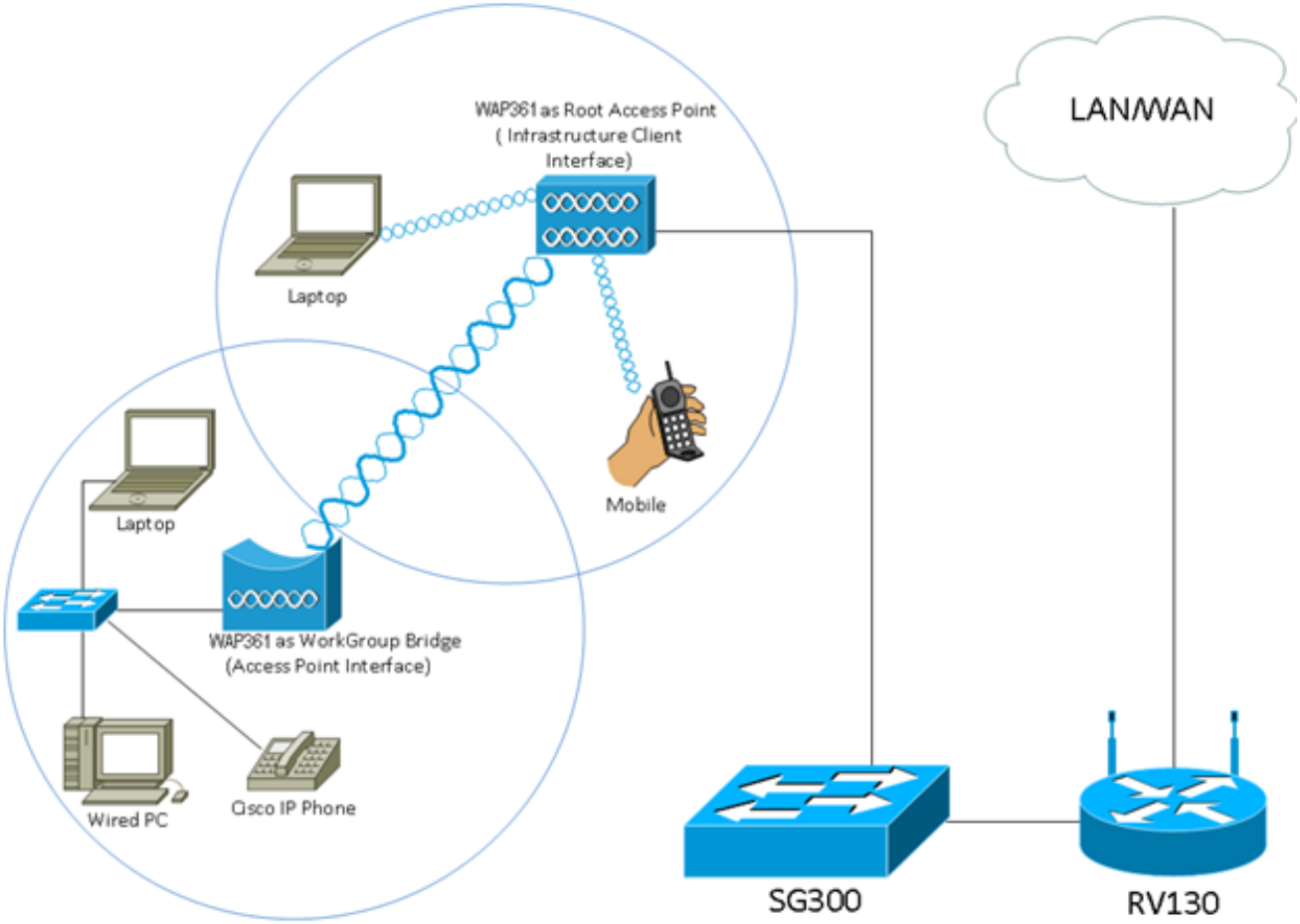
WAP(Wireless Access Point)에서 작업 그룹 브리지 구성

목표

WorkGroup Bridge 기능을 사용하면 WAP(Wireless Access Point)가 원격 클라이언트와 WorkGroup Bridge Mode에 연결된 무선 LAN(Local Area Network) 간의 트래픽을 연결할 수 있습니다.원격 인터페이스와 연결된 WAP 디바이스를 액세스 포인트 인터페이스로, 무선 LAN과 연결된 WAP 디바이스를 인프라 인터페이스로 알려져 있습니다.WorkGroup Bridge를 사용하면 유선 연결만 있는 디바이스가 무선 네트워크에 연결할 수 있습니다.WDS(Wireless Distribution System) 기능을 사용할 수 없는 경우 작업 그룹 브리지 모드를 대안으로 권장합니다.



참고:위의 토폴로지는 샘플 WorkGroup Bridge 모델을 보여줍니다.유선 장치는 WAP의 LAN 인터페이스에 연결되는 스위치에 테더링됩니다.WAP는 액세스 포인트 인터페이스 역할을 하며 인프라 인터페이스에 연결됩니다.

이 문서에서는 두 WAP 간에 WorkGroup Bridge를 구성하는 방법을 보여 줍니다.

적용 가능한 디바이스

- WAP100 시리즈
- WAP300 시리즈
- WAP500 시리즈

소프트웨어 버전

- 1.0.0.17 —WAP571, WAP571E
- 1.0.1.7 — WAP150, WAP361
- 1.0.2.5 — WAP131, WAP351
- 1.0.6.5 — WAP121, WAP321
- 1.2.1.3 — WAP551, WAP561
- 1.3.0.3 — WAP371

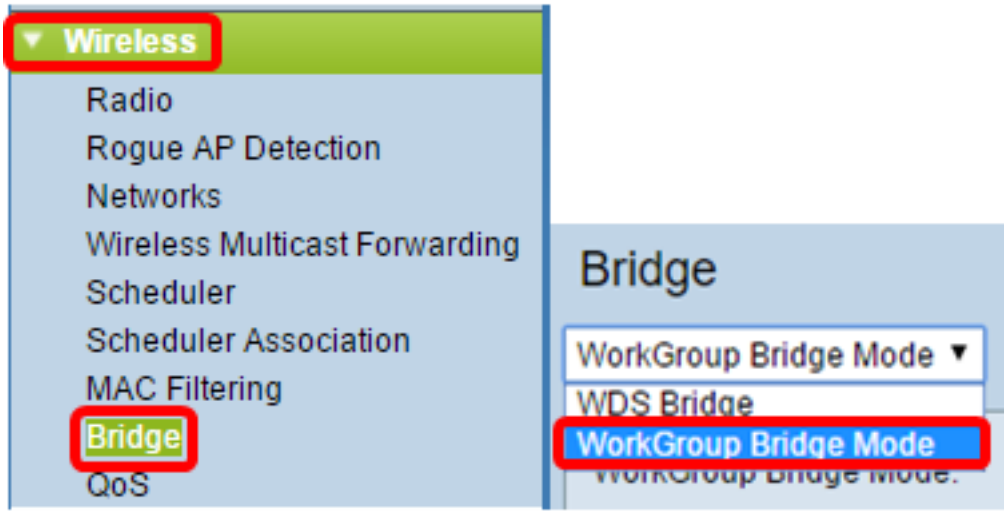
WorkGroup 브리지 구성

인프라 클라이언트 인터페이스

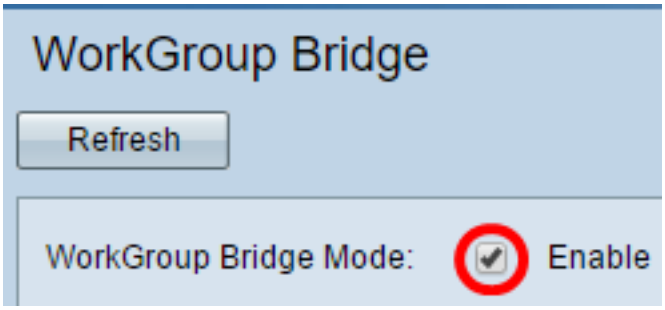
1단계. WAP의 웹 기반 유틸리티에 로그인하고 **무선 > WorkGroup Bridge**를 선택합니다.

참고:메뉴 옵션은 사용 중인 디바이스의 모델에 따라 달라질 수 있습니다.별도의 언급이 없는 한 아래 이미지는 WAP361에서 가져온 것입니다.

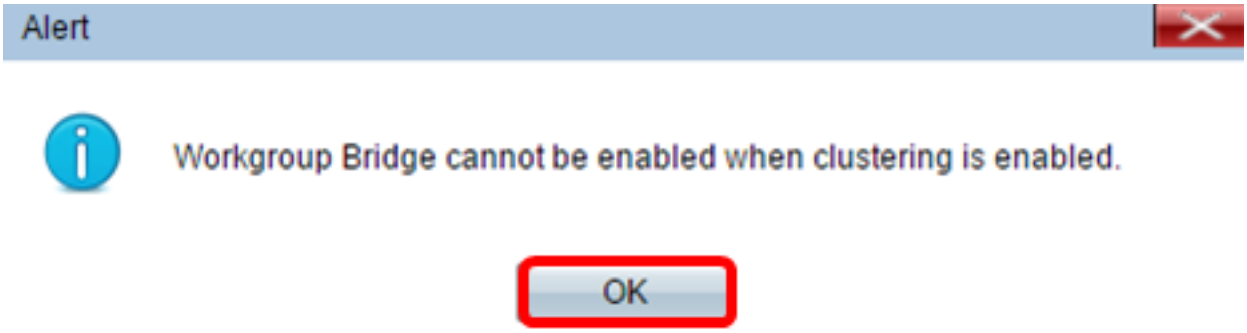
WAP571 및 WAP571E의 경우 **Wireless > Bridge > WorkGroup Bridge Mode**를 선택합니다.



2단계. Enable **WorkGroup** Bridge Mode(작업 그룹 브리지 모드 활성화) 확인란을 선택합니다.

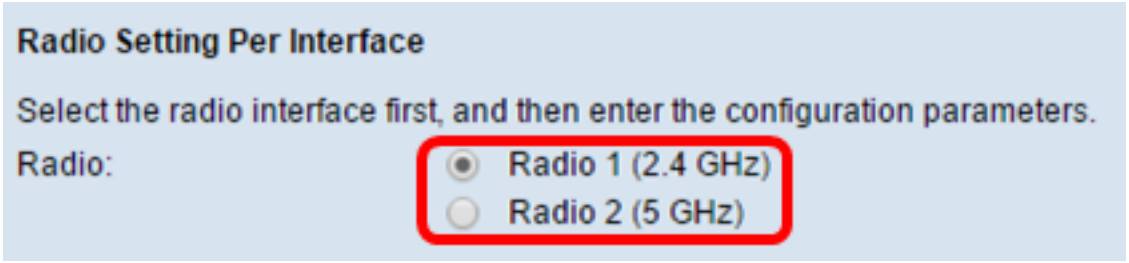


참고:WAP에서 클러스터링이 활성화된 경우, WorkGroup Bridge가 작동하기 위해 팝업에서 클러스터링을 비활성화하라는 메시지를 표시합니다.OK(**확인**)를 클릭하여 계속합니다.클러스터링을 비활성화하려면 탐색 창에서 **Single Point Setup(단일 지점 설정)**을 선택한 다음 Access Points(액세스 포인트) **> Disable Single Point Setup(단일 지점 설정 비활성화)을 선택합니다**.



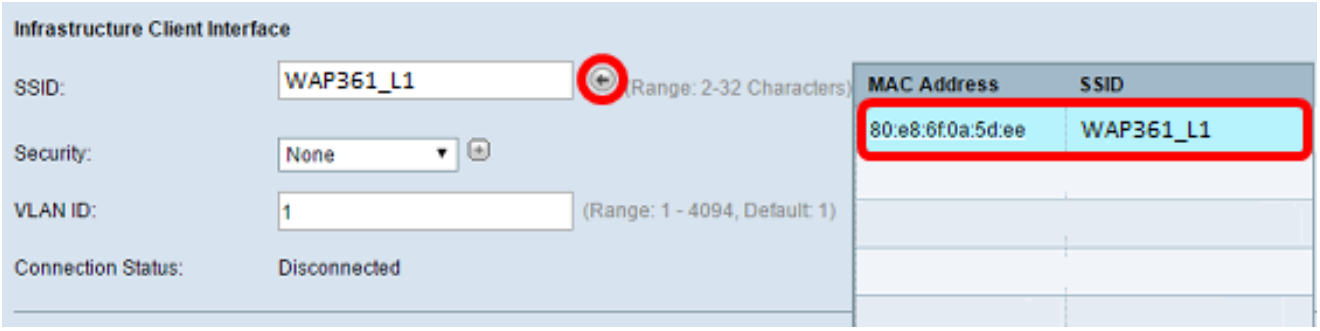
3단계. WorkGroup Bridge의 라디오 인터페이스를 클릭합니다.한 라디오를 WorkGroup Bridge로 구성하면 다른 라디오가 계속 작동합니다.무선 인터페이스는 WAP의 무선 주파수 대역폭에 해당합니다.WAP는 서로 다른 두 라디오 인터페이스에서 브로드캐스트할 수 있습니다.한 라디오 인터페이스에 대한 설정을 구성해도 다른 라디오 인터페이스에 영향을 주지 않습니다.무선 인터페이스 옵션은 WAP 모델에 따라 달라질 수 있습니다.일부 WAP에서는 라디오 1을 2.4GHz로 표시하고, 일부 WAP에서는 라디오 2를 2.4GHz로 표시합니다.

참고:이 단계는 이중 대역폭이 있는 다음 WAP에 대해서만 수행됩니다.WAP131, WAP150, WAP351, WAP361, WAP371, WAP561, WAP571, WAP571E.이 예에서는 라디오 1이 선택됩니다.



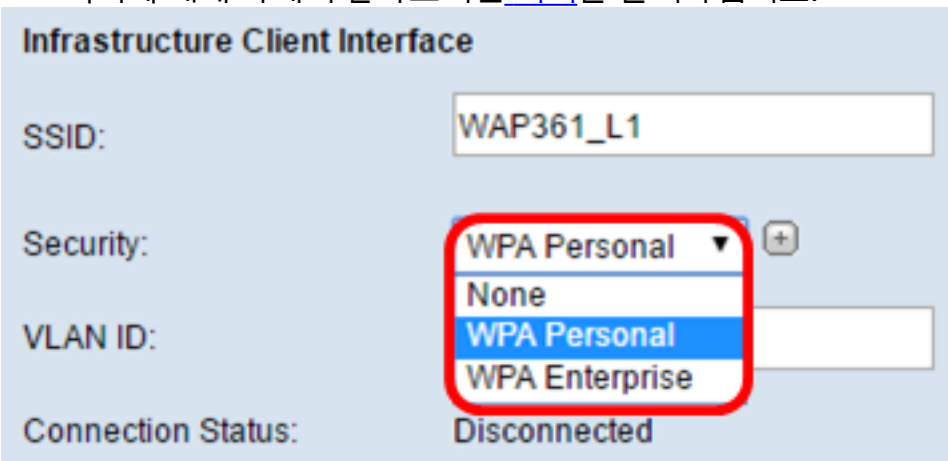
4단계. *SSID* 필드에 SSID(Service Set Identifier) 이름을 입력하거나 필드 옆의 화살표 버튼을 클릭하여 인접 디바이스를 검색합니다.이는 디바이스와 원격 클라이언트 간의 연결 역할을 합니다.인프라 클라이언트 SSID에 2~32자를 입력할 수 있습니다.

참고:비인가 AP 탐지를 활성화하는 것이 중요합니다.해당 기능을 활성화하는 방법에 대한 자세한 내용을 보려면 여기를 클릭하십시오.이 예에서 화살표 버튼을 클릭하여 인프라 클라이언트 인터페이스의 SSID로 WAP361_L1을 선택합니다.



5단계. Infrastructure Client Interface(인프라 클라이언트 인터페이스) 영역의 Security(보안) 드롭다운 목록에서 업스트림 WAP 디바이스에서 클라이언트 스테이션으로 인증할 보안 유형을 선택합니다.옵션은 다음과 같습니다.

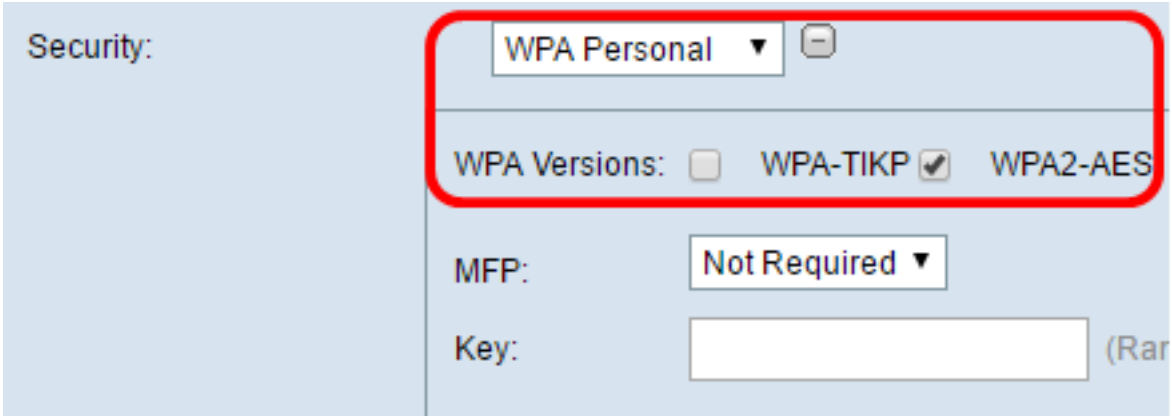
- None(없음) — Open(열기) 또는 No Security(보안 없음).이것이 기본값입니다.이 옵션을 선택한 경우 18단계로 건너뜁니다.
- WPA Personal — WPA Personal은 8-63자의 키를 지원할 수 있습니다.WPA2는 보다 강력한 암호화 표준을 사용하므로 권장됩니다.구성하려면 6단계로 건너뜁니다.
- WPA Enterprise — WPA Enterprise는 WPA Personal보다 진보적이며 인증에 권장되는 보안입니다.PEAP(Protected Extensible Authentication Protocol) 및 TLS(Transport Layer Security)를 사용합니다. 구성하려면 9단계로 건너뜁니다.이러한 유형의 보안은 사무실 환경에서 자주 사용되며 RADIUS(Remote Authentication Dial-In User Service) 서버를 구성해야 합니다.RADIUS 서버에 대해 자세히 알아보려면 여기를 클릭하십시오.



참고:이 예에서는 WPA Personal이 선택됩니다.

6단계. **+**를 클릭하고 WPA-TKIP 또는 WPA2-AES 확인란을 선택하여 인프라 클라이언트 인터페이스에서 사용할 WPA 암호화의 종류를 결정합니다.

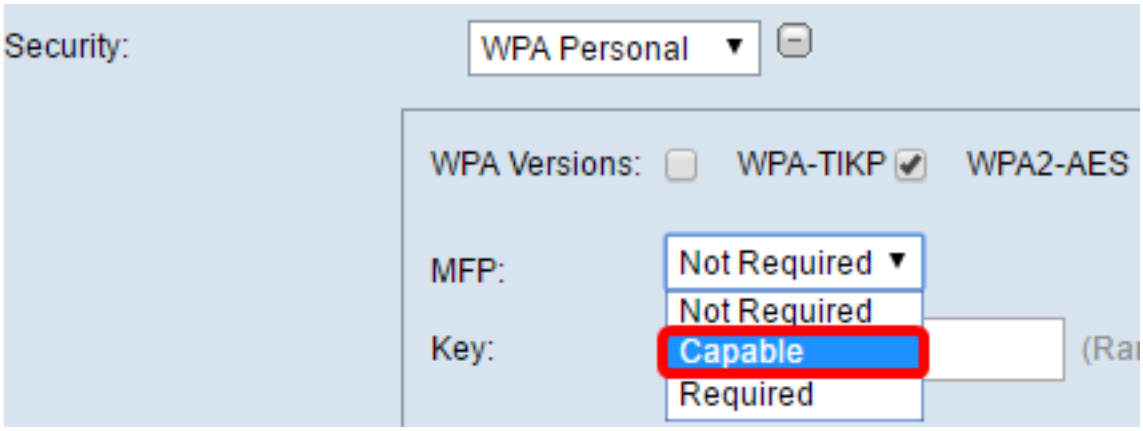
참고:모든 무선 장비가 WPA2를 지원하는 경우 인프라 클라이언트 보안을 WPA2-AES로 설정합니다.암호화 방법은 WPA2용 WPA 및 WPA2용 AES(Advanced Encryption Standard)의 RC4입니다. WPA2는 보다 강력한 암호화 표준을 사용하므로 권장됩니다.이 예에서는 WPA2-AES가 사용됩니다.



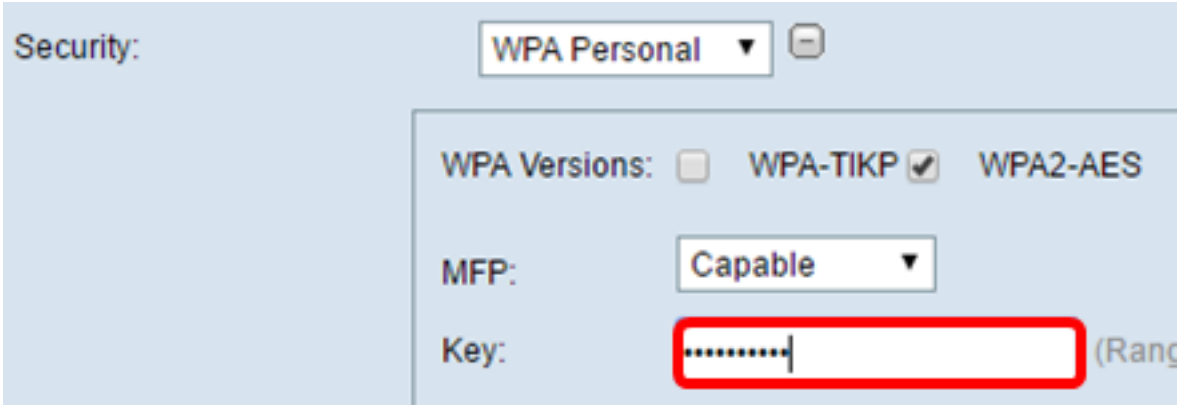
7단계. (선택 사항) 6단계에서 WPA2-AES를 선택한 경우 WAP에 보호된 프레임이 필요할지 여부를 MFP(Management Frame Protection) 드롭다운 목록에서 옵션을 선택합니다.MFP에 대해 자세히 알아보려면 여기를 클릭하십시오.옵션은 다음과 같습니다.

- Not Required — MFP에 대한 클라이언트 지원을 비활성화합니다.
- Capable — MFP를 지원하지 않는 클라이언트와 MFP를 모두 지원하는 네트워크에 연결할 수 있습니다.WAP의 기본 MFP 설정입니다.
- 필수 - MFP가 협상된 경우에만 클라이언트를 연결할 수 있습니다.디바이스가 MFP를 지원하지 않으면 네트워크에 가입할 수 없습니다.

참고:이 예에서는 Capable을 선택합니다.



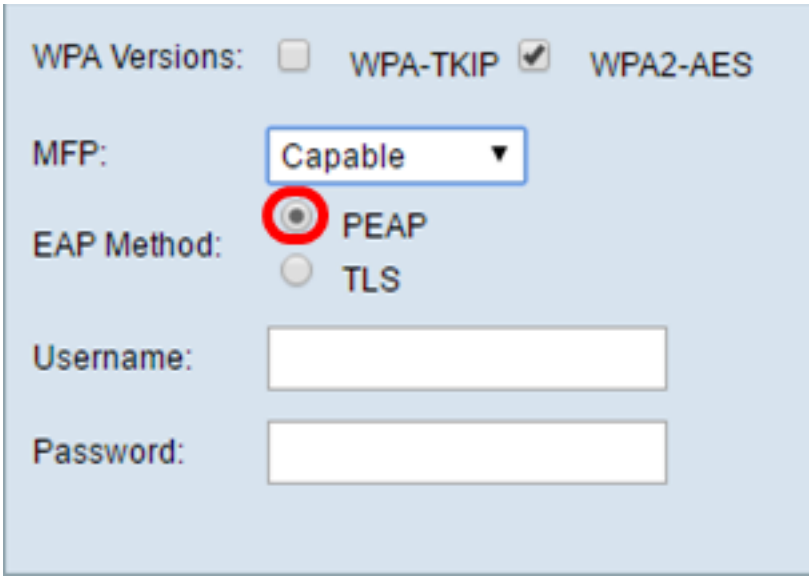
8단계. *Key* 필드에 WPA 암호화 키를 입력합니다.키는 8~63자여야 합니다.문자, 숫자 및 특수 문자의 조합입니다.무선 네트워크에 처음 연결할 때 사용하는 암호입니다.그런 다음 18단계로 건너뜁니다.



9단계. 5단계에서 WPA Enterprise를 선택한 경우 EAP 방법에 대한 라디오 버튼을 클릭합니다.

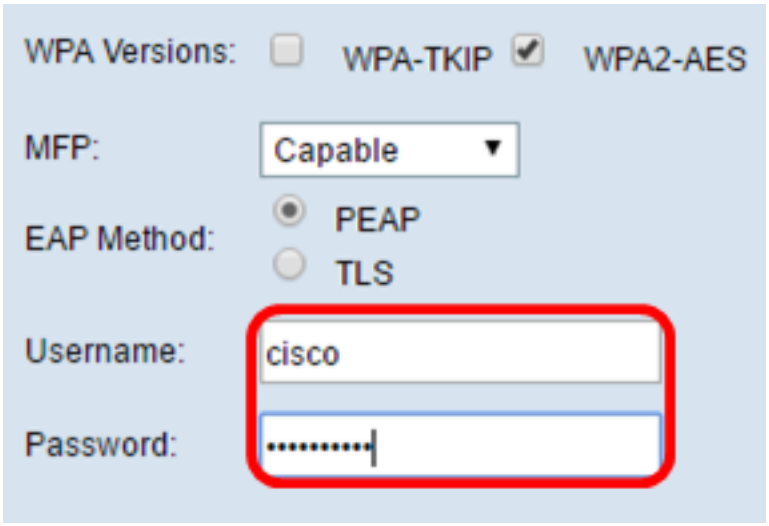
사용 가능한 옵션은 다음과 같이 정의됩니다.

- PEAP —이 프로토콜은 AES 암호화 표준을 지원하는 WAP 개별 사용자 이름과 비밀번호를 각 무선 사용자에게 제공합니다.PEAP는 비밀번호 기반 보안 방법이므로 Wi-Fi 보안은 클라이언트의 디바이스 자격 증명을 기반으로 합니다.PEAP는 암호가 약하거나 안전하지 않은 클라이언트가 있는 경우 잠재적으로 심각한 보안 위험을 야기할 수 있습니다.TLS에 의존하지만 모든 클라이언트에 디지털 인증서를 설치하지 않습니다.대신 사용자 이름과 비밀번호를 통해 인증을 제공합니다.
- TLS — TLS는 각 사용자에게 액세스 권한을 부여할 추가 인증서를 요구합니다.네트워크에 사용자를 인증하는 데 필요한 추가 서버 및 인프라가 있는 경우 TLS가 더 안전합니다.



참고:이 예에서는 PEAP가 선택됩니다.

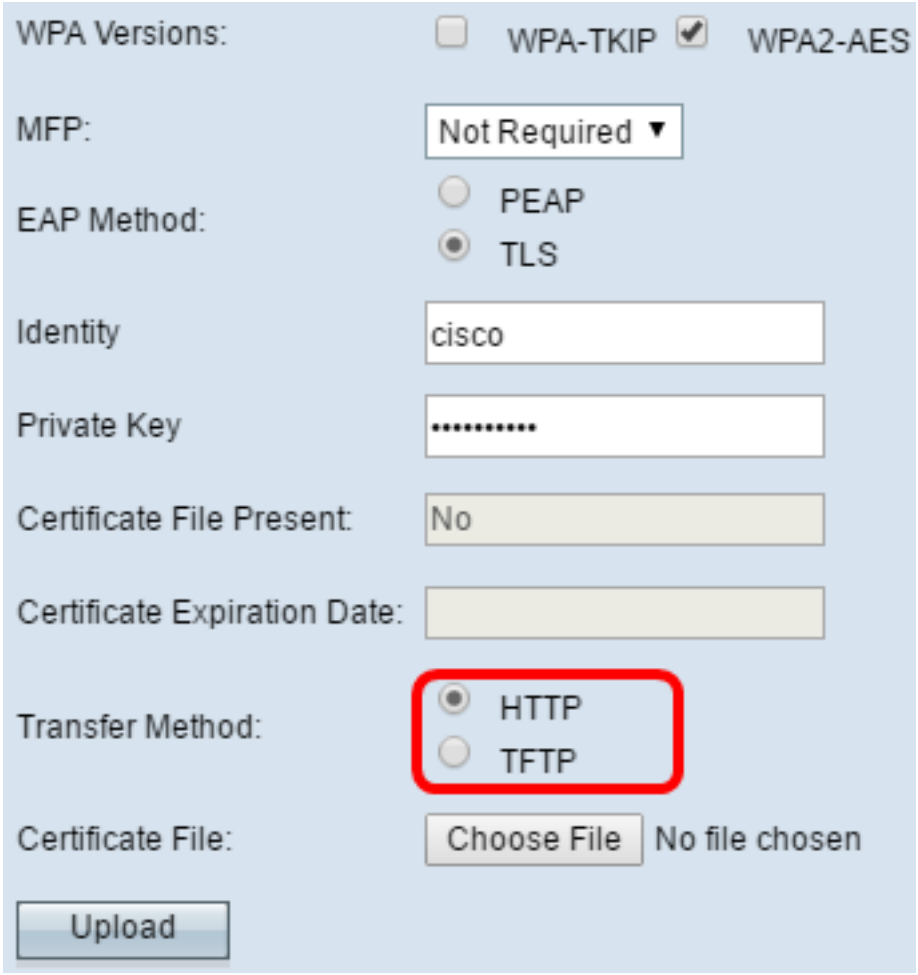
10단계. Username(사용자 이름) 및 Password(비밀번호) 필드에 인프라 클라이언트의 사용자 이름과 비밀번호를 입력합니다.인프라 클라이언트 인터페이스에 연결하는 데 사용되는 로그인 정보입니다.이 정보는 인프라 클라이언트 인터페이스를 참조하십시오.그런 다음 18단계로 건너뜁니다.



11단계. 9단계에서 TLS를 클릭한 경우 *Identity* 및 *Private Key 필드*에 인프라 클라이언트의 ID 및 개인 키를 입력합니다.

12단계. 전송 방법 영역에서 다음 옵션의 라디오 버튼을 클릭합니다.

- TFTP — TFTP(Trivial File Transfer Protocol)는 간소화된 비보안 버전의 FTP(File Transfer Protocol)입니다. 주로 기업 네트워크 간에 소프트웨어를 배포하거나 장치를 인증하는 데 사용됩니다.TFTP를 클릭한 경우 15단계로 건너뜁니다.
- HTTP — HTTP(Hypertext Transfer Protocol)는 클라이언트가 인증 프레임워크를 제공하는 데 사용할 수 있는 간단한 챌린지 응답 인증 프레임워크를 제공합니다.

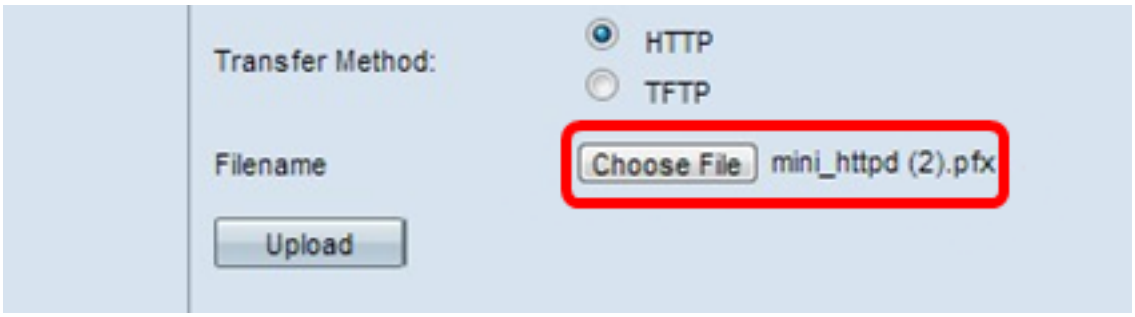


참고: WAP에 인증서 파일이 이미 있는 경우 *Certificate File Present* 및 *Certificate Expiration Date* 필드는 관련 정보로 이미 채워집니다.그렇지 않으면 비어 있습니다.

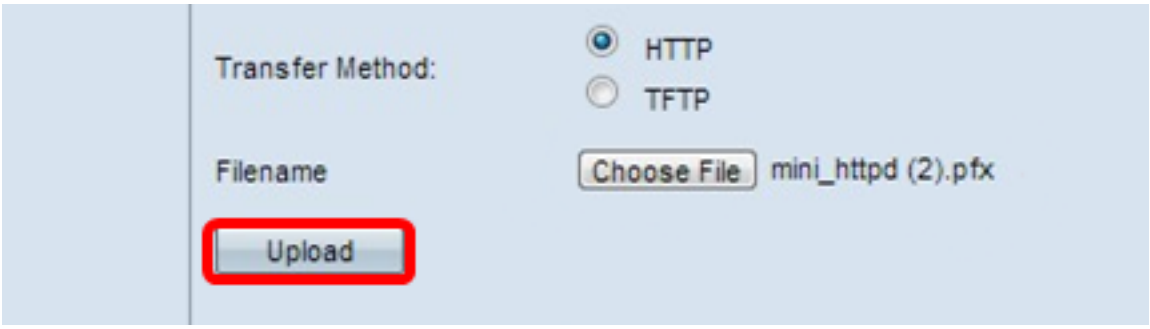
HTTP

13단계. **Choose File(파일 선택)** 버튼을 클릭하여 인증서 파일을 찾아 선택합니다.파일에 올바른 인증서 파일 확장명(예: .pem 또는 .pfx)이 있어야 합니다. 그렇지 않으면 파일이 허용되지 않습니다.

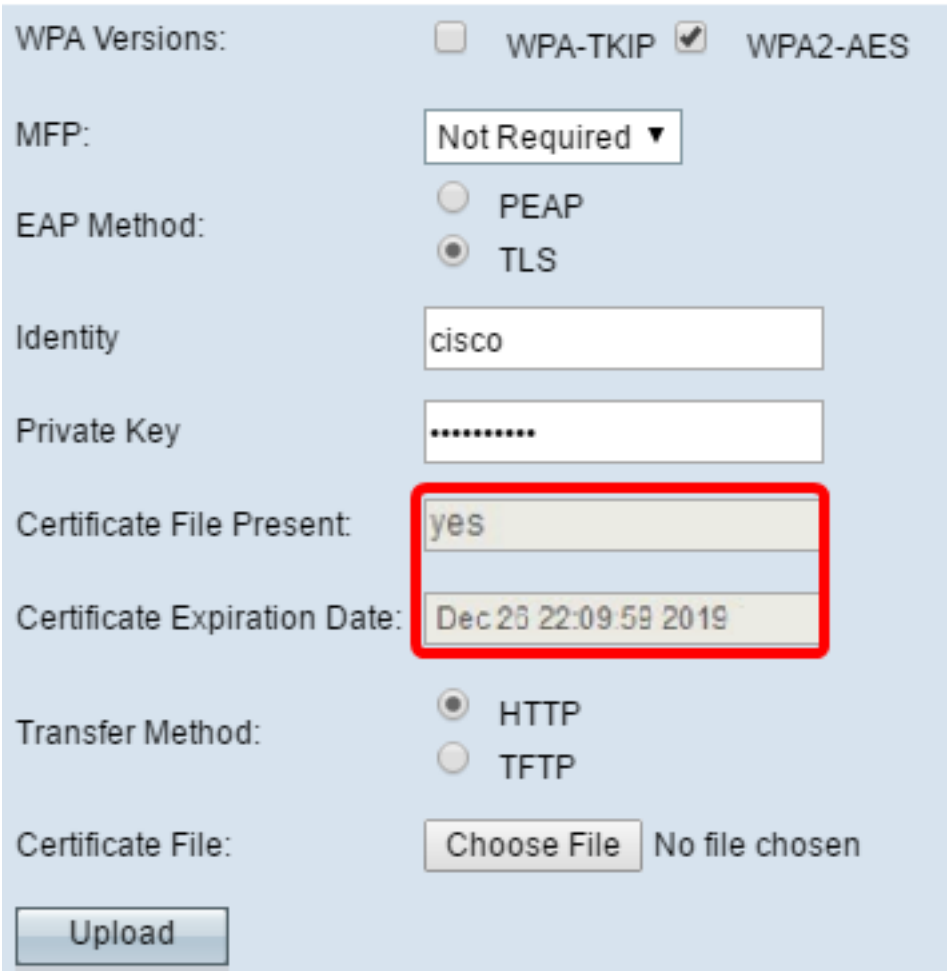
참고:이 예에서는 mini_httpd(2).pfx가 선택됩니다.



14단계. **Upload(업로드)**를 클릭하여 선택한 인증서 파일을 업로드합니다.18단계로 건너뜁니다.



Certificate *File Present* 및 *Certificate Expiration Date* 필드가 자동으로 업데이트됩니다.



TFTP

15단계. 12단계에서 TFTP를 클릭한 경우 인증서 파일의 파일 이름을 Filename *필드*에 입력합니다.

참고:이 예에서는 mini_httpd.pem이 사용됩니다.

16단계. TFTP Server IPv*4 Address(TFTP 서버 IPv4 주소)* 필드에 TFTP 서버 주소를 입력합니다.

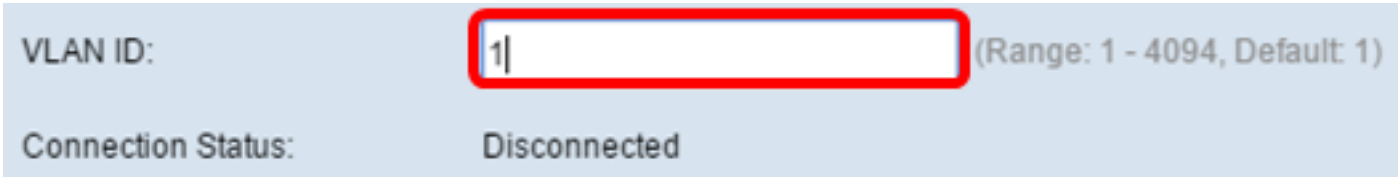
참고:이 예에서는192.168.1.20은 TFTP 서버 주소로 사용됩니다.

17단계. **Upload(업로드)** 버튼을 클릭하여 지정된 인증서 파일을 업로드합니다.

Certificate *File Present* 및 *Certificate Expiration Date* 필드가 자동으로 업데이트됩니다.

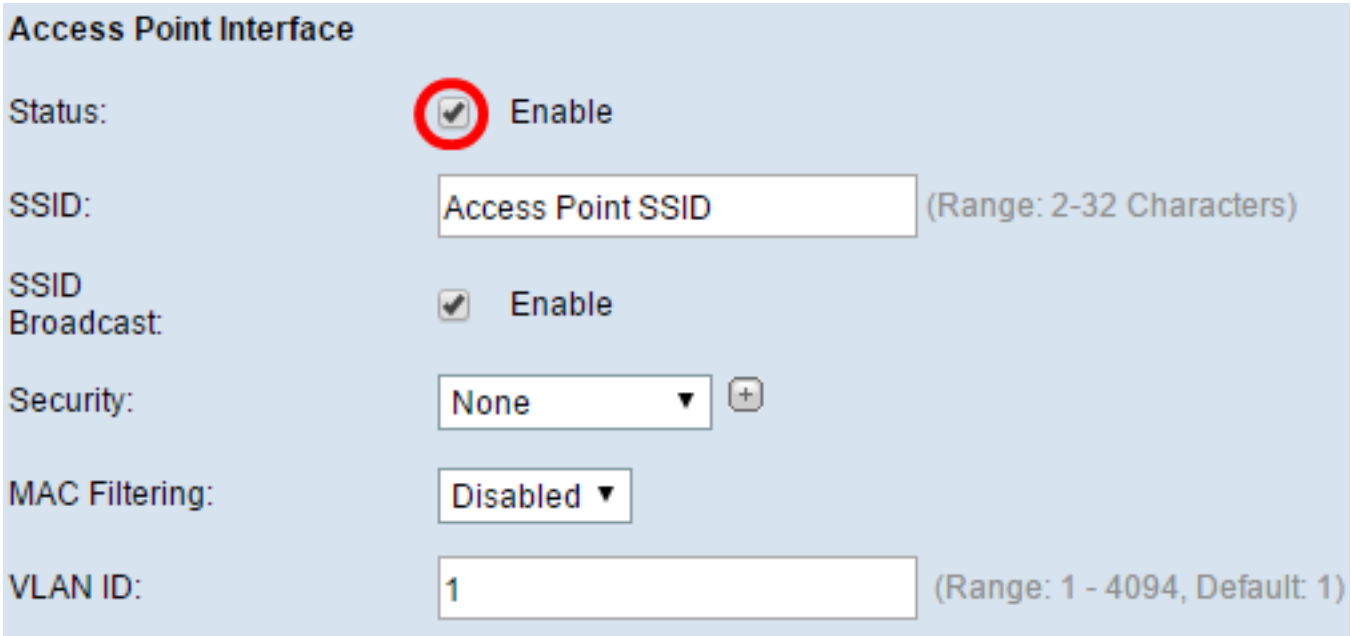
18단계. 인프라 클라이언트 인터페이스의 VLAN ID를 입력합니다.기본값은 1입니다.

참고:이 예에서는 기본 VLAN ID가 사용됩니다.



액세스 포인트 인터페이스

1단계. 액세스 포인트 인터페이스에서 브리징을 **활성화하려면** Enable Status 확인란을 선택합니다.

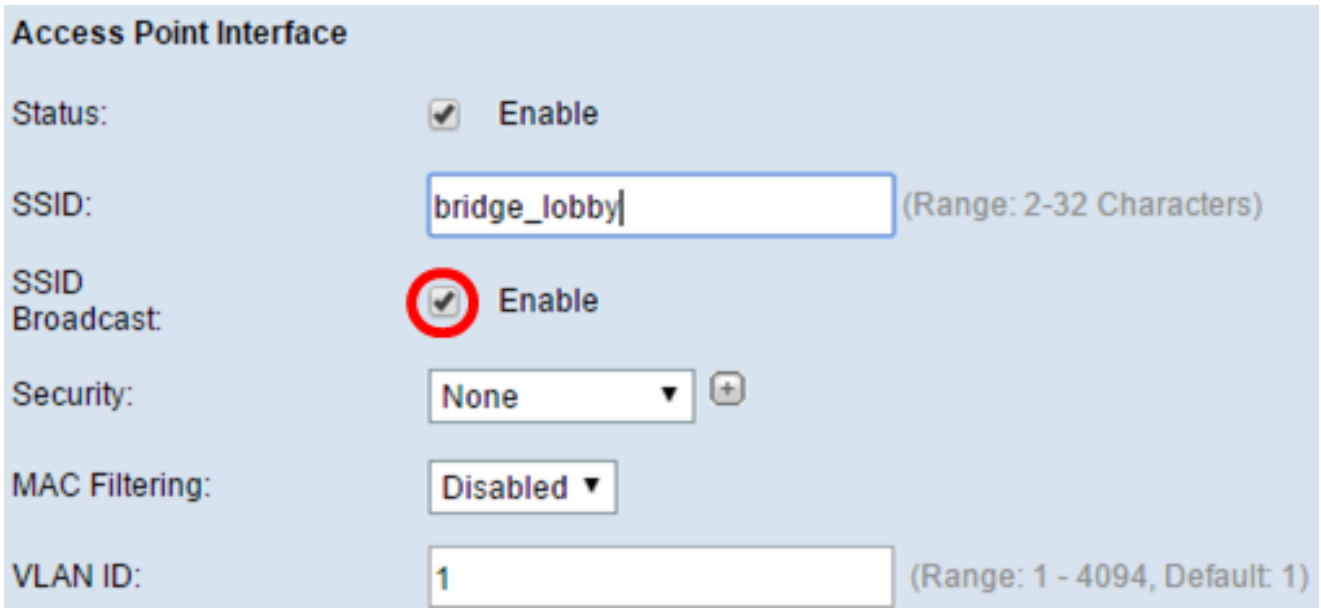


2단계. SSID 필드에 액세스 포인트의 SSID를 *입력합니다*.SSID 길이는 2자에서 32자 사이여

야 합니다.기본값은 액세스 포인트 SSID입니다.

참고:이 예에서 사용된 SSID는 bridge_lobby입니다.

3단계. (선택 사항) SSID를 브로드캐스트하지 않으려면 Enable SSID Broadcast 확인란을 선택 취소합니다.이렇게 하면 무선 액세스 포인트를 검색하는 액세스 포인트가 보이지 않게 됩니다.SSID를 이미 알고 있는 사람에게만 연결할 수 있습니다.SSID 브로드캐스트는 기본적으로 활성화되어 있습니다.

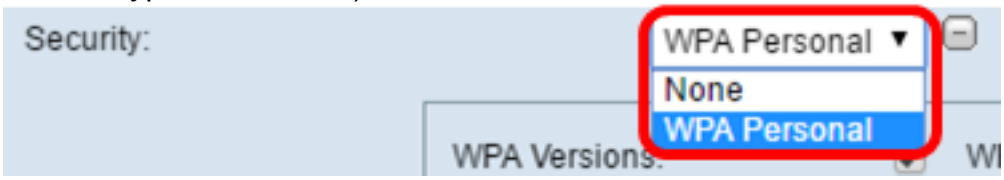


4단계. 보안 드롭다운 목록에서 WAP에 대한 다운스트림 클라이언트 스테이션을 인증할 보안 유형을 선택합니다.

사용 가능한 옵션은 다음과 같이 정의됩니다.

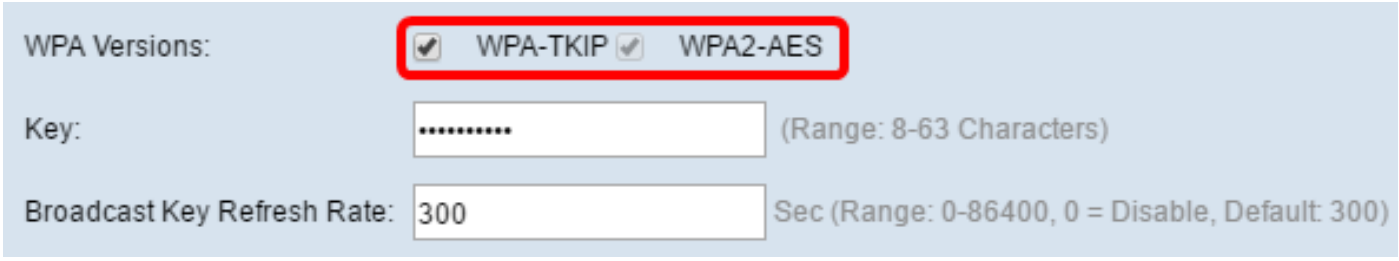
- None — 보안이 열려 있거나 없습니다.이것이 기본값입니다.이 옵션을 선택한 경우 10단계로 건너뜁니다.
- WPA Personal — WPA(Wi-Fi Protected Access) Personal은 8~63자의 키를 지원할 수 있습니다.암호화 방법은 TKIP 또는 CCMP(Counter Cipher Mode with Block Chaining Message Authentication Code Protocol)입니다.CCMP를 사용하는 WPA2는 64비트 RC4 표준만 사용하

는 TKIP(Temporal Key Integrity Protocol)와 비교하여 더 강력한 암호화 표준인 AES(Advanced Encryption Standard)가 있으므로 권장됩니다.

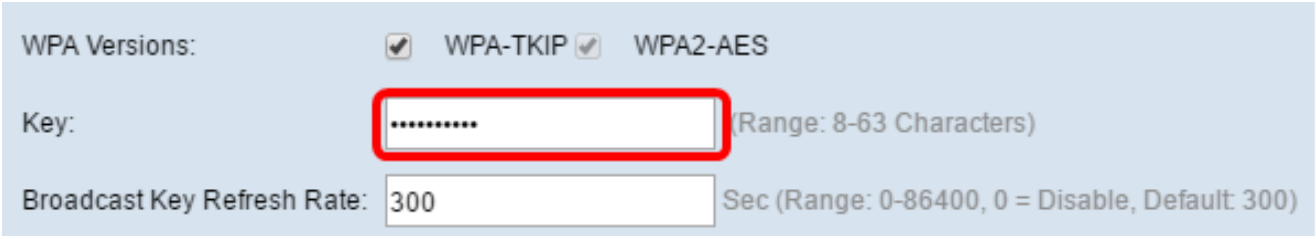


5단계. **WPA-TKIP** 또는 **WPA2-AES** 확인란을 선택하여 액세스 포인트 인터페이스에서 사용할 WPA 암호화 종류를 결정합니다.기본적으로 활성화되어 있습니다.

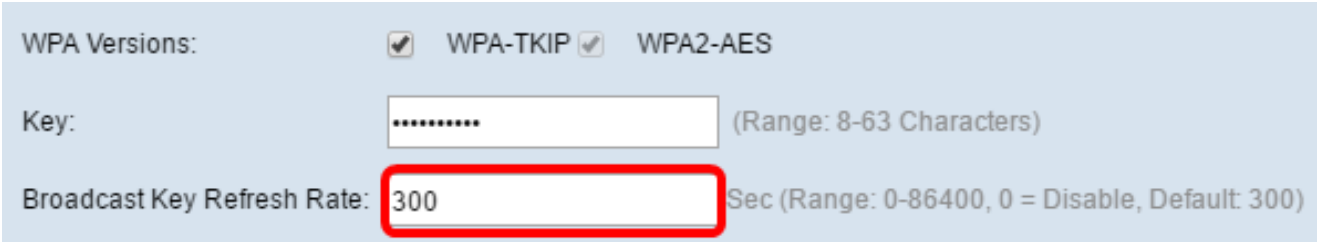
참고:모든 무선 장비가 WPA2를 지원하는 경우 인프라 클라이언트 보안을 WPA2-AES로 설정합니다.암호화 방법은 WPA2용 WPA 및 WPA2용 AES(Advanced Encryption Standard)의 RC4입니다. WPA2는 보다 강력한 암호화 표준을 사용하므로 권장됩니다.이 예에서는 WPA2-AES가 사용됩니다.



6단계. *키 필드*에 공유 WPA 키를 입력합니다.키는 8~63자여야 하며 영숫자, 대문자 및 소문자, 특수 문자를 포함할 수 있습니다.



7단계. Broadcast *Key Refresh Rate* 필드에 속도를 입력합니다.브로드캐스트 키 새로 고침 속도는 이 액세스 포인트에 연결된 클라이언트에 대해 보안 키를 새로 고치는 간격을 지정합니다.속도는 0에서 86400 사이여야 하며 값을 0으로 설정하면 기능이 비활성화됩니다.기본값은 300입니다.



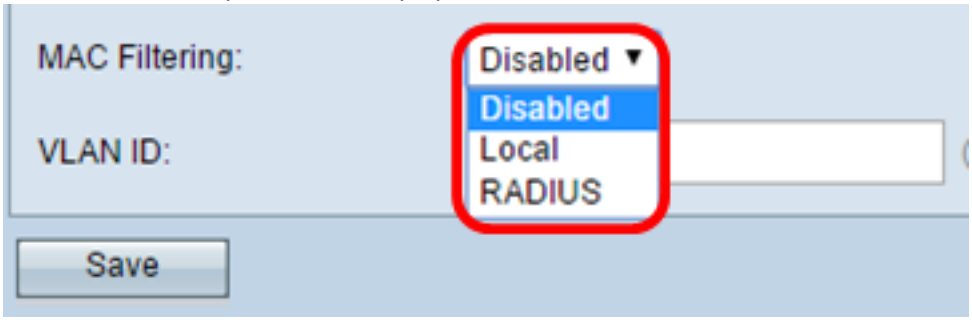
8단계. MAC Filtering 드롭다운 목록에서 액세스 포인트 인터페이스에 대해 구성할 MAC 필터링 유형을 선택합니다.활성화되면 사용자는 사용하는 클라이언트의 MAC 주소를 기반으로 WAP에 대한 액세스 권한을 부여받거나 거부됩니다.

사용 가능한 옵션은 다음과 같이 정의됩니다.

- Disabled(비활성화됨) — 모든 클라이언트가 업스트림 네트워크에 액세스할 수 있습니다.이것이 기본값입니다.
- 로컬 — 업스트림 네트워크에 액세스할 수 있는 클라이언트 세트는 로컬로 정의된 MAC 주소

목록에 지정된 클라이언트로 제한됩니다.

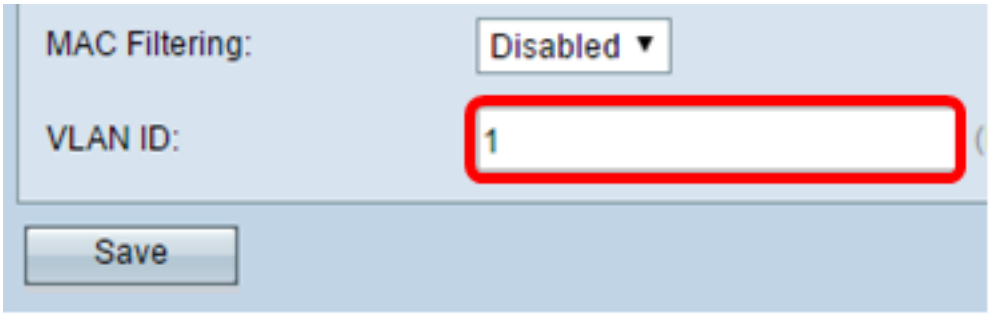
- RADIUS — 업스트림 네트워크에 액세스할 수 있는 클라이언트 집합은 RADIUS 서버의 MAC 주소 목록에 지정된 클라이언트로 제한됩니다.



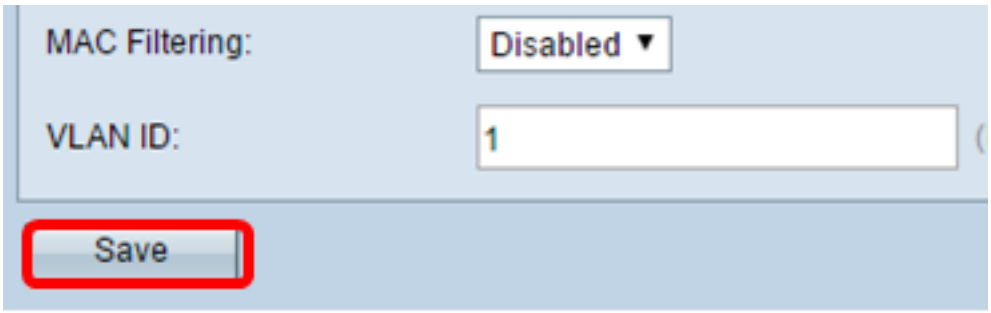
참고:이 예에서는 Disabled가 선택됩니다.

9단계. 액세스 포인트 인터페이스의 *VLAN ID* 필드에 VLAN ID를 입력합니다.

참고: 패킷 브리징을 허용하려면 액세스 포인트 인터페이스 및 유선 인터페이스의 VLAN 컨피그레이션이 인프라 클라이언트 인터페이스의 VLAN 컨피그레이션과 일치해야 합니다.



10단계. 저장을 클릭하여 변경 사항을 저장합니다.



이제 무선 액세스 포인트에서 WorkGroup Bridge를 구성했어야 합니다.