

# WAP에서 무선 보안 설정 구성

## 소개

무선 액세스 포인트(WAP)에 무선 보안을 구성하는 것은 무선 장치의 개인 정보 및 무선 네트워크를 통해 전송되는 데이터를 손상시킬 수 있는 침입자로부터 무선 네트워크를 보호하는 데 매우 중요합니다. MAC 필터, WPA/WPA2(Wi-Fi Protected Access) Personal 및 WPA/WPA2 Enterprise를 설정하여 무선 네트워크에서 무선 보안을 구성할 수 있습니다.

MAC 필터링은 무선 클라이언트가 MAC 주소를 사용하여 네트워크에 액세스하도록 필터링하는 데 사용됩니다. 기본 설정에 따라 목록의 주소가 네트워크에 액세스하도록 허용하거나 차단하도록 클라이언트 목록이 구성됩니다. MAC 필터링에 대한 자세한 내용을 보려면 [여기](#)를 클릭하십시오.

WPA/WPA2 Personal 및 WPA/WPA2 Enterprise는 무선 네트워크를 통해 전송된 데이터를 암호화하여 개인 정보를 보호하는 데 사용되는 보안 프로토콜입니다. WPA/WPA2는 IEEE 표준 802.11E 및 802.11i와 호환됩니다. WEP(Wired Equivalent Privacy) 보안 프로토콜과 비교하여 WPA/WPA2는 인증 및 암호화 기능을 개선했습니다.

WPA/WPA2 Personal은 가정용 제품이며 WPA/WPA2 Enterprise는 비즈니스 규모 네트워크용입니다. WPA/WPA2 Enterprise는 WPA/WPA2 Personal에 비해 네트워크에 대한 보안 및 중앙 집중식 제어를 강화합니다.

이 시나리오에서는 WPA/WPA2 개인 및 엔터프라이즈 설정을 사용하여 네트워크를 침입으로부터 보호하기 위해 WAP에 무선 보안이 구성됩니다.

## 목표

이 문서에서는 무선 네트워크의 보안 및 개인 정보를 개선하기 위해 WPA/WPA2 개인 및 기업 보안 프로토콜을 구성하는 방법을 보여 줍니다.

**참고:** 이 문서에서는 WAP에서 SSID(Service Set Identifier) 또는 WLAN(Wireless Local Area Network)이 이미 생성되었다고 가정합니다.

## 적용 가능한 디바이스

- WAP100 시리즈
- WAP300 시리즈
- WAP500 시리즈

## 소프트웨어 버전

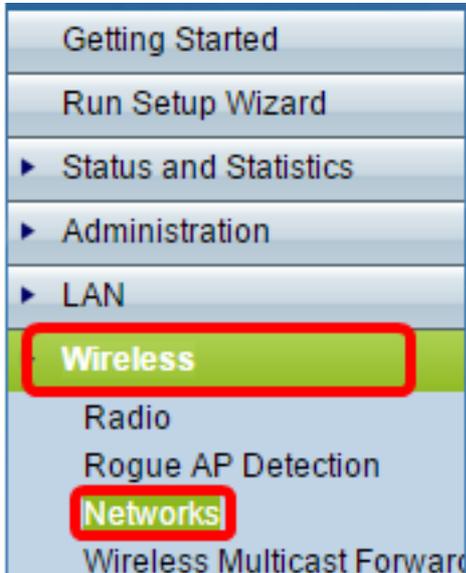
- 1.0.2.14 - WAP131, WAP351
- 1.0.6.5 - WAP121, WAP321
- 1.3.0.4 - WAP371
- 1.1.0.7 - WAP150, WAP361
- 1.2.1.5 - WAP551, WAP561
- 1.0.1.11 - WAP571, WAP571E

# 무선 보안 설정 구성

## WPA/WPA2 개인 구성

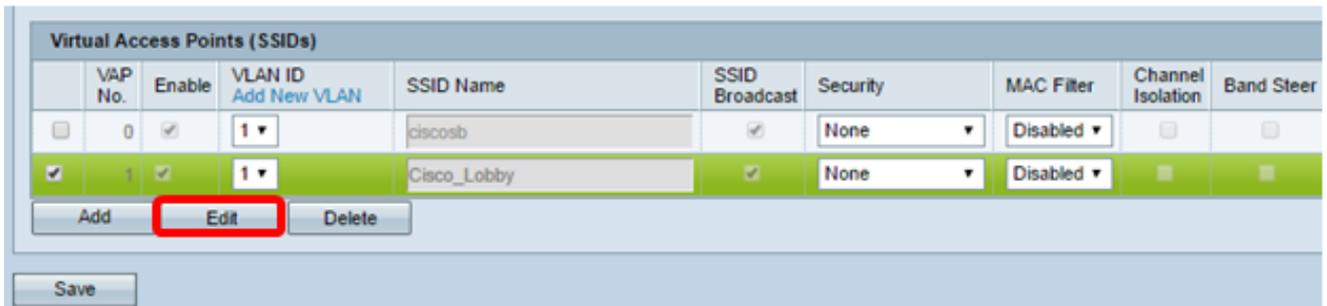
1단계. 액세스 포인트의 웹 기반 유틸리티에 로그인하고 **무선 > 네트워크**를 선택합니다.

**참고:**아래 그림에서 WAP361의 웹 기반 유틸리티가 예로 사용됩니다.메뉴 옵션은 디바이스의 모델에 따라 달라질 수 있습니다.

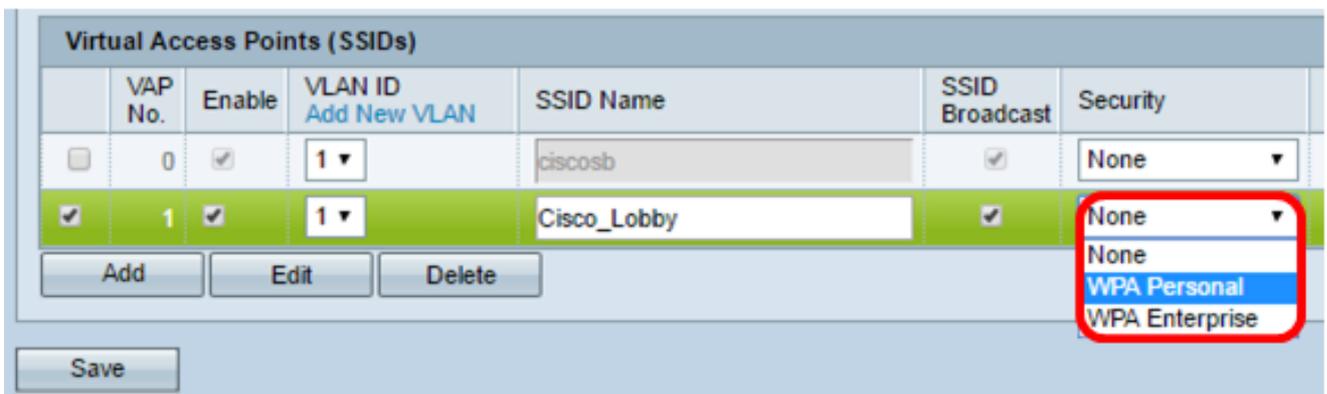


2단계. Virtual Access Points (SSIDs)(가상 액세스 포인트(SSID)) 영역 아래에서 구성할 SSID의 확인란을 선택하고 Edit(수정)를 클릭합니다.

**참고:**이 예에서는 VAP1이 선택됩니다.



3단계. 보안 드롭다운 목록에서 **WPA 개인**을 클릭합니다.

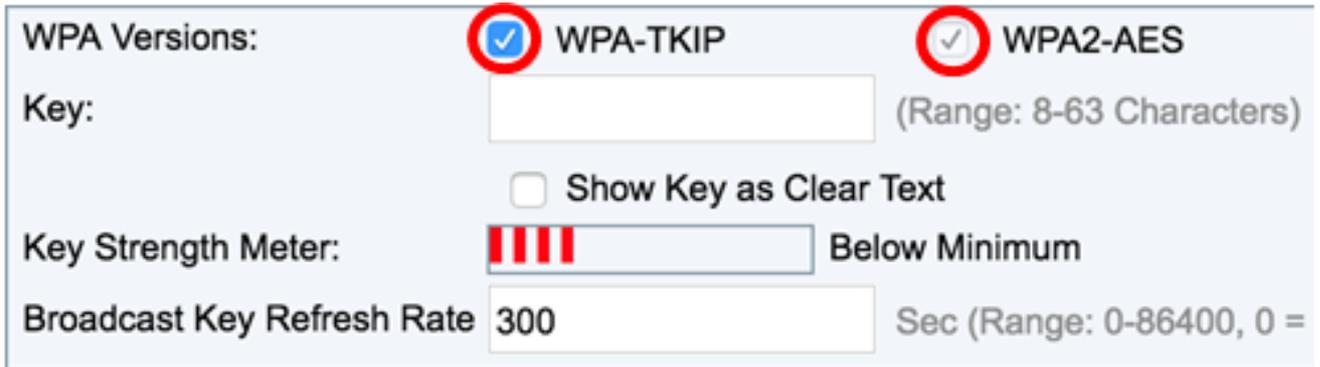


4단계. 확인란을 선택하여 WPA 버전(WPA-TKIP 또는 WPA2-AES)을 선택합니다.두 개를 동

시에 선택할 수 있습니다.

- WPA-TKIP — Wi-Fi 보호 액세스 임시 키 무결성 도구네트워크에는 원래 WPA 및 TKIP 보안 프로토콜만 지원하는 일부 클라이언트 스테이션이 있습니다. 최신 Wi-Fi 제휴 요구 사항에 따라 액세스 포인트에 대해 WPA-TKIP만 선택할 수 없습니다.
- WPA2-AES — Wi-Fi 보호 액세스 고급 암호화 표준네트워크의 모든 클라이언트 스테이션은 WPA2 및 AES-CCMP 암호/보안 프로토콜을 지원합니다. 이 WPA 버전은 IEEE 802.11i 표준에 따라 최상의 보안을 제공합니다. 최신 Wi-Fi Alliance 요건에 따라 WAP는 항상 이 모드를 지원해야 합니다.

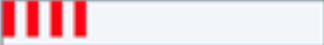
참고: 이 예제에서는 두 확인란을 모두 선택합니다.



WPA Versions:  WPA-TKIP  WPA2-AES

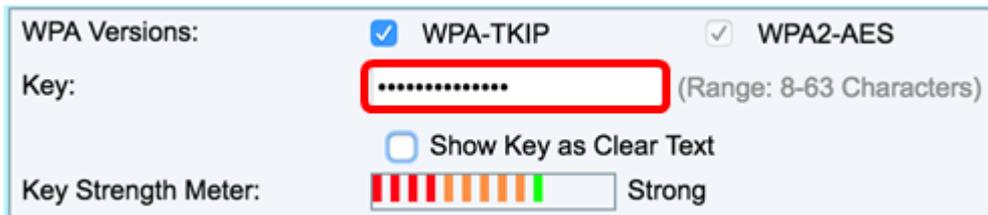
Key:  (Range: 8-63 Characters)

Show Key as Clear Text

Key Strength Meter:  Below Minimum

Broadcast Key Refresh Rate  Sec (Range: 0-86400, 0 =

5단계. 8-63자로 구성된 비밀번호를 생성하고 Key 필드에 입력합니다.



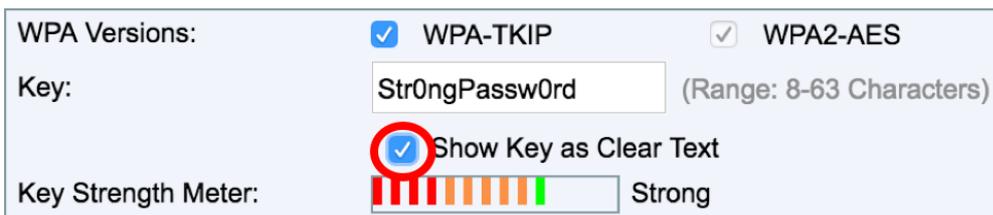
WPA Versions:  WPA-TKIP  WPA2-AES

Key:  (Range: 8-63 Characters)

Show Key as Clear Text

Key Strength Meter:  Strong

참고: Show Key as Clear Text(키를 Clear Text로 표시) 상자를 선택하여 생성한 비밀번호를 표시할 수 있습니다.



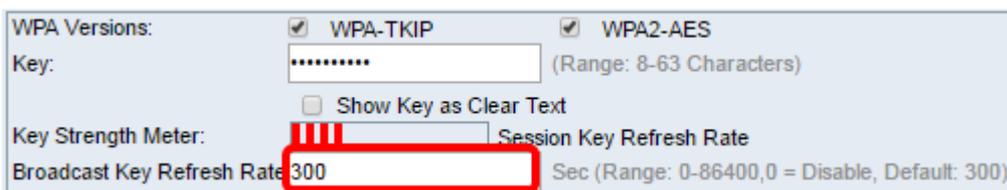
WPA Versions:  WPA-TKIP  WPA2-AES

Key:  (Range: 8-63 Characters)

Show Key as Clear Text

Key Strength Meter:  Strong

6단계. (선택 사항) Broadcast Key Refresh Rate(브로드캐스트 키 새로 고침 빈도) 필드에 이 VAP와 연결된 클라이언트에 대해 브로드캐스트(그룹) 키를 새로 고칠 간격을 입력합니다. 기본값은 300초이며 유효한 범위는 0~86400초입니다. 값이 0이면 브로드캐스트 키가 새로 고쳐지지 않음을 나타냅니다.



WPA Versions:  WPA-TKIP  WPA2-AES

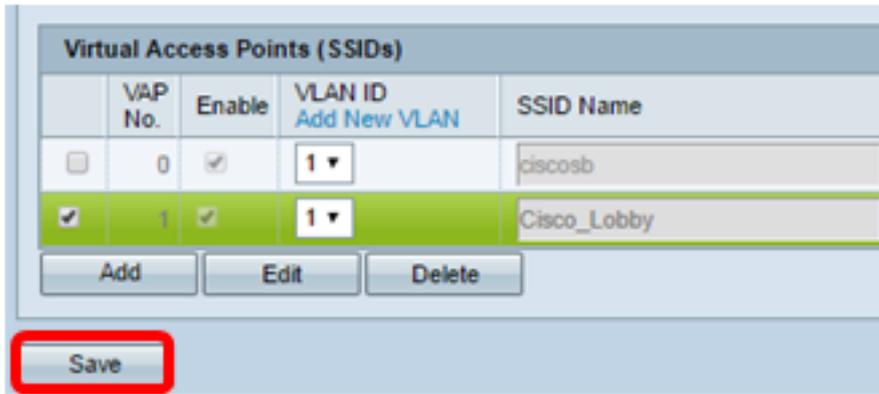
Key:  (Range: 8-63 Characters)

Show Key as Clear Text

Key Strength Meter:  Session Key Refresh Rate

Broadcast Key Refresh Rate  Sec (Range: 0-86400, 0 = Disable, Default: 300)

7단계. 저장을 클릭합니다.

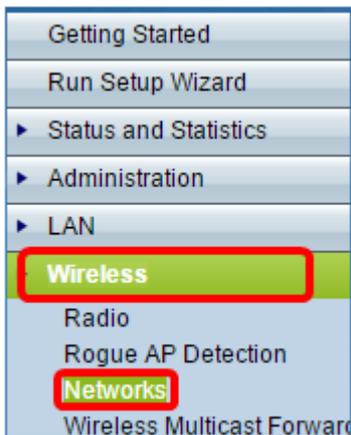


이제 WAP에서 WPA Personal을 구성했습니다.

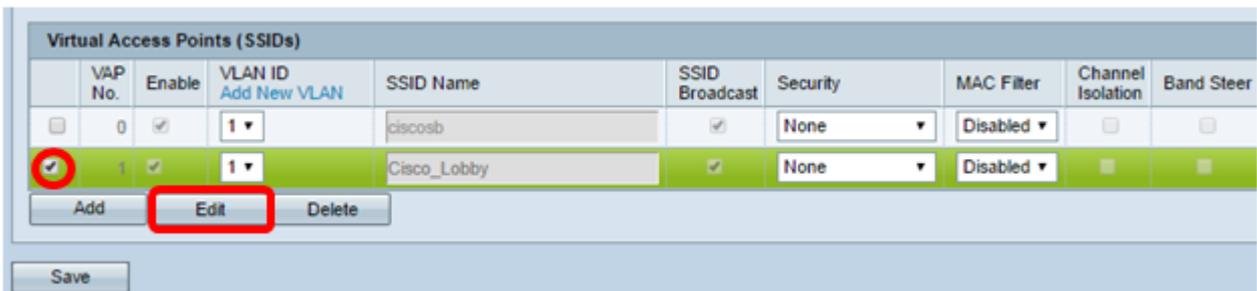
## WPA/WPA2 엔터프라이즈 구성

1단계. 액세스 포인트의 웹 기반 유틸리티에 로그인하고 무선 > 네트워크를 선택합니다.

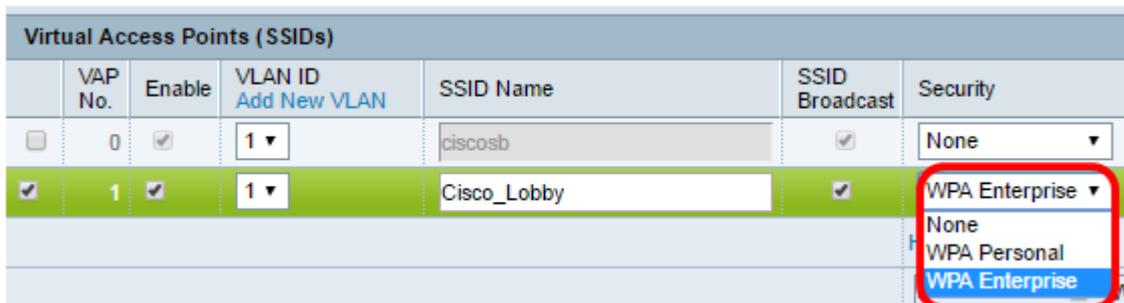
참고:아래 그림에서 WAP361의 웹 기반 유틸리티가 예로 사용됩니다.



2단계. Virtual Access Points (SSIDs)(가상 액세스 포인트(SSID)) 영역 아래에서 구성할 SSID를 선택하고 아래에 있는 Edit(편집) 버튼을 클릭합니다.



3단계. 보안 드롭다운 목록에서 WPA Enterprise를 선택합니다.



4단계. WPA 버전(WPA-TKIP, WPA2-AES 및 사전 인증 사용)을 선택합니다.

- 사전 인증 활성화— WPA 버전으로 WPA2-AES만 또는 WPA-TKIP 및 WPA2-AES를 모두 선택한 경우 WPA2-AES 클라이언트에 대해 사전 인증을 활성화할 수 있습니다. WPA2 무선 클라이언트가 사전 인증 패킷을 전송하도록 하려면 이 옵션을 선택합니다. 사전 인증 정보는 클라이언트가 현재 사용 중인 WAP 디바이스에서 대상 WAP 디바이스로 릴레이됩니다. 이 기능을 활성화하면 여러 AP(액세스 포인트)에 연결하는 로밍 클라이언트에 대한 인증 속도를 높일 수 있습니다.

**참고:** 원래 WPA는 이 기능을 지원하지 않으므로 WPA 버전에 대해 WPA-TKIP를 선택한 경우에는 이 옵션이 적용되지 않습니다.

Hide Details

WPA Versions:  WPA-TKIP  WPA2-AES  
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type:  IPv4  IPv6

Server IP Address-1: 192.168.1.101 (xxx.xxx.xxx.xxx)  
Server IP Address-2: (xxx.xxx.xxx.xxx)  
Server IP Address-3: (xxx.xxx.xxx.xxx)  
Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: ..... (Range: 1 - 64 Characters)  
Key-2: ..... (Range: 1 - 64 Characters)  
Key-3: ..... (Range: 1 - 64 Characters)  
Key-4: ..... (Range: 1 - 64 Characters)

Enable RADIUS Accounting

Active Server: Server IP Address-1 ▼

Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400, 0 = Disable, Default: 300)

Session Key Refresh Rate: 0 Sec (Range: 30-86400, 0 = Disable, Default: 0)

5단계. (선택 사항) Use global RADIUS server settings(전역 RADIUS 서버 설정 사용) 확인란을 선택 취소하여 설정을 편집합니다.



WPA Versions:  WPA-TKIP  WPA2-AES  
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type:  IPv4  IPv6

Server IP Address-1:  (xxx.xxx.xxx.xxx)  
Server IP Address-2:  (xxx.xxx.xxx.xxx)  
Server IP Address-3:  (xxx.xxx.xxx.xxx)  
Server IP Address-4:  (xxx.xxx.xxx.xxx)

Key-1:  (Range: 1 - 64 Characters)  
Key-2:  (Range: 1 - 64 Characters)  
Key-3:  (Range: 1 - 64 Characters)  
Key-4:  (Range: 1 - 64 Characters)

Enable RADIUS Accounting

Active Server:  ▼

Broadcast Key Refresh Rate:  Sec (Range: 0-86400, 0 = Disable, Default: 300)  
Session Key Refresh Rate:  Sec (Range: 30-86400, 0 = Disable, Default: 0)

7단계. Server IP Address 필드에 RADIUS 서버의 IP 주소를 입력합니다.

참고: 이 예에서는 192.168.1.101이 사용됩니다.

WPA Versions:  WPA-TKIP  WPA2-AES  
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type:  IPv4  IPv6

Server IP Address-1:  (xxx.xxx.xxx.xxx)  
Server IP Address-2:  (xxx.xxx.xxx.xxx)  
Server IP Address-3:  (xxx.xxx.xxx.xxx)  
Server IP Address-4:  (xxx.xxx.xxx.xxx)

Key-1:  (Range: 1 - 64 Characters)  
Key-2:  (Range: 1 - 64 Characters)  
Key-3:  (Range: 1 - 64 Characters)  
Key-4:  (Range: 1 - 64 Characters)

Enable RADIUS Accounting

Active Server:  ▼

Broadcast Key Refresh Rate:  Sec (Range: 0-86400, 0 = Disable, Default: 300)  
Session Key Refresh Rate:  Sec (Range: 30-86400, 0 = Disable, Default: 0)

8단계. Key(키) 필드에 WAP가 RADIUS 서버를 인증하는 데 사용하는 RADIUS 서버에 해당하는 비밀번호 키를 입력합니다. 1~64 표준 영숫자 및 특수 문자를 사용할 수 있습니다.

**참고:** 키는 대/소문자를 구분하며 RADIUS 서버에 구성된 키와 일치해야 합니다.

9단계. (선택 사항) WAP가 통신할 네트워크의 모든 RADIUS 서버에 대해 7-8단계를 반복합니다.



WPA Versions:  WPA-TKIP  WPA2-AES  
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type:  IPv4  IPv6

Server IP Address-1:  (xxx.xxx.xxx.xxx)  
Server IP Address-2:  (xxx.xxx.xxx.xxx)  
Server IP Address-3:  (xxx.xxx.xxx.xxx)  
Server IP Address-4:  (xxx.xxx.xxx.xxx)

Key-1:  (Range: 1 - 64 Characters)  
Key-2:  (Range: 1 - 64 Characters)  
Key-3:  (Range: 1 - 64 Characters)  
Key-4:  (Range: 1 - 64 Characters)

Enable RADIUS Accounting

Active Server:  ▼

Broadcast Key Refresh Rate:  Sec (Range: 0-86400, 0 = Disable, Default: 300)  
Session Key Refresh Rate:  Sec (Range: 30-86400, 0 = Disable, Default: 0)

11단계. 을 클릭합니다 .

이제 WAP에 WPA/WPA2 엔터프라이즈 보안을 성공적으로 구성했습니다.