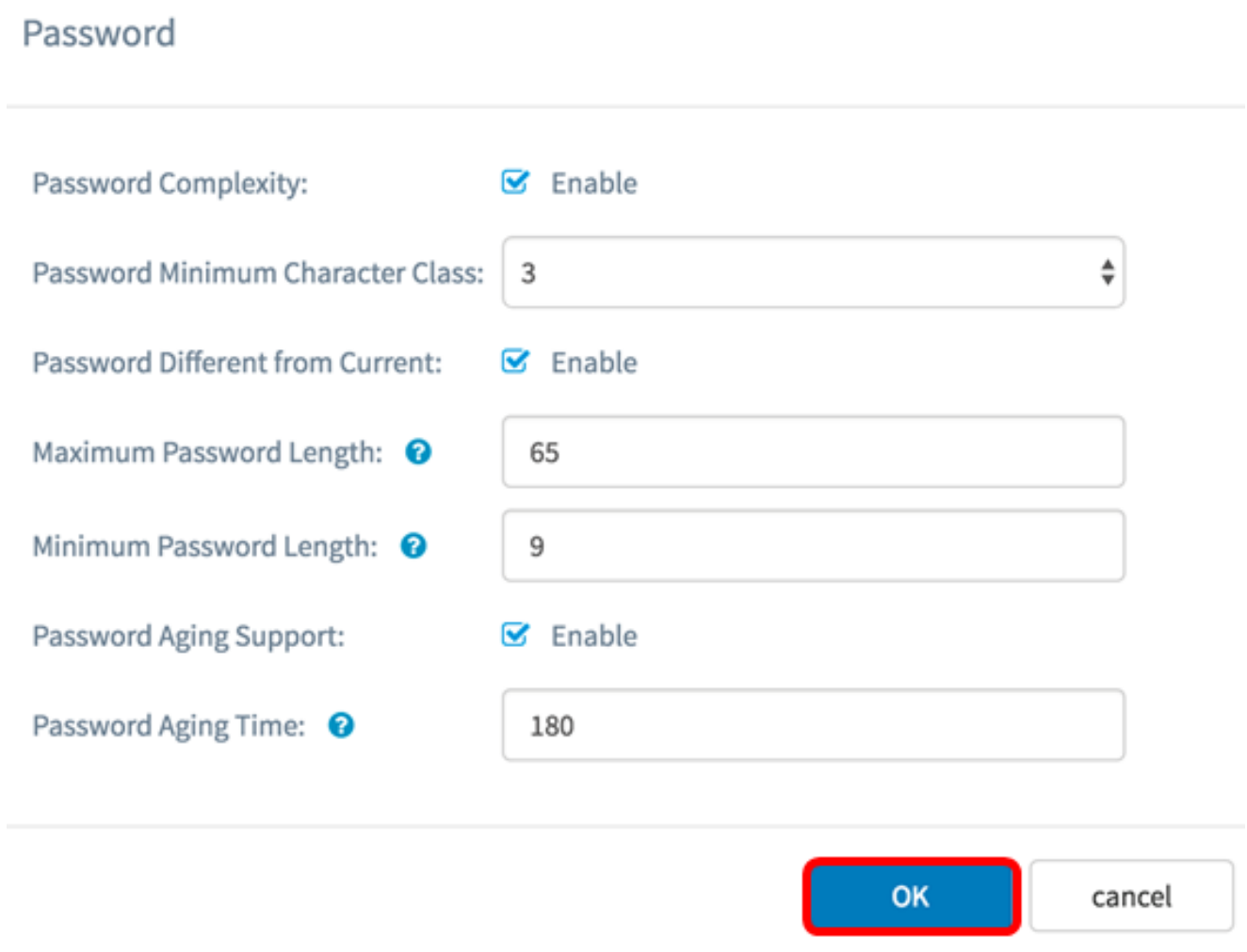


10단계. *Password Aging Time* 필드에 1~365의 값을 입력하여 새로 생성된 비밀번호가 만료되기 전 일수를 설정합니다.기본값은 180일입니다.

참고:이 예에서는 180이 사용됩니다.



11단계. **확인**을 클릭합니다.기본 보안 구성 페이지로 돌아갑니다.

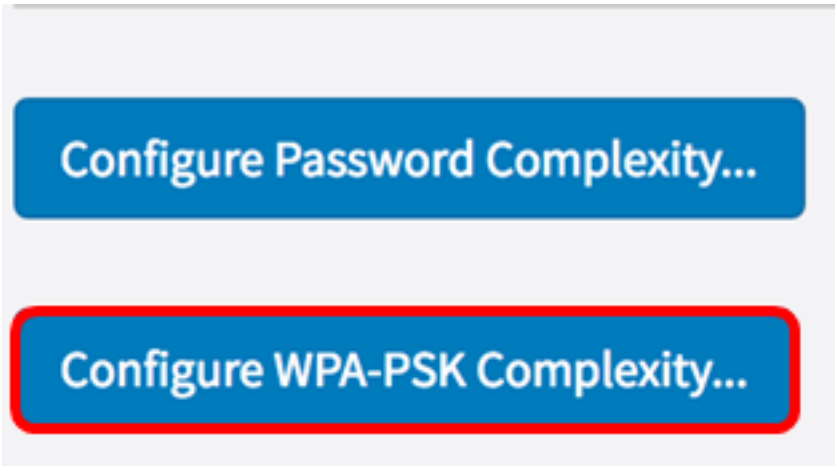


12단계. Save(**저장**) 버튼을 클릭하여 구성된 설정을 저장합니다.

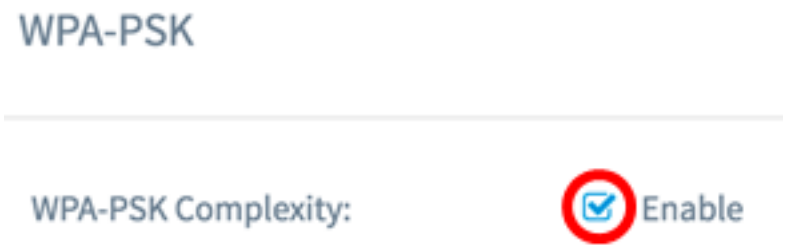
이제 WAP에서 비밀번호 복잡성 보안 설정을 성공적으로 구성했어야 합니다.

WPA-PSK 복잡성 구성

1단계. WPA-**PSK 복잡성 구성** 버튼**을** 클릭합니다.



2단계. **Enable WPA**-PSK Complexity 확인란을 선택하여 비밀번호 복잡성 설정 단계를 활성화합니다.

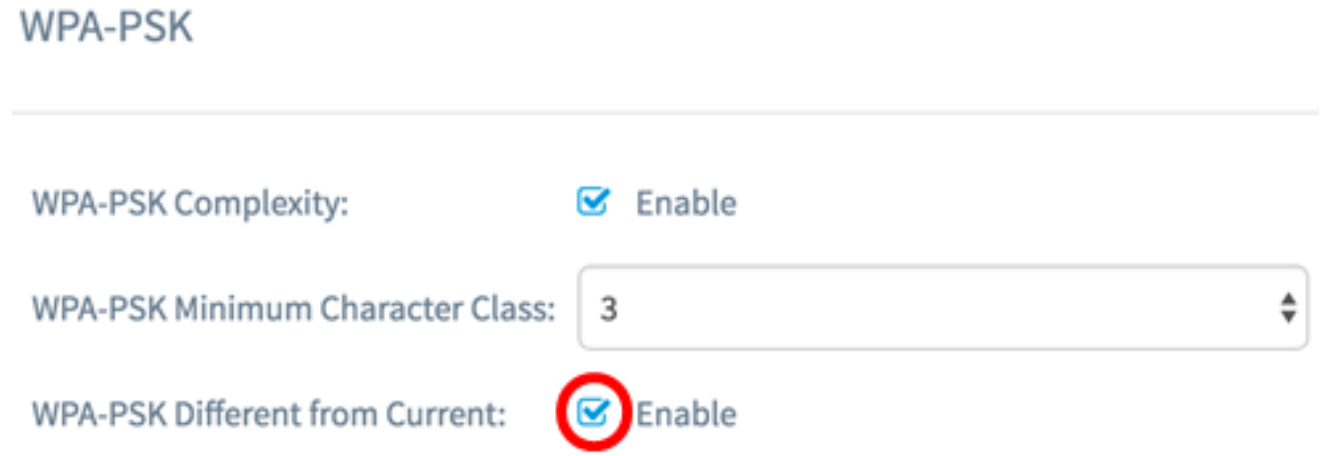


3단계. WPA-PSK 최소 문자 클래스 드롭다운 목록에서 값을 선택합니다.입력한 숫자는 다른 클래스의 최소 또는 최대 문자 수를 나타냅니다.

- 비밀번호는 대문자(ABCD)로 구성됩니다.
- 비밀번호는 소문자(abcd)로 구성됩니다.
- 암호는 숫자 문자(1234)로 구성됩니다.
- 암호는 특수 문자(!@#$)로 구성됩니다.

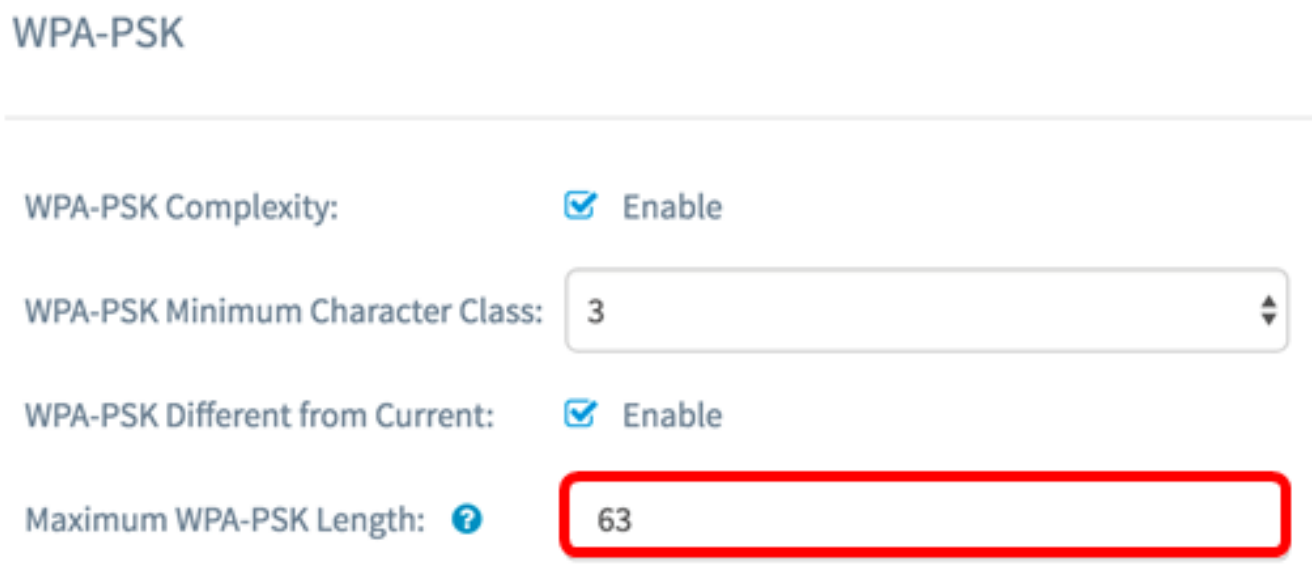
참고:이 예에서는 3이 선택됩니다.

4단계. **Enable WPA**-PSK Different from Current 확인란을 선택하여 사용자가 만료될 때 비밀번호를 업데이트할 수 있도록 합니다.이 옵션을 선택하지 않으면 만료될 때 동일한 비밀번호를 다시 입력할 수 있습니다.



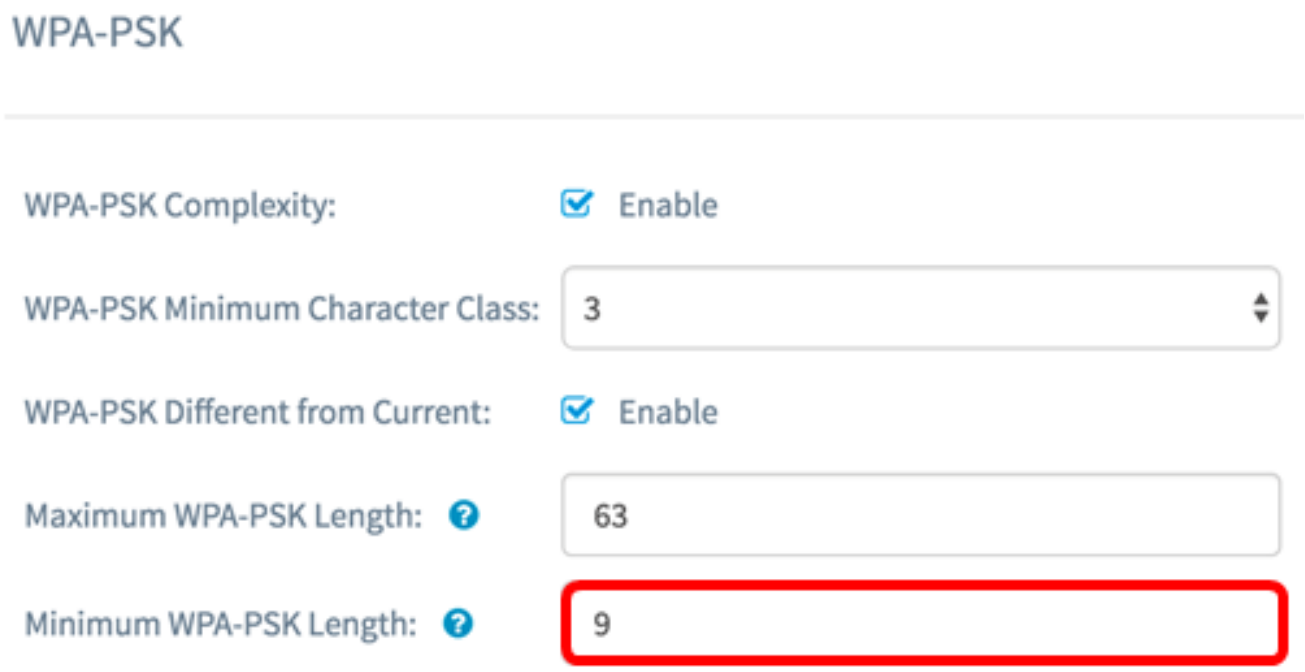
5단계. Maximum *WPA-PSK Length* 필드에 32~63의 값을 입력하여 문자 수와 비밀번호 길이를 정의합니다.기본값은 63입니다.

참고:이 예에서는 63이 사용됩니다.

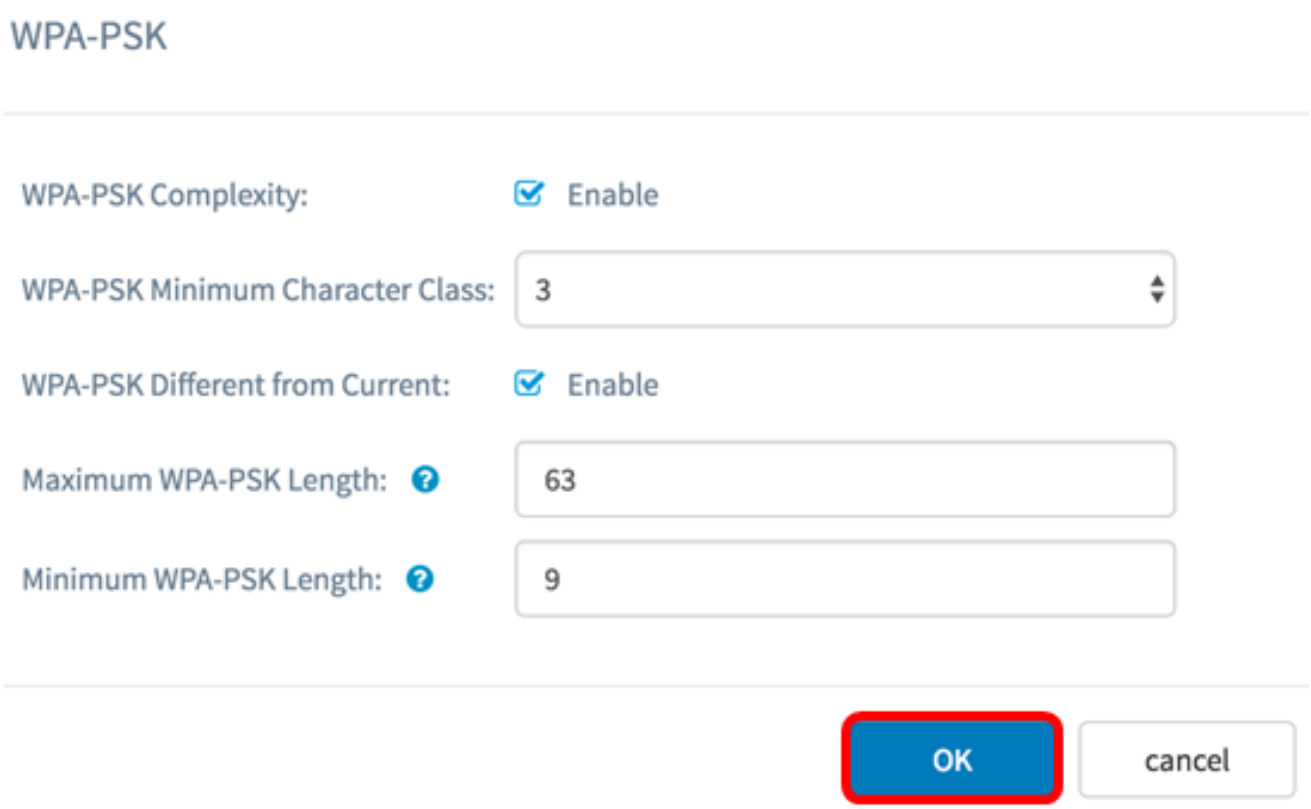


6단계. *Minimum WPA-PSK Length* 필드에 0~32의 값을 입력하여 비밀번호에 필요한 최소 문자 수를 설정합니다.기본값은 8입니다.

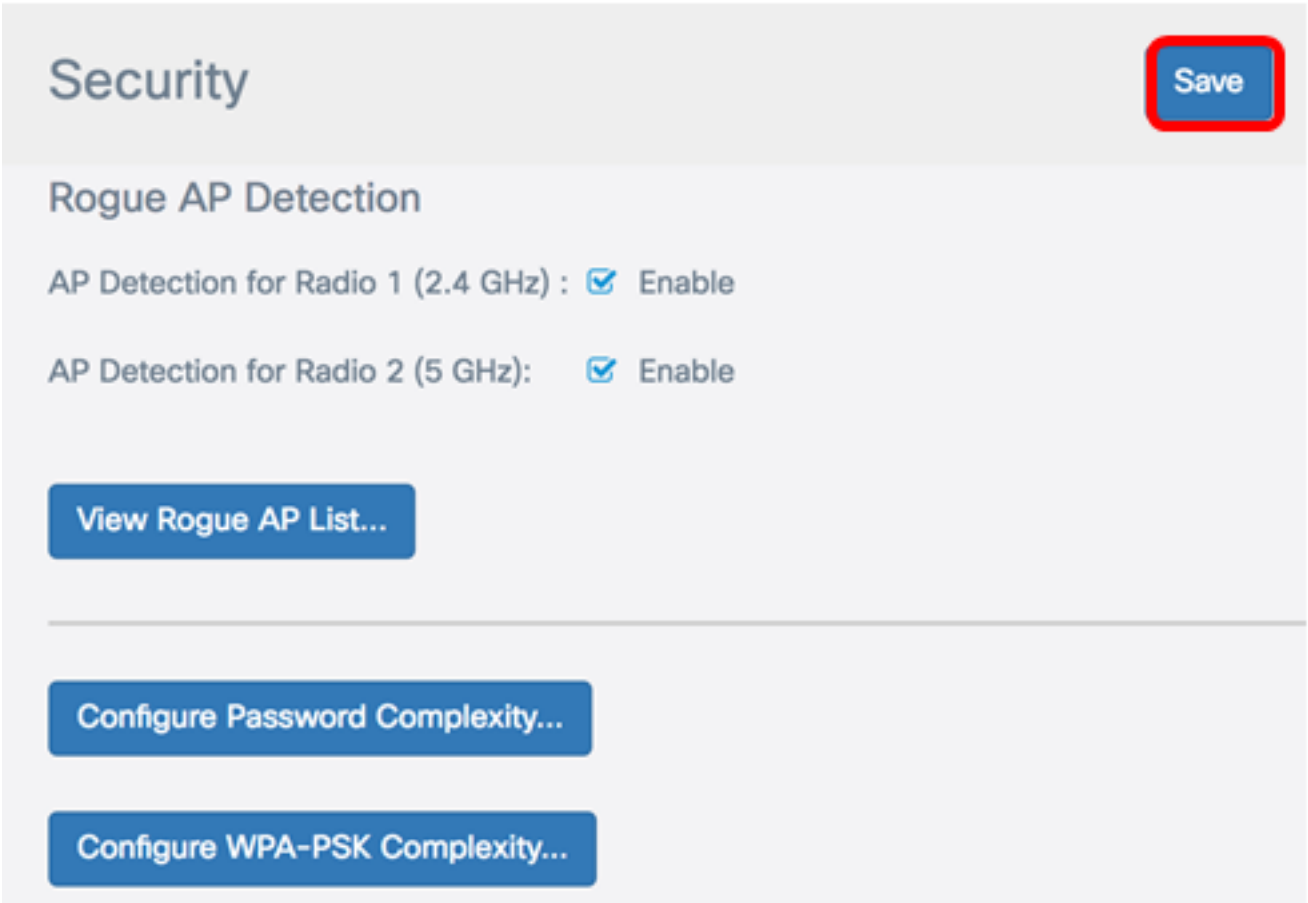
참고:이 예에서 최소 비밀번호 길이는 9입니다.



7단계. **확인**을 클릭합니다.기본 보안 구성 페이지로 돌아갑니다.



8단계. Save(**저장**) 버튼을 클릭하여 구성된 설정을 저장합니다.



이제 WAP에서 WPA-PSK 복잡성 보안 설정을 구성했어야 합니다.