Cisco WAP121 및 WAP321 액세스 포인트의 비밀번호 복잡성 구성

목표

비밀번호 복잡성이 증가하면 보안 침해의 위험이 감소합니다.해커는 보통 몇 시간 안에 길이가 8자 미만인 비밀번호를 해독할 수 있습니다.따라서 대문자와 소문자, 숫자 및 기호를 조합하여 긴 비밀번호를 사용하는 것이 중요합니다.

이 문서에서는 WAP121 및 WAP321 액세스 포인트의 비밀번호 복잡성 구성에 대해 설명합니다.

적용 가능한 디바이스

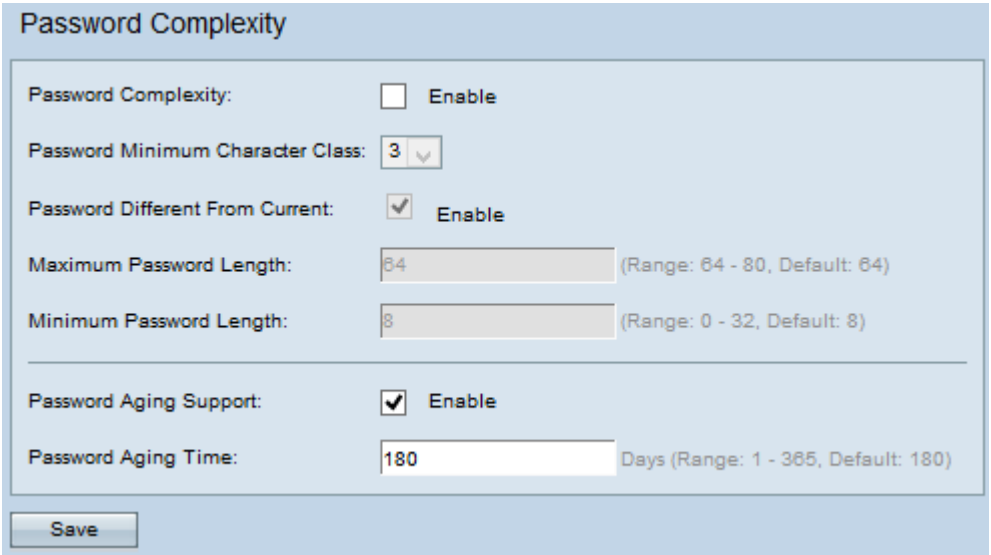
·WAP121
· WAP321

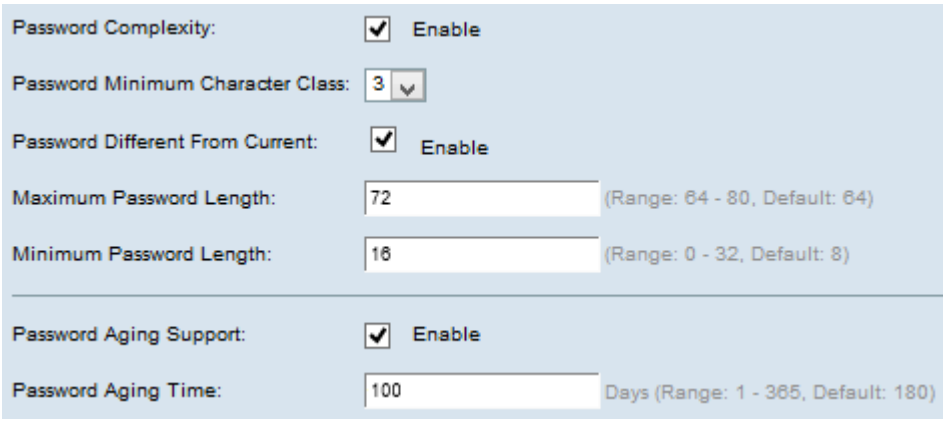
소프트웨어 버전

•1.0.3.4

비밀번호 복잡성 구성

1단계. 웹 구성 유틸리티에 로그인하고 **시스템 보안 > 암호 복잡성**을 선택합니다.비밀번호 *복잡성* 페이지가 열립니다.





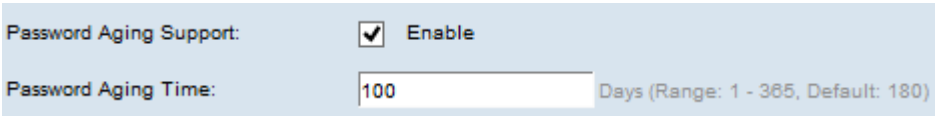
2단계. 비밀번호 복잡성 필드에서 활성화를 선택하여 비밀번호 복잡성을 활성화합니다.

3단계. Password Minimum Character Class 드롭다운 목록에서 적절한 최소 문자 클래스 수를 선택합니다.표준 키보드에서 사용할 수 있는 대문자, 소문자, 숫자 및 특수 문자는 4가지 문자 클래스입니다.

4단계. (선택 사항) 현재 비밀번호가 만료될 때 다른 비밀번호를 입력하도록 하려면 Password Different From Current 필드에서 Enable을 선택합니다.비활성화된 경우 이전에 사용한 것과 동일한 비밀번호를 다시 입력할 수 있습니다.

5단계. Maximum Password Length(최대 비밀번호 길이) 필드에 비밀번호의 최대 문자 수를 입력합니다.범위는 64~80입니다.

6단계. 비밀번호에 포함해야 할 최소 문자 수를 Minimum Password Length 필드에 입력합니다.범위는 0~32입니다.



7단계. (선택 사항) **Enable** in the Password Aging Support(비밀번호 에이징 지원) 필드에서 특정 시간 후에 비밀번호가 만료되도록 선택합니다.

8단계. 이전 단계에서 비밀번호 에이징 지원을 활성화한 경우 비밀번호 에이징 시간 필드에 비밀번호가 만료될 때까지의 일수를 입력합니다.범위는 1~365일입니다.

9단계. **저장**을 클릭하여 설정을 저장합니다.