Cisco Business Wireless Access Point에서 RADIUS 구성

목표

이 문서의 목적은 CBW(Cisco Business Wireless) 액세스 포인트(AP)에서 RADIUS를 구성하는 방법을 보여 주는 것입니다.

적용 가능한 디바이스 | 펌웨어 버전

- 140AC(데이터 시트) | 10.4.1.0 (최신 다운로드)
- 145AC(데이터 시트) | 10.4.1.0 (최신 다운로드)
- 240AC(데이터시트) | 10.4.1.0(최신 다운로드)

소개

CBW AP에서 RADIUS를 구성하려는 경우 올바른 위치에 도달했습니다!CBW AP는 더 높은 성능, 더 높은 액세스 및 고밀도 네트워크를 위해 최신 802.11ac Wave 2 표준을 지원합니다.강력한 모바일 최종 사용자 환경을 위해 매우 안전하고 안정적인 무선 연결을 통해 업계 최고의 성능을 제공합니다.

RADIUS(Remote Authentication Dial-In User Service)는 디바이스가 네트워크 서비스를 연결하고 사용하기 위한 인증 메커니즘입니다.중앙 집중식 인증, 권한 부여 및 계정 관리 용도로 사용됩니다.RADIUS 서버는 입력한 로그인 자격 증명을 통해 사용자의 ID를 확인하여 네트워크에 대한 액세스를 제어합니다.예를 들어, 공용 Wi-Fi 네트워크는 대학 캠퍼스에 설치됩니다.암호를 가진 학생만 이러한 네트워크에 액세스할 수 있습니다.RADIUS 서버는 사용자가 입력한 비밀번호를 확인하고 필요에 따라 WLAN(Wireless Local Area Network)에 대한 액세스를 허용하거나 거부합니다.

CBW AP에서 RADIUS를 구성할 준비가 되었으면 지금 시작하십시오!

목차

- CBW AP에서 RADIUS 구성
- WLAN 구성
- 확인

CBW AP에서 RADIUS 구성

이 전환된 섹션에서는 초보자를 위한 팁을 강조합니다.

로그인

기본 AP의 UI(웹 사용자 인터페이스)에 로그인합니다.이렇게 하려면 웹 브라우저를 열고 https://ciscobusiness.cisco을 입력합니다.계속하기 전에 경고를 받을 수 있습니다.자격 증명을 입력하십시오.웹 브라우저에 기본 AP의 https://[ipaddress](기본 AP)를 입력하여 기본 AP에 액세스할 수도 있습니다.

도구 팁

사용자 인터페이스의 필드에 대한 질문이 있는 경우 다음과 같은 툴 팁을 확인합니다.

주 메뉴 확장 아이콘을 찾는 데 문제가 있습니까?

화면 왼쪽에 있는 메뉴로 이동하고 메뉴 단추가 표시되지 않으면 이 아이콘을 클릭하여 사이드 바 메뉴를 엽니다.

Cisco 비즈니스 앱

이러한 디바이스에는 웹 사용자 인터페이스와 일부 관리 기능을 공유하는 동반 앱이 있습니다.웹 사용자 인터페이스의 일부 기능을 앱에서 사용할 수 있는 것은 아닙니다.

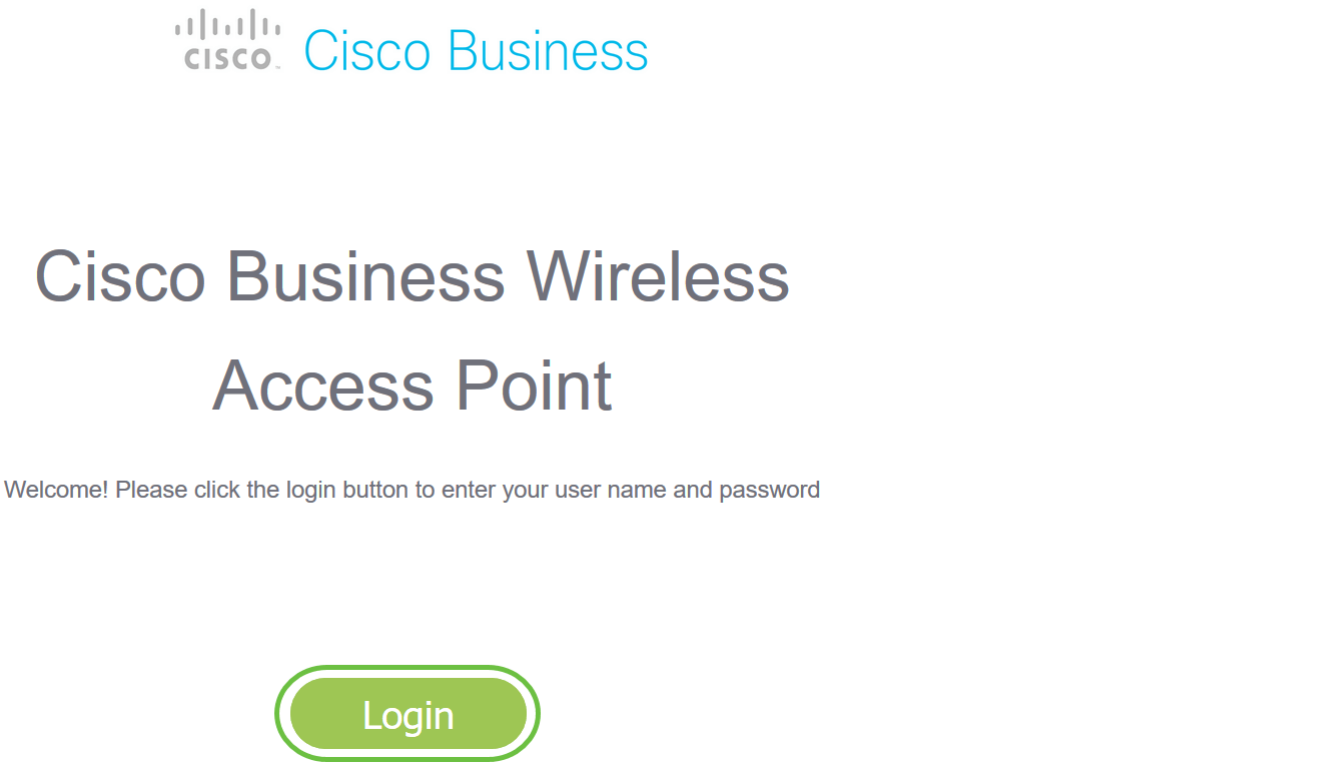
iOS 앱 다운로드 Android 앱 다운로드

자주 묻는 질문(FAQ)

아직 답변이 되지 않은 질문이 있는 경우 자주 묻는 질문 문서를 확인할 수 있습니다.FAQ

1단계

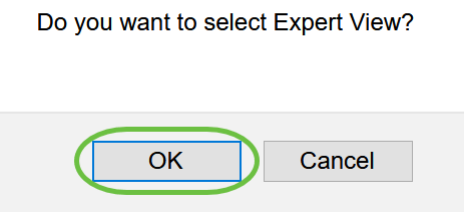
유효한 사용자 이름과 비밀번호를 사용하여 CBW AP에 로그인합니다.



2단계

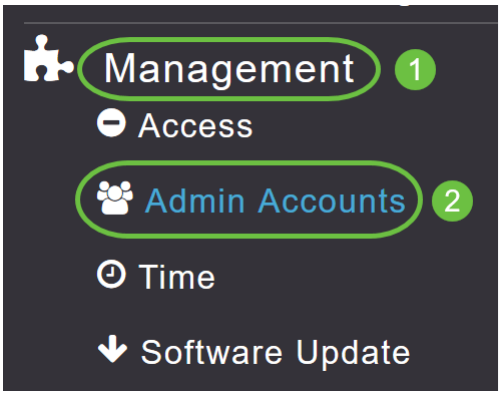
UI(웹 사용자 인터페이스) 상단의 **양방향 화살표** 기호를 클릭하여 *Switch to Expert View를 클릭합니다*.

다음 팝업 화면이 표시됩니다.OK(**확인**)를 클릭하여 진행합니다.



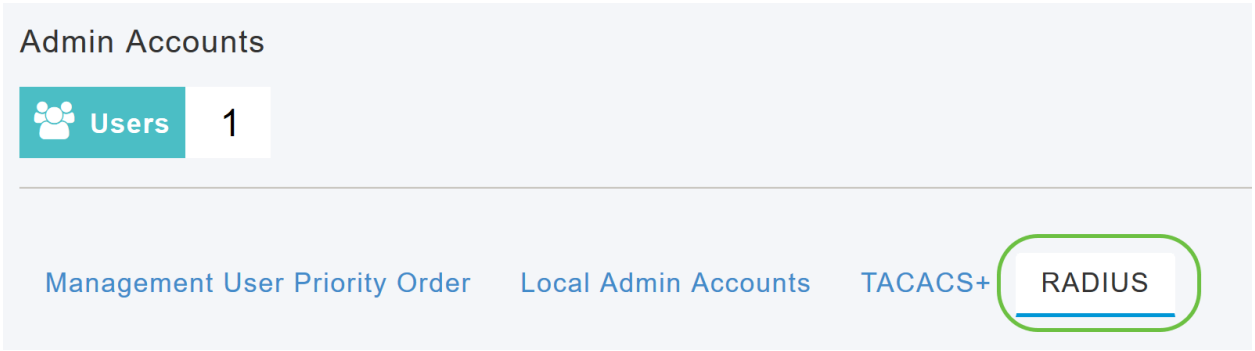
3단계

Management(**관리**) > **Admin Accounts(관리 계정)로 이동합니다**.



4단계

RADIUS 서버를 추가하려면 **RADIUS** 탭을 클릭합니다.

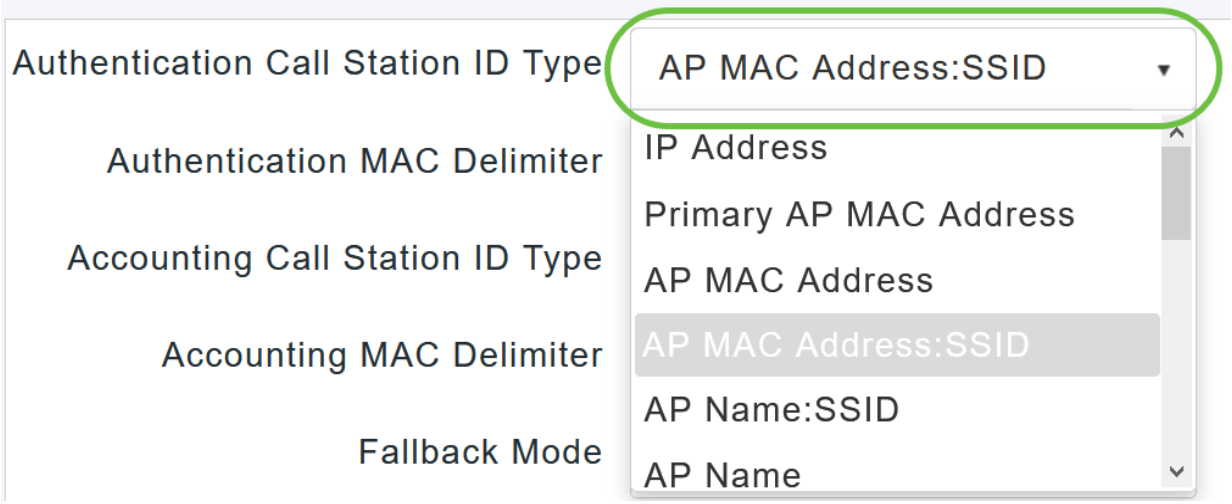


5단계

Authentication *Call Station ID Type(인증 통화 스테이션 ID 유형)* 드롭다운 목록에서 Access-Request 메시지의 RADIUS 서버로 전송되는 옵션을 선택합니다.다음 옵션을 사용할 수 있습니다.

- *IP 주소*
- *기본 AP MAC 주소*
- *AP MAC 주소*

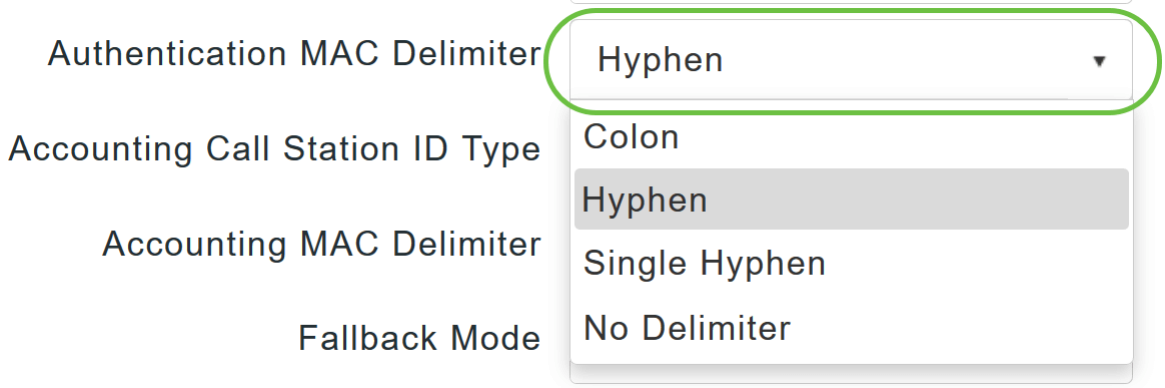
- *AP MAC 주소:SSID*
- *AP 이름:SSID*
- *AP 이름*
- *AP 그룹*
- *플렉스 그룹*
- *AP 위치*
- *VLAN ID*
- *AP 이더넷 MAC 주소*
- *AP 이더넷 MAC 주소:SSID*
- *AP 레이블 주소*
- *AP 레이블 주소:SSID*
- *AP MAC:SSID AP 그룹*
- *AP Eth MAC:SSID AP 그룹*



6단계

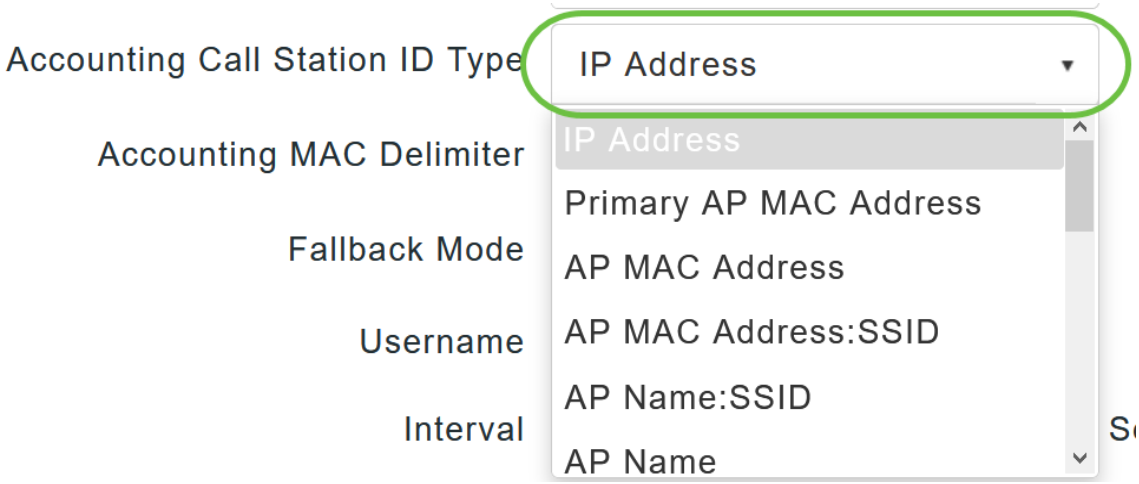
드롭다운 목록에서 *Authentication MAC Delimiter(인증 MAC 구분 기호)*를 선택합니다.옵션은 다음과 같습니다.

- *콜론*
- *하이픈*
- *단일 하이픈*
- *구분 기호 없음*



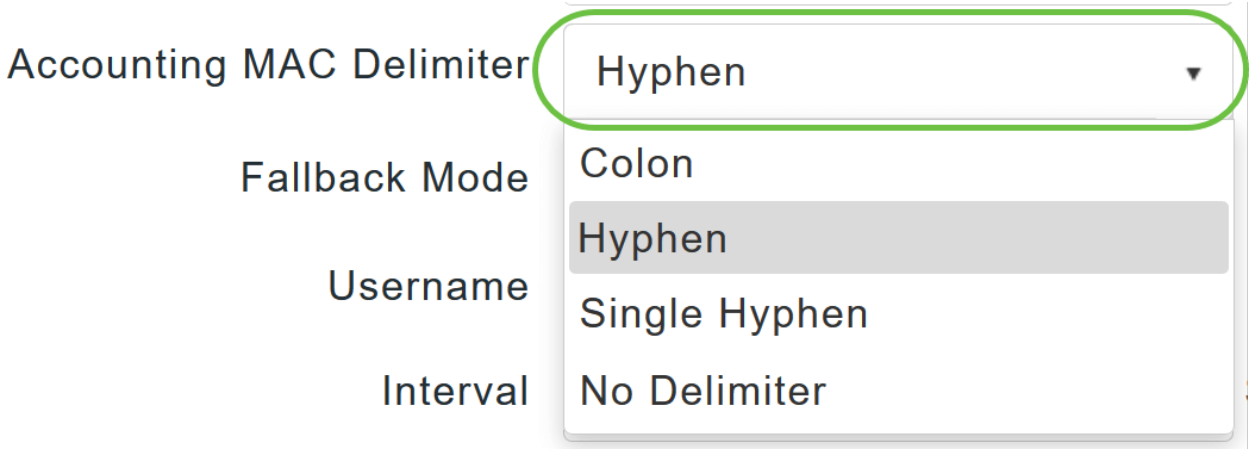
7단계

드롭다운 목록에서 *Accounting Call Station ID Type(계정 관리 통화 스테이션 ID 유형)*을 선택합니다.



8단계

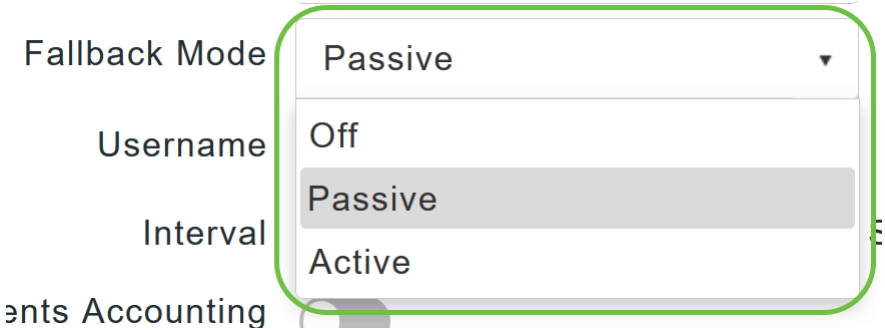
드롭다운 목록에서 *Accounting MAC Delimiter(계정 관리 MAC 구분 기호)*를 선택합니다.



9단계

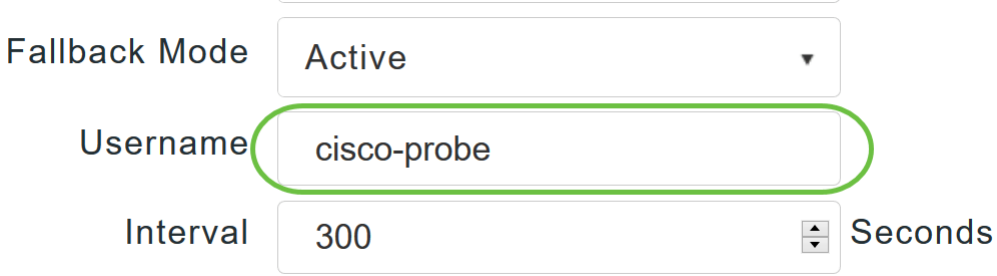
드롭다운 목록에서 RADIUS 서버 *대체 모드*를 지정합니다.다음 중 하나일 수 있습니다.

- *꺼짐* - RADIUS 서버 폴백을 비활성화합니다.이것이 기본값입니다.
- *패시브* - 기본 AP가 외부 프로브 메시지를 사용하지 않고 사용 가능한 백업 서버에서 우선 순위가 낮은 서버로 돌아갑니다.기본 AP는 일정 기간 동안 모든 비활성 서버를 무시하고 나중에 RADIUS 메시지를 전송해야 할 때 다시 시도합니다.
- *Active*(활성) - RADIUS 프로브 메시지를 사용하여 비활성으로 표시된 서버가 다시 온라인 상태인지 미리 확인하여 기본 AP가 사용 가능한 백업 서버에서 낮은 우선 순위를 가진 서버로 되돌아갑니다.기본 AP는 모든 활성 RADIUS 요청에 대해 모든 비활성 서버를 무시합니다.주 서버가 복구된 ACS 서버로부터 응답을 수신하면 활성 폴백 RADIUS 서버는 더 이상 활성 프로브 인증을 요청하는 서버로 프로브 메시지를 보내지 않습니다.



10단계

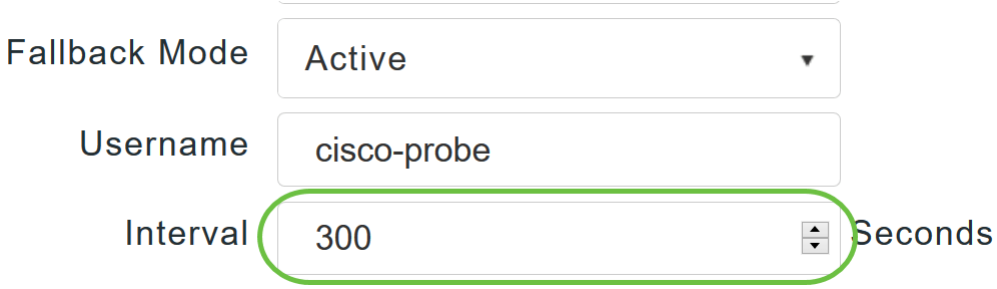
*액티브 폴백 모드*를 활성화한 경우 비활성 서버 프로브에서 전송할 이름을 *Username* 필드에 입력합니다.



최대 16자의 영숫자를 입력할 수 있습니다.기본값은 **cisco-probe입니다**.

11단계

*액티브 폴백 모드*를 활성화한 경우 Interval 필드에 프로브 간격 값(초)을 입력합니다.이 간격은 액티브 모드에서 비활성 시간 및 프로브 간격으로 사용됩니다.

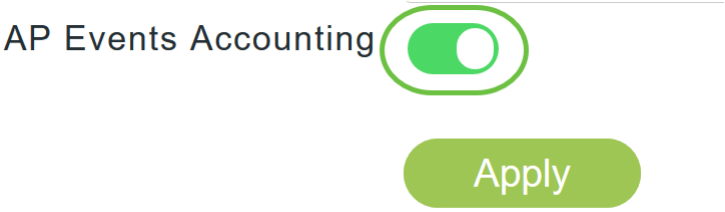


유효한 범위는 180~3600초이고 기본값은 **300**초입니다.

12단계

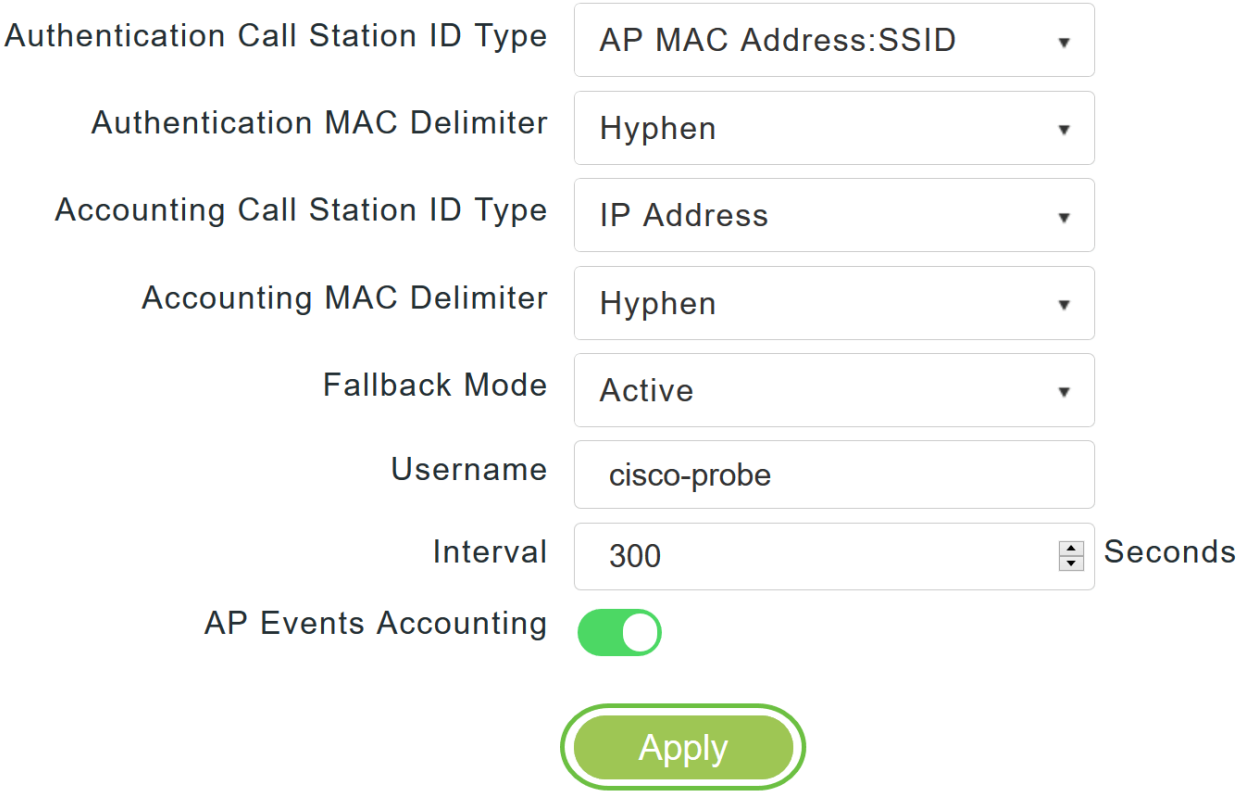
RADIUS 서버에 어카운팅 요청 전송을 활성화하려면 *AP Events Accounting*(AP 이벤트 어카운팅) 슬라이더 버튼을 활성화합니다.

네트워크 문제 중에 AP는 기본 AP에서 가입/탈퇴합니다.이 옵션을 활성화하면 네트워크 문제를 탐지하는 데 도움이 되도록 이러한 이벤트가 모니터링되고 어카운팅 요청이 RADIUS 서버로 전송됩니다.



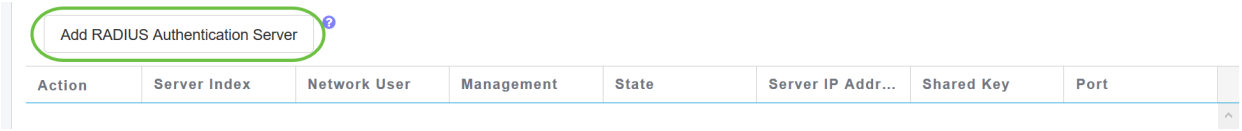
13단계

Apply를 **클릭합니다**.



14단계

RADIUS 인증 서버를 구성하려면 Add RADIUS **Authentication Server(RADIUS 인증 서버 추가)**를 클릭합니다.



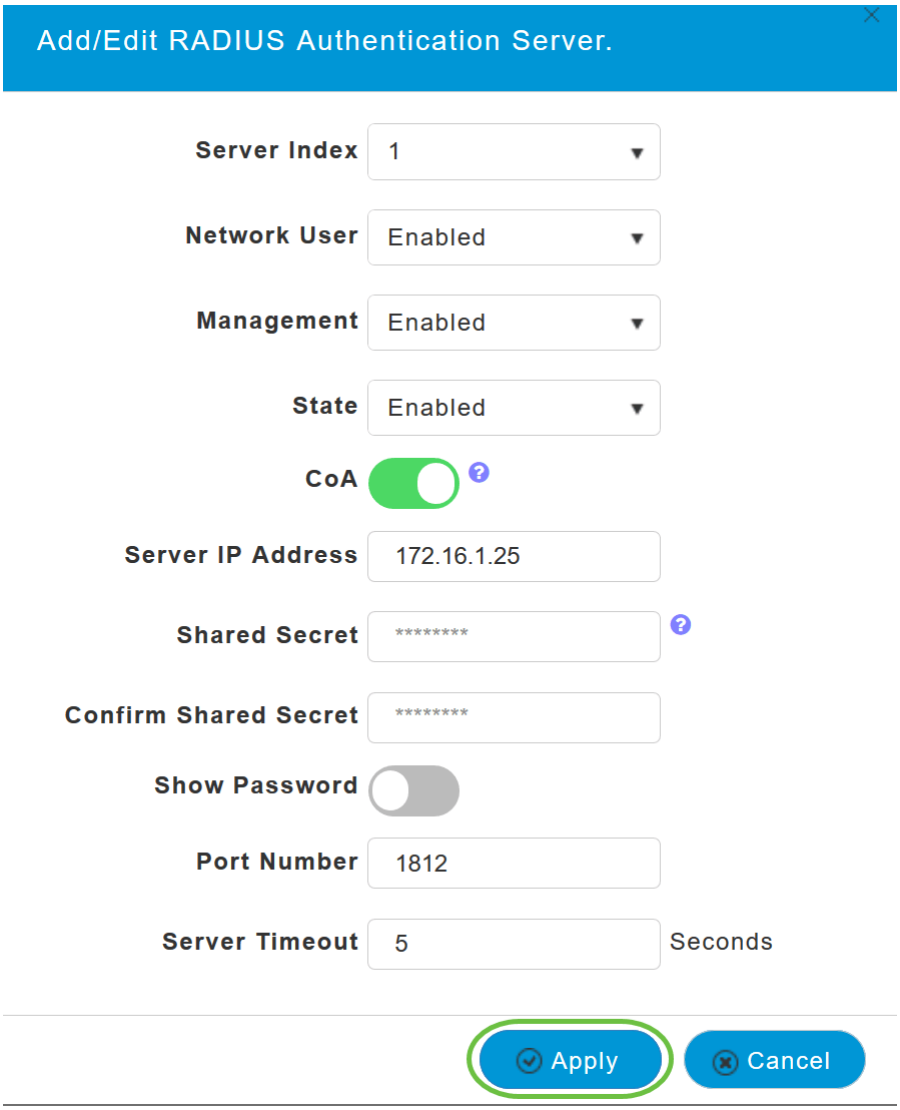
15단계

Add/*Edit RADIUS Authentication* 팝업 창에서 다음을 구성합니다.

- *서버 인덱스* - 1부터 6까지 선택
- *네트워크 사용자* - 상태를 활성화합니다.기본적으로 이 기능은 Enabled입니다.
- *관리* - 상태를 활성화합니다.기본적으로 이 기능은 Enabled입니다.
- *상태* - 상태를 활성화합니다.기본적으로 이 기능은 Enabled입니다.
- *CoA* - 슬라이더 버튼을 이동하여 이 옵션을 사용하도록 선택할 수 있습니다.
- *서버 IP 주소* - RADIUS 서버의 IPv4 주소를 입력합니다.

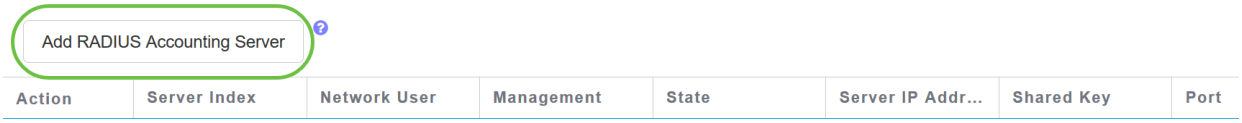
- *공유 암호* - 공유 암호를 입력합니다.
- *Port Number*(포트 번호) - RADIUS 서버와 통신하는 데 사용할 포트 번호를 입력합니다.
- *Server Timeout(서버 시간* 제한) - 서버 시간 제한을 입력합니다.

Apply를 **클릭합니다**.



16단계

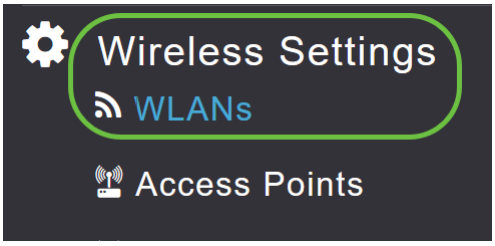
RADIUS *Accounting Server*를 추가하려면 페이지에 유사한 필드가 포함되어 있으므로 15단계와 동일한 단계를 수행합니다.



WLAN 구성

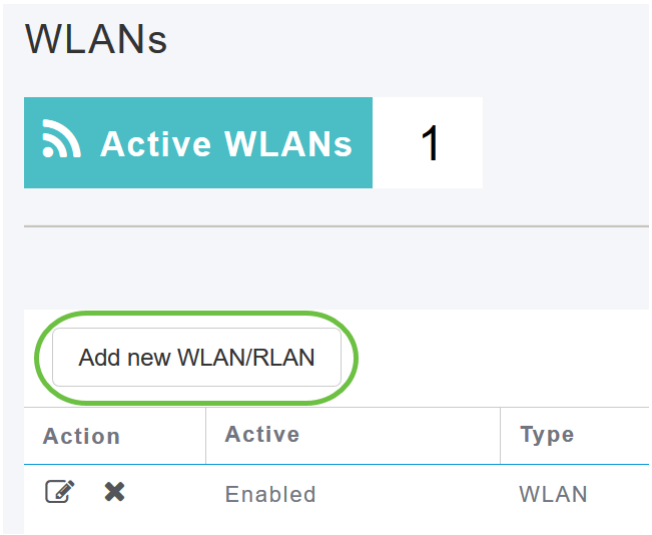
1단계

RADIUS를 사용하여 WPA2 인증을 처리할 WLAN을 구성하려면 Wireless settings(무선 **설정) > WLAN으로 이동합니다**.



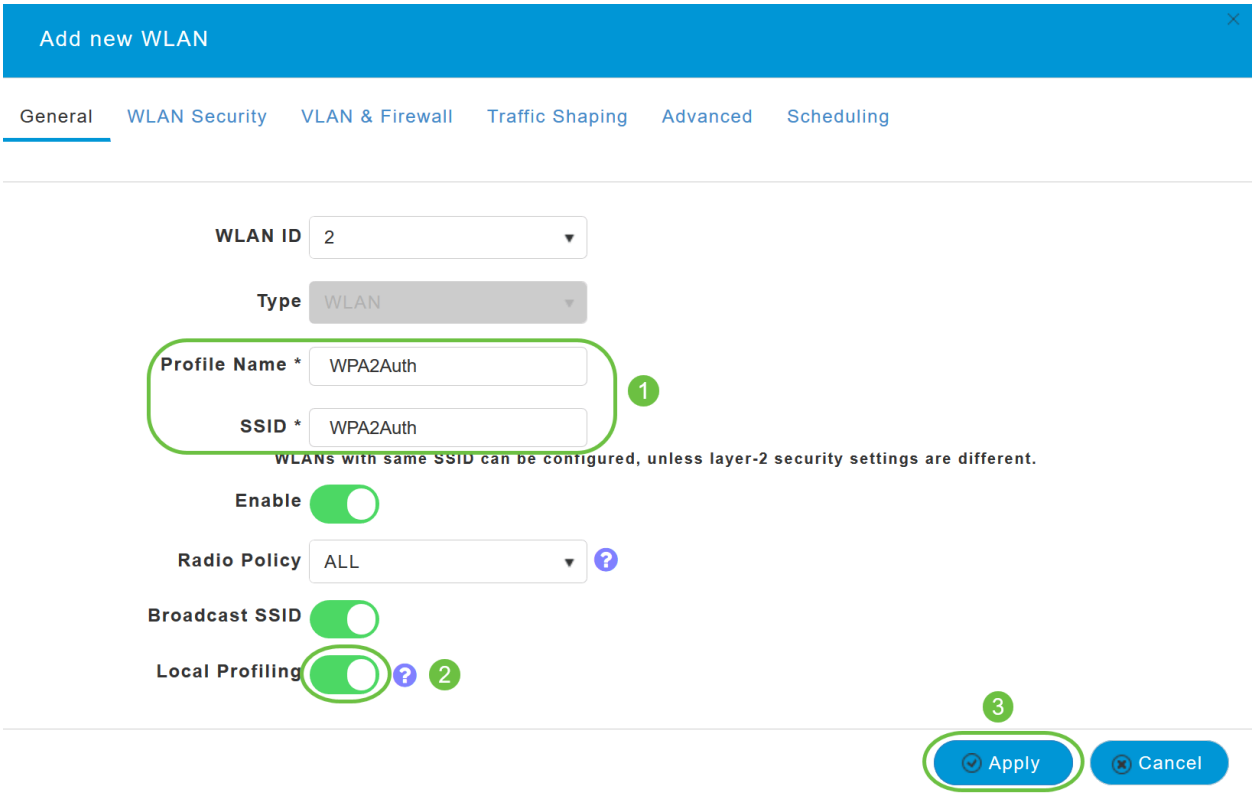
2단계

Add **New WLAN/RLAN(새 WLAN/RLAN 추가)를 클릭합니다**.



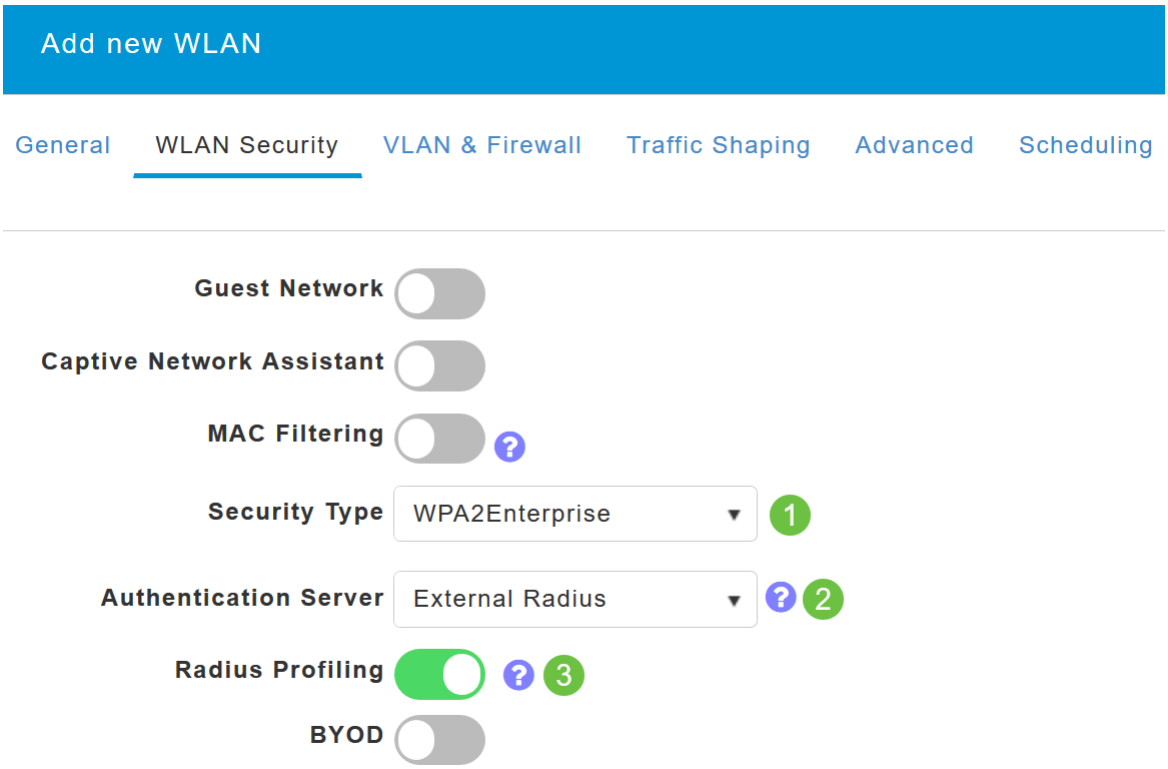
3단계

General(*일반*) 탭에서 Profile Name(*프로파일 이름)을 입력합니다*.SSID 필드가 자동으로 채워집니다.로컬 프로파일링을 사용하도록 선택할 수 *있습니다*.Apply를 **클릭합니다**.



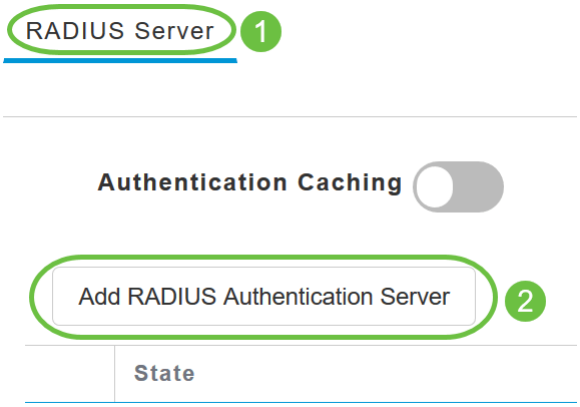
4단계

WLAN Security(WLAN 보안) 탭으로 이동합니다.*보안 유형* 드롭다운 메뉴에서 **WPA2Enterprise**를 선택합니다.External **Radius**를 *Authentication Server*로 *선택합니다*.Radius 프로파일링을 활성화하도록 선택할 수 *있습니다*.



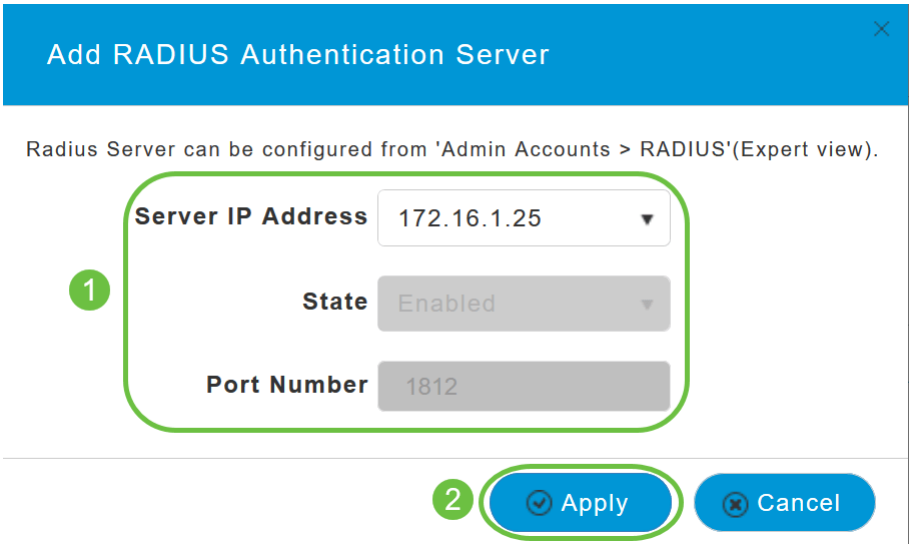
5단계

RADIUS *Server* 섹션으로 이동합니다.Add RADIUS **Authentication Server를 클릭합니다**.



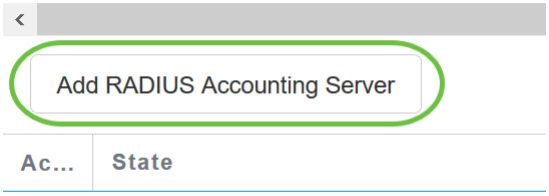
6단계

구성한 RADIUS 인증 서버의 세부 정보를 확인하고 Apply(적용)를 **클릭합니다**.



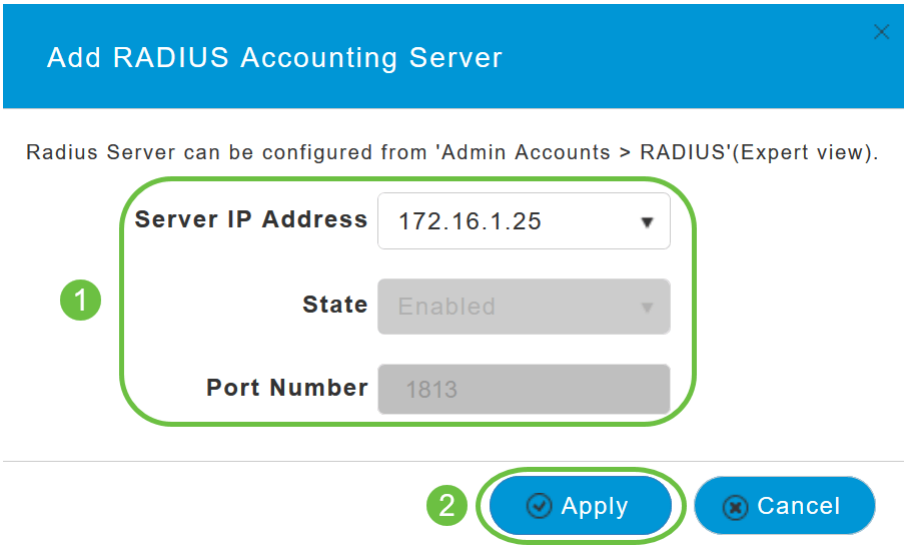
7단계

Add RADIUS Accounting **Server(RADIUS 계정 관리 서버 추가)를 클릭합니다**.



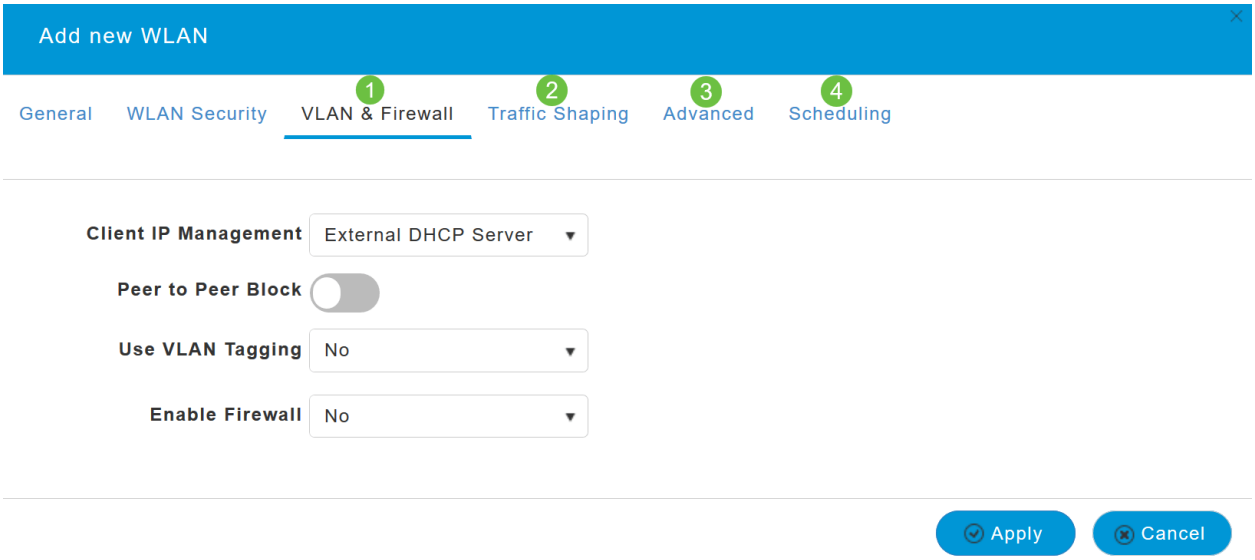
8단계

구성한 RADIUS 어카운팅 서버의 세부 정보를 확인하고 Apply(적용)를 **클릭합니다**.



9단계

VLAN *& Firewall*, *Traffic Shaping*, *Advanced* 및 *Scheduling* 탭으로 이동하여 네트워크 환경 설정에 따라 설정을 구성합니다.Apply를 **클릭합니다**.

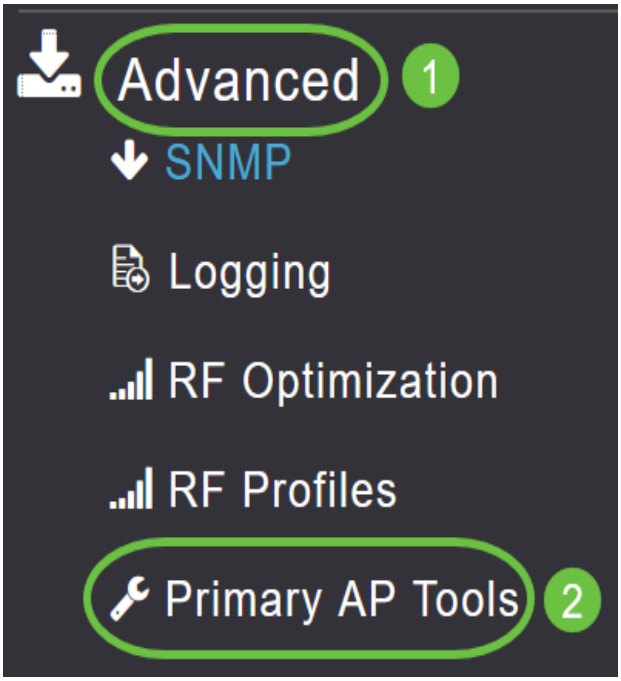


확인

RADIUS 인증을 테스트하려면 다음을 수행합니다.

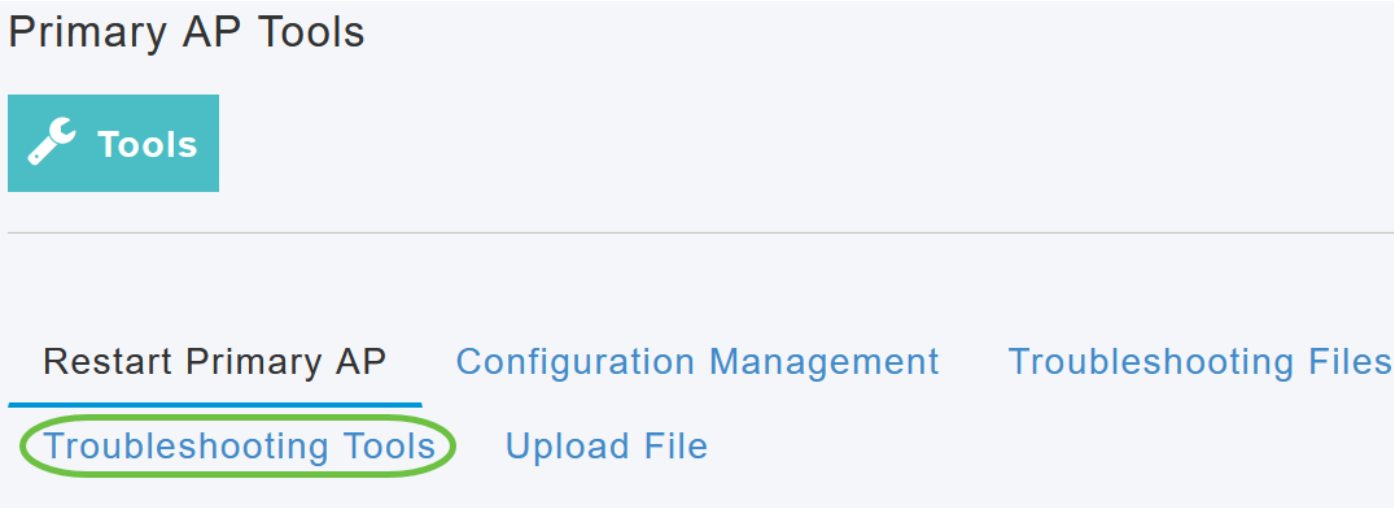
1단계

Advanced(고급) **> Primary AP Tools(기본 AP 툴)로 이동합니다**.



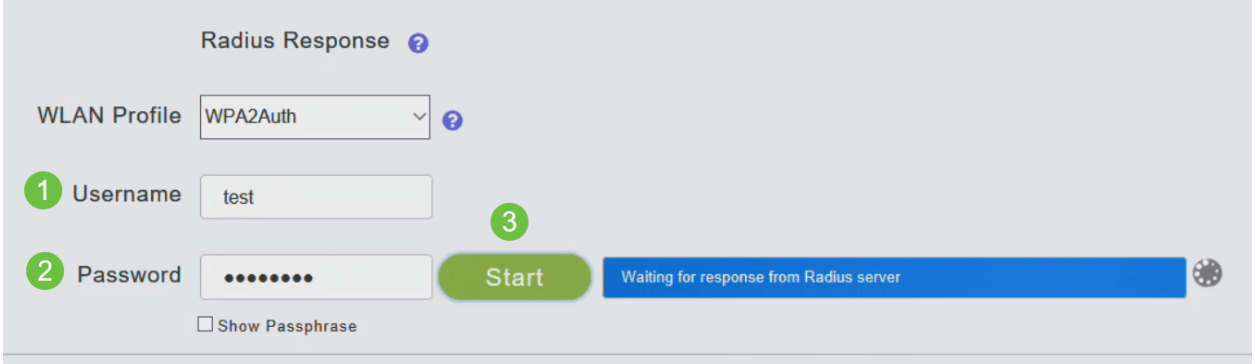
2단계

Troubleshooting **Tools를 클릭합니다**.



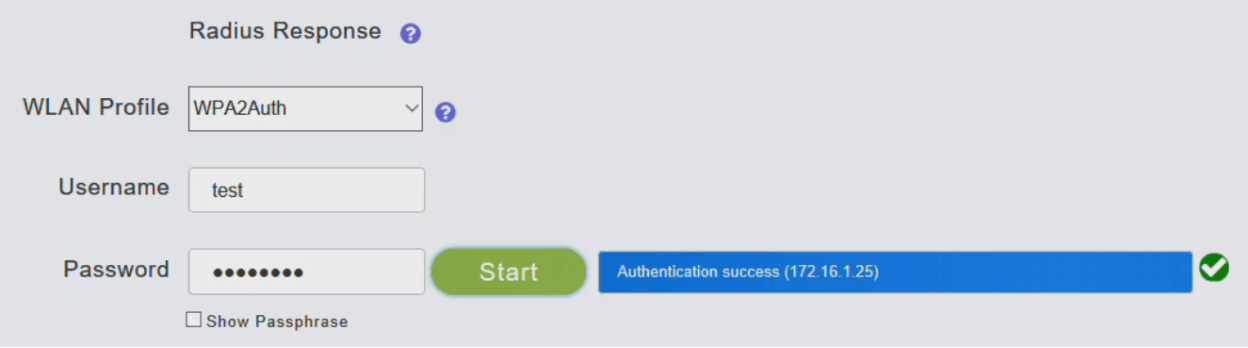
3단계

Radius *Response* 섹션에서 이전에 구성한 WLAN 프로파일의 *Username* 및 *Password*를 입력하고 **Start(시작)를 클릭합니다**.



4단계

확인이 성공적으로 완료되면 화면에 다음 알림이 표시됩니다.



결론

여기 있습니다!이제 CBW AP에서 RADIUS를 구성하는 단계를 배웠습니다.고급 컨피그레이션에 대한 자세한 내용은 *Cisco Business Wireless Access Point 관리 설명서를 참조하십시오.*

자주 묻는 질문(FAQ) 펌웨어 업그레이드 RLAN 애플리케이션 프로파일링 클라이언트 프로파일링 기본 AP 툴 Umbrella WLAN 사용자 로깅 트래픽 셰이핑 비인가 간섭 요인 컨피그레이션 관리 포트 컨피그레이션 메시 모드