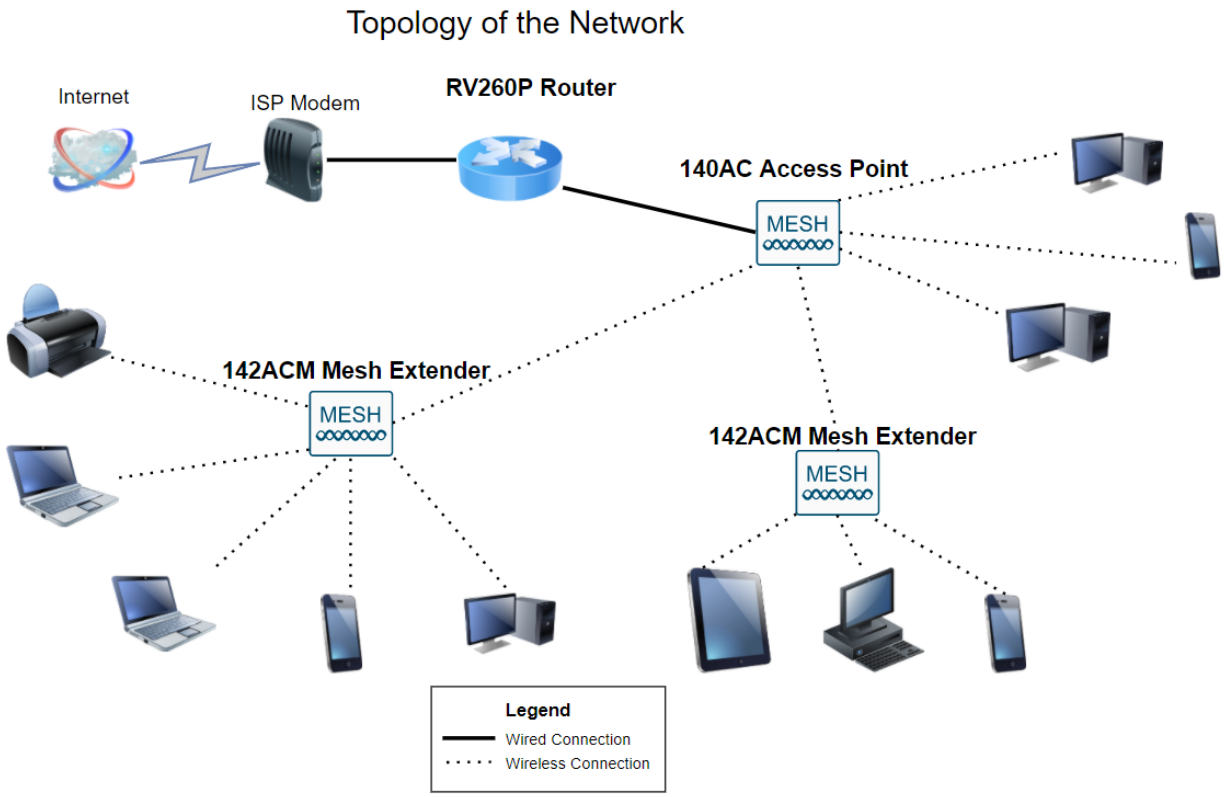
총 네트워크 구성:RV260P with Cisco Business Wireless 및 웹 UI

목표:

이 설명서에서는 RV260P 라우터, CBW140AC 액세스 포인트 및 2개의 CBW142ACM 메시 익스텐더를 사용하여 무선 메시 네트워크를 구성하는 방법을 보여줍니다.

이 문서에서는 UI(웹 사용자 인터페이스)를 사용하여 메시 무선 네트워크를 설정합니다.손쉬운 무선 설정에 권장되는 모바일 애플리케이션을 사용하려면 클릭하여 모바일 애플리케이션을 사용하는 문서로 이동합니다.웹 UI를 사용하려면 계속 읽으십시오!

토폴로지:



소개

이제 새 네트워크를 설정할 준비가 되었습니다.신나는 날이야!이 시나리오에서는 RV260P 라우터를 사용합니다.이 라우터는 스위치 대신 CBW140AC를 라우터에 연결할 수 있는 PoE(Power over Ethernet)를 제공합니다.무선 메시 네트워크를 만드는 데 CBW140AC 및 CBW142ACM 메시 익스텐더를 사용할 것입니다.

이 문서에서 사용되는 일부 용어를 잘 모르거나 메시 네트워킹에 대한 자세한 내용을 보려면 다음 문서를 참조하십시오.

- Cisco 비즈니스:새 용어 용어집
- Cisco Business Wireless Mesh Networking 시작
- Cisco Business Wireless 네트워크에 대한 FAQ(자주 묻는 질문)

준비됐어요?빨리 가자!

적용 가능한 디바이스 | 소프트웨어 버전

- RV260P | 1.0.0.17
- CBW140AC | 10.3.1.0
- CBW142ACM | 10.3.1.0(메시 네트워크에 하나 이상의 메시 익스텐더가 필요함)

목차

- 시작하기 전에
- RV260P 라우터 구성
    - RV260P Out of the Box
    - 라우터 설정
    - 인터넷 연결 문제 해결
    - 초기 컨피그레이션
    - 필요한 경우 펌웨어 업그레이드
    - VLAN 구성(선택 사항)
    - IP 주소 수정(선택 사항)
    - 고정 IP 추가
- CBW140AC 구성
    - CBW140AC 발신
    - 웹 UI에서 140AC 기본 무선 액세스 포인트 설정
- 무선 문제 해결 팁
- 웹 UI를 사용하여 CBW142ACM 메시 익스텐더 구성
- 웹 UI를 사용하여 소프트웨어 확인 및 업데이트
- 웹 UI에서 WLAN 생성
- 웹 UI를 사용하여 게스트 WLAN 생성(선택 사항)
- 웹 UI를 사용하여 애플리케이션 프로파일링(선택 사항)
- 웹 UI를 사용하여 클라이언트 프로파일링(선택 사항)

시작하기 전에

1. 설치할 현재 인터넷 연결이 있는지 확인하십시오.
2. RV260 라우터를 사용하는 경우 ISP에 문의하여 특별한 지침을 확인하십시오.일부 ISP는 라우터가 내장된 게이트웨이를 제공합니다.통합 라우터가 있는 게이트웨이가 있는 경우 라우터를 비활성화하고 WAN(Wide Area Network) IP 주소(인터넷 공급자가 계정에 할당하는 고유 인터넷 프로토콜 주소)와 모든 네트워크 트래픽을 새 라우터에 전달해야 할 수 있습니다.
3. 라우터를 배치할 위치를 결정합니다.가능하다면 오픈공간을 원하실 겁니다라우터를 인터넷 서비스 공급자(ISP)에서 광대역 게이트웨이(모뎀)에 연결해야 하기 때문에 이 방법이 쉽지 않을 수 있습니다.

RV260P 라우터 구성

라우터는 패킷을 라우팅하기 때문에 네트워크에서 필수적입니다.컴퓨터가 동일한 네트워크 또는 서브넷에 있지 않은 다른 컴퓨터와 통신할 수 있습니다.라우터는 라우팅 테이블에 액세스하여 패킷을 전송할 위치를 결정합니다.라우팅 테이블에는 대상 주소가 나열됩니다.특정 대상에 패킷을 가져오기 위해 라우팅 테이블에 정적 및 동적 컨피그레이션을 모두 나열할 수 있습니다.

RV260P에는 많은 소규모 비즈니스에 최적화된 기본 설정이 포함되어 있습니다.그러나 네트워크 요구 사항이나 ISP(Internet Service Provider)에서는 이러한 설정 중 일부를 수정해야 할 수 있습니다.요구 사항에 대해 ISP에 문의하면 UI(웹 사용자 인터페이스)를 사용하여 변경할 수 있습니다.

RV260P Out of the Box

1단계

RV260P LAN(이더넷) 포트 중 하나에서 컴퓨터의 이더넷 포트에 이더넷 케이블을 연결합니다.컴퓨터에 이더넷 포트가 없는 경우 어댑터가 필요합니다.초기 컨피그레이션을 수행하려면 터미널이 RV260P와 동일한 유선 하위 네트워크에 있어야 합니다.

2단계

RV260P와 함께 제공되는 전원 어댑터를 사용해야 합니다.다른 전원 어댑터를 사용하면 RV260P가 손상되거나 USB 동글이 손상될 수 있습니다.전원 스위치는 기본적으로 켜져 있습니다.

전원 어댑터를 RV260P의 12VDC 포트에 연결하되 아직 전원을 연결하지 마십시오.

3단계

모뎀이 꺼져 있는지 확인합니다.

4단계

이더넷 케이블을 사용하여 케이블 또는 DSL 모뎀을 RV260P의 WAN 포트에 연결합니다.

5단계

RV260P 어댑터의 반대쪽 끝을 전기 콘센트에 꽂습니다.이렇게 하면 RV260의 전원이 켜집니다. 모뎀을 다시 꽂으면 전원이 켜질 수 있습니다.전원 어댑터가 제대로 연결되어 있고 RV260P 부팅이 완료되면 전면 패널의 전원 표시등이 녹색으로 켜집니다.

라우터 설정

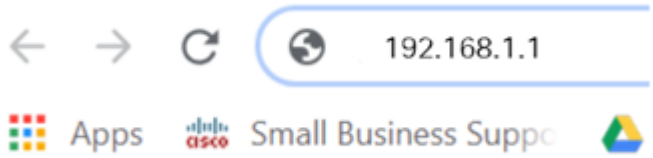
준비 작업이 완료되었으므로 이제 몇 가지 구성을 수행해야 합니다!웹 UI를 시작하려면 다음 단계를 수행합니다.

1단계

컴퓨터가 DHCP(Dynamic Host Configuration Protocol) 클라이언트가 되도록 구성된 경우 192.168.1.x 범위의 IP 주소가 PC에 할당됩니다.DHCP는 컴퓨터에 IP 주소, 서브넷 마스크, 기본 게이트웨이 및 기타 설정을 할당하는 프로세스를 자동화합니다.주소를 얻으려면 DHCP 프로세스에 참여하도록 컴퓨터를 설정해야 합니다.이 작업은 컴퓨터의 TCP/IP 속성에서 자동으로 IP 주소를 가져오도록 선택하여 수행합니다.

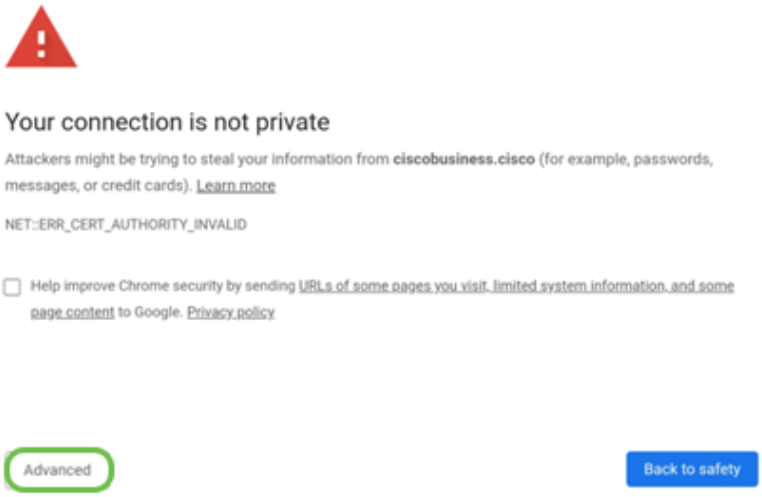
2단계

Safari, Internet Explorer 또는 Firefox와 같은 웹 브라우저를 엽니다.주소 표시줄에 RV260P의 기본 IP 주소(192.168.1.1)을 입력합니다.



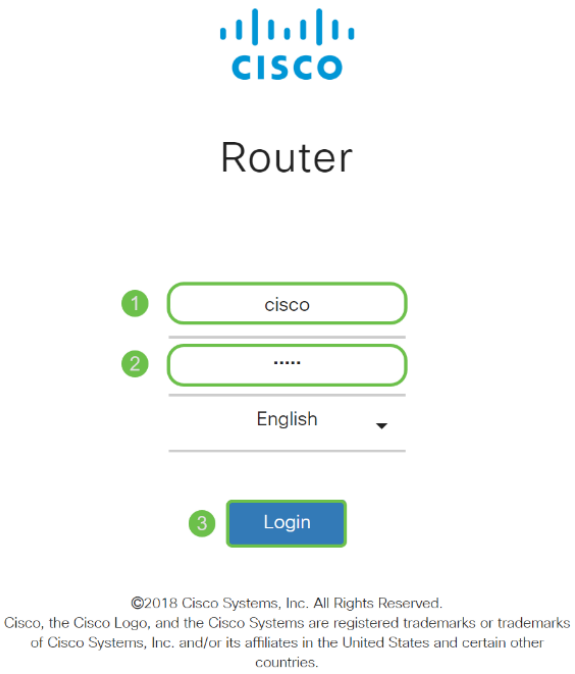
3단계

웹 사이트를 신뢰할 수 없다는 경고 메시지가 브라우저에 표시될 수 있습니다.웹 사이트로 이동합니다.연결되어 있지 않으면 Troubleshooting the Internet Connection(인터넷 연결 문제 해결)으로 이동합니다.



4단계

로그인 페이지가 나타나면 기본 사용자 이름 cisco 및 기본 비밀번호 *cisco를 입력합니다.*사용자 이름과 비밀번호 모두 대/소문자를 구분합니다.



5단계

Login(**로그인)을 클릭합니다**.Getting *Started* 페이지가 나타납니다.이제 연결을 확인하고 라우터에 로그인했으므로 이 문서의 Initial Configuration 섹션으로 이동합니다.

인터넷 연결 문제 해결

이런, 여러분이 이것을 읽고 있다면 인터넷 또는 웹 UI에 연결하는 데 문제가 있을 것입니다.이러한 솔루션 중 하나가 도움이 됩니다.

연결된 Windows OS에서 명령 프롬프트를 열어 네트워크 연결을 테스트할 수 있습니다.ping 192.168.1.1(라우터의 기본 IP 주소)를 입력합니다. 요청이 시간 초과되면 라우터와 통신할 수 없습니다.

연결이 설정되지 않은 경우 RV160 및 RV260 라우터에서 문제 해결을 확인할 수 있습니다.

다음과 같은 작업을 수행할 수 있습니다.

1. 웹 브라우저가 [오프라인으로 작업]으로 설정되어 있지 않은지 확인합니다.
2. 이더넷 어댑터의 LAN 연결 설정을 확인합니다.PC는 DHCP를 통해 IP 주소를 받아야 합니다.또는 PC에 기본 게이트웨이가 192.168.1.1(RV260P의 기본 IP 주소)로 설정된 192.168.1.x 범위의 고정 IP 주소가 있을 수 있습니다. 연결하려면 RV260P의 네트워크 설정을 수정해야 할 수 있습니다. Windows 10을 사용하는 경우 Windows 10 방향을 확인하여 네트워크 설정을 수정합니다.
3. 192.168.1.1 IP 주소를 점유하는 기존 장비가 있는 경우 네트워크가 작동하려면 이 충돌을 해결해야 합니다.이 섹션의 끝에서 자세히 알아보거나 여기를 클릭하여 직접 이동하십시오.
4. 두 장치의 전원을 끄면 모뎀과 RV260P를 재설정합니다.그런 다음 모뎀을 켜고 약 2분 동안 유휴 상태로 둡니다.그런 다음 RV260P의 전원을 켜십시오.이제 WAN IP 주소를 받아야 합니다.

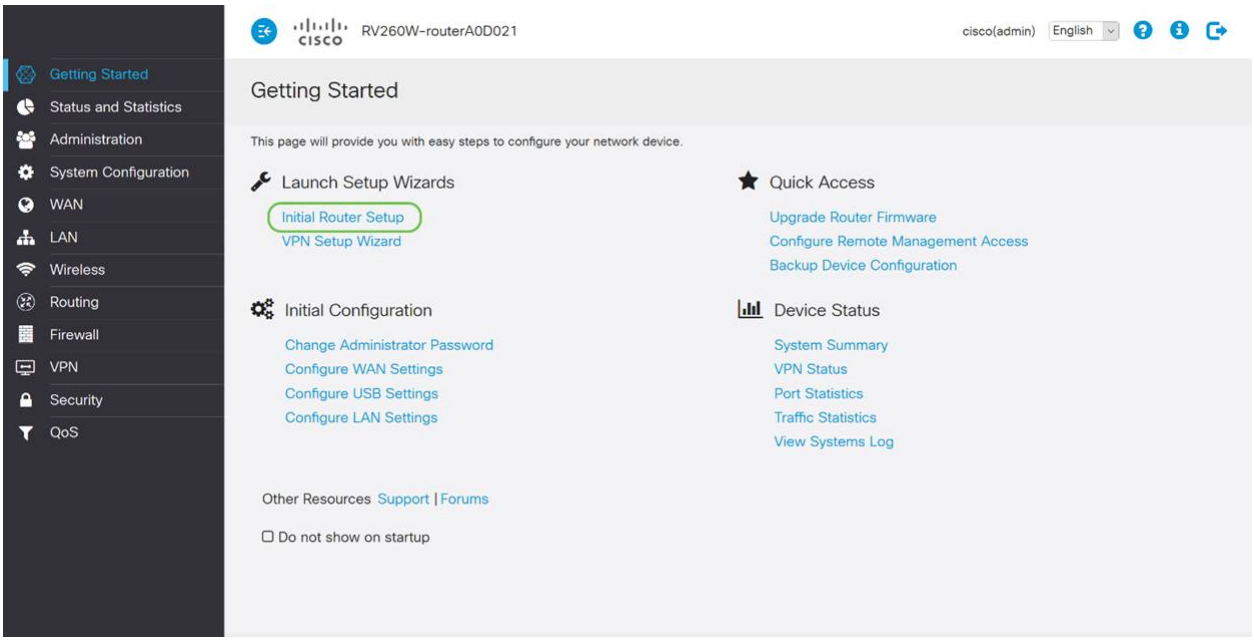
5. DSL 모뎀이 있는 경우 ISP에 DSL 모뎀을 브리지 모드로 설정하도록 요청합니다.

초기 컨피그레이션

이 섹션에 나열된 초기 설정 마법사 단계를 진행하는 것이 좋습니다.언제든지 이러한 설정을 변경할 수 있습니다.

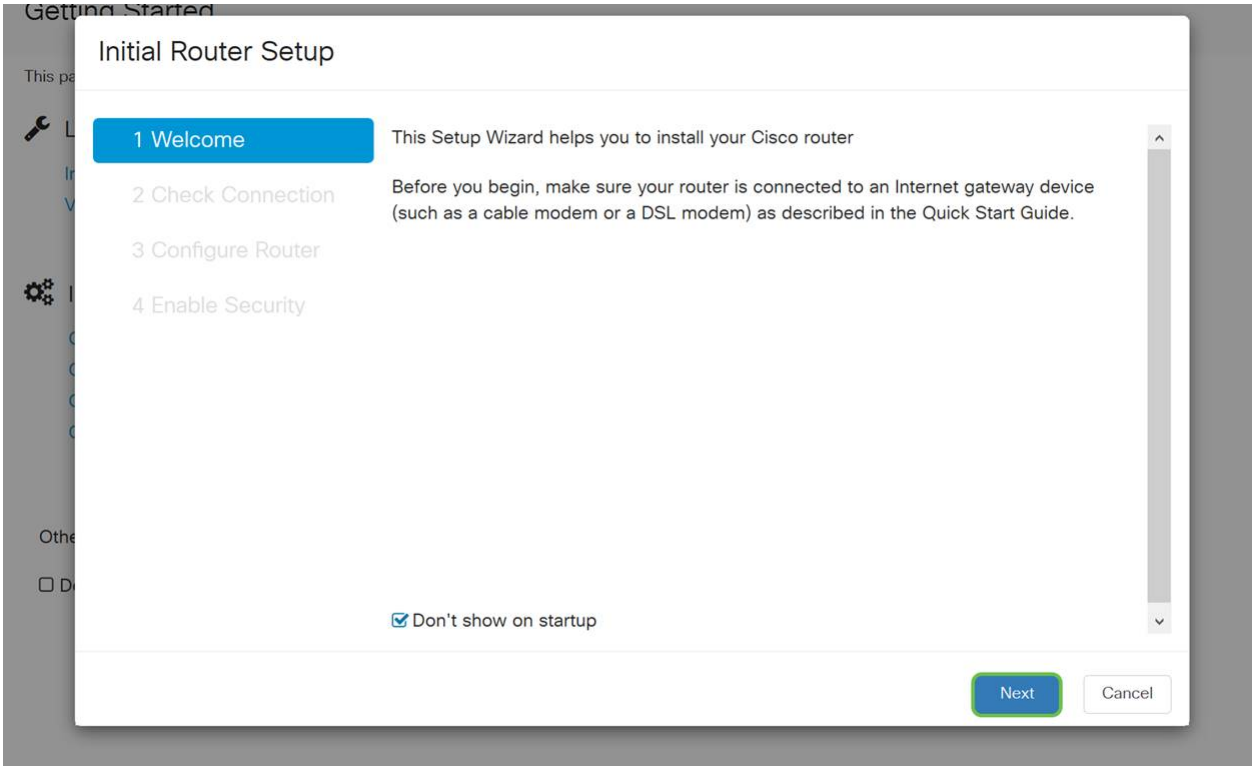
1단계

시작 *페이지*에서 **초기 설정 마법사**를 클릭합니다.



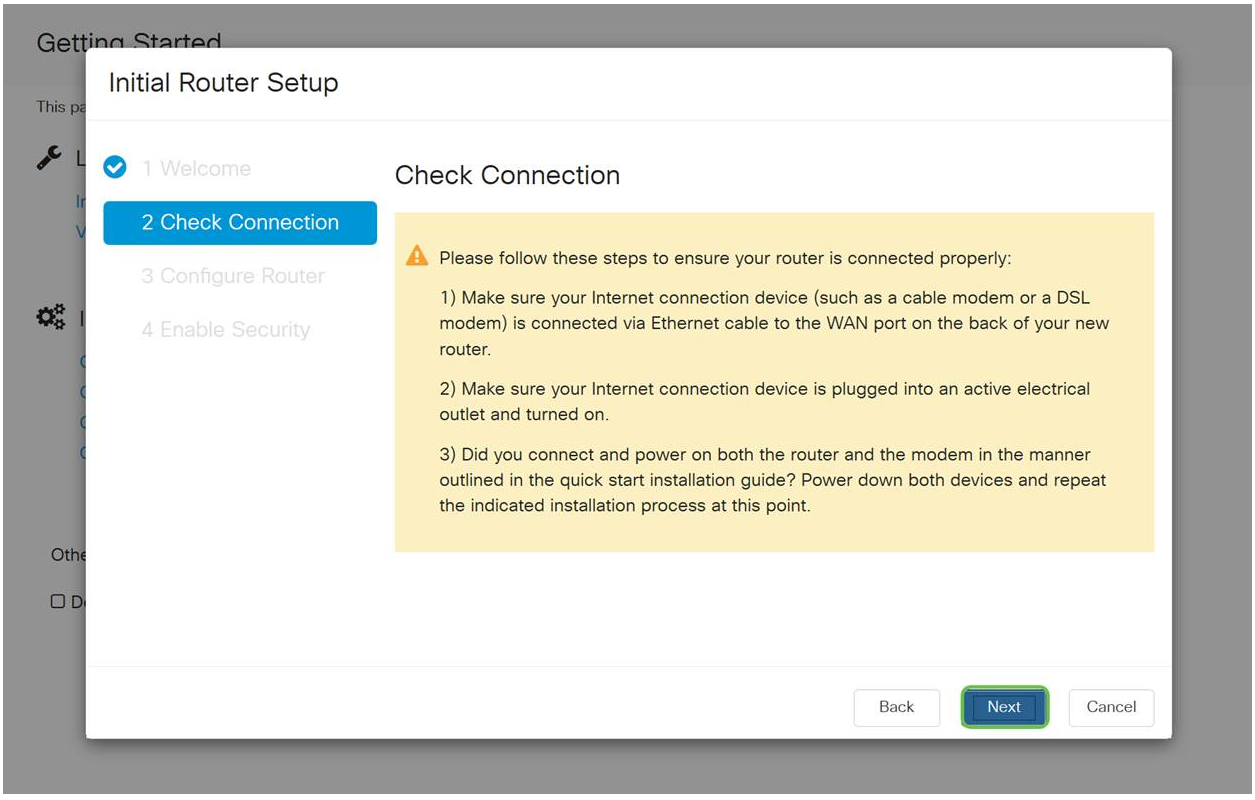
2단계

이 단계에서는 케이블이 연결되어 있는지 확인합니다.이미 확인했으므로 **다음**을 클릭합니다.



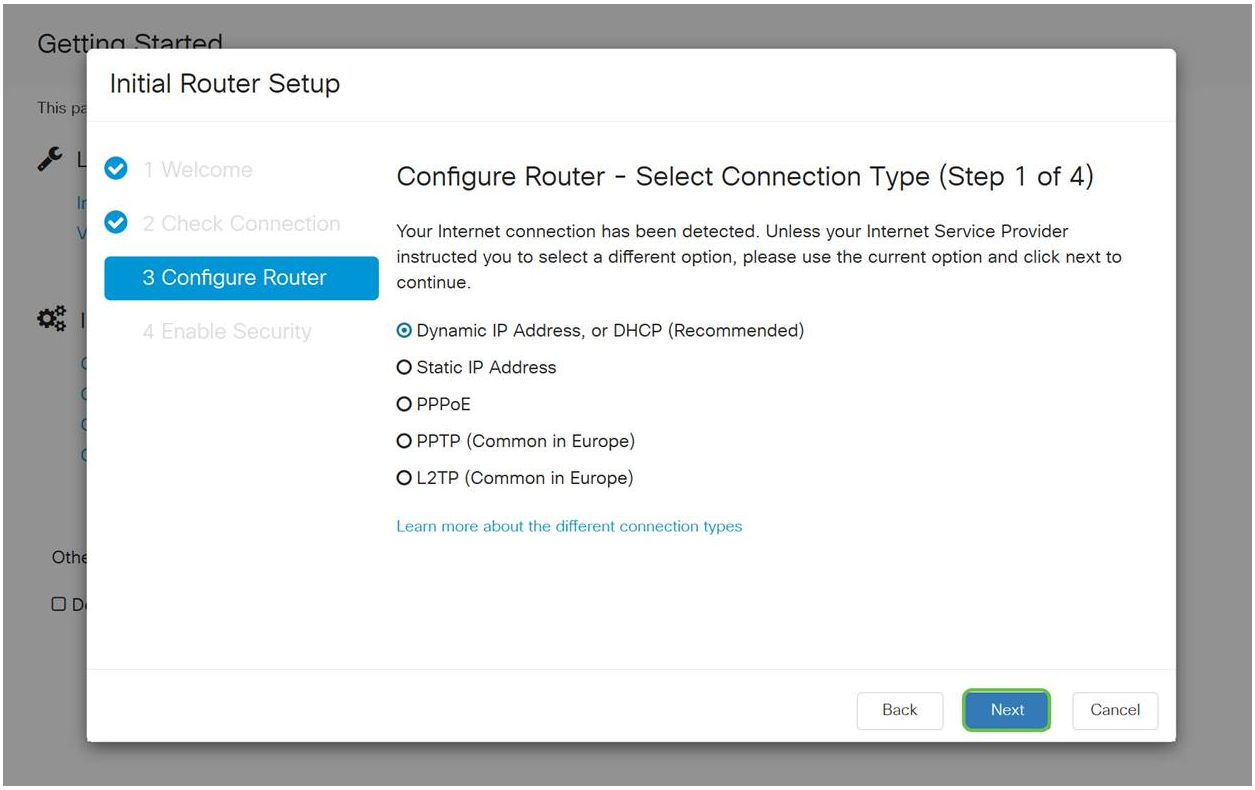
3단계

이 단계에서는 라우터가 연결되어 있는지 확인하는 기본 단계를 다룹니다.이미 확인했으므로 **다음**을 클릭합니다.



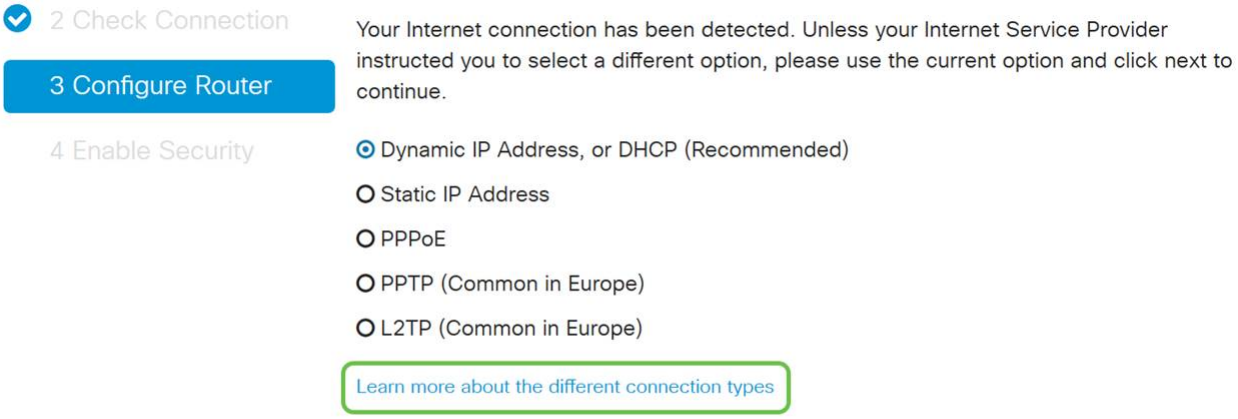
4단계

다음 화면에는 라우터에 IP 주소를 할당하는 옵션이 표시됩니다.이 시나리오에서 DHCP를 선택해야 합니다.Next(**다음)를 클릭합니다**.



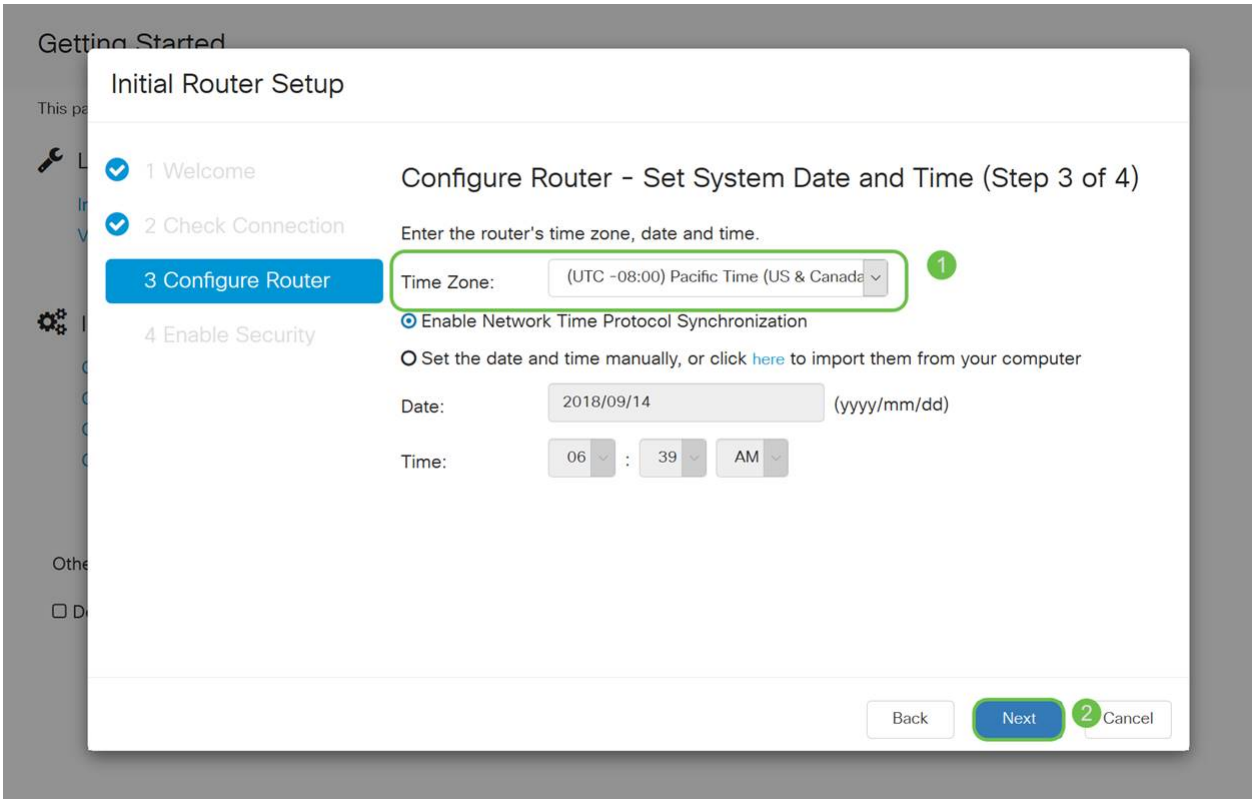
이 초기 설정에 DHCP를 사용해야 하지만 향후 참조를 위해 화면 맨 아래*에 있는 다른 연결 유형*에 *대해 자세히 알아보기*를 선택할 수 있습니다.자세한 내용은 다음 문서를 참조하십시오.

- RV160x 및 RV260x 디바이스의 WAN 컨피그레이션
- RV160 및 RV260에서 고정 라우팅 구성



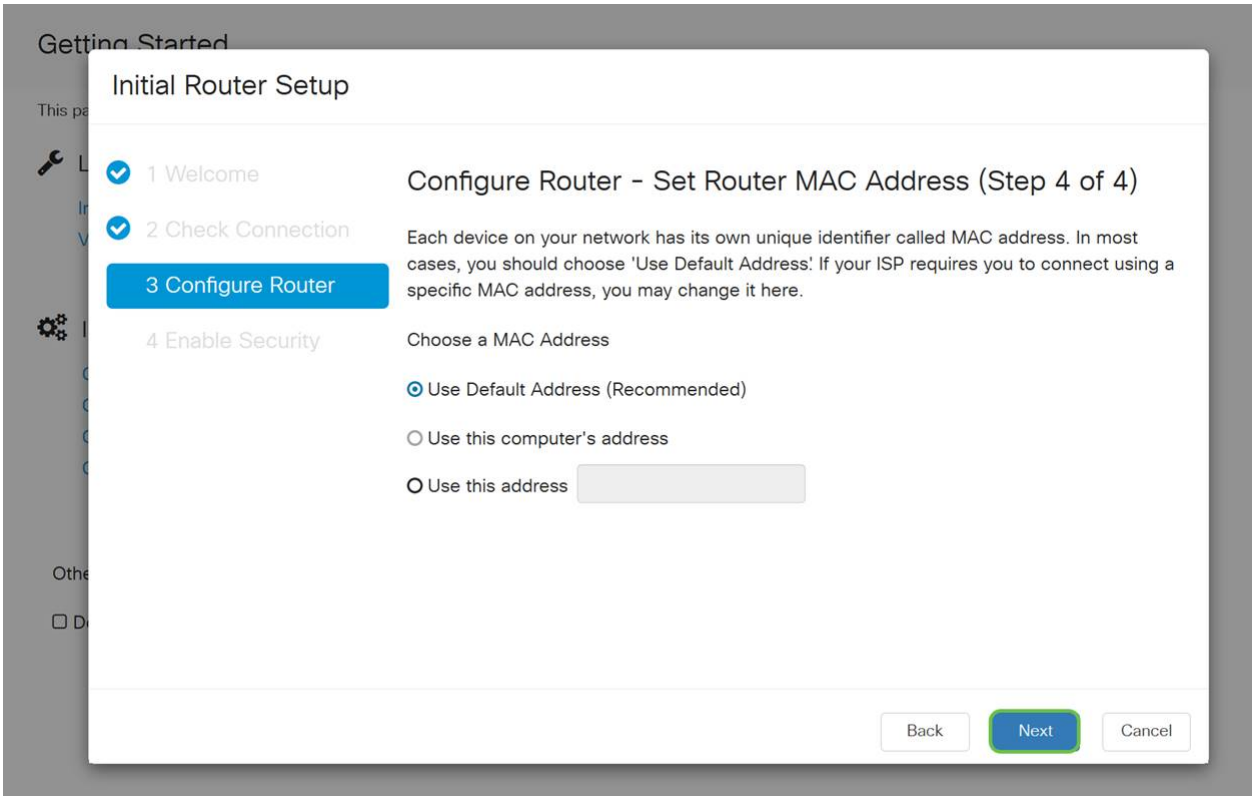
5단계

여기에서는 라우터 시간 설정을 지정하라는 메시지가 표시됩니다.이는 로그 또는 문제 해결 이벤트를 검토할 때 정밀도를 활성화하므로 중요합니다.표준 **시간대**를 선택한 다음 **다음**을 클릭합니다.



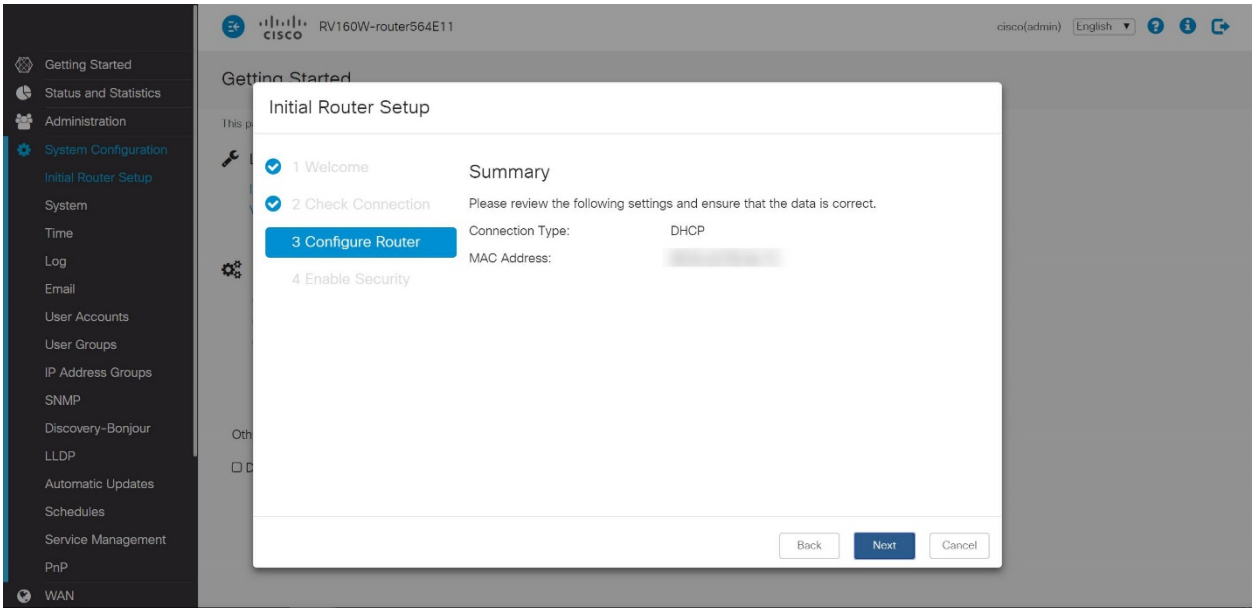
6단계

이 화면에서 디바이스에 할당할 MAC 주소를 선택합니다.대부분의 경우 기본 주소를 사용합니다.Next(**다음)를 클릭합니다**.



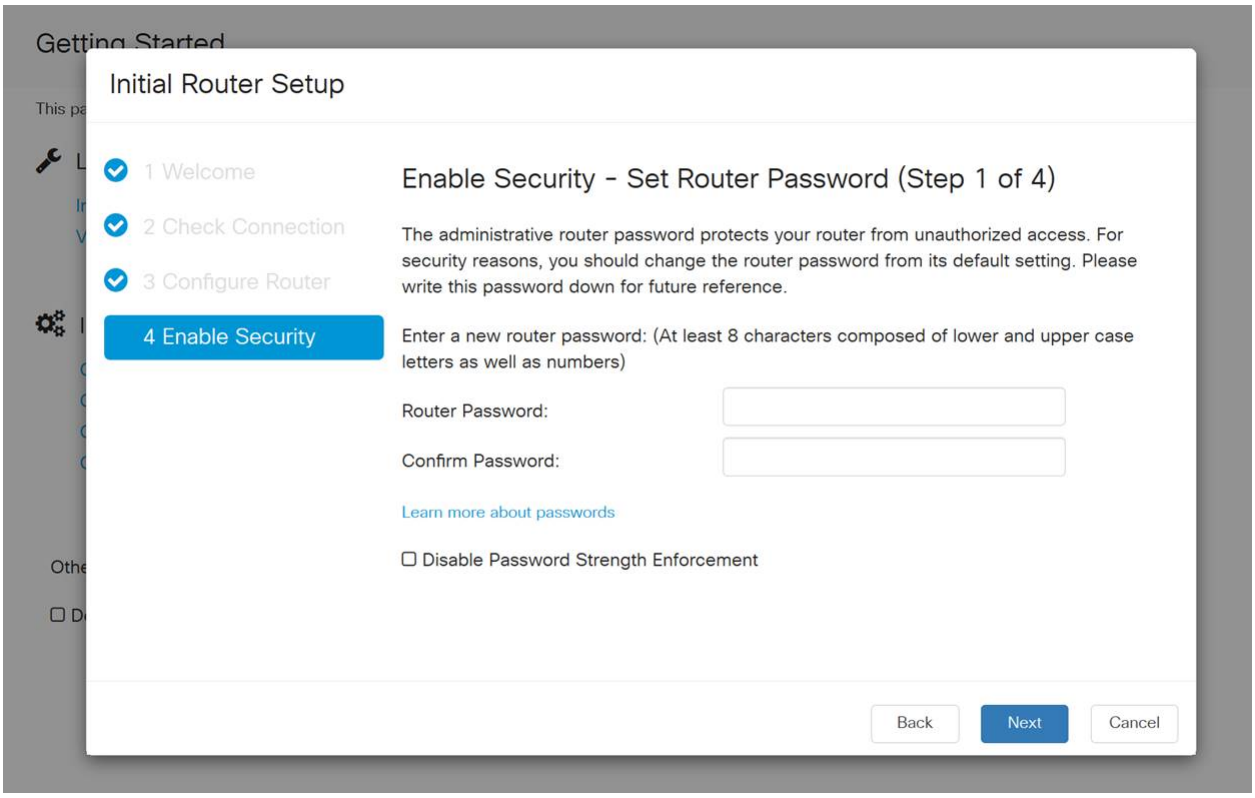
7단계

다음 페이지는 선택한 옵션의 요약입니다.검토 후 **Next(다음)**를 클릭합니다.



8단계

다음 단계에서는 라우터에 로그인할 때 사용할 비밀번호를 선택합니다.비밀번호의 표준은 8자 이상(대문자 및 소문자 모두)을 포함해야 하며 숫자를 포함합니다. **강도** 요구 사항을 준수하는 **비밀번호를** 입력합니다.Next(**다음)를 클릭합니다**.향후 로그인 시 비밀번호를 기록해 두십시오.



Disable Password Strength Enforcement(비밀번호 강도 적용 비활성화)*를* 선택하는 것이 *좋습니다*.이 옵션을 사용하면 123처럼 간단하게 비밀번호를 선택할 수 있습니다. 이 경우 악의적인 사용자가 1-2-3만큼 쉽게 암호를 해독할 수 있습니다.

9단계

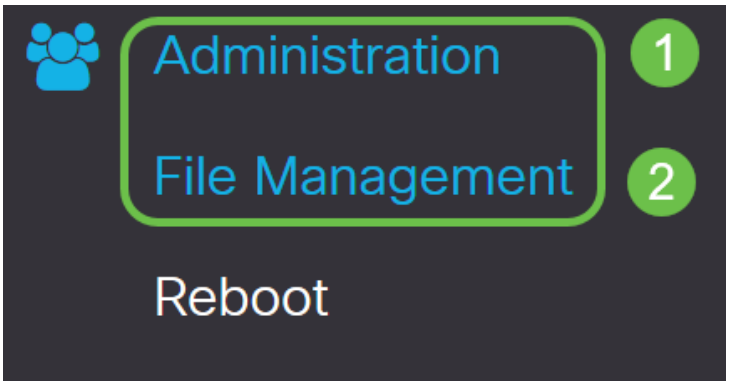
저장 아이콘을 클릭합니다.

필요한 경우 펌웨어 업그레이드

이 부분은 중요한 부분이므로 건너뛰지 마십시오!

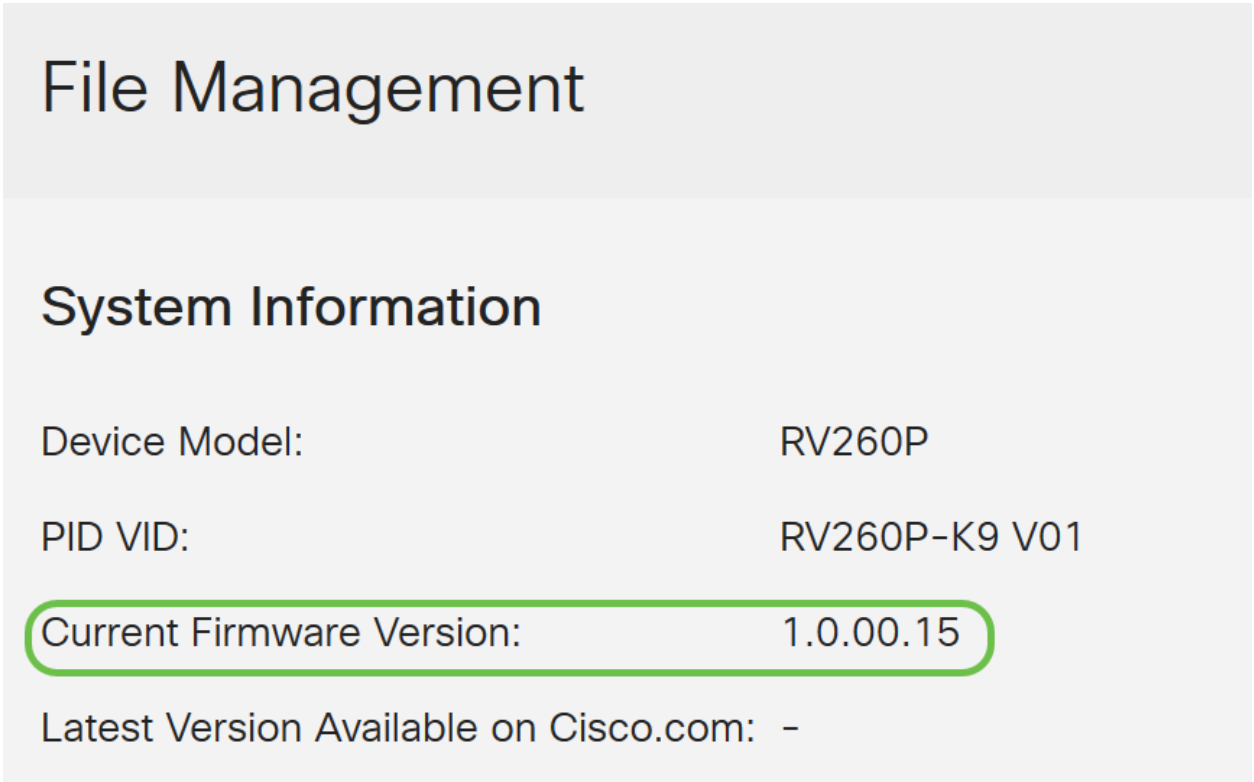
1단계

관리 **> 파일 관리를 선택합니다.**



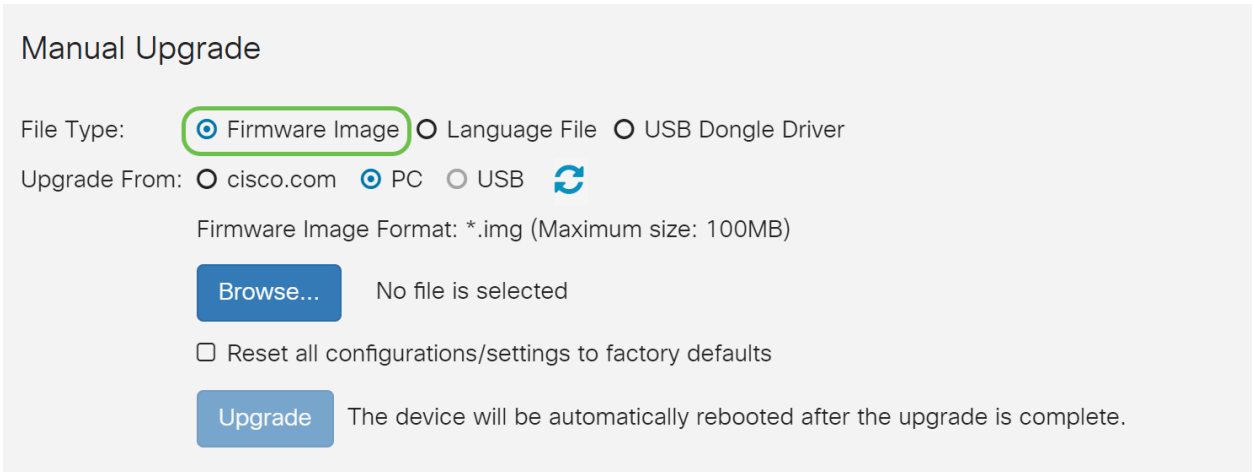
시스템 정보 영역에서 다음 하위 영역에 대해 설명합니다.

- Device Model(디바이스 모델) - 디바이스의 모델을 표시합니다.
- PID VID - 라우터의 제품 ID 및 공급업체 ID입니다.
- 현재 펌웨어 버전 - 디바이스에서 현재 실행 중인 펌웨어.
- Cisco.com에서 사용 가능한 최신 버전 - Cisco 웹 사이트에서 사용할 수 있는 소프트웨어의 최신 버전입니다.
- 펌웨어가 마지막으로 업데이트됨 - 라우터에서 마지막으로 펌웨어 업데이트를 수행한 날짜 및 시간입니다.



2단계

Manual Upgrade(*수동 업그레이드*) 섹션에서 File Type(파일 유형)에 대한 **Firmware Image(펌웨어 이미지)** 라디오 버튼*을 클릭합니다*.



3단계

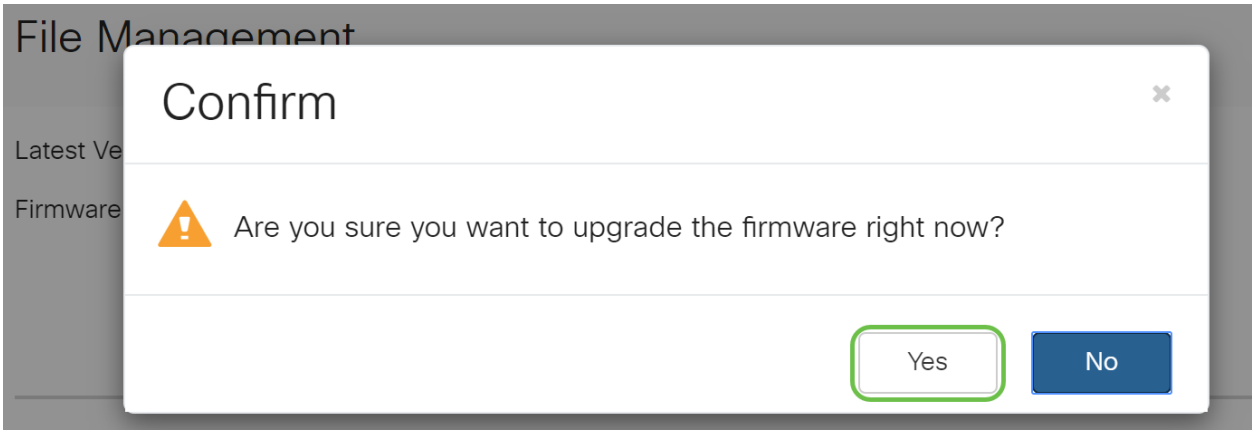
수동 업그레이드 페이지에서 라디오 버튼을 클릭하여 cisco.com을 선택합니다.다른 몇 가지 옵션도 있지만 업그레이드를 수행하는 가장 쉬운 방법입니다.이 프로세스에서는 Cisco Software Downloads 웹 페이지에서 직접 최신 업그레이드 파일을 설치합니다.

4단계

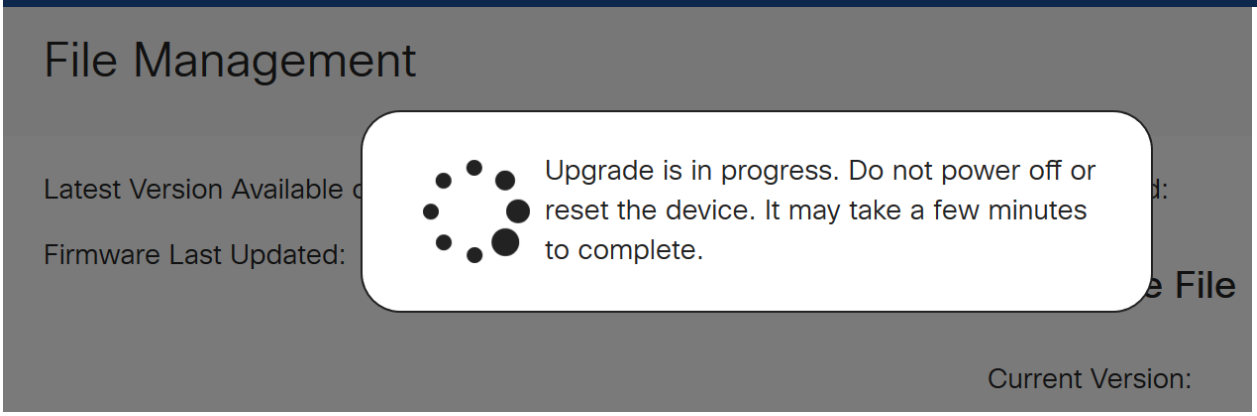
Upgrade(**업그레이드)를 클릭합니다**.

5단계

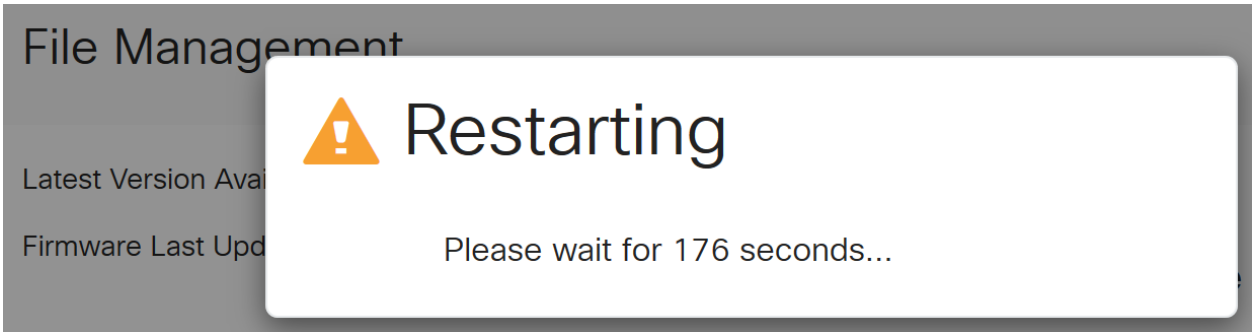
확인 창에서 **예**를 클릭하여 계속합니다.



업데이트 프로세스를 중단 없이 실행해야 합니다.업그레이드가 진행되는 동안 화면에 다음 메시지가 표시됩니다.

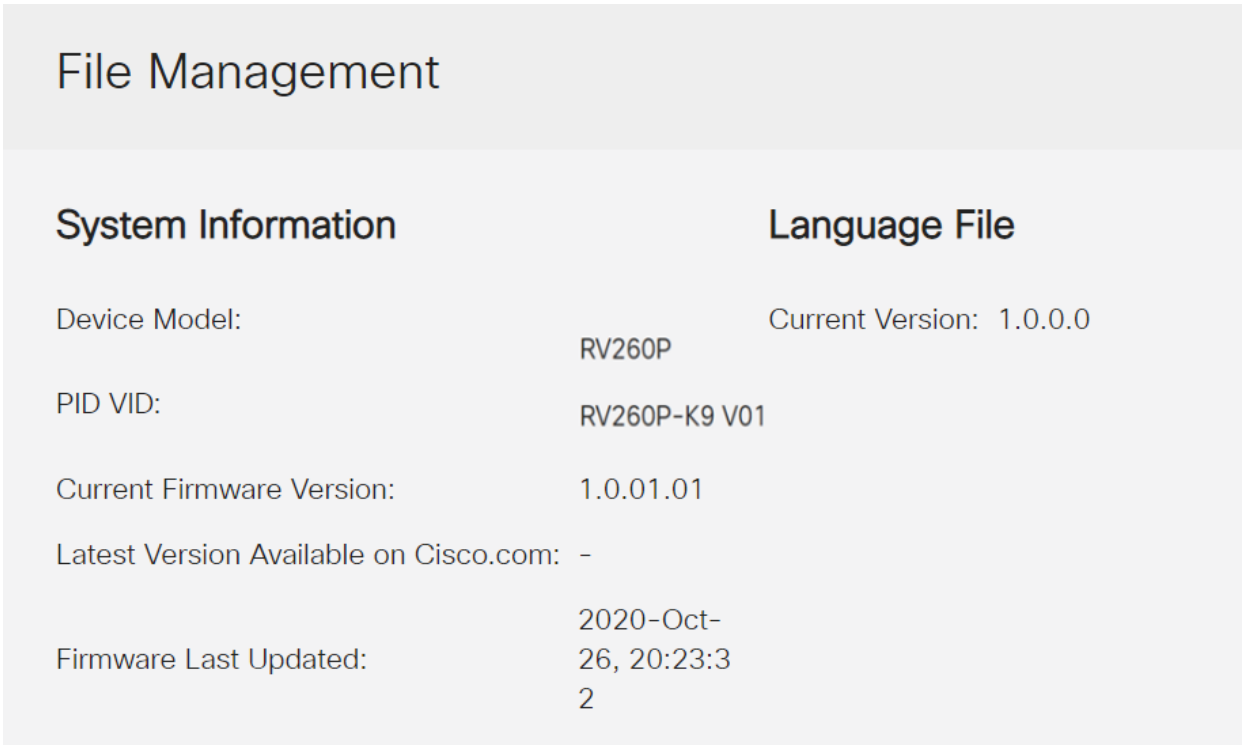


업그레이드가 완료되면 알림 창이 팝업되어 라우터가 프로세스가 완료되는 예상 시간을 카운트다운하여 *다시* 시작됨을 알립니다.이렇게 하면 로그아웃됩니다.



6단계

웹 기반 유틸리티에 다시 로그인하여 라우터 펌웨어가 업그레이드되었는지 확인하고 *시스템 정보*로 스크롤합니다.Current *Firmware Version(현재 펌웨어 버전)* 영역에 업그레이드된 펌웨어 버전이 표시됩니다.



축하합니다. 라우터의 기본 설정이 완료되었습니다!앞으로 몇 가지 컨피그레이션 옵션이 있습니다.

이 옵션에 대해 자세히 알아보고 귀하에게 적용되는지 확인하기 위해 계속 기사를 스크롤해 주시기 바랍니다.원하는 경우 하이퍼링크를 클릭하여 섹션으로 이동할 수 있습니다.

- VLAN 구성(선택 사항)
- IP 주소 수정(선택 사항)
- 고정 IP 주소 추가(선택 사항)
- 네트워크의 메시 무선 부분을 구성할 준비가 되었습니다!

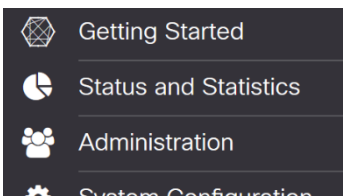
VLAN 구성(선택 사항)

VLAN(Virtual Local Area Network)을 사용하면 LAN(Local Area Network)을 서로 다른 브로드캐스트 도메인으로 논리적으로 분할할 수 있습니다.네트워크에서 민감한 데이터를 브로드캐스트할 수 있는 시나리오에서는 특정 VLAN에 브로드캐스트를 지정하여 보안을 강화하기 위해 VLAN을 생성할 수 있습니다.또한 VLAN을 사용하여 불필요한 대상으로 브로드캐스트 및 멀티캐스트를 보낼 필요가 없으므로 성능을 높일 수 있습니다.VLAN을 생성할 수 있지만, VLAN이 하나 이상의 포트에 수동으로 또는 동적으로 연결될 때까지 이 작업은 적용되지 않습니다.포트는 항상 하나 이상의 VLAN에 속해야 합니다.

VLAN을 생성하지 않으려면 다음 섹션으로 건너뛸 수 있습니다.

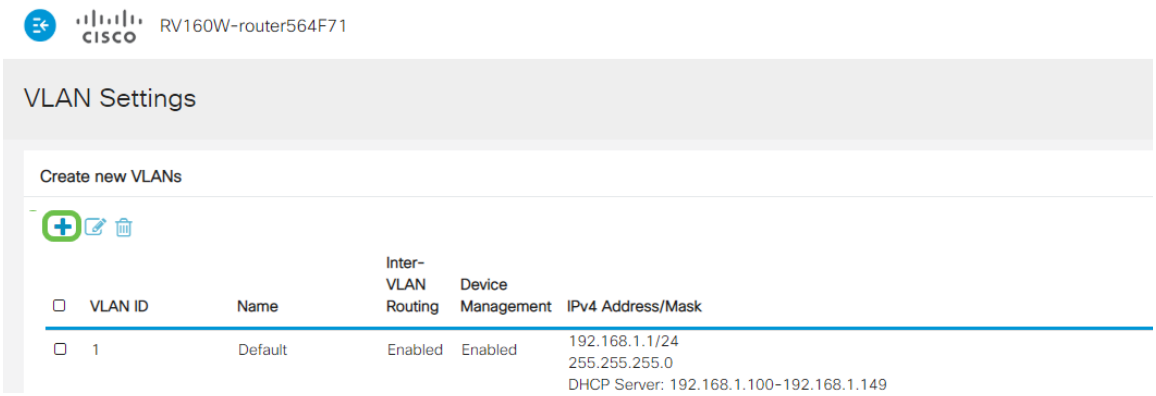
1단계

LAN > VLAN Settings(VLAN 설정)로 이동합니다.



2단계

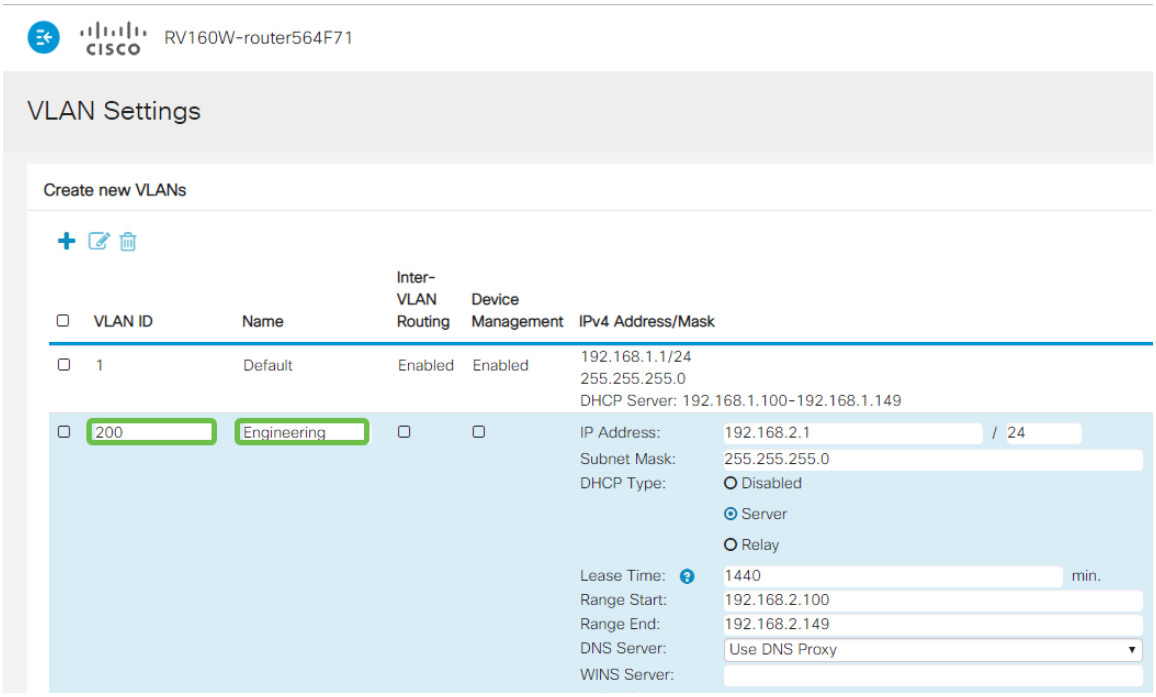
Add(**추가**)를 클릭하여 새 VLAN을 생성합니다.



3단계

생성할 *VLAN ID*와 해당 *이름*을 입력합니다.VLAN *ID* 범위는 1~4093입니다.

VLAN의 *이름*으로 *VLAN ID* 및 **엔지니어링**을 *200*으로 입력했습니다.



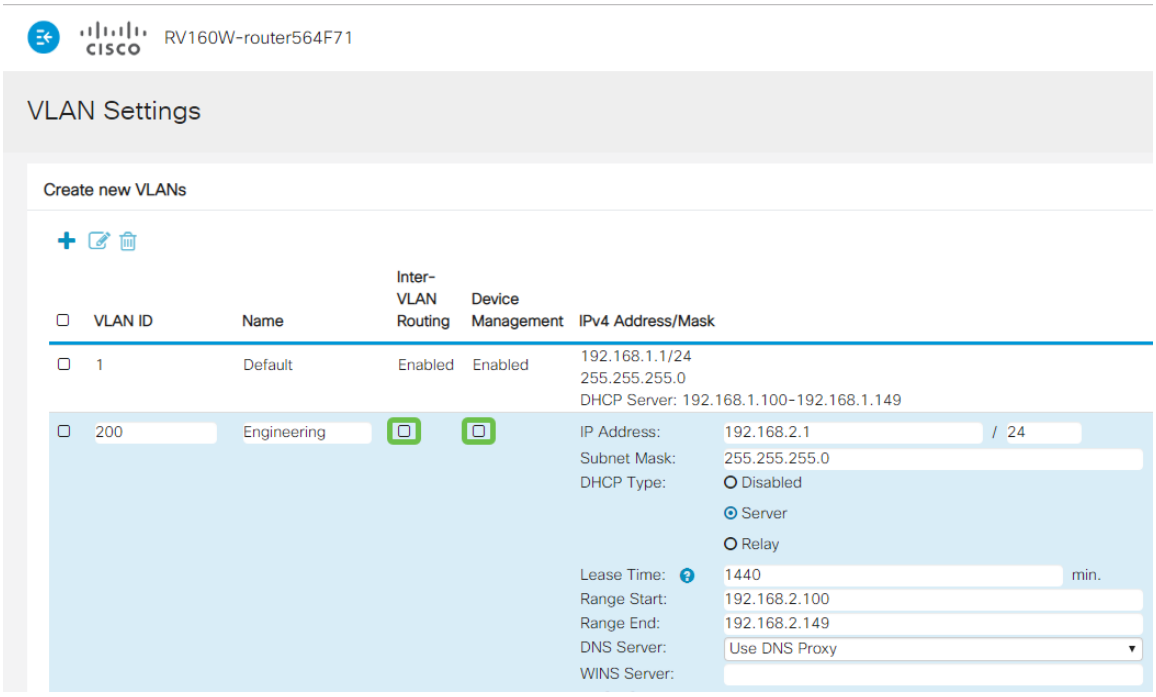
4단계

필요한 경우 *Inter-VLAN Routing* and Device Management(VLAN *간 라우팅* 및 디바이스 *관리)* 모두에 대해 Enabled(활성화됨) 상자를 선택 취소합니다.

VLAN 간 라우팅은 한 VLAN에서 다른 VLAN으로 패킷을 라우팅하는 데 사용됩니다.일반적으로 게스트 네트워크에서 VLAN을 덜 안전하게 유지하려는 게스트 사용자를 격리하려는 경우에는 이 옵션을 사용하지 않는 것이 좋습니다.VLAN이 서로 라우팅해야 하는 경우가 있습니다.이 경우 VLAN 간에 허용하는 특정 트래픽을 구성하려면 Targeted ACL Restrictions(대상 ACL 제한)가 있는 RV34x Router에서 Inter-VLAN Routing(VLAN 간 라우팅)을 확인하십시오.

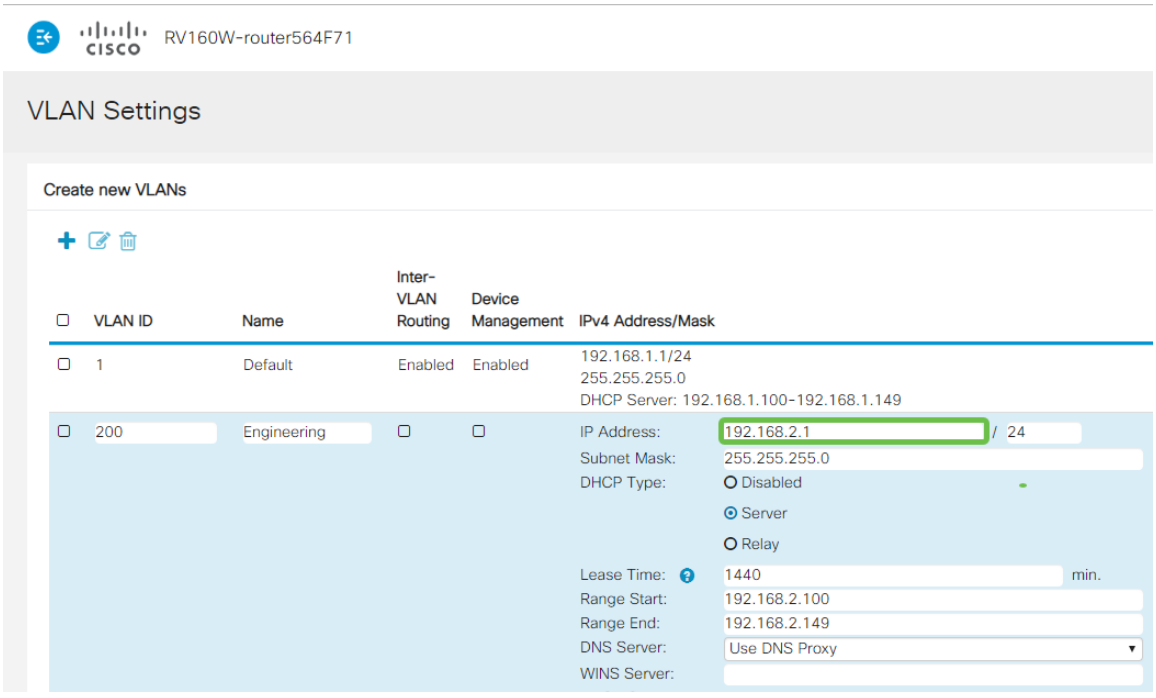
Device Management는 브라우저를 사용하여 VLAN에서 RV260P의 웹 UI에 로그인하고 RV260P를 관리할 수 있는 소프트웨어입니다.게스트 네트워크에서도 비활성화되어야 합니다.

이 예에서는 VLAN을 더 안전하게 *유지하기 위해 Inter-VLAN Routing* 또는 *Device Management*를 활성화하지 않았습니다.



5단계

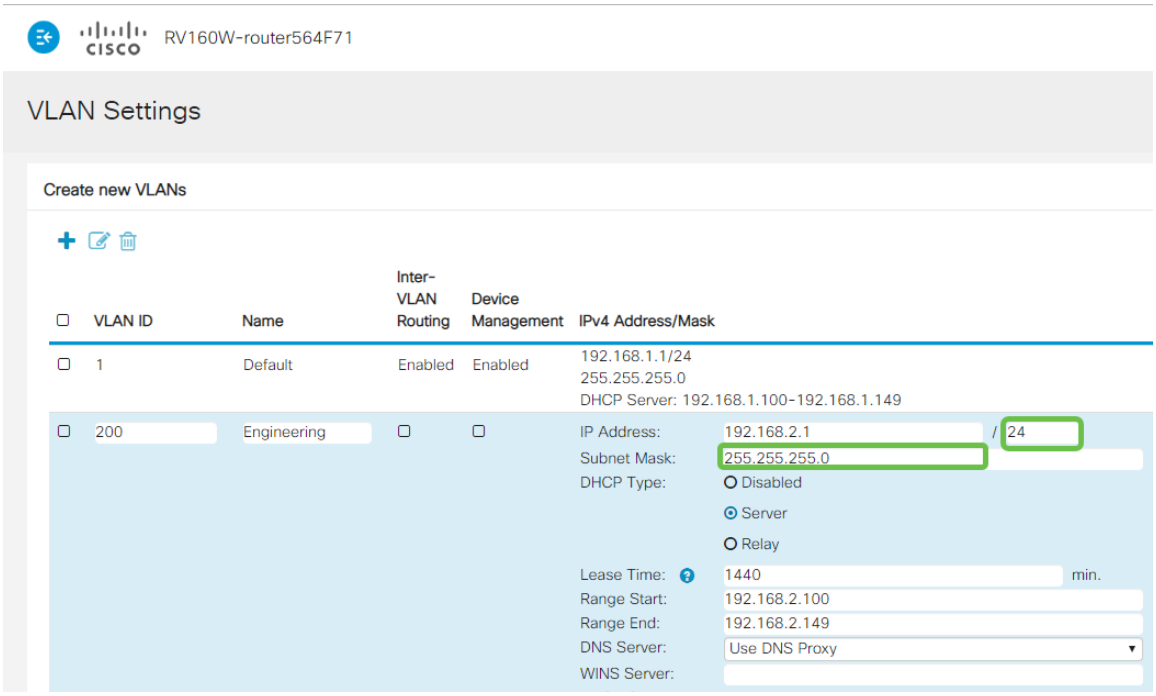
프라이빗 IPv4 주소가 *IP Address* 필드에 자동으로 채워집니다.이 옵션을 선택하면 조정할 수 있습니다.이 예에서는 서브넷에 DHCP에 사용할 수 있는 192.168.2.100-192.168.2.149 IP 주소가 있습니다.192.168.2.1-192.168.2.99 및 192.168.2.150-192.168.2.254은 고정 IP 주소에 사용할 수 있습니다.



6단계

서브넷 마스크 아래의 서브넷 마스크*가* 자동으로 채워집니다.변경한 경우 필드가 자동으로 조정됩니다.

이 데모에서는 서브넷 *마스크*를 **255.255.255.0** 또는 **/24로 둡니다**.



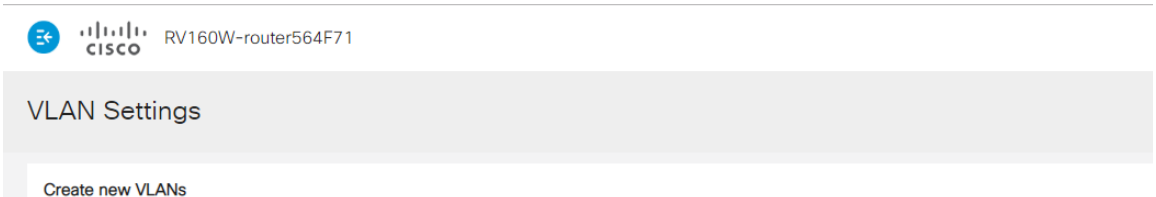
7단계

DHCP*(Dynamic Host Configuration Protocol) 유형을 선택합니다*.다음 옵션은 다음과 같습니다.

Disabled(비활성화됨) - VLAN에서 DHCP IPv4 서버를 비활성화합니다.이는 테스트 환경에서 권장됩니다.이 시나리오에서는 모든 IP 주소를 수동으로 구성해야 하며 모든 통신은 내부 것이어야 합니다.

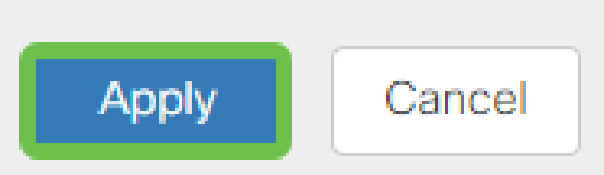
서버 - 가장 자주 사용하는 옵션입니다.

- Lease Time(리스 시간) - 5~43,200분의 시간 값을 입력합니다.기본값은 1440분(24시간과 같음)입니다.
- Range Start and Range End(범위 시작 및 범위 끝) - 동적으로 할당할 수 있는 IP 주소의 시작 및 끝 범위를 입력합니다.
- DNS Server(DNS 서버) - DNS 서버를 프록시로 사용하거나 드롭다운 목록에서 ISP에서 선택합니다.
- WINS 서버 - WINS 서버 이름을 입력합니다.
- DHCP 옵션:
    - 옵션 66 - TFTP 서버의 IP 주소를 입력합니다.
    - 옵션 150 - TFTP 서버 목록의 IP 주소를 입력합니다.
    - 옵션 67 - 구성 파일 이름을 입력합니다.
- 릴레이 - 원격 DHCP 서버 IPv4 주소를 입력하여 DHCP 릴레이 에이전트를 구성합니다.이는 보다 고급 컨피그레이션입니다.



8단계

Apply(**적용**)를 클릭하여 새 VLAN을 생성합니다.



포트에 VLAN 할당

RV260에서 16개의 VLAN을 구성할 수 있으며 WAN(Wide Area Network)용 VLAN은 1개입니다.포트에 없는 VLAN은 *제외해야* 합니다.이렇게 하면 사용자가 특별히 할당한 VLAN/VLAN에 대해서만 해당 포트의 트래픽이 유지됩니다.그것은 모범 사례로 여겨진다.

포트는 액세스 포트 또는 트렁크 포트로 설정할 수 있습니다.

- 액세스 포트 - 하나의 VLAN을 할당했습니다. 태그 없는 프레임이 전달됩니다.
- 트렁크 포트 - 둘 이상의 VLAN을 전달할 수 있습니다.802.1q트렁킹을 사용하면 네이티브 VLAN이 태그 처리되지 않을 수 있습니다.트렁크에서 원하지 않는 VLAN은 제외해야 합니다.

하나의 VLAN에 고유한 포트가 할당되었습니다.

- 액세스 포트로 간주됩니다.
- 이 포트가 할당된 VLAN에 Untagged(태그 없음)라는 레이블이 지정되어야 합니다.
- 다른 모든 VLAN은 해당 포트에 대해 Excluded(제외) 레이블이 지정되어야 합니다.

하나의 포트를 공유하는 두 개 이상의 VLAN:

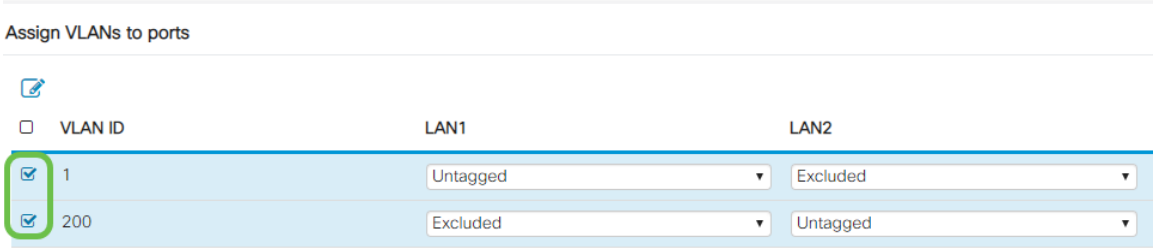
- 트렁크 포트로 간주됨
- VLAN 중 하나에 Untagged(태그 없음)라는 레이블이 지정될 수 있습니다.
- 트렁크 포트의 일부인 나머지 VLAN에 Tagged라는 레이블이 지정되어야 합니다.
- 트렁크 포트에 속하지 않은 VLAN은 해당 포트에 대해 Excluded(제외) 레이블이 지정되어야 합니다.

참고: 이 예에서는 트렁크가 없습니다.

9단계

수정할 *VLAN ID*를 선택합니다.Edit를 **클릭합니다**.

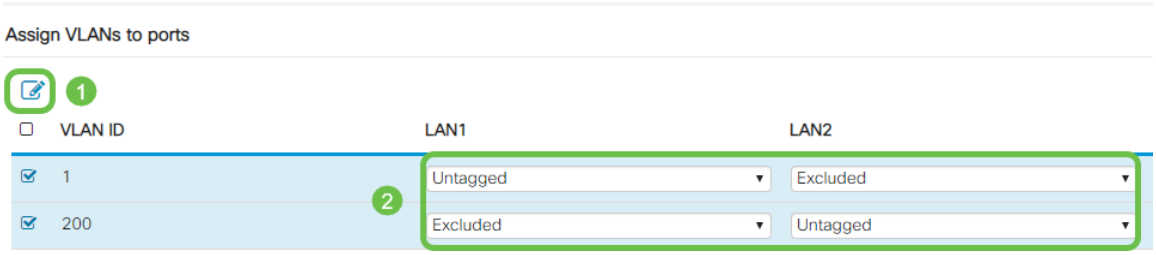
이 예에서는 *VLAN 1*과 VLAN *200을* 선택했습니다.



10단계

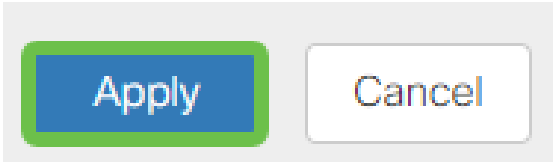
Edit(**수정**)를 클릭하여 LAN 포트에 VLAN을 할당하고 각 설정을 Tagged(태그), Untagged(태그 *없음*) 또는 Excluded(*제외됨*)로 *지정합니다*.

이 예에서 LAN1에서는 VLAN 1을 태그 **없음**으로, VLAN 200을 제외됨으로 **지정했습니다**.LAN2의 경우 VLAN 1은 Excluded(제외됨)로, **VLAN** 200은 Untagged(태그 없음)로 **할당했습니다**.



11단계

Apply(**적용**)를 클릭하여 컨피그레이션을 저장합니다.



이제 새 VLAN을 생성하고 RV260의 포트에 대해 VLAN을 구성했어야 합니다. 프로세스를 반복하여 다른 VLAN을 생성합니다.예를 들어, VLAN300은 192.168.3.x 서브넷의 마케팅용으로 생성되고 VLAN400은 192.168.4.x 서브넷의 어카운팅용으로 생성됩니다.

이것이 VLAN의 기본입니다.하이퍼링크를 클릭하여 Cisco Business Router용 VLAN 모범 사례 및 보안 팁에 대해 자세히 알아보십시오.

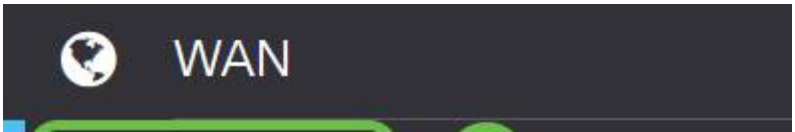
IP 주소 수정(선택 사항)

*초기 설정 마법사*를 완료한 후 VLAN 설정을 편집하여 라우터에 고정 IP 주소를 설정할 수 있습니다.초기 설정 마법사 재실행을 건너뛰고 이 변경을 수행하려면 아래 단계를 수행하십시오.

IP 주소를 편집할 필요가 없는 경우 이 문서의 다음 섹션으로 이동할 수 있습니다.

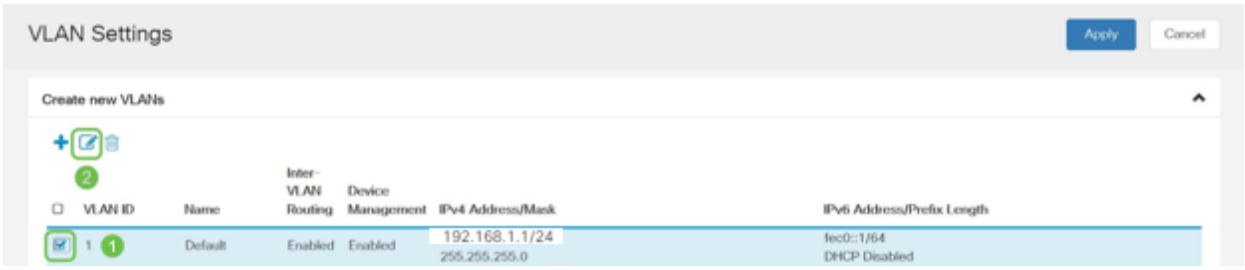
1단계

왼쪽 메뉴 모음에서 **LAN > VLAN Settings(VLAN 설정)를** 클릭합니다.



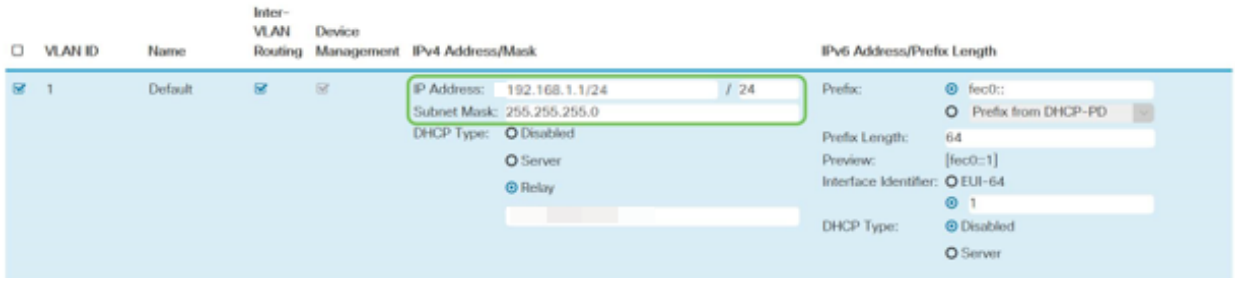
2단계

그런 다음 라우팅 디바이스가 포함된 VLAN을 선택한 다음 **수정 아이콘**을 클릭합니다.



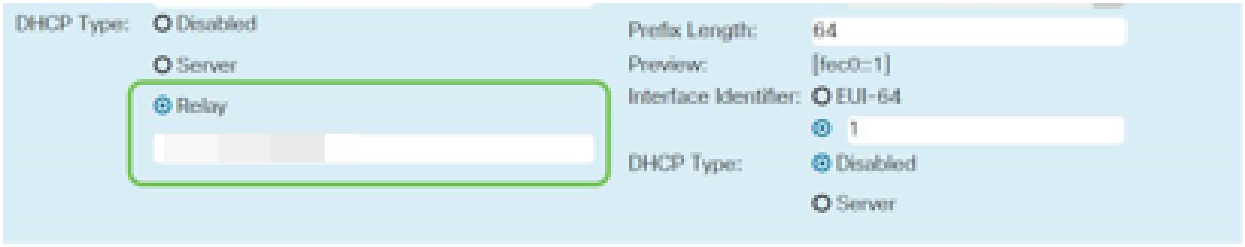
3단계

원하는 **고정 IP 주소**를 입력하고 오른쪽 상단 모서리에서 Apply를 클릭합니다.



4단계(선택 사항)

라우터가 IP 주소를 할당하는 DHCP 서버/디바이스가 아닌 경우 DHCP 릴레이 기능을 사용하여 DHCP 요청을 특정 IP 주소로 보낼 수 있습니다.IP 주소는 WAN/인터넷에 연결된 라우터일 가능성이 높습니다.



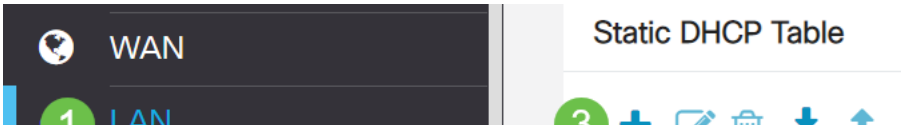
고정 IP 추가

특정 디바이스가 다른 VLAN에 도달할 수 있도록 하려면 해당 디바이스에 고정 로컬 IP 주소를 부여하고 액세스 규칙을 생성하여 액세스할 수 있도록 할 수 있습니다.이는 VLAN 간 라우팅이 활성화된 경우에만 작동합니다.정적 IP가 유용할 수 있는 다른 상황이 있습니다.고정 IP 주소 설정에 대한 자세한 내용은 Cisco 비즈니스 하드웨어에서 고정 IP 주소 설정을 위한 모범 사례를 참조하십시오.

고정 IP 주소를 추가할 필요가 없는 경우 이 문서의 다음 섹션으로 이동하여 액세스 포인트를 구성할 수 있습니다.

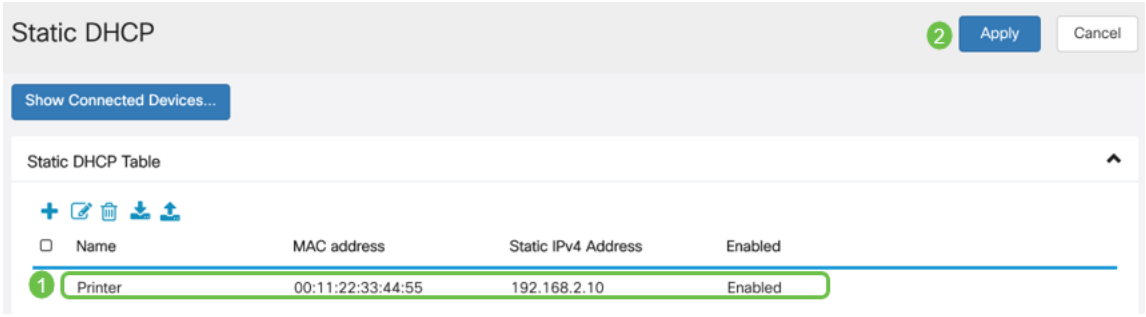
1단계

LAN > Static DHCP로 이동합니다.더하기 아이콘을 클릭합니다.



2단계

디바이스에 대한 **정적 DHCP** 정보를 추가합니다.이 예에서는 디바이스가 프린터입니다 .



축하합니다. RV260P 라우터의 구성을 완료했습니다.이제 Cisco Business Wireless 디바이스를 구성합니다.

CBW140AC 구성

CBW140AC 발신

먼저 CBW140AC의 PoE 포트에서 RV260P의 PoE 포트에 이더넷 케이블을 연결합니다 .RV260P의 처음 4개 포트는 PoE를 제공할 수 있으므로 모든 포트를 사용할 수 있습니다.

표시등 표시등의 상태를 확인합니다.액세스 포인트를 부팅하는 데 약 10분이 걸립니다 .LED는 여러 패턴에서 녹색으로 깜박이며 녹색, 빨간색, 황색을 빠르게 번갈아 가며 녹색이 다시 됩니다.LED 색상 강도와 색조가 단위마다 약간 다를 수 있습니다.LED 표시등이 녹색으로 깜박이면 다음 단계로 진행합니다.

기본 AP의 PoE 이더넷 업링크 포트는 LAN에 업링크를 제공하는 데만 사용할 수 있으며 다른 기본 지원 또는 메시 익스텐더 장치에 연결하지 않습니다.

액세스 포인트가 새로운 것이 아닌 경우, Wi-Fi 옵션에 표시할 *CiscoBusiness-Setup* SSID의 공장 기본 설정으로 재설정되었는지 확인합니다.이에 대한 자세한 내용은 RV260 라우터의 How to Reboot and Reset to Factory Default Settings를 참조하십시오 .

웹 UI에서 140AC 기본 무선 액세스 포인트 설정

모바일 응용 프로그램 또는 웹 UI를 사용하여 액세스 포인트를 설정할 수 있습니다.이 문서에서는 설정에 웹 UI를 사용합니다. 따라서 더 많은 구성 옵션을 제공하지만 좀 더 복잡합니다.다음 섹션에 모바일 애플리케이션을 사용하려면 을 클릭하여 모바일 애플리케이션 지침에 액세스합니다.

연결에 문제가 있는 경우 이 문서의 무선 문제 해결 팁 섹션을 참조하십시오.

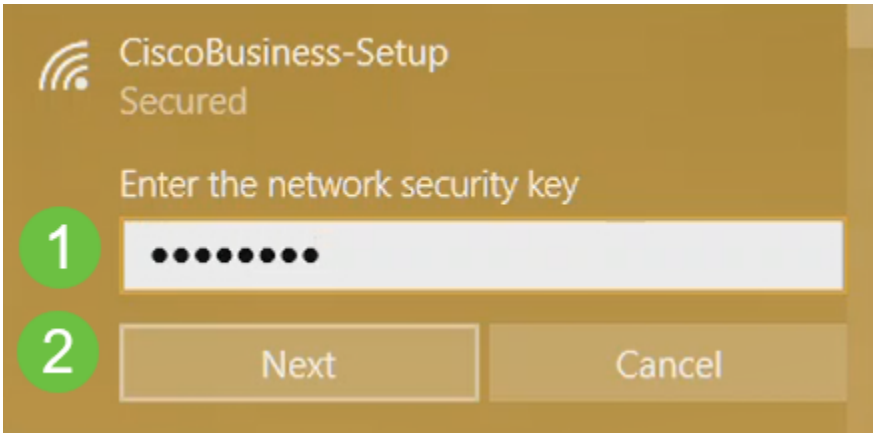
1단계

PC에서 **Wi-Fi 아이콘**을 클릭하고 *CiscoBusiness-Setup* 무선 네트워크를 선택합니다.연결을 클릭합니다.

액세스 포인트가 새로운 것이 아닌 경우, Wi-Fi 옵션에 표시할 *CiscoBusiness-Setup* SSID의 공장 기본 설정으로 재설정되었는지 확인합니다.

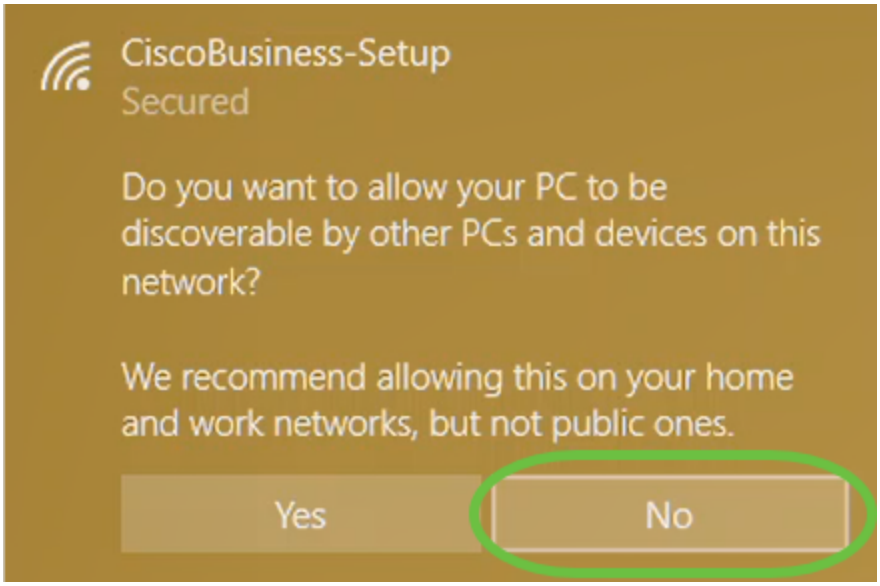
2단계

암호 **cisco123**을 입력하고 **Next**를 클릭합니다.



3단계

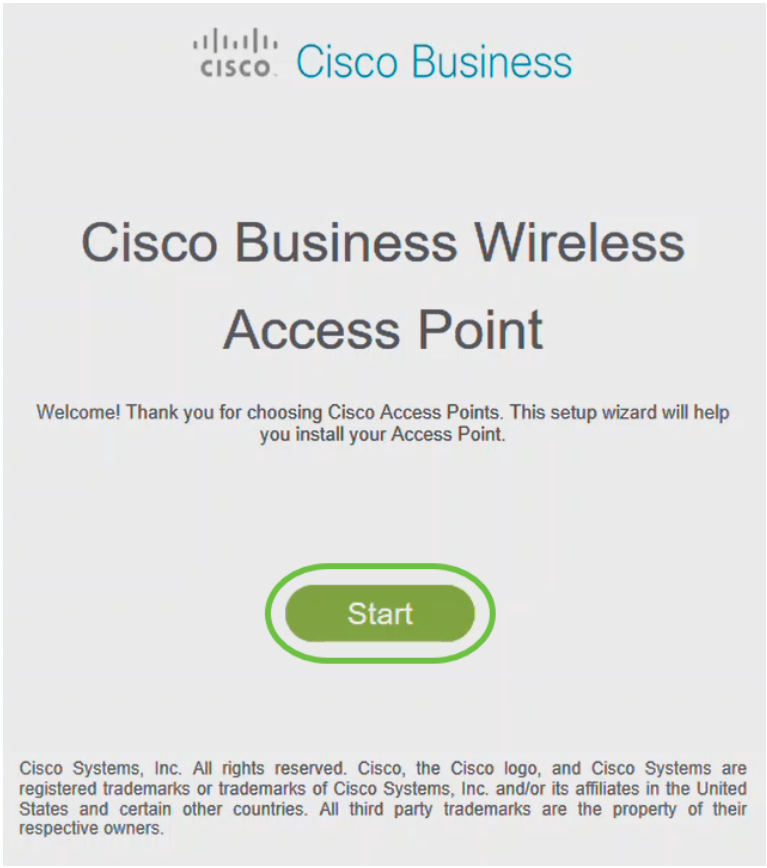
다음 화면이 표시됩니다.한 번에 하나의 디바이스만 구성할 수 있으므로 **No**를 클릭합니다.



CiscoBusiness-Setup SSID에는 하나의 디바이스만 연결할 수 있습니다.두 번째 디바이스가 연결을 시도하면 연결할 수 없습니다.SSID에 연결할 수 없고 비밀번호를 검증한 경우 다른 디바이스에서 연결을 했을 수 있습니다.AP를 다시 시작하고 다시 시도하십시오.

4단계

연결되면 웹 브라우저가 CBW AP 설정 마법사로 자동 리디렉션됩니다.그렇지 않은 경우 Internet Explorer, Firefox, Chrome 또는 Safari와 같은 웹 브라우저를 엽니다.주소 표시줄에 http://ciscobusiness.cisco을 **입력하고 Enter**를 **누릅니다**.웹 페이지에서 시작을 클릭합니다.



웹 페이지가 표시되지 않으면 몇 분 정도 기다리거나 페이지를 다시 로드하십시오.이 초기 설정 후 https://ciscobusiness.cisco을 사용하여 로그인합니다.웹 브라우저가 http://으로 자동 입력되는 경우 *https://*에 수동으로 입력하여 액세스해야 합니다.

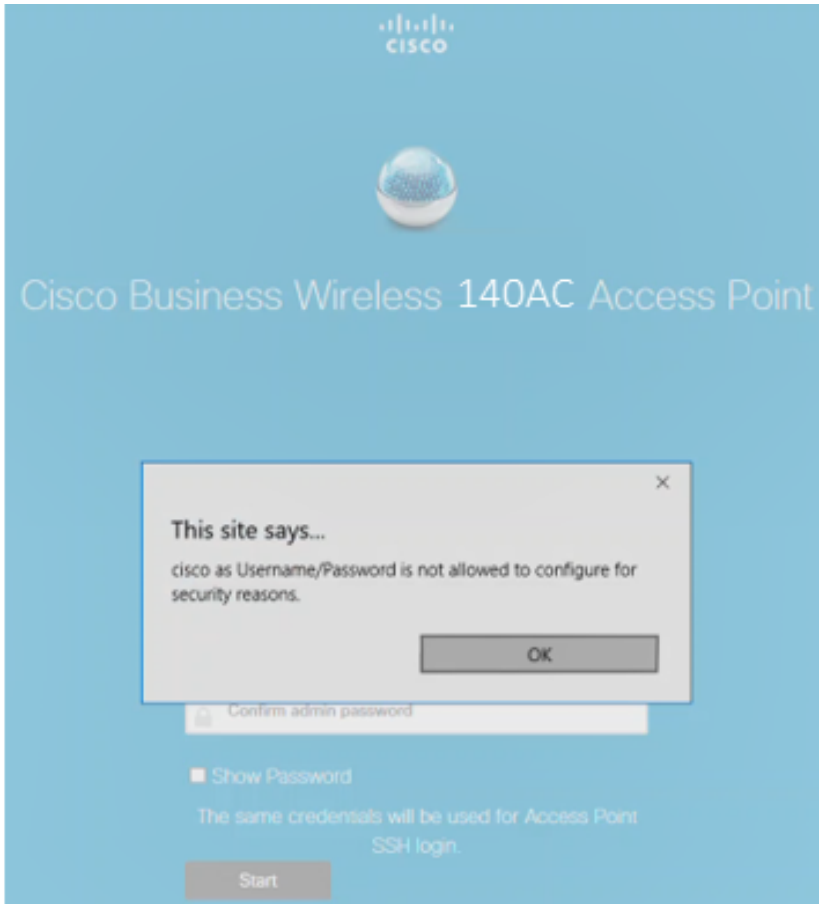
5단계

다음을 입력하여 *관리자 계정*을 생성합니다.

- 관리자 사용자 이름(최대 24자)
- 관리자 비밀번호
- 관리자 암호 확인

비밀번호 표시 옆의 확인란을 선택하여 비밀번호를 표시하도록 선택할 수 *있습니다*.**시작**을 **클릭합니다**.

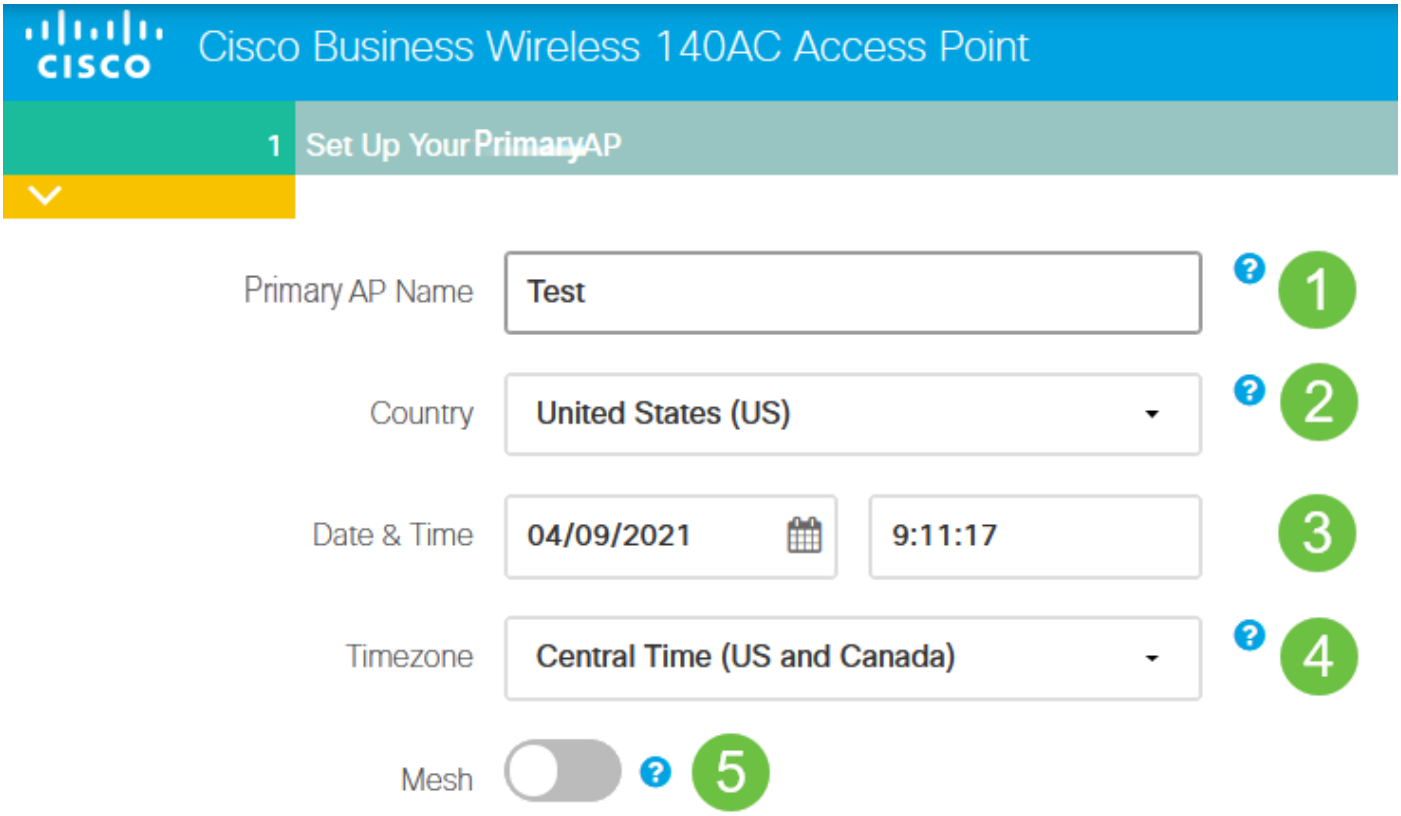
cisco 또는 사용자 이름 또는 비밀번호 필드에서 이를 사용하지 마십시오.이렇게 하면 아래와 같은 오류 메시지가 표시됩니다.



6단계

다음을 입력하여 *기본 AP*를 설정합니다.

- 기본 AP 이름
- 국가
- 날짜 및 시간
- 표준 시간대
- 메시



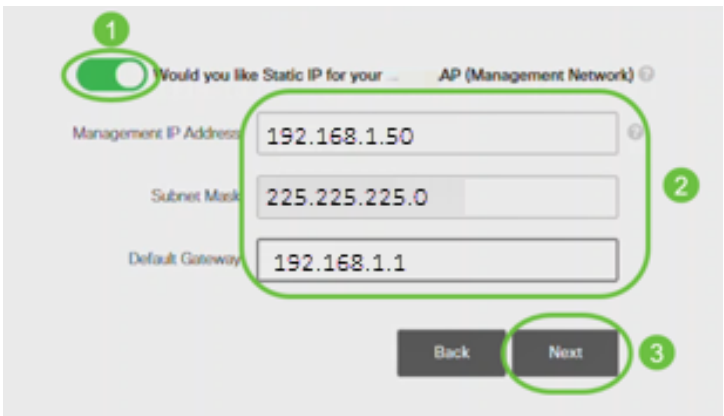
*메시*는 메시 네트워크를 생성하려는 경우에만 활성화해야 합니다.기본적으로 비활성화되어 있습니다.

7단계

(선택 사항) 관리 목적으로 *CBW*140AC*에 대해 고정 IP*를 활성화할 수 있습니다.그렇지 않으면 인터페이스가 DHCP 서버에서 IP 주소를 가져옵니다.고정 IP를 구성하려면 다음을 입력합니다.

- 관리 IP 주소
- 서브넷 마스크
- 기본 게이트웨이

Next(**다음)를 클릭합니다**.



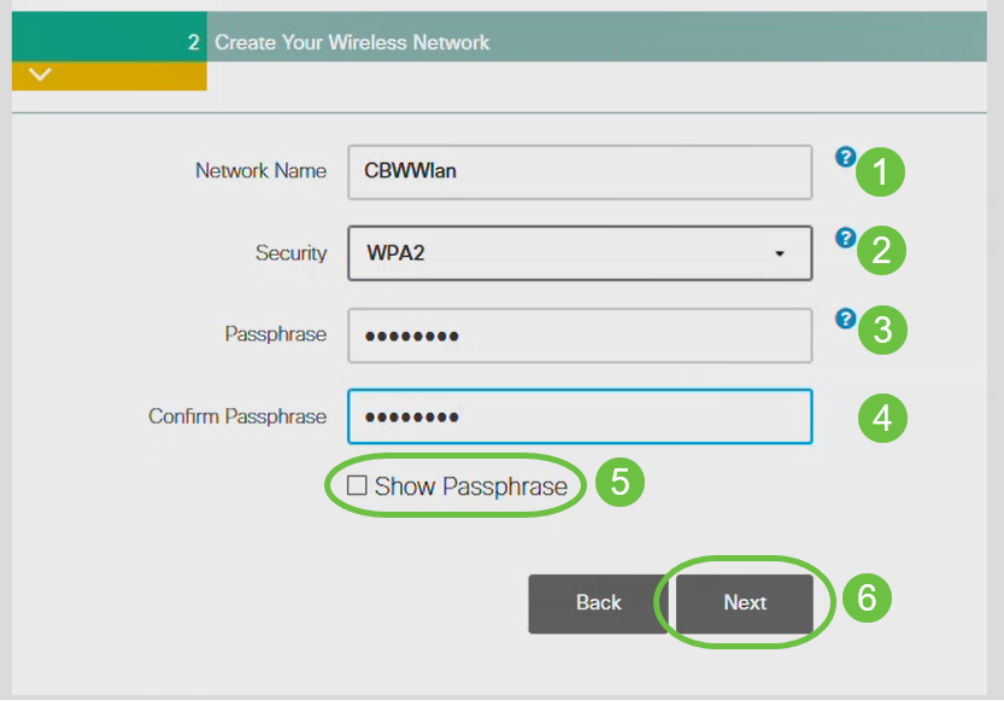
기본적으로 이 옵션은 비활성화되어 있습니다.

8단계

다음을 입력하여 *무선 네트워크*를 생성합니다.

- 네트워크 이름
- 보안 선택
- 암호
- 암호 확인
- (선택 사항) Show Passphrase(패스프레이즈 표시) 확인란을 선택합니다.

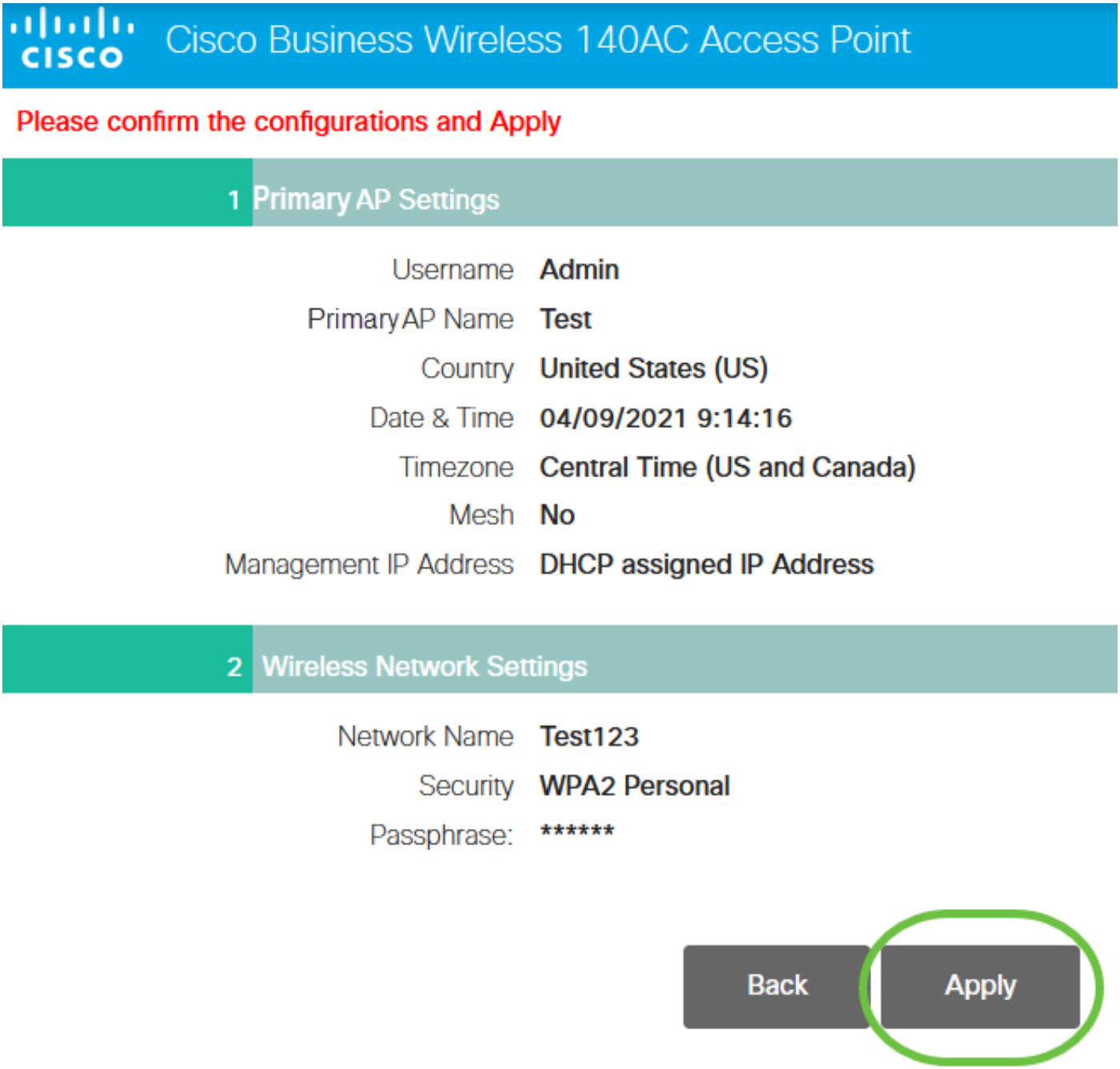
Next(**다음)를 클릭합니다**.



WPA2(Wi-Fi Protected Access) 버전 2(WPA2)는 현재 Wi-Fi 보안 표준입니다.

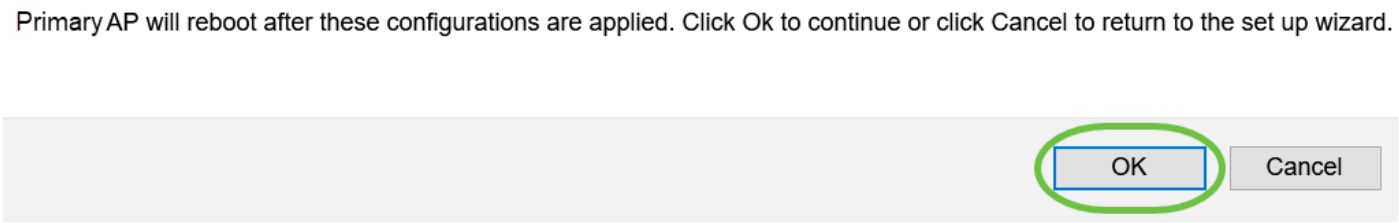
9단계

설정을 확인하고 Apply를 **클릭합니다**.

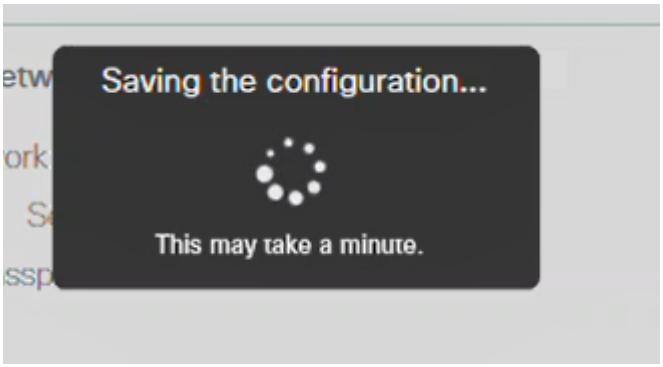


10단계

확인을 클릭하여 설정을 적용합니다.



컨피그레이션을 저장하고 시스템이 재부팅되는 동안 다음 화면이 표시됩니다.10분 정도 걸릴 수 있습니다.

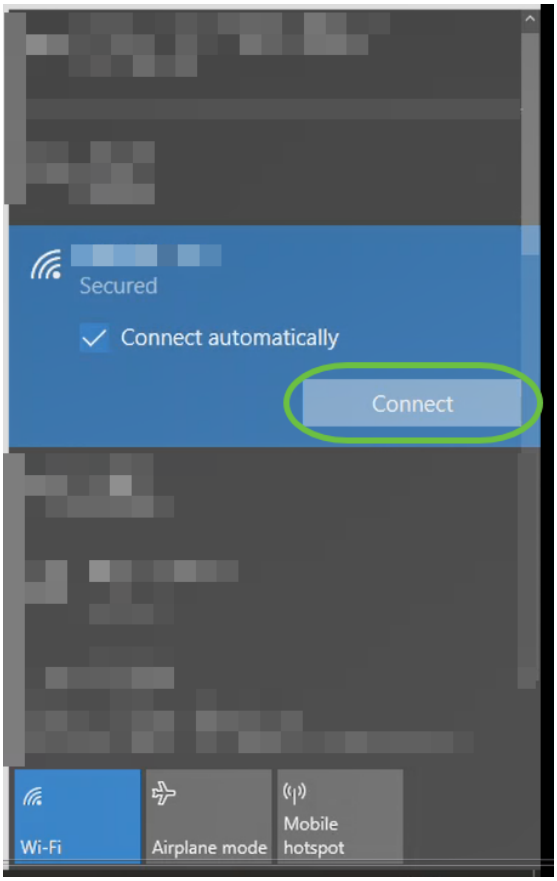


재부팅하는 동안 액세스 포인트의 LED가 여러 색상 패턴을 거칩니다.LED가 녹색으로 깜박이면 다음 단계로 진행합니다.LED가 빨간색 깜박임 패턴을 통과하지 못하면 네트워크에 DHCP 서버가 없음을 나타냅니다.AP가 스위치 또는 DHCP 서버가 있는 라우터에 연결되어 있는지 확인합니다.

11단계

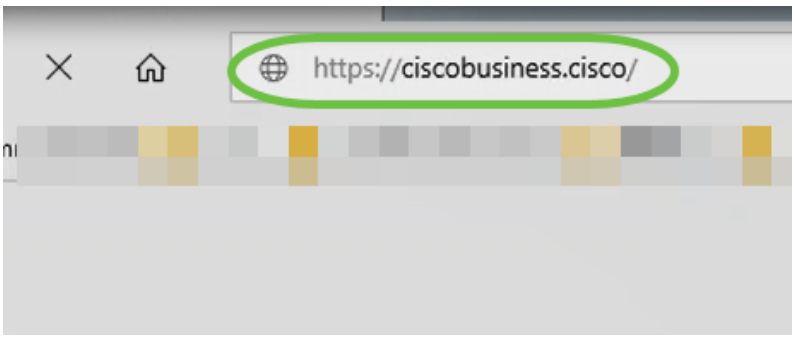
PC의 무선 옵션으로 이동하여 구성한 네트워크를 선택합니다.**연결**을 **클릭합니다**.

재부팅 *후 CiscoBusiness-Setup* SSID가 사라집니다.



12단계

웹 브라우저를 열고 https://*[CBW AP의 IP 주소]를 입력합니다.*또는 주소 표시줄에 *https://ciscobusiness.cisco*를 입력하고 Enter 키를 누를 수 있습니다.



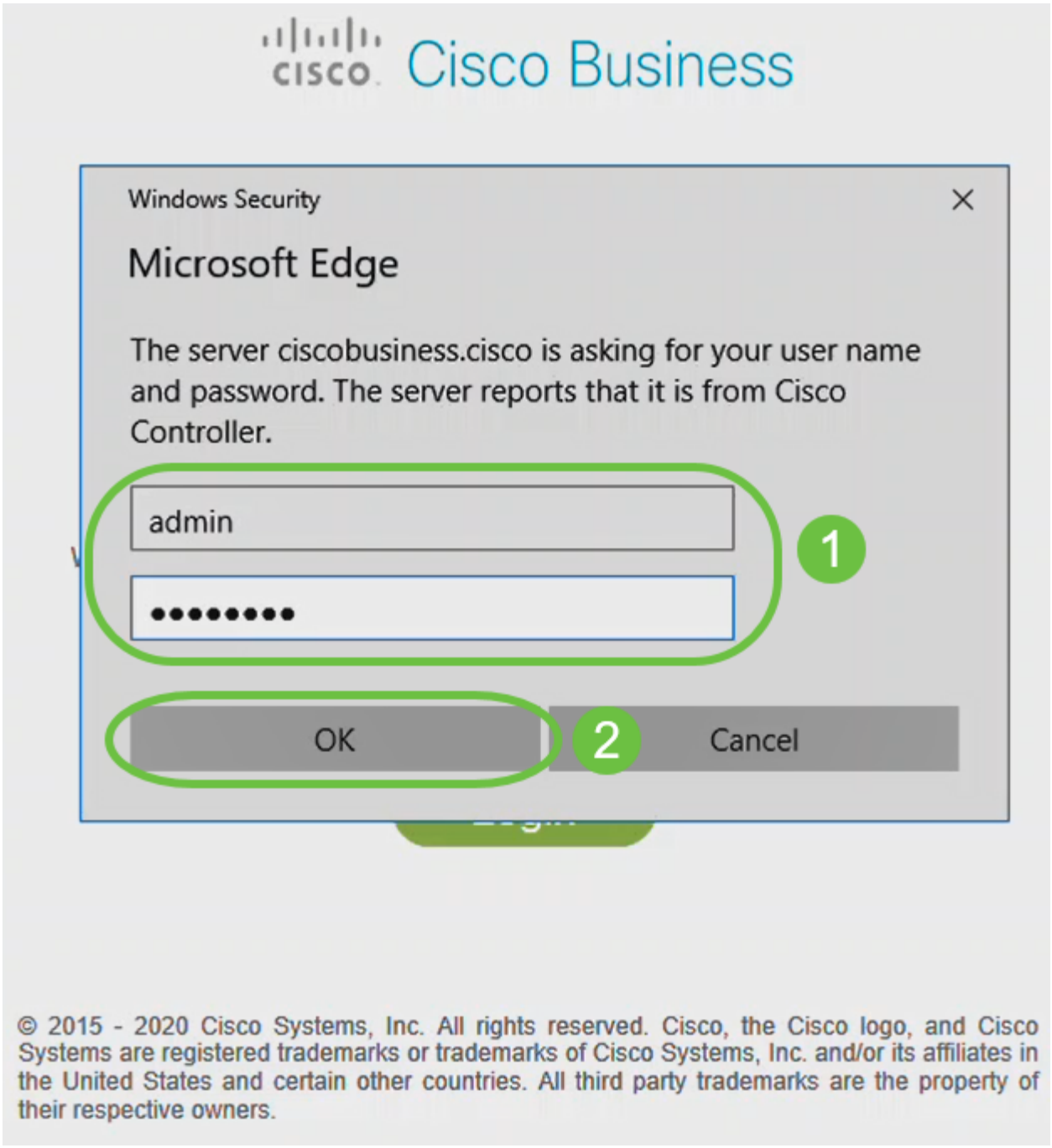
이 단계에서 https를 *입력하고 http*를 *입력하지* 마십시오.

13단계

Login(**로그인)을 클릭합니다**.

14단계

구성된 자격 증명을 사용하여 로그인합니다.**확인을 클릭합니다**.



15단계

AP의 웹 UI 페이지에 액세스할 수 있습니다.

무선 문제 해결 팁

문제가 있는 경우 다음 팁을 확인하십시오.

- 올바른 SSID(Service Set Identifier)가 선택되었는지 확인합니다.무선 네트워크에 대해 생성한 이름입니다.
- 모바일 앱 또는 랩톱에 대한 VPN의 연결을 끊습니다.모바일 서비스 공급자가 사용자가 알지 못할 수도 있는 VPN에 연결되어 있을 수도 있습니다.예를 들어 Google Fi를 서비스 제공자로 사용하는 Android(픽셀 3) 폰에는 알림 없이 자동 연결하는 내장형 VPN이 있습니다.기본 AP를 찾으려면 이 기능을 비활성화해야 합니다.
- 기본 AP에 https://<기본 AP의 IP 주소>로 로그인합니다.
- 초기 설정을 한 후에는 ciscobusiness.*cisco*에 로그인할지 아니면 웹 브라우저에 IP 주소를 입력할지 여부에 https://가 사용되는지 확인하십시오.설정에 따라, 처음 로그인했을 때 사용한 것이므로 컴퓨터가 http://으로 자동 입력될 수 있습니다.
- AP를 사용하는 동안 웹 UI 또는 브라우저 문제에 액세스하는 데 도움이 되도록 웹 브라우저(이 경우 Firefox)에서 Open(열기) 메뉴를 클릭하고 Help(도움말) > Troubleshooting Information(문제 해결 정보)으로 이동한 다음 Firefox 새로 고침을 클릭합니다.

웹 UI를 사용하여 CBW142ACM 메시 익스텐더 구성

이 네트워크 설정을 위한 홈 스트레치에는 메시 확장기만 추가하면 됩니다!

1단계

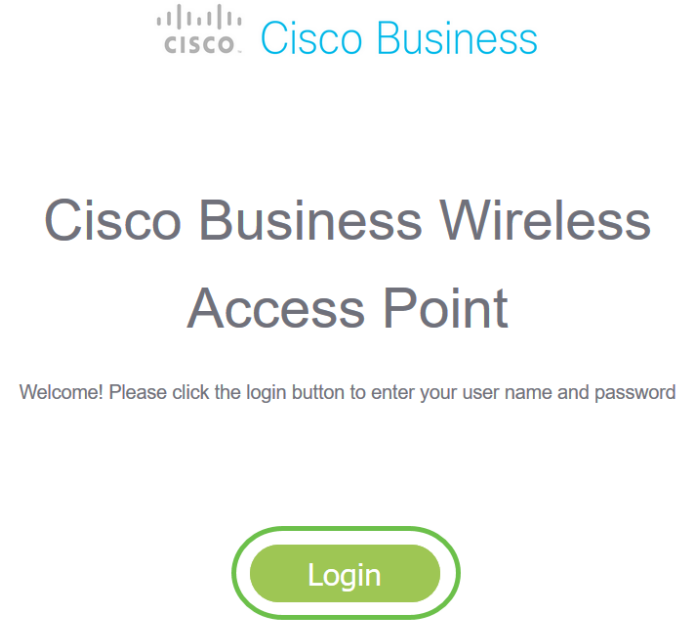
선택한 위치의 벽에 두 개의 메시 확장기를 연결합니다.각 메시 익스텐더의 MAC 주소를 기록합니다.

2단계

메시 익스텐더가 부팅될 때까지 10분 정도 기다립니다.

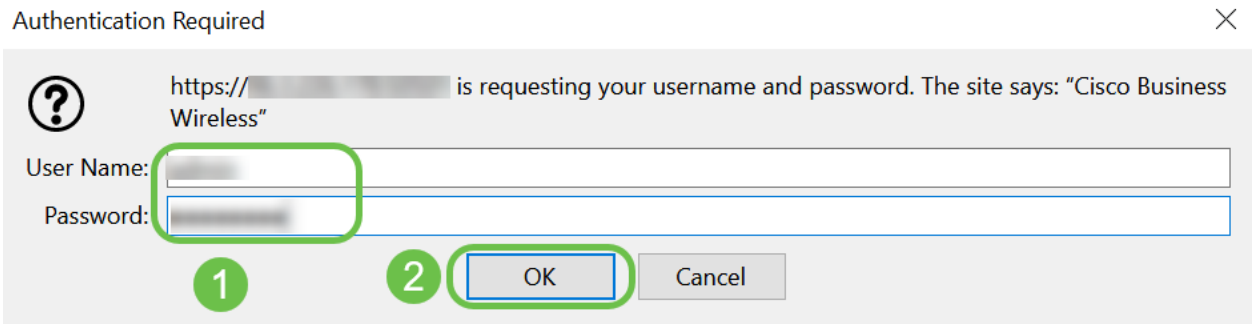
3단계

웹 브라우저에 기본 액세스 포인트(AP) IP 주소를 입력합니다.Login(**로그인**)을 클릭하여 기본 AP에 액세스합니다.



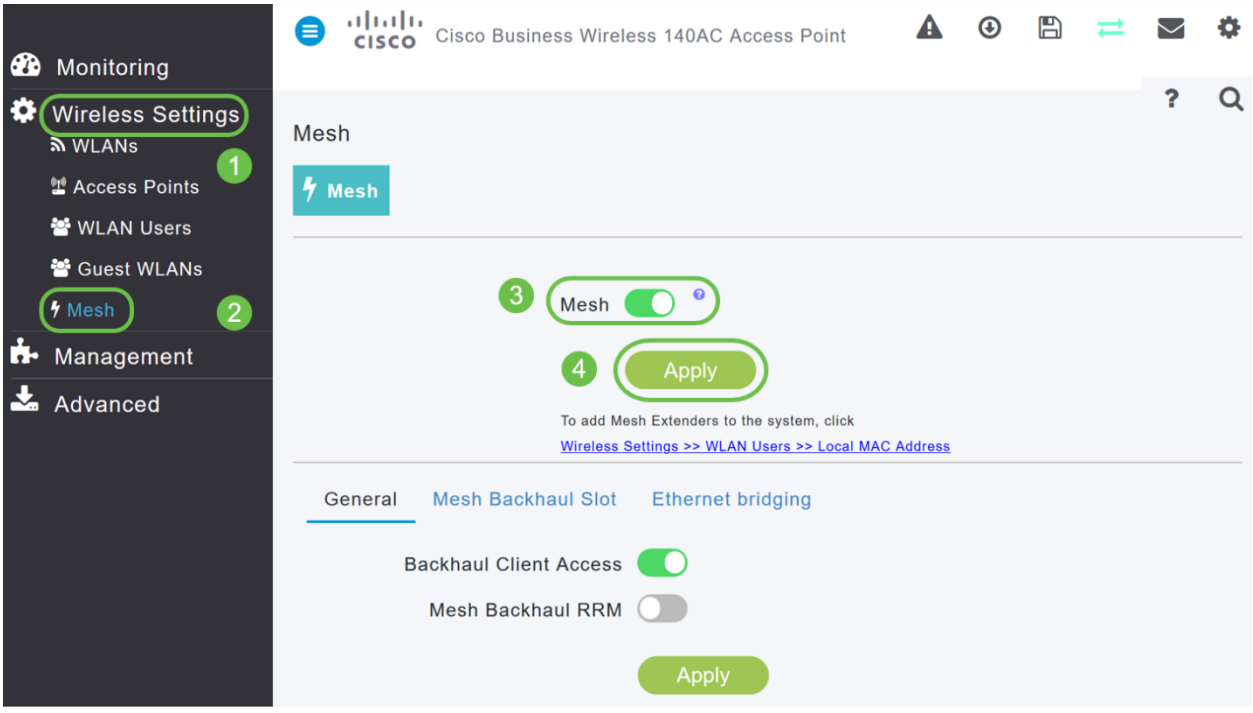
4단계

기본 AP에 액세스하려면 *사용자 이름* 및 *비밀번호* 자격 증명을 입력합니다.**확인**을 **클릭합니다**.



5단계

Wireless Settings(**무선 설정**) > **Mesh(메시)로 이동합니다**. *메시*가 활성화되었는지 확인합니다.Apply를 **클릭합니다**.

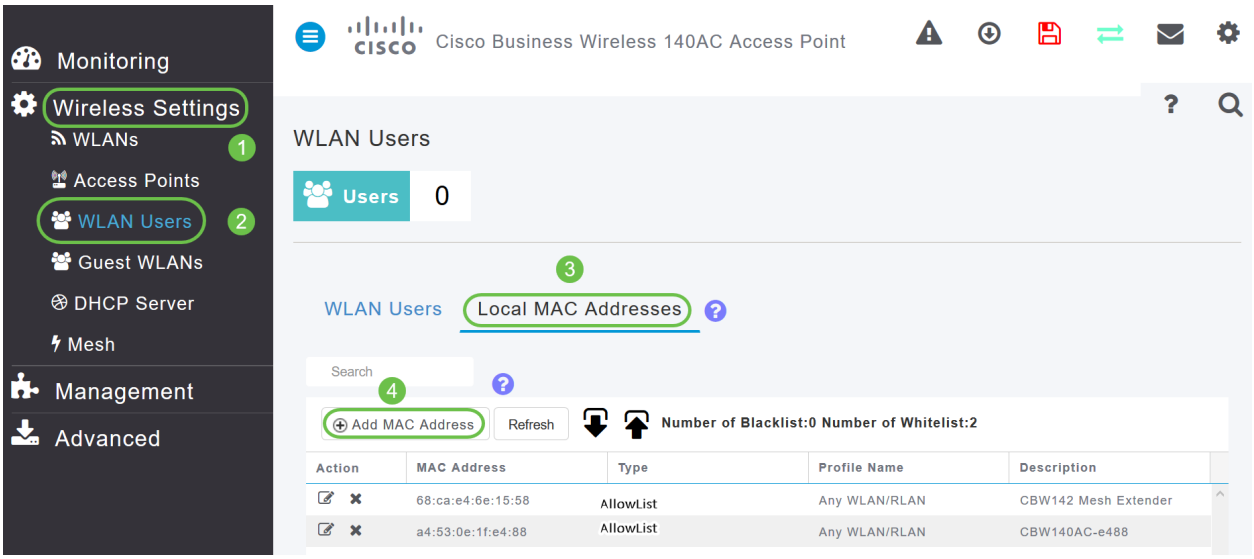


6단계

Mesh가 아직 활성화되지 않은 경우 WAP에서 재부팅을 수행해야 할 수 있습니다.재부팅을 수행하는 팝업이 나타납니다.확인10분 정도 걸립니다.재부팅하는 동안 LED가 여러 패턴에서 녹색으로 깜박이며 녹색, 빨간색, 황색으로 빠르게 번갈아 가며 녹색으로 다시 바뀝니다.LED 색상 강도와 색조가 단위마다 약간 다를 수 있습니다.

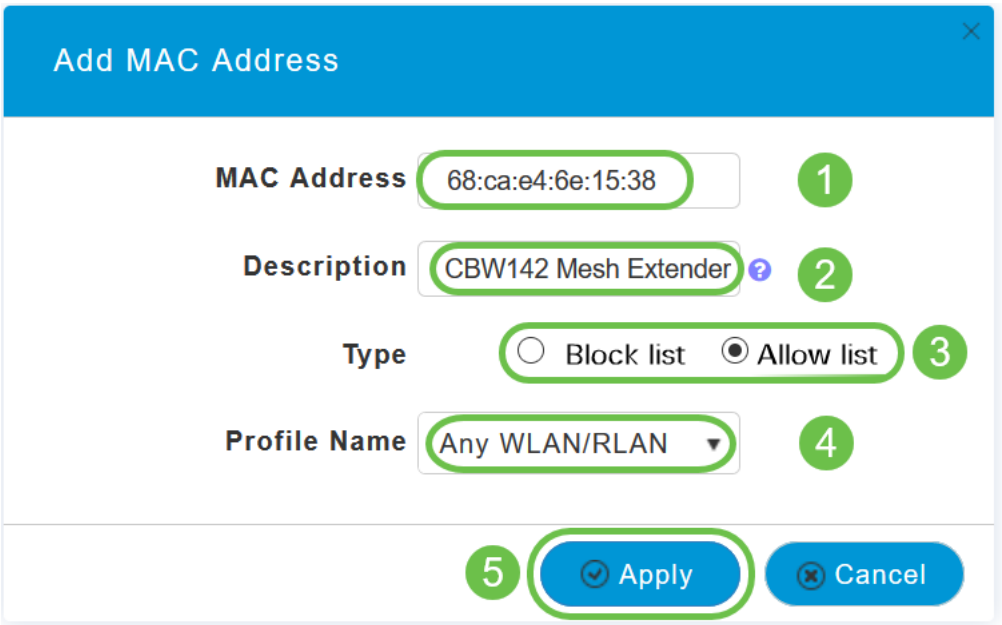
7단계

Wireless Settings(**무선 설정**) > **WLAN Users(WLAN 사용자)** > **Local MAC Addresses(로컬 MAC 주소)로 이동합니다**.Add **MAC Address를 클릭합니다**.



8단계

메시 익스텐더의 MAC 주소 및 설명을 입력합니다.Type(*유형*)을 Allow(허용) 목록으로 선택합니다.드롭다운 메뉴에서 *Profile Name(프로필 이름)*을 선택합니다.Apply를 **클릭합니다**.



9단계

화면의 오른쪽 상단 창에서 **저장 아이콘**을 눌러 모든 컨피그레이션을 저장해야 합니다.

각 메시 확장기에 대해 반복합니다.

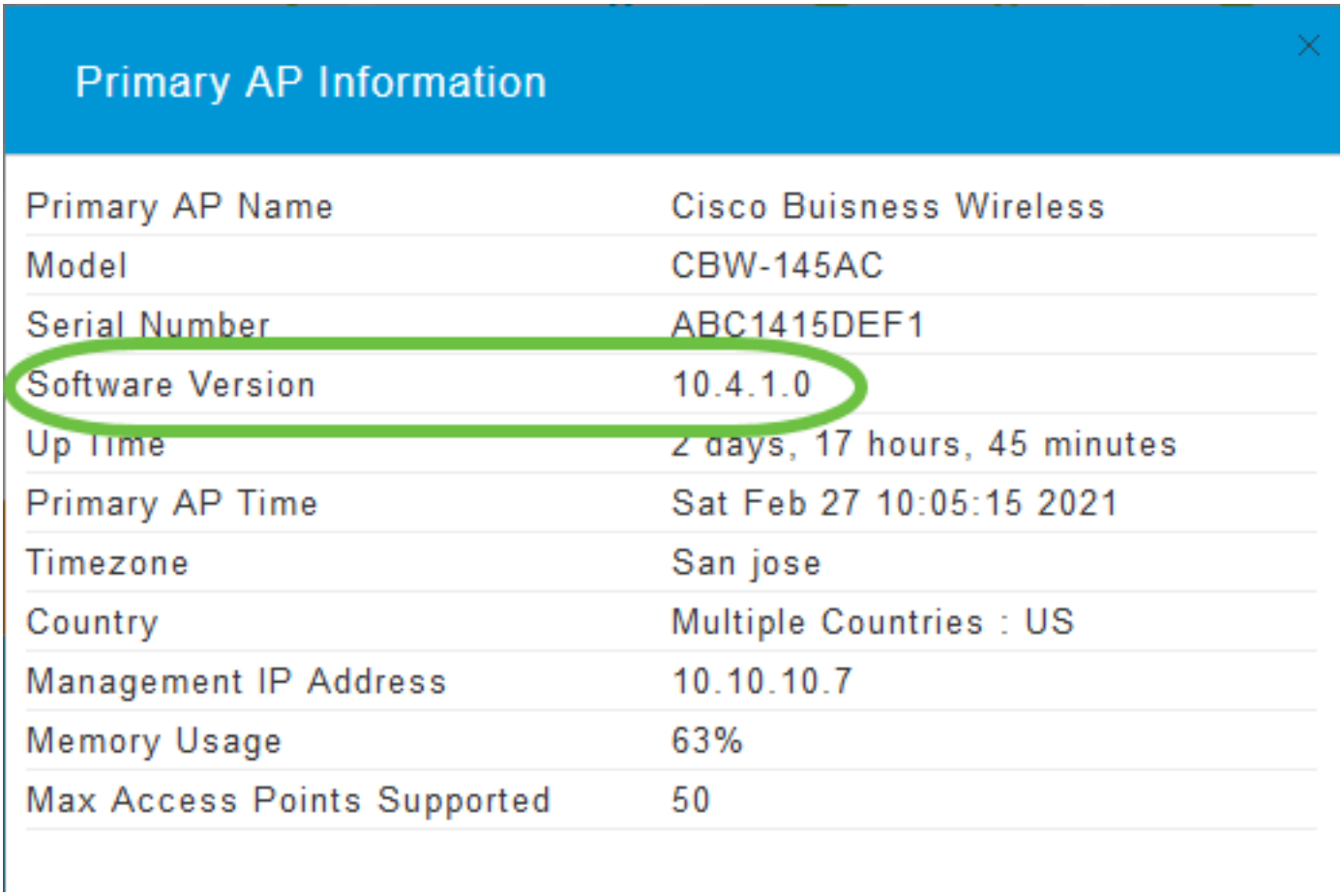
웹 UI를 사용하여 소프트웨어 확인 및 업데이트

이 중요한 단계를 건너뛰지 마십시오!소프트웨어를 업데이트하는 방법에는 몇 가지가 있지만 웹 UI를 사용할 때 아래 나열된 단계를 가장 쉽게 실행하는 것이 좋습니다.

기본 AP의 현재 소프트웨어 버전을 보고 업데이트하려면 다음 단계를 수행하십시오.

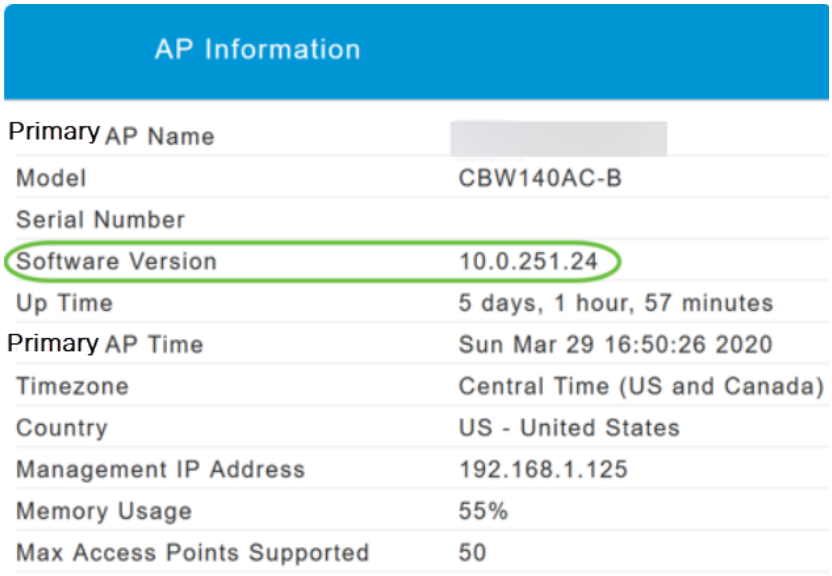
1단계

웹 인터페이스의 오른쪽 상단 모서리에 있는 **기어 모양 아이콘**을 클릭한 다음 기본 **AP 정보**를 클릭합니다.



2단계

실행 중인 버전을 최신 소프트웨어 버전과 비교합니다.소프트웨어를 업데이트해야 하는 경우 창을 닫습니다.

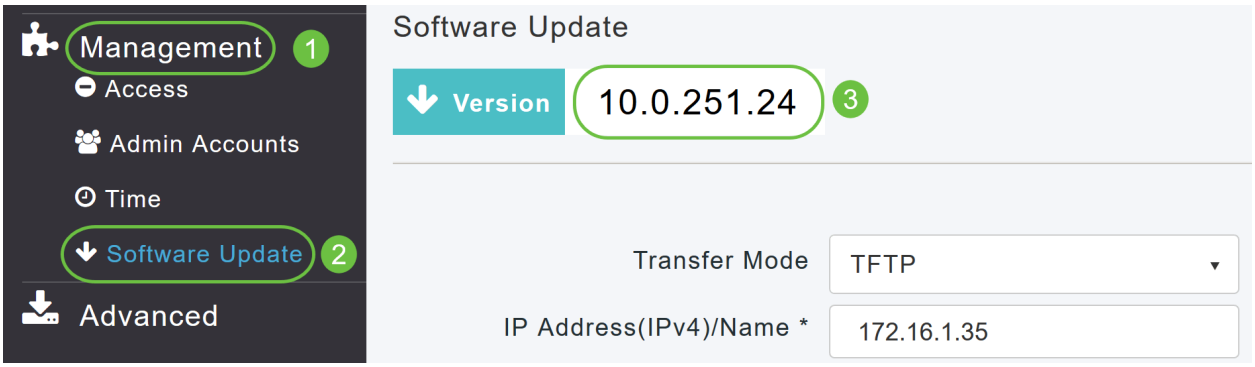


최신 버전의 소프트웨어를 실행 중인 경우 Create WLANs(WLAN 생성) 섹션으로 이동할 수 있습니다.

3단계

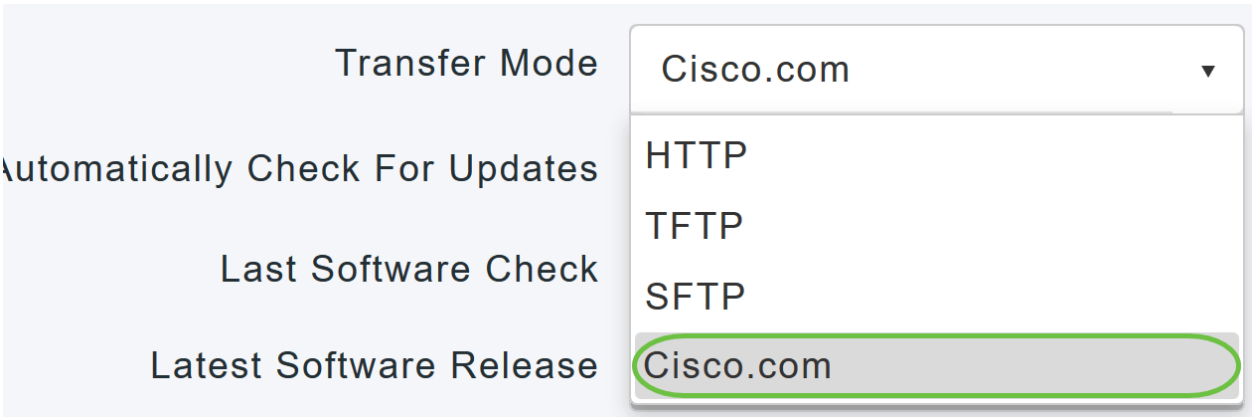
메뉴에서 **Management(관리) > Software Update(소프트웨어 업데이트)**를 선택합니다.

소프트웨어 *업데이트* 창이 상단에 현재 소프트웨어 버전 번호가 표시된 상태로 표시됩니다.



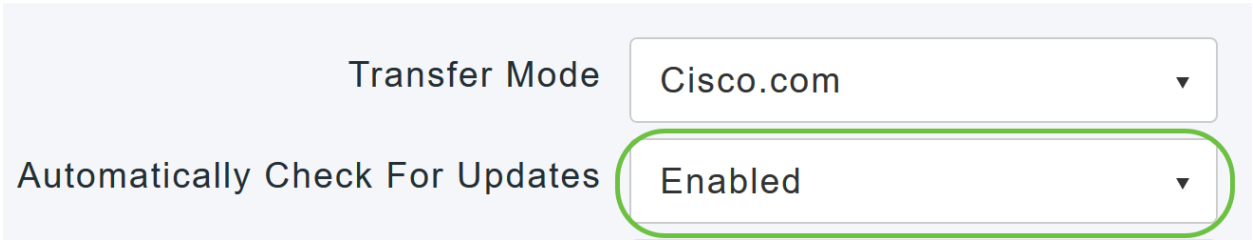
CBW AP 소프트웨어를 업데이트할 수 있으며 기본 AP의 현재 구성은 삭제되지 않습니다.

Transfer Mode 드롭다운 목록에서 **Cisco.com을** 선택합니다.



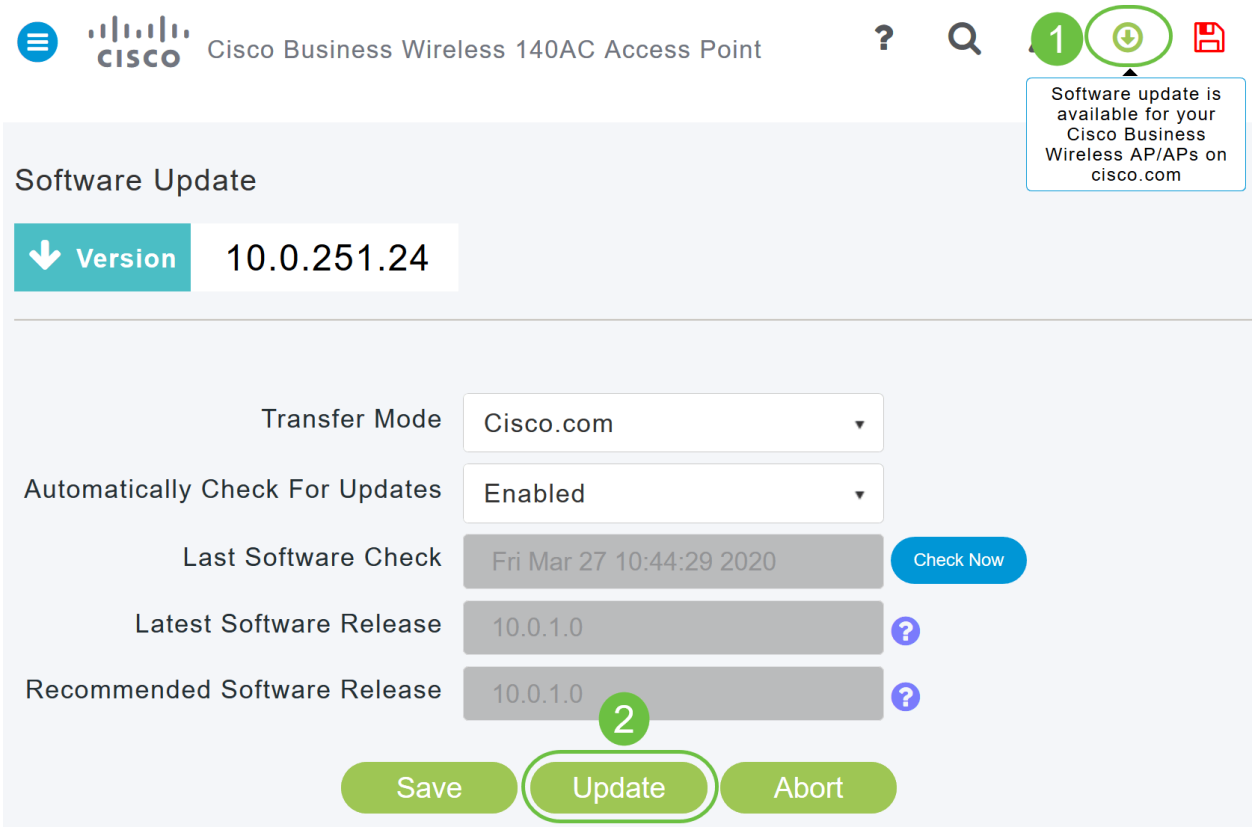
4단계

기본 AP가 소프트웨어 업데이트를 자동으로 확인하도록 설정하려면 Automatically Check for Updates 드롭다운 목록에서 **Enabled***(활성화됨)*를 선택합니다.기본적으로 활성화되어 있습니다.



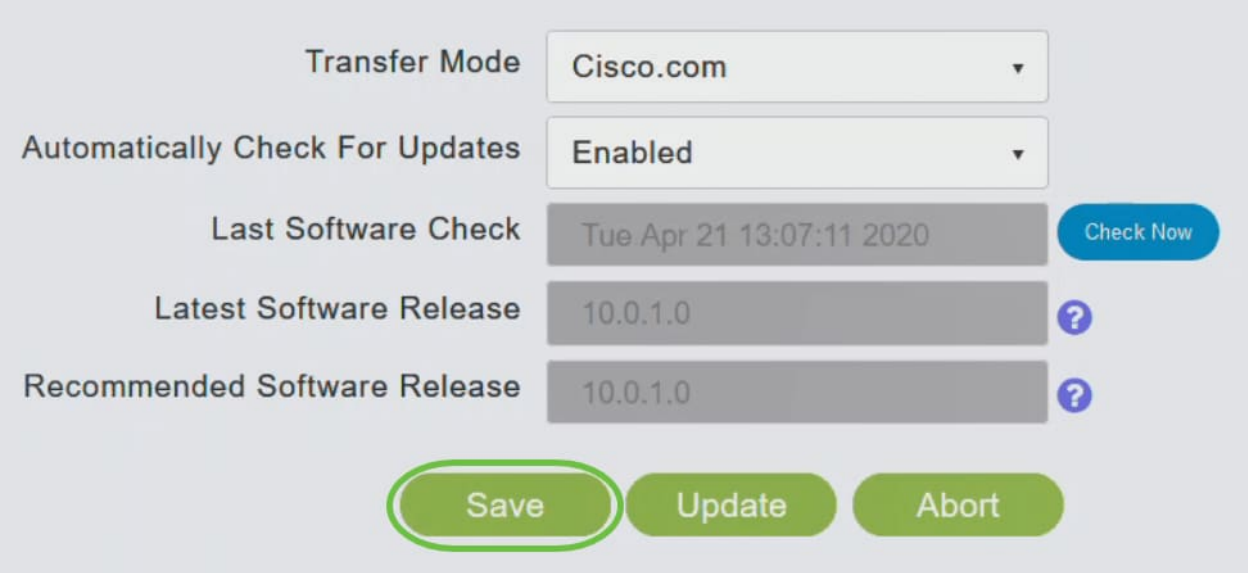
소프트웨어 확인이 완료되고 Cisco.com에서 최신 소프트웨어 업데이트 또는 권장 소프트웨어 업데이트가 제공되는 경우 다음을 수행합니다.

- 웹 UI의 오른쪽 상단 모서리에 있는 **소프트웨어 업데이트 경고 아이콘**은 녹색(또는 회색)입니다. 아이콘을 클릭하면 소프트웨어 업데이트 페이지로 이동합니다.
- *소프트웨어 업데이트* 페이지 하단의 업데이트 버튼이 활성화됩니다.

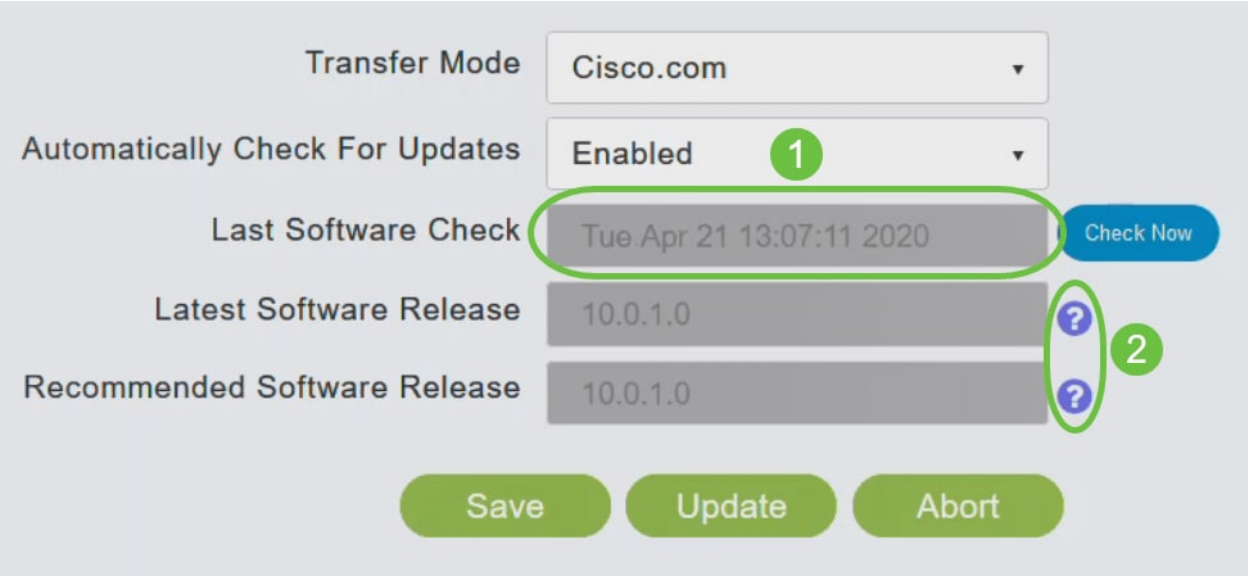


5단계

저장을 **클릭합니다**.이렇게 하면 *전송 모드*에서 수행한 항목 또는 변경 사항이 저장되고 *자동 업데이트 확인이 수행됩니다*.

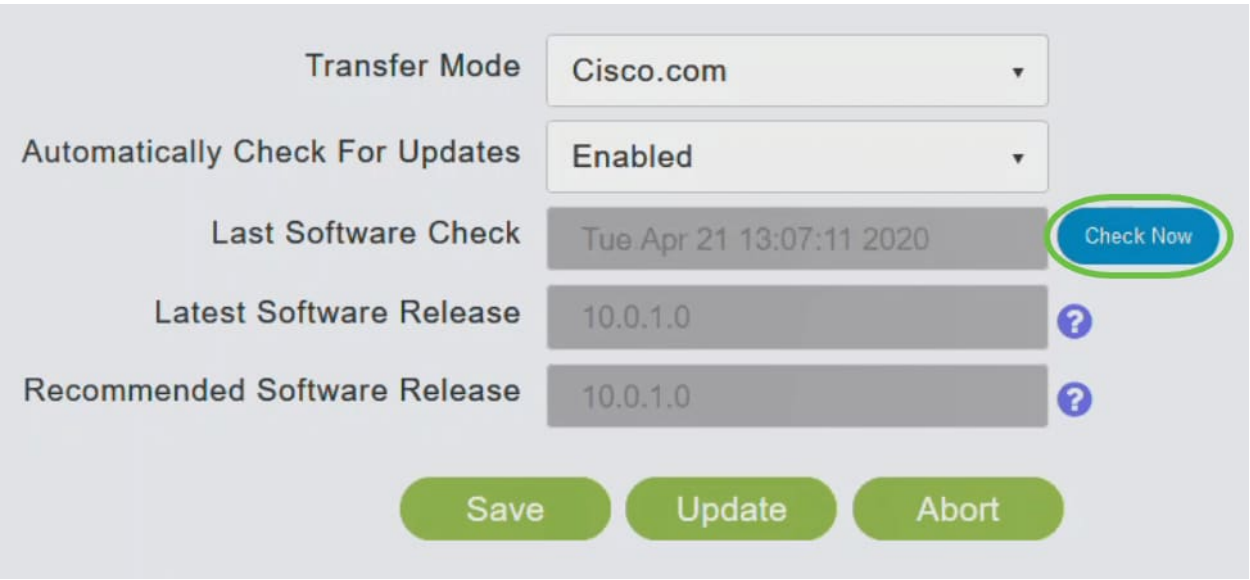


Last *Software Check*(마지막 소프트웨어 확인) 필드는 마지막 자동 또는 수동 소프트웨어 확인의 타임스탬프를 표시합니다.옆에 있는 **물음표 아이콘**을 클릭하여 표시된 릴리스의 노트를 볼 수 있습니다.



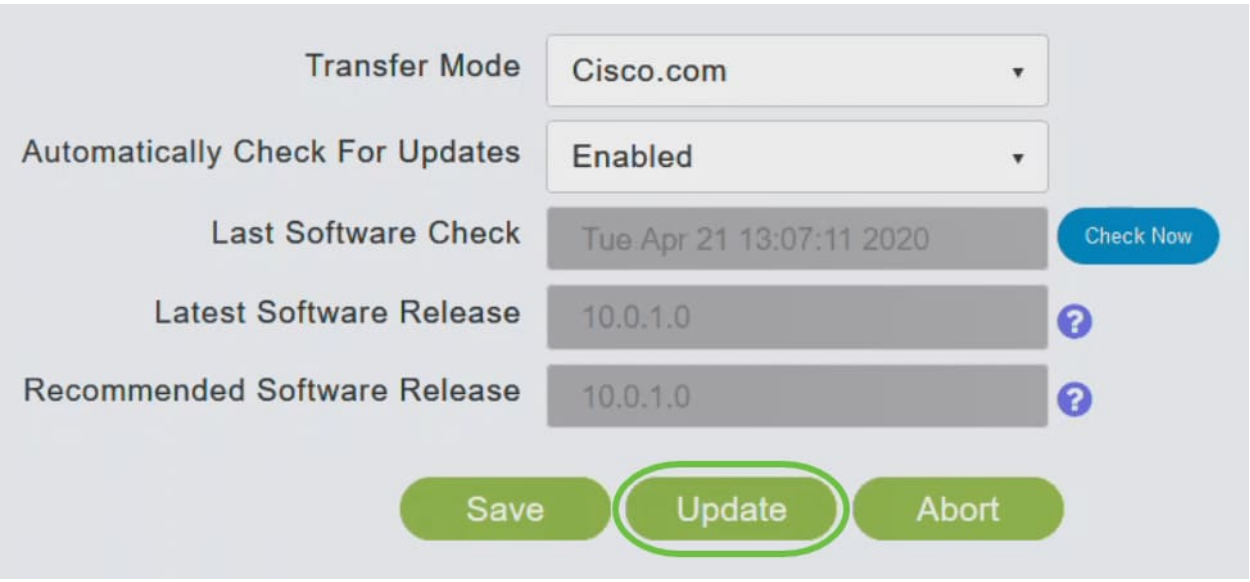
6단계

Check Now(지금 확인)를 클릭하면 언제든지 소프트웨어 검사를 수동으로 실행할 수 *있습니다*.



7단계

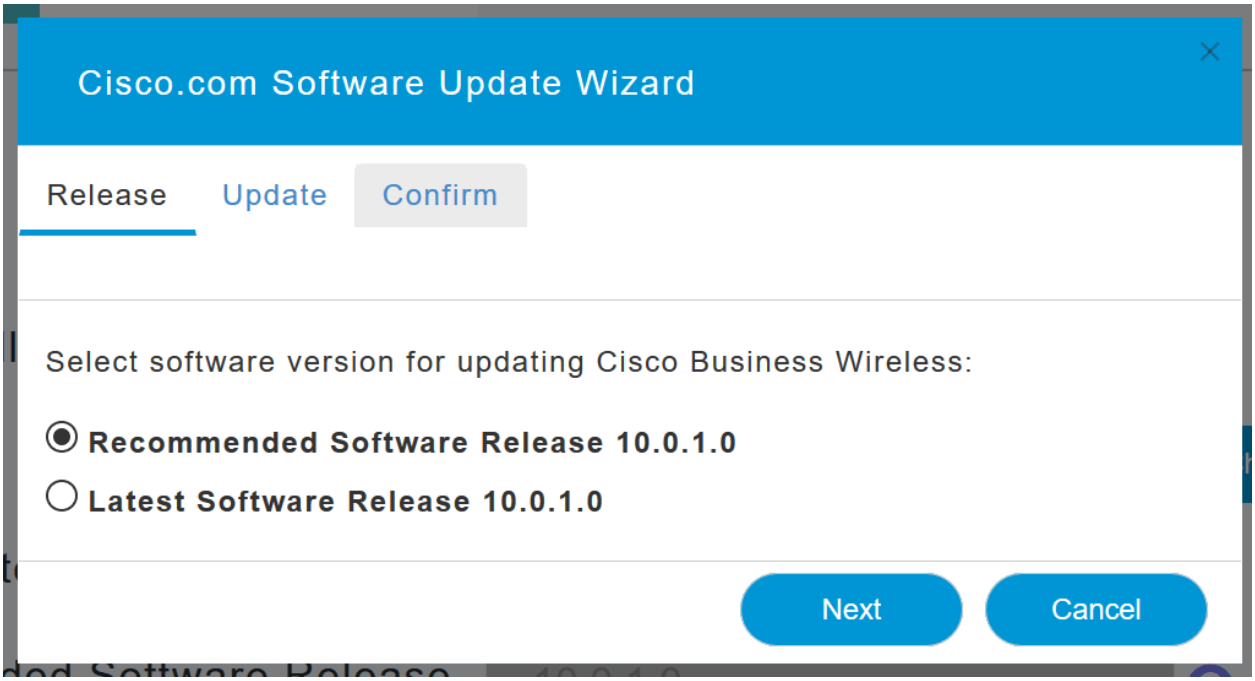
소프트웨어 업데이트를 계속하려면 Update(**업데이트**)를 클릭합니다.



*소프트웨어 업데이트 마법사*가 나타납니다.마법사는 다음 세 개의 탭을 순서대로 안내합니다.

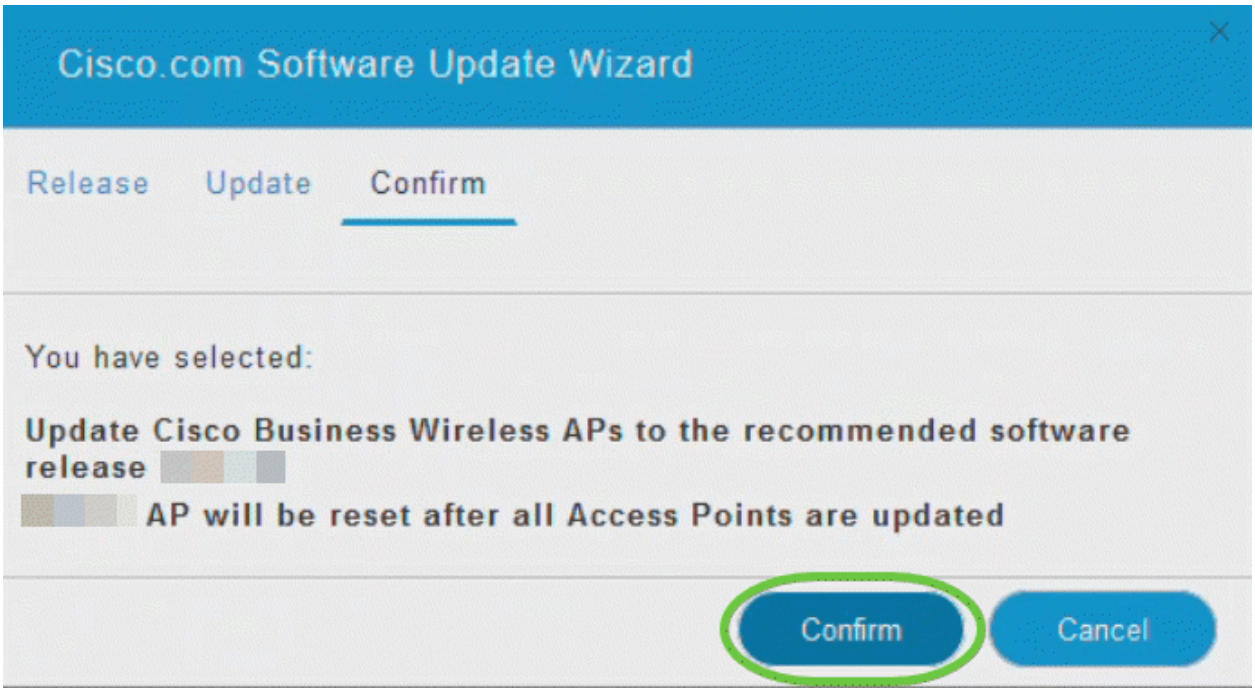
- Release(릴리스) 탭 - 권장 소프트웨어 릴리스 또는 최신 소프트웨어 릴리스로 업데이트할지 지정합니다.
- Update(업데이트) 탭 - AP를 재설정해야 하는 시기를 지정합니다.지금 바로 끝내거나 나중에 예약하도록 선택할 수 있습니다.이미지 사전 다운로드가 완료된 후 기본 AP가 자동으로 재부팅되도록 설정하려면 Auto Restart(자동 재시작) 확인란을 선택합니다.
- 확인 탭 - 선택 사항을 확인합니다.

마법사의 지침을 따릅니다.*확인*을 클릭하기 전에 언제든지 원하는 탭으로 돌아갈 수 있습니다.



8단계

확인을 **클릭합니다**.

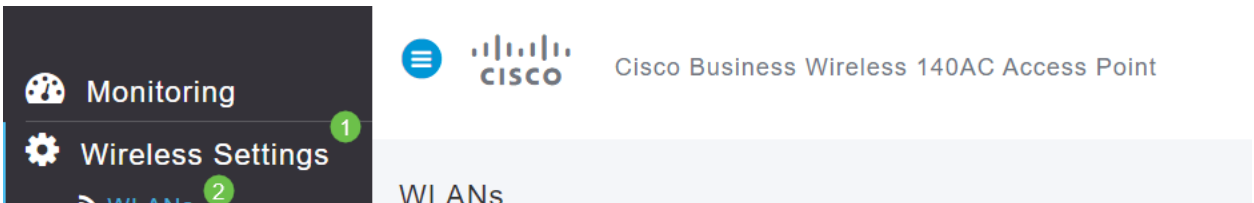


웹 UI에서 WLAN 생성

이 섹션에서는 WLAN(Wireless Local Area Network)을 생성할 수 있습니다.

1단계

WLAN은 Wireless Settings(무선 설정) **> WLANs(WLAN)로 이동하여 생성할** 수 있습니다.그런 다음 **Add new WLAN/RLAN(새 WLAN/RLAN 추가)를** 선택합니다.



2단계

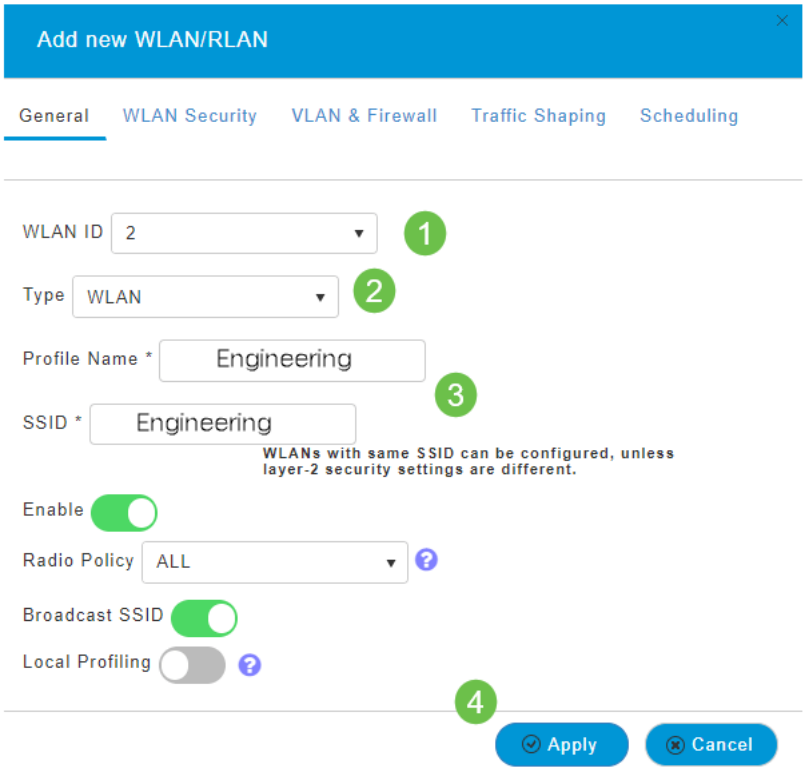
일반 탭에서 다음 정보를 입력합니다.

- WLAN ID - WLAN의 번호 선택
- 유형 - **WLAN 선택**
- Profile Name(프로파일 이름) - 이름을 입력하면 SSID가 동일한 이름으로 자동 채워집니다.이름은 고유해야 하며 31자를 초과할 수 없습니다.

다음 필드는 이 예제에서 기본값으로 남겨졌지만, 설명을 다르게 구성하려는 경우 이 필드가 나열됩니다.

- SSID - 프로파일 이름도 SSID의 역할을 합니다.원하시면 변경할 수 있습니다이름은 고유해야 하며 31자를 초과할 수 없습니다.
- Enable(활성화) - WLAN이 작동하려면 이 설정을 사용하도록 설정해야 합니다.
- Radio Policy(무선 정책) - 일반적으로 **All(모두)**로 유지하여 2.4GHz 및 5GHz 클라이언트가 네트워크에 액세스할 수 있도록 합니다.
- Broadcast SSID(브로드캐스트 SSID) - 일반적으로 SSID를 검색하면 이 SSID를 Enabled(활성화됨)로 유지할 수 있습니다.
- 로컬 프로파일링 - 클라이언트에서 실행 중인 운영 체제를 보거나 사용자 이름을 보려면 이 옵션을 활성화하기만 하면 됩니다.

Apply를 **클릭합니다**.



3단계

WLAN Security 탭으로 이동합니다.

이 예에서는 다음 옵션이 기본값으로 남았습니다.

- 게스트 네트워크, Captive Network Assistant 및 MAC Filtering이 비활성화된 상태로 남았습니다.게스트 네트워크 설정에 대한 자세한 내용은 다음 섹션에 자세히 설명되어 있습니다.
- WPA2 Personal - PSK(Pre-Shared Key) 암호 형식의 Wi-Fi Protected Access 2 - ASCII.이 옵션은 PSK(Pre-Shared Key)가 있는 Wi-Fi Protected Access 2를 나타냅니다.

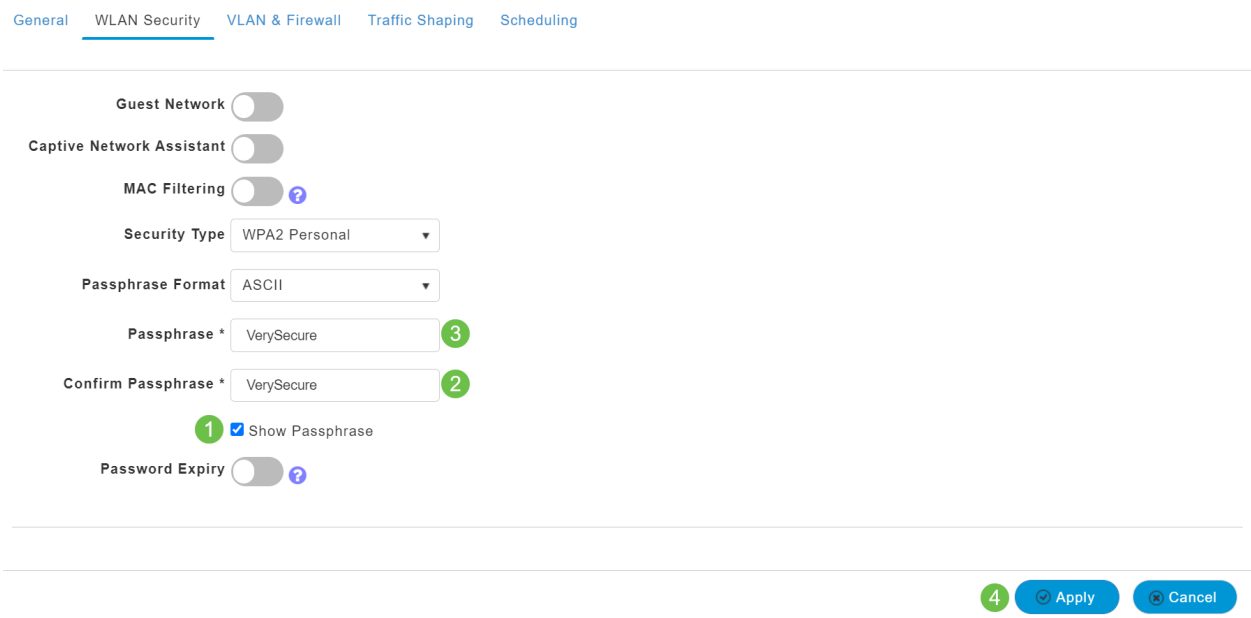
WPA2 Personal은 PSK 인증을 사용하여 네트워크를 보호하는 데 사용되는 방법입니다.PSK는 기본 AP, WLAN 보안 정책 및 클라이언트에서 각각 구성됩니다.WPA2 Personal은 네트워크에서 인증 서버를 사용하지 않습니다.

- Passphrase Format - **ASCII가 기본값으로 유지됩니다.**

이 시나리오에서는 다음 필드를 입력했습니다.

- Show Passphrase(패스프레이즈 표시) - 입력한 패스프레이즈를 보려면 확인란을 클릭합니다.
- Passphrase(패스프레이즈) - 패스프레이즈(비밀번호)의 이름을 입력합니다.
- 암호 확인 - 암호를 다시 입력하여 확인합니다.

Apply를 **클릭합니다**.그러면 새 WLAN이 자동으로 활성화됩니다.

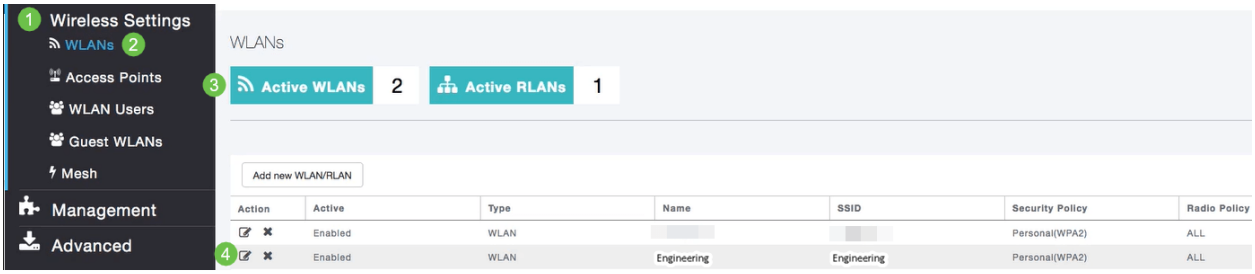


4단계

Web UI 화면 오른쪽 상단 패널에서 **저장 아이콘**을 클릭하여 컨피그레이션을 저장해야 합니다.

5단계

생성한 WLAN을 보려면 Wireless **Settings(무선 설정) > WLANs(WLAN)를** 선택합니다.활성 WLAN 수가 2로 증가되고 새 WLAN이 표시됩니다.



생성하려는 다른 WLAN에 대해 이 단계를 반복합니다.

선택적 무선 구성

이제 모든 기본 컨피그레이션이 설정되어 롤아웃할 준비가 되었습니다.몇 가지 옵션이 있으므로 다음 섹션으로 이동하십시오.

- 웹 UI를 사용하여 게스트 WLAN 생성(선택 사항)
- 애플리케이션 프로파일링(선택 사항)
- 클라이언트 프로파일링(선택 사항)
- 이제 마무리하고 네트워크를 사용할 준비가 되었습니다!

웹 UI를 사용하여 게스트 WLAN 생성(선택 사항)

게스트 WLAN은 Cisco Business Wireless 네트워크에 대한 게스트 액세스를 제공합니다.

1단계

기본 AP의 웹 UI에 로그인합니다. 웹 브라우저를 열고 www.https://ciscobusiness.cisco을 입력합니다.계속하기 전에 경고를 받을 수 있습니다.자격 증명을 입력합니다.기본 AP의 IP 주소를 입력하여 액세스할 수도 있습니다.

2단계

무선 WLAN(Local Area Network)은 Wireless Settings(무선 설정) **> WLANs(WLAN)로 이동하여 생성할** 수 있습니다.그런 다음 **Add new WLAN/RLAN(새 WLAN/RLAN 추가)를** 선택합니다.

3단계

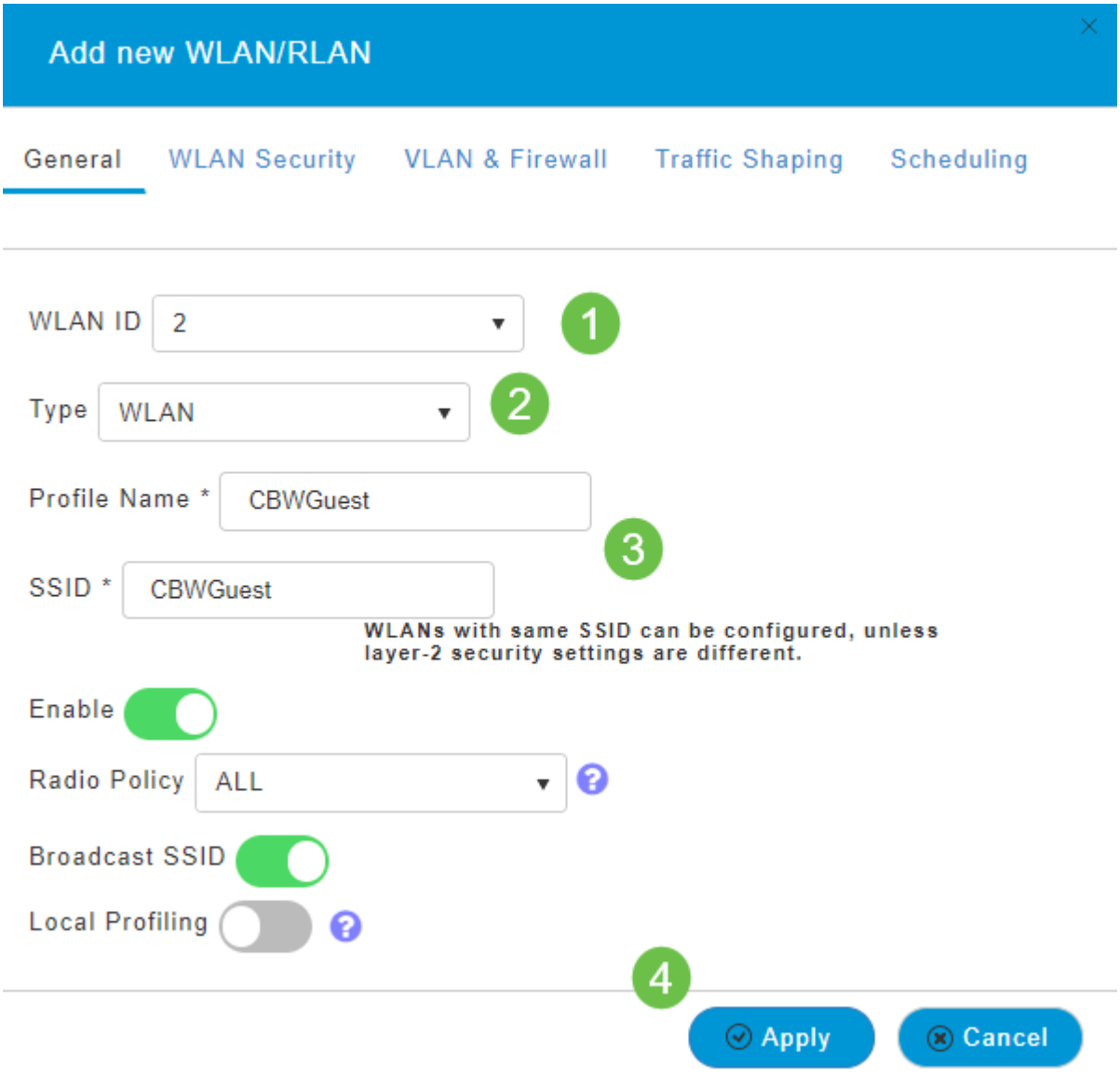
일반 탭에서 다음 정보를 입력합니다.

WLAN ID - WLAN의 번호 선택
유형 - **WLAN** 선택
프로파일 이름 - 이름을 입력하면 SSID가 동일한 이름으로 자동 채워집니다.이름은 고유해야 하며 31자를 초과할 수 없습니다.

다음 필드는 이 예제에서 기본값으로 남겨졌지만, 설명을 다르게 구성하려는 경우 이 필드가 나열됩니다.

SSID - 프로파일 이름도 SSID의 역할을 합니다.원하시면 변경할 수 있습니다이름은 고유해야 하며 31자를 초과할 수 없습니다.
Enable(활성화) - WLAN이 작동하려면 이 설정을 사용하도록 설정해야 합니다.
무선 정책 - 일반적으로 2.4GHz 및 5GHz 클라이언트가 네트워크에 액세스할 수 있도록 이를 All(모두)로 남겨두고자 합니다.
Broadcast SSID - 일반적으로 SSID를 검색하도록 하여 이를 Enabled(활성화됨)로 둡니다.
로컬 프로파일링 - 클라이언트에서 실행 중인 운영 체제를 보거나 사용자 이름을 보려면 이 옵션만 활성화하면 됩니다.

Apply를 **클릭합니다**.



4단계

WLAN Security 탭으로 이동합니다.이 예에서는 다음 옵션을 선택했습니다.

- 게스트 네트워크 - 활성화
- Captive Network Assistant - Mac 또는 IOS를 사용하는 경우 이를 활성화할 수 있습니다.이 기능은 무선 네트워크 연결에 대한 웹 요청을 전송하여 종속 포털의 존재를 탐지합니다.이 요청은 iPhone 모델에 대한 URL(Uniform Resource Locator)로 전달되며, 응답이 수신되면 인터넷 액세스를 사용할 수 있다고 가정하고 추가 상호 작용이 필요하지 않습니다.응답이 수신되지 않으면 종속 포털에 의해 인터넷 액세스가 차단되는 것으로 간주되고 Apple의 CNA(Captive Network Assistant)가 자동으로 의사 브라우저를 실행하여 제어 창에서 포털 로그인을 요청합니다.ISE(Identity Services Engine) 종속 포털로 리디렉션할 때 CNA가 중단될 수 있습니다.기본 AP는 이 유사 브라우저가 팝업되는 것을 방지합니다.
- Captive Portal(종속 포털) - 이 필드는 Guest Network(게스트 네트워크) 옵션이 활성화된 경우에만 표시됩니다.인증 용도로 사용할 수 있는 웹 포털의 유형을 지정하는 데 사용됩니다.기본 Cisco 웹 포털 기반 인증을 사용하려면 Internal Splash Page를 선택합니다.네트워크 외부의 웹 서버를 사용하여 종속 포털 인증을 갖게 될 경우 External Splash Page(외부 스플래시 페이지)를 선택합니다.또한 Site URL 필드에 서버의 URL을 지정합니다.

이 예에서는 활성화된 소셜 로그인 액세스 유형의 게스트 WLAN이 생성됩니다.사용자가 이 게스트 WLAN에 연결되면 Google 및 Facebook의 로그인 버튼을 찾을 수 있는 Cisco 기본 로그인 페이지로 리디렉션됩니다.사용자는 Google 또는 Facebook 계정을 사용하여 로그인하여 인터넷에 액세스할 수 있습니다.

5단계

동일한 탭의 드롭다운 메뉴에서 *액세스 유형*을 선택합니다.이 예에서는 *Social Login*이 선택되었습니다.게스트가 Google 또는 Facebook 자격 증명을 사용하여 네트워크를 인증하고 액세스할 수 있도록 하는 옵션입니다.

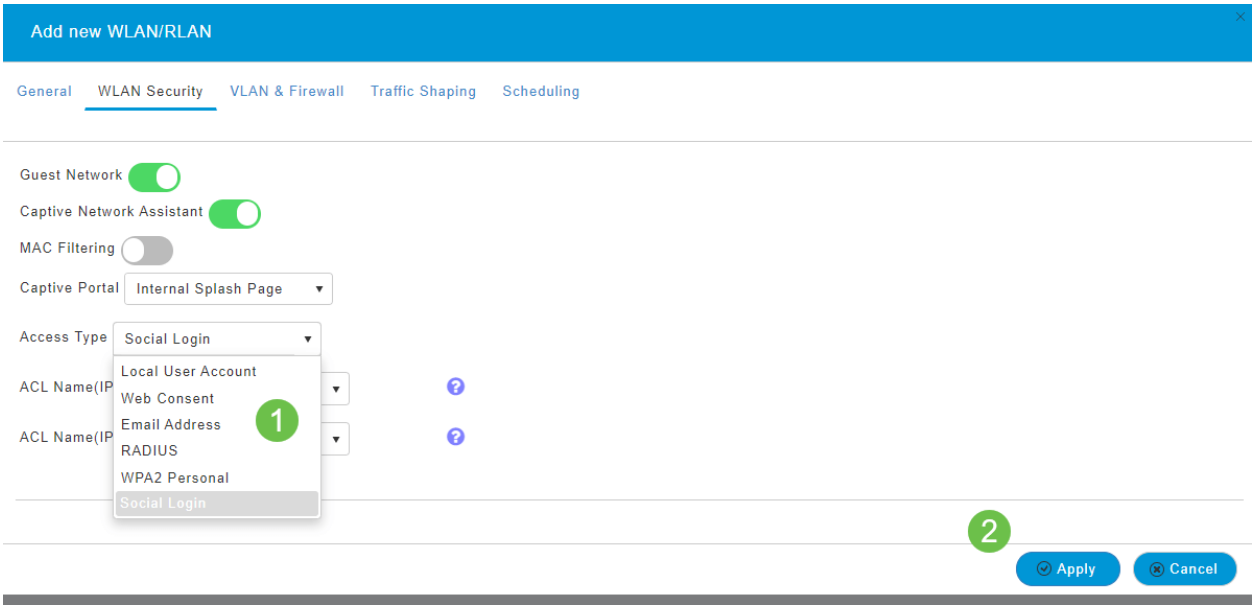
*액세스 유형*에 대한 기타 옵션은 다음과 같습니다.

로컬 사용자 계정 - 기본 옵션입니다.이 WLAN의 게스트 사용자에 대해 지정할 수 있는 사용자 이름 및 비밀번호를 사용하여 게스트를 인증하려면 이 옵션을 Wireless **Settings(무선 설정) > WLAN Users(WLAN 사용자)에서 선택합니다**.기본 내부 시작 페이지의 예입니다.

Wireless Settings(무선 설정) **> Guest WLANs(게스트 WLAN)**로 이동하여 이**를 사용자 정의할** 수 있습니다.여기에서 *페이지 헤드라인* 및 *페이지 메시지*를 입력할 수 있습니다.Apply**를 클릭합니다**.미리 **보기**를 **클릭합니다**.

Web Consent(웹 동의) - 표시된 이용 약관에 동의하면 게스트가 WLAN에 액세스할 수 있습니다.게스트 사용자는 사용자 이름과 비밀번호를 입력하지 않고 WLAN에 액세스할 수 있습니다.
이메일 주소 - 게스트 사용자는 네트워크에 액세스하려면 이메일 주소를 입력해야 합니다.
RADIUS - 외부 인증 서버에서 사용합니다.
WPA2 개인 - PSK(Pre-Shared Key)가 있는 Wi-Fi Protected Access 2

Apply**를 클릭합니다**.



6단계

Web UI 화면 오른쪽 상단 패널에서 **저장 아이콘**을 클릭하여 컨피그레이션을 저장해야 합니다.

이제 CBW 네트워크에서 사용 가능한 게스트 네트워크를 생성했습니다.손님들께서 편리하신 것에 감사해 하실 겁니다

웹 UI를 사용하여 애플리케이션 프로파일링(선택 사항)

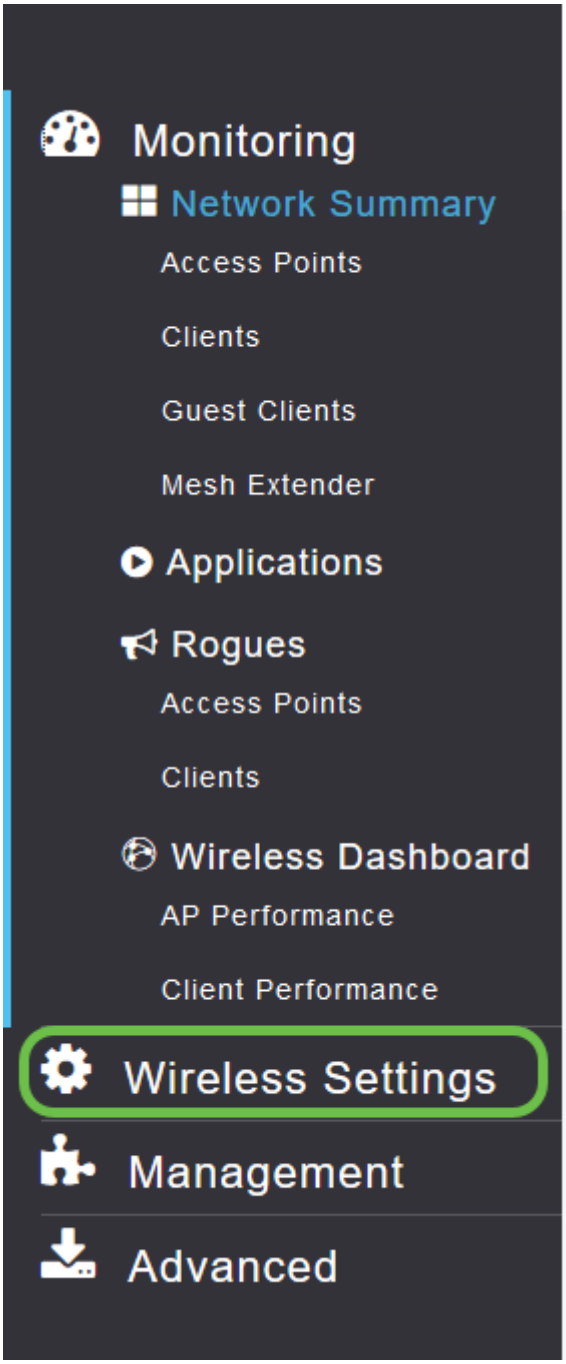
프로파일링은 조직 정책을 구체화하는 기능의 하위 집합입니다.트래픽 유형을 매칭하고 우선순위를 지정할 수 있습니다.유사 규칙에서는 트래픽의 순위를 매기거나 삭제하는 방법을 결정합니다.Cisco Business Mesh Wireless 시스템은 클라이언트 및 애플리케이션 프로파일링을 제공합니다.사용자가 네트워크에 액세스하는 작업은 많은 정보 교환에서 시작됩니다. 그 중 하나는 트래픽 유형입니다.정책은 플로우 차트와 마찬가지로 경로를 전달하기 위해 트래픽 흐름을 중단합니다.기타 정책 기능 유형에는 게스트 액세스, 액세스 제어 목록, QoS 등이 있습니다.

1단계

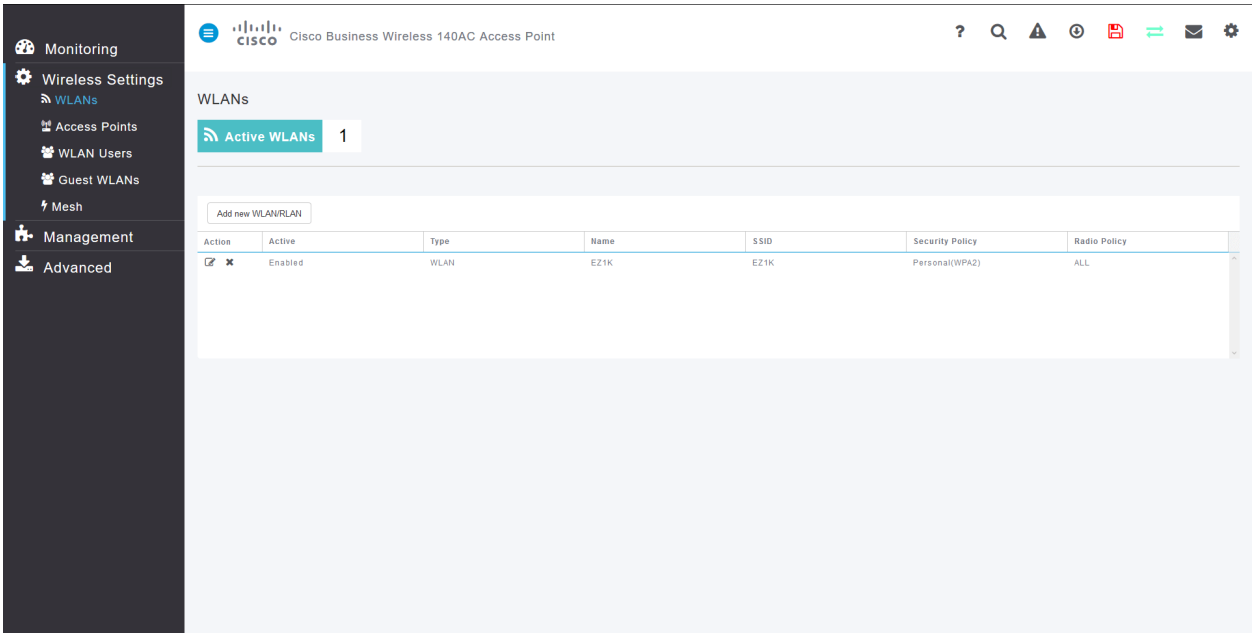
왼쪽 메뉴 모음이 표시되지 않으면 화면 왼쪽에 있는 메뉴로 이동합니다.

2단계

디바이스에 로그인하면 기본적으로 Monitoring 메뉴가 로드됩니다.**무선 설정**을 클릭해야 합니다.

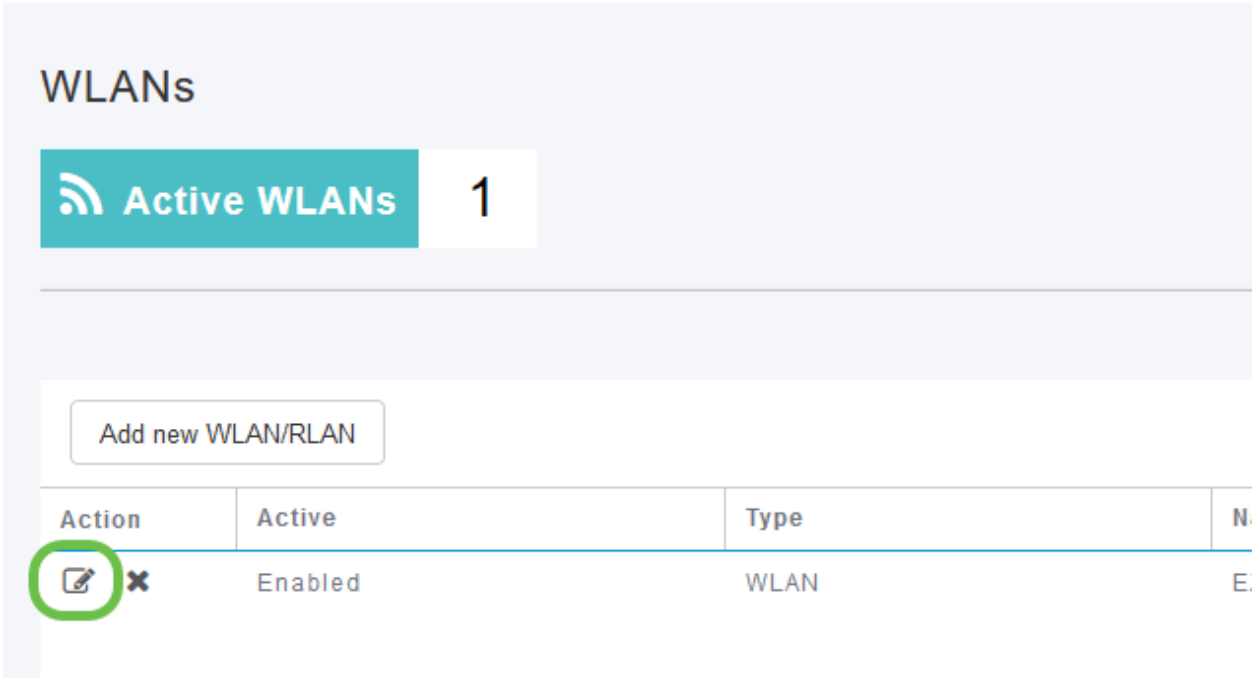


아래 이미지는 무선 설정 링크를 클릭할 때 표시되는 이미지와 유사합니다.

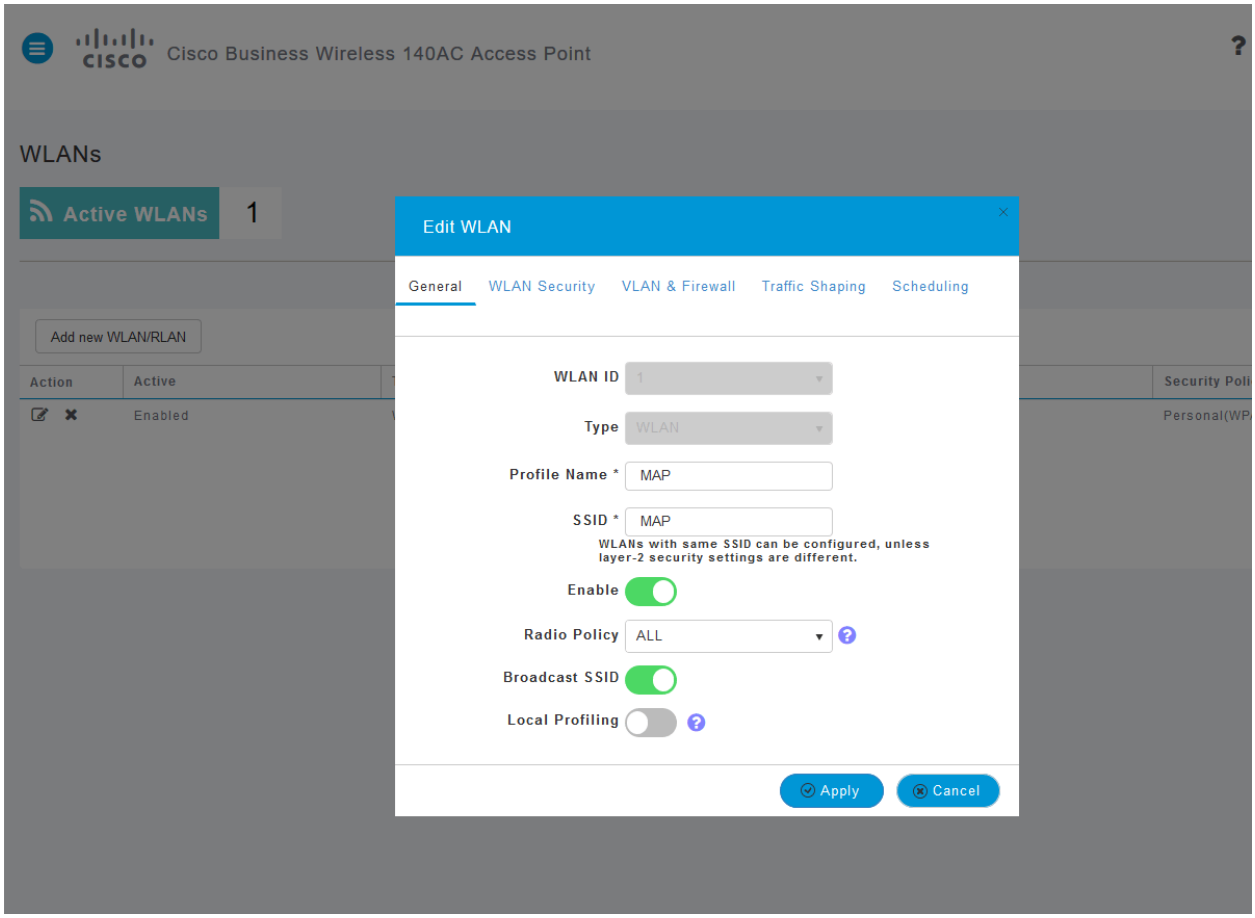


3단계

애플리케이션을 활성화할 무선 LAN 왼쪽에 있는 **수정 아이콘**을 클릭합니다.

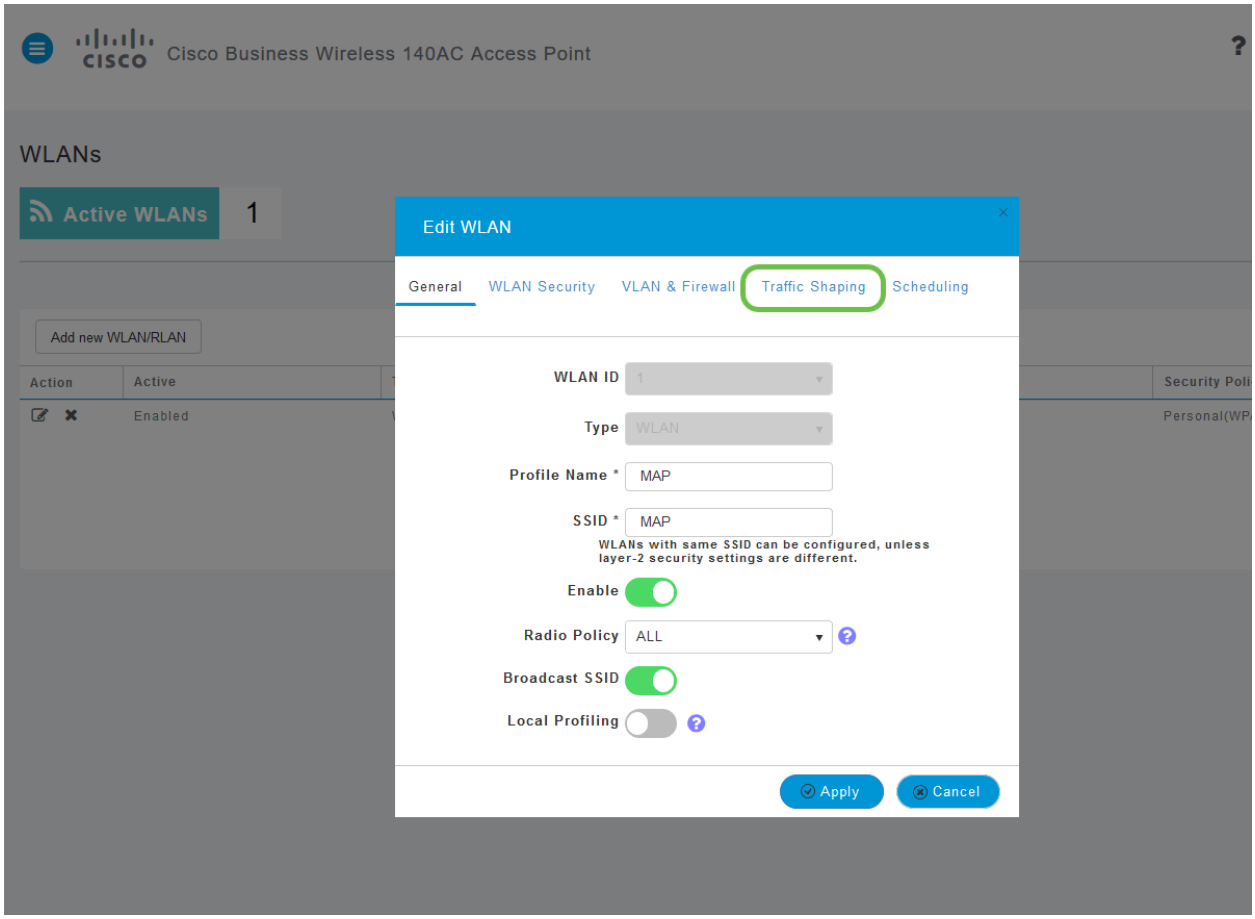


최근에 WLAN을 추가했으므로 *Edit WLAN(WLAN 편집)* 페이지가 아래와 유사하게 나타날 수 있습니다.

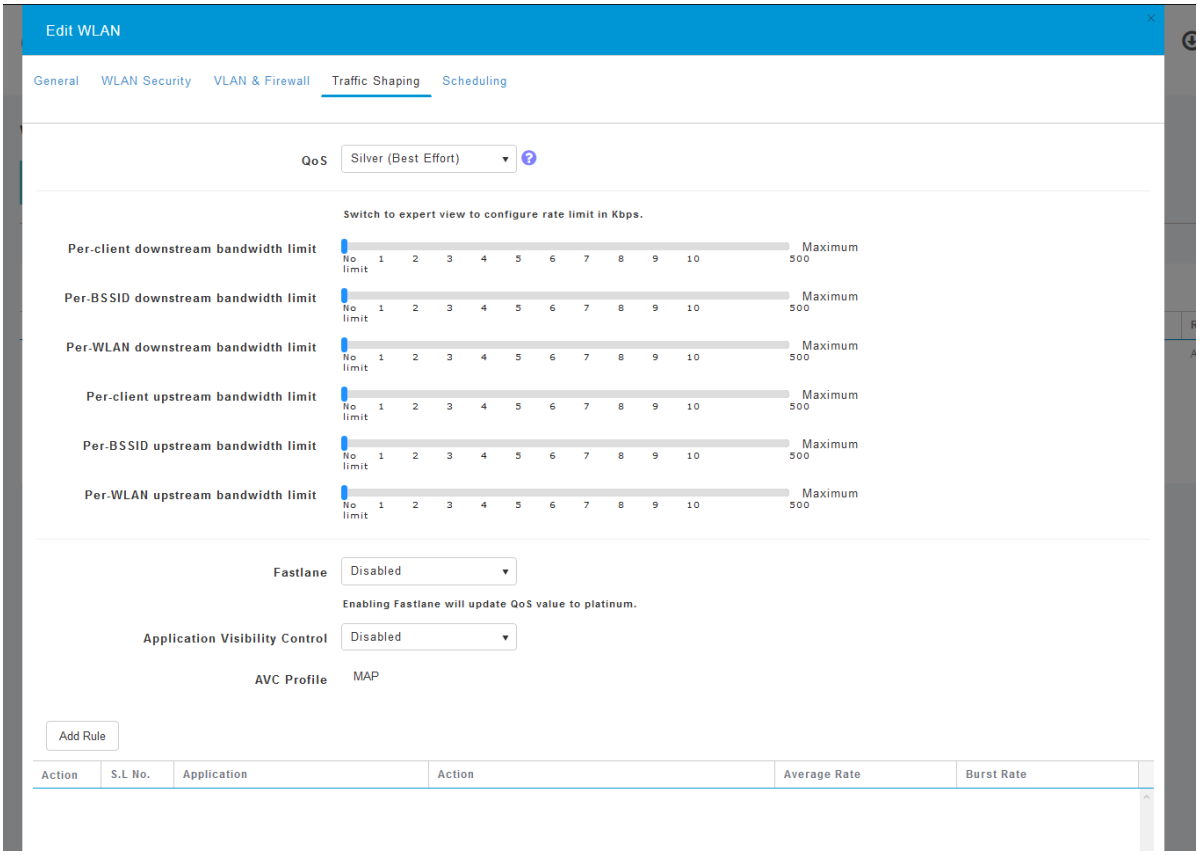


4단계

Traffic Shaping(**트래픽 셰이핑**) 탭을 클릭하여 해당 탭으로 이동합니다.

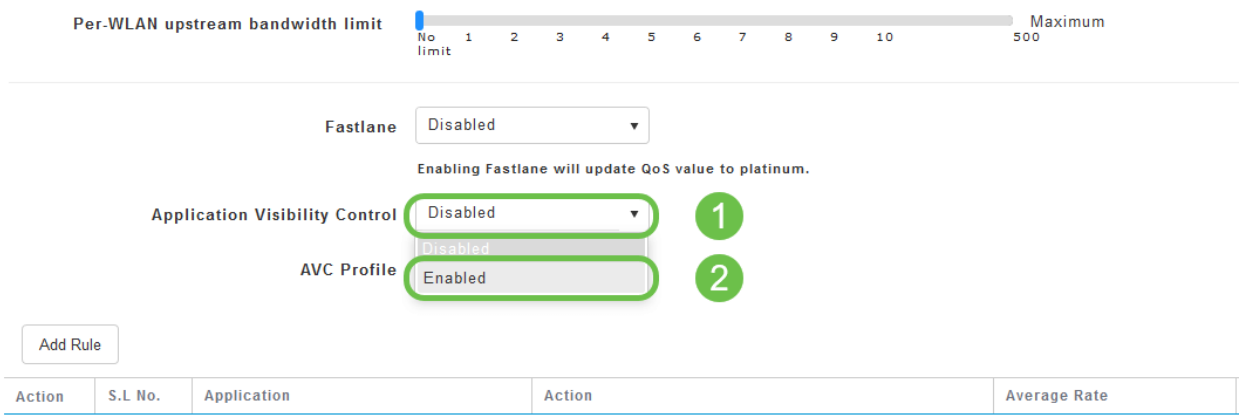


화면이 다음과 같이 표시될 수 있습니다.



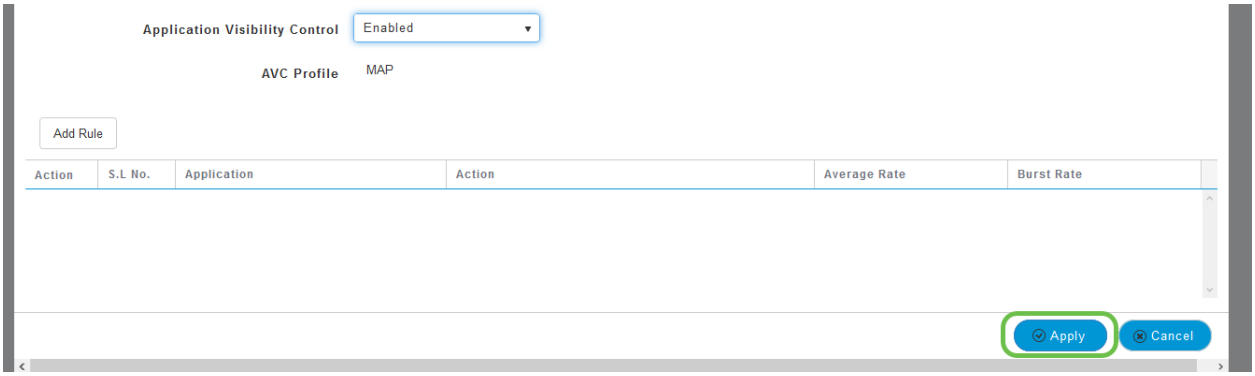
5단계

페이지 하단에는 *Application Visibility Control* 기능이 있습니다.기본적으로 비활성화되어 있습니다. 드롭다운을 클릭하고 [사용]을 **선택하십시오**.



6단계

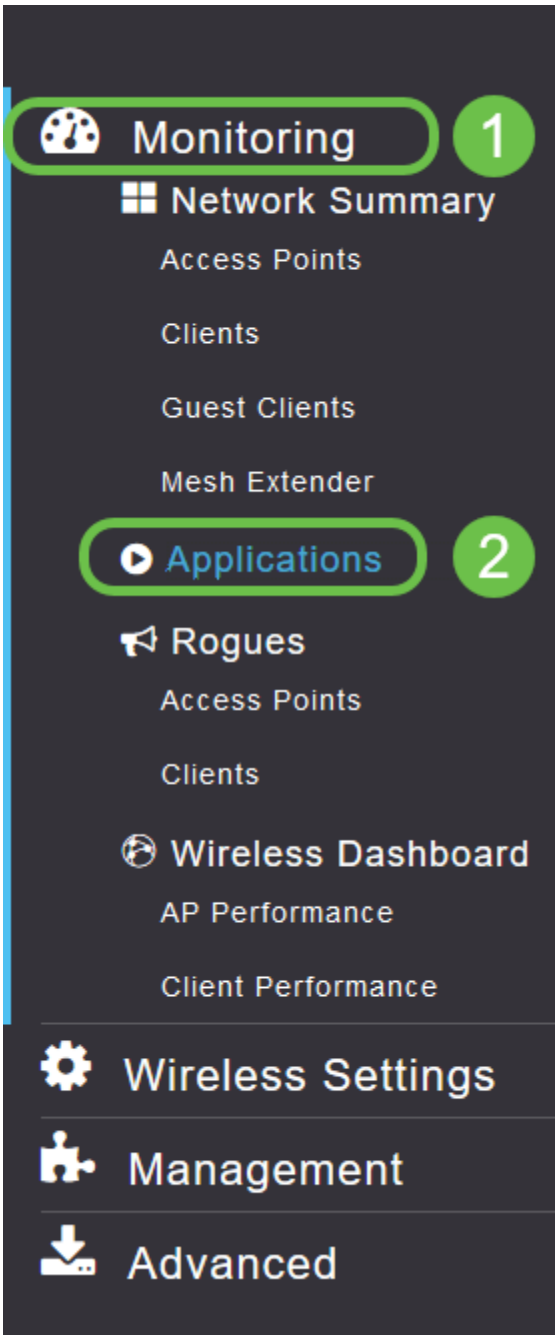
Apply(적용) 버튼을 클릭합니다.



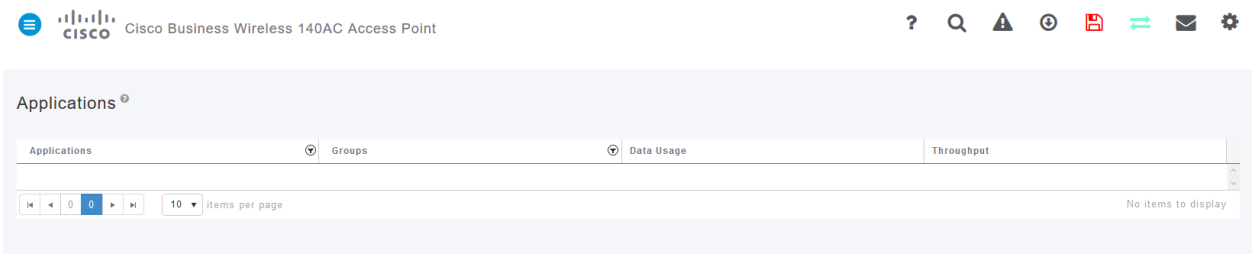
이 설정을 사용하도록 설정해야 합니다. 그렇지 않으면 기능이 작동하지 않습니다.

7단계

취소 버튼을 클릭하여 WLAN 하위 메뉴를 닫습니다.그런 다음 왼쪽 메뉴 모음에서 Monitoring 메뉴를 클릭합니다.가능하다면 **애플리케이션** 메뉴 항목을 클릭합니다.



소스에 대한 트래픽이 없는 경우 아래와 같이 페이지가 비어 있습니다.



이 페이지에는 다음 정보가 표시됩니다.

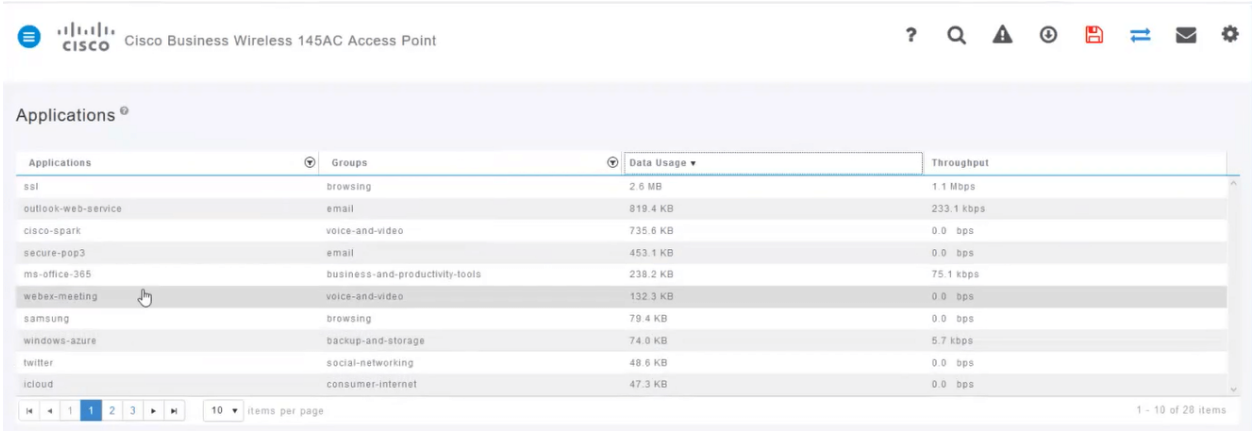
- 애플리케이션 - 다양한 유형 포함
- Groups(그룹) - 보다 쉽게 정렬할 수 있는 애플리케이션 그룹의 유형을 나타냅니다.
- 데이터 사용량 - 이 서비스에서 사용하는 전체 데이터 양
- 처리량 - 애플리케이션에서 사용하는 대역폭의 양

탭을 클릭하여 가장 큰 탭에서 가장 작은 탭으로 정렬할 수 있으며, 이는 네트워크 리소스의 가장 큰 소비자를 식별하는 데 도움이 됩니다.

이 기능은 WLAN 리소스를 세부적으로 관리하는 데 매우 유용합니다.다음은 보다 일반적인 그룹 및 애플리케이션 유형 중 일부입니다.목록에는 다음 그룹 및 예를 포함하여 더 많은 항목이 포함될 수 있습니다.

- 검색
  - 예:클라이언트별, SSL
- Email
  - 예:Outlook, Secure-pop3
- 음성 및 비디오
  - 예:WebEx, Cisco Spark,
- 비즈니스 및 생산성 도구
  - 예:Microsoft Office 365,
- 백업 및 스토리지
  - 예:Windows-Azure,
- 소비자-인터넷
  - iCloud, Google 드라이브
- 소셜 네트워킹
  - 예:트위터, Facebook
- 소프트웨어 업데이트
  - 예:Google-Play, IOS
- 인스턴트 메시징
  - 예:행아웃, 메시지

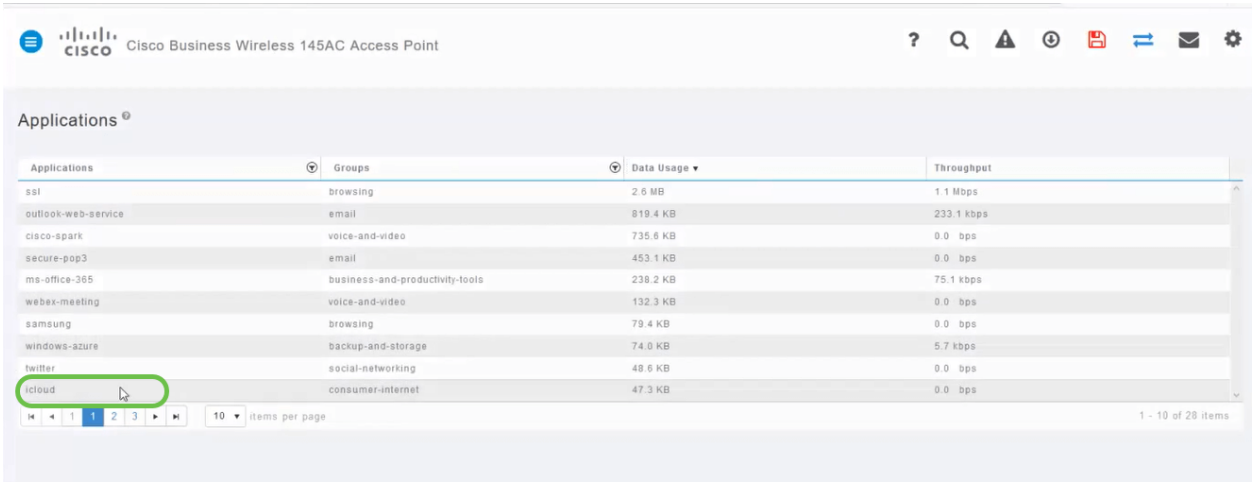
다음은 페이지를 채울 때의 모양을 보여주는 예입니다.



각 테이블 제목을 클릭하면 정렬이 가능하며, 이는 *데이터 사용량* 및 *처리량* 필드에 특히 유용합니다.

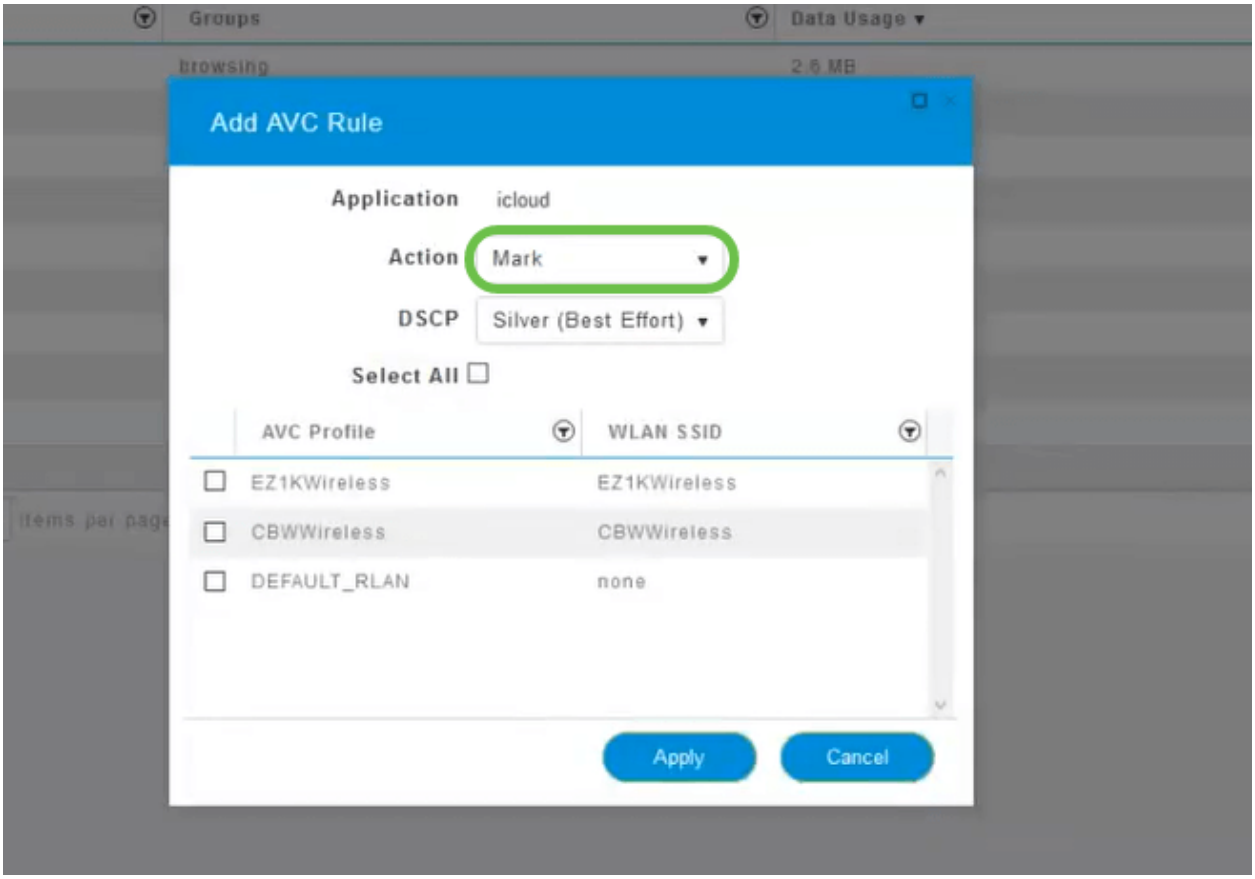
8단계

관리할 트래픽 유형의 행을 클릭합니다.



9단계

Action 드롭다운 상자를 클릭하여 해당 트래픽 유형을 처리하는 방법을 선택합니다.



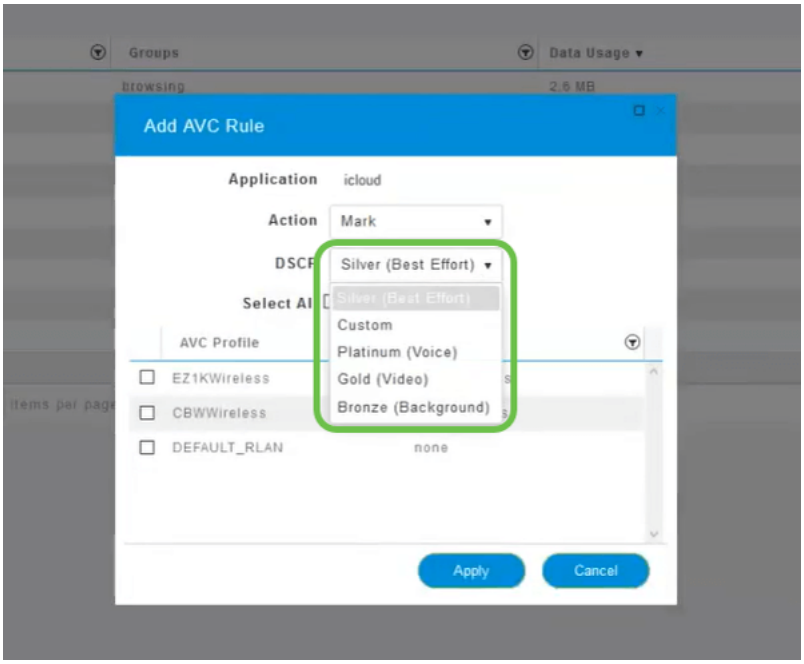
이 예제에서는 이 옵션을 *Mark*로 *둡니다*.

트래픽에 대한 조치

- Mark - 트래픽 유형을 DSCP(Differentiated Services Code Point) 3 계층 중 하나에 배치하여 애플리케이션 유형에 사용할 수 있는 리소스 수를 제어합니다.
- Drop(삭제) - 트래픽을 폐기하지 않고 아무것도 수행하지 않습니다.
- 속도 제한 - 평균 속도, 버스트 속도(Kbps)를 설정할 수 있습니다.

10단계

DSCP 필드의 드롭다운 상자를 **클릭하여** 다음 옵션 중에서 선택합니다.



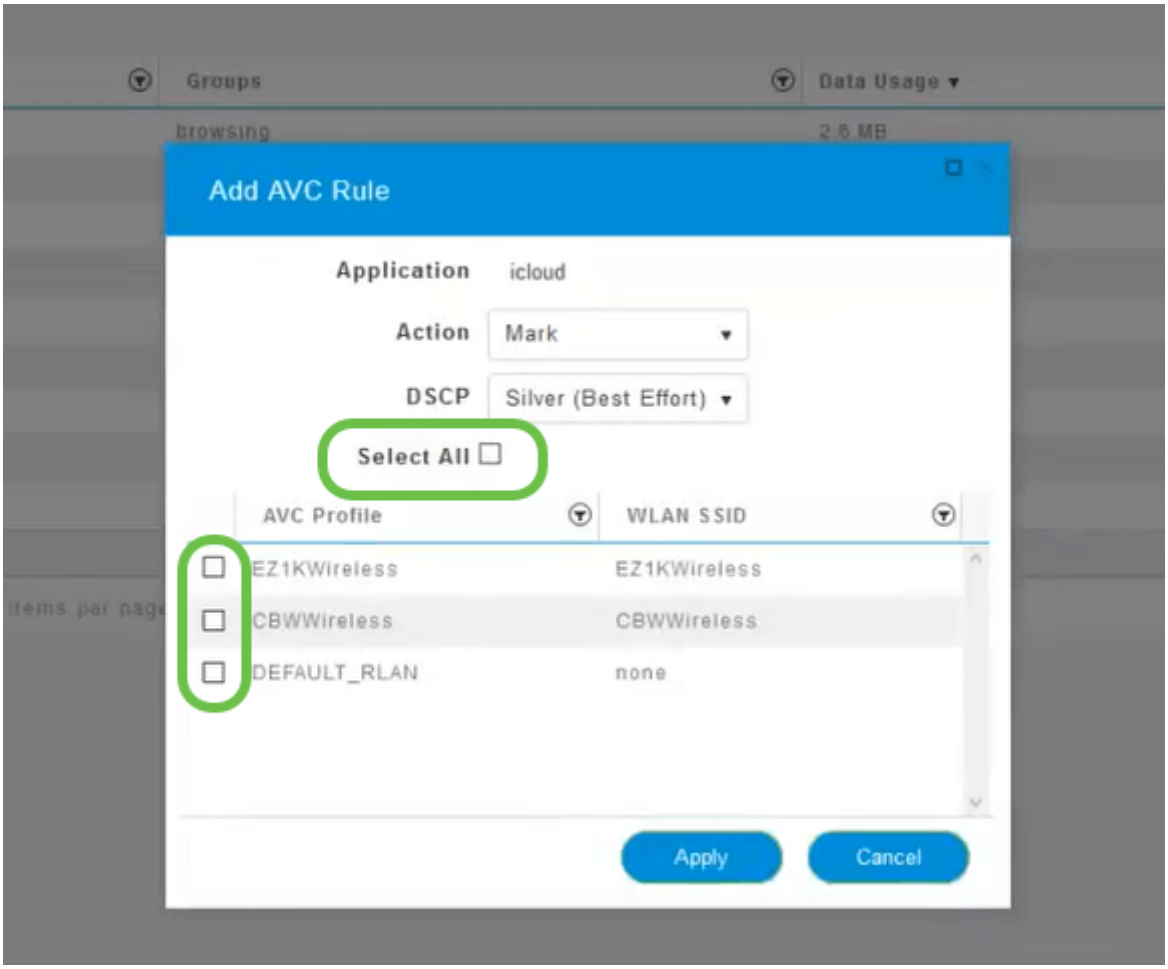
다음은 표시할 트래픽에 대한 DSCP 옵션입니다.이러한 옵션은 더 적은 리소스에서 편집 중인 트래픽 유형에 사용할 수 있는 더 많은 리소스로 진행됩니다.

- Bronze(배경) - 작음
- 실버(최선형)
- 골드(비디오)
- 플래티넘(음성) 자세히
- 사용자 지정 - 사용자 집합

웹 규칙으로서, 트래픽은 SSL 브라우징으로 마이그레이션되어 네트워크에서 WAN으로 이동하는 패킷의 내부 상황을 확인할 수 없습니다.따라서 웹 트래픽의 대부분은 SSL을 사용합니다.우선 순위가 낮은 SSL 트래픽을 설정하면 검색 환경에 영향을 줄 수 있습니다.

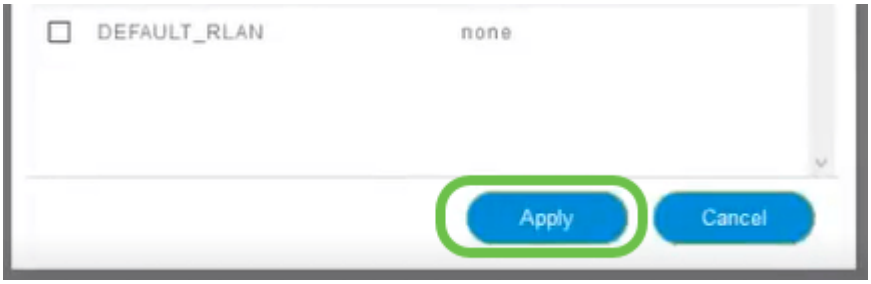
11단계

이제 이 정책을 실행할 개별 SSID를 선택하거나 Select **All**(모두 선택)을 클릭합니다.



12단계

이제 Apply(**적용)**를 클릭하여 이 정책을 시작합니다.



이 기능이 적용될 수 있는 두 가지 사례:

- 많은 양의 트래픽을 스트리밍하여 미션 크리티컬 트래픽이 통과되지 않도록 하는 게스트/사용자Voice의 우선 순위를 높이거나 Netflix 트래픽의 우선 순위를 낮춤으로써 상황을 개선할 수 있습니다.
- 업무 시간 중에 다운로드되는 대규모 소프트웨어 업데이트는 우선 순위가 조정되거나 속도가 제한될 수 있습니다.

네가 해냈어!애플리케이션 프로파일링은 다음 섹션에 자세히 설명되어 있는 것처럼 클라이언트 프로파일링을 활성화하여 더욱 활성화할 수 있는 매우 강력한 툴입니다.

웹 UI를 사용하여 클라이언트 프로파일링(선택 사항)

네트워크에 연결되면 디바이스는 클라이언트 프로파일링 정보를 교환합니다.기본적으

로 *클라이언트 프로파일링*은 비활성화되어 있습니다.이 정보에는 다음이 포함될 수 있습니다.

- 호스트 이름 또는 디바이스의 이름
- 운영 체제 - 디바이스의 핵심 소프트웨어
- OS 버전 - 해당 소프트웨어의 반복입니다.

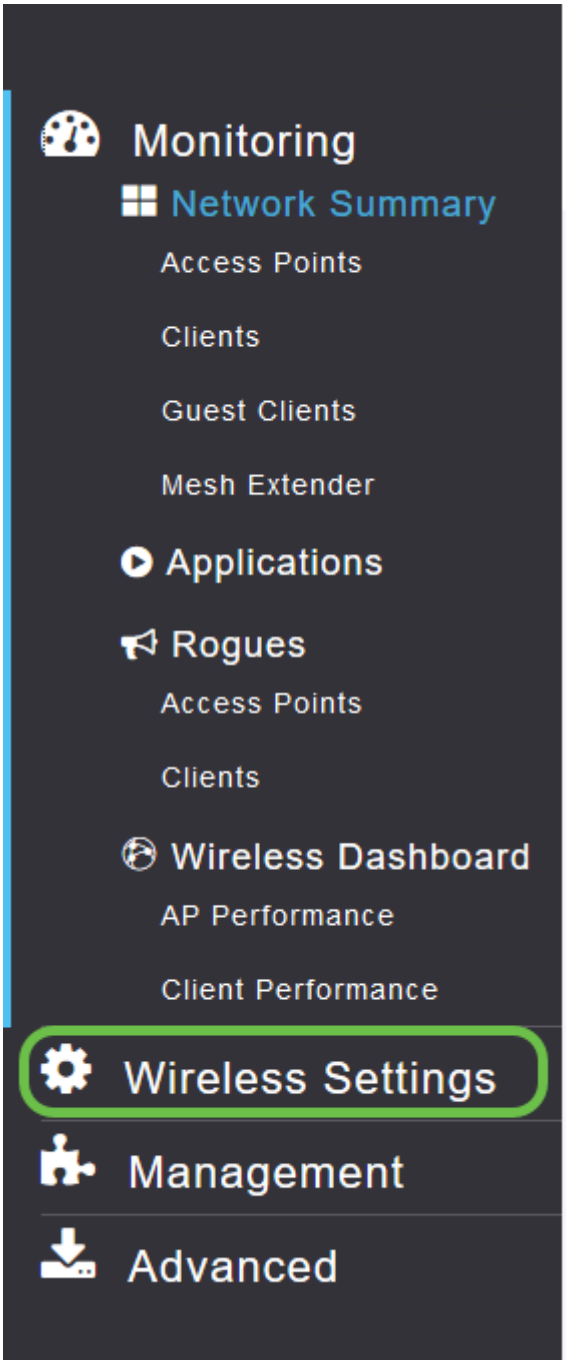
이러한 클라이언트에 대한 통계에는 사용된 데이터의 양과 처리량이 포함됩니다.

클라이언트 프로파일을 추적하면 무선 LAN을 더 효과적으로 제어할 수 있습니다.또는 다른 기능의 함수로 사용할 수도 있습니다.업무에 미션 크리티컬 데이터를 전달하지 않는 애플리케이션 제한 디바이스 유형 사용 등의 문제가 있습니다.

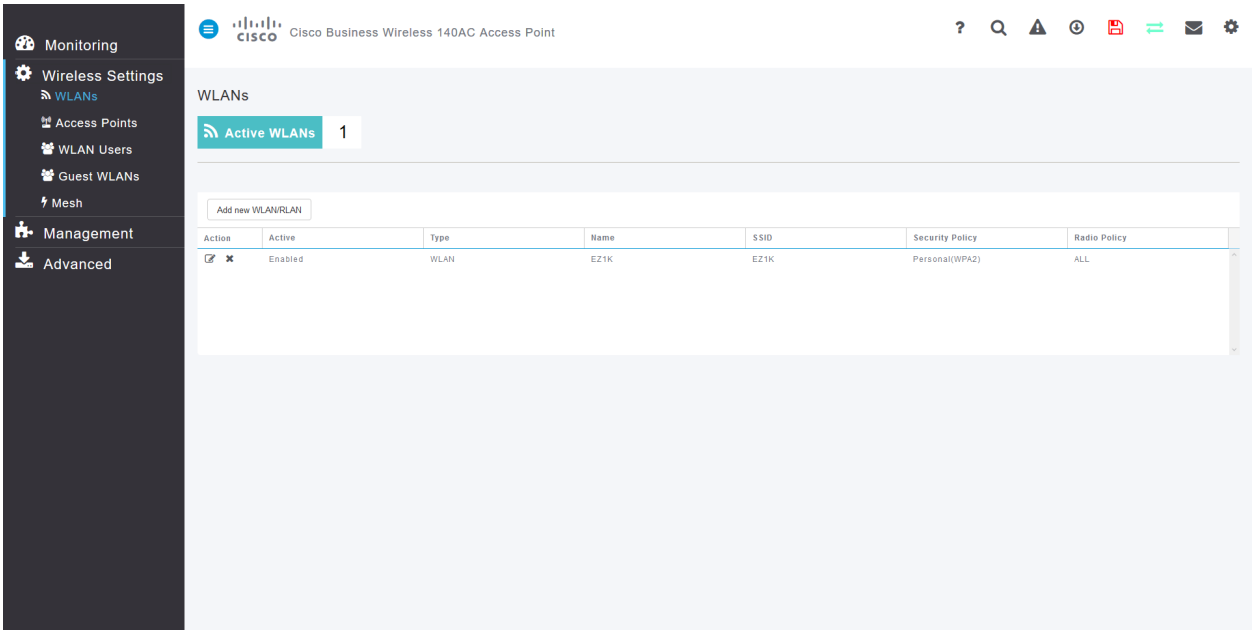
활성화되면 웹 UI의 Monitoring(모니터링) 섹션에서 네트워크에 대한 클라이언트 세부 정보를 찾을 수 있습니다.

1단계

무선 설정을 **클릭합니다**.

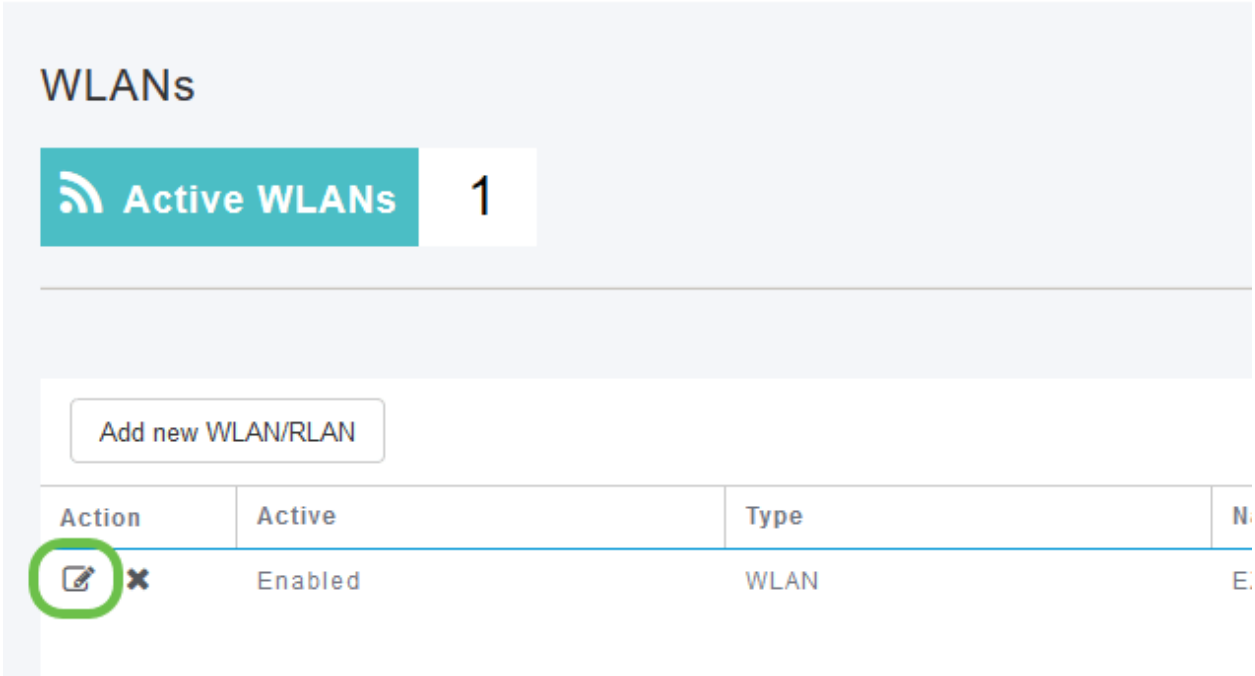


아래는 무선 설정 링크를 클릭할 때 표시되는 것과 유사합니다.



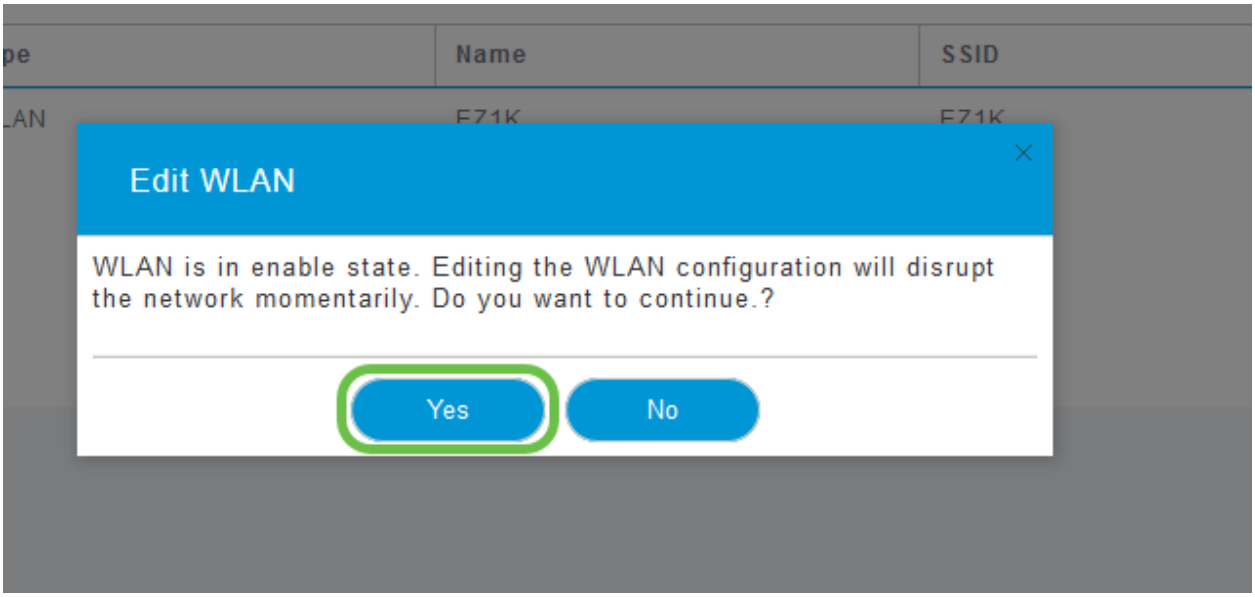
2단계

애플리케이션에 사용할 WLAN을 결정하고 왼쪽의 **수정 아이콘**을 클릭합니다.



3단계

팝업 메뉴가 아래와 유사하게 나타날 수 있습니다.이 중요한 메시지는 일시적으로 네트워크의 서비스에 영향을 미칠 수 있습니다.**예**를 클릭하여 앞으로 이동합니다.

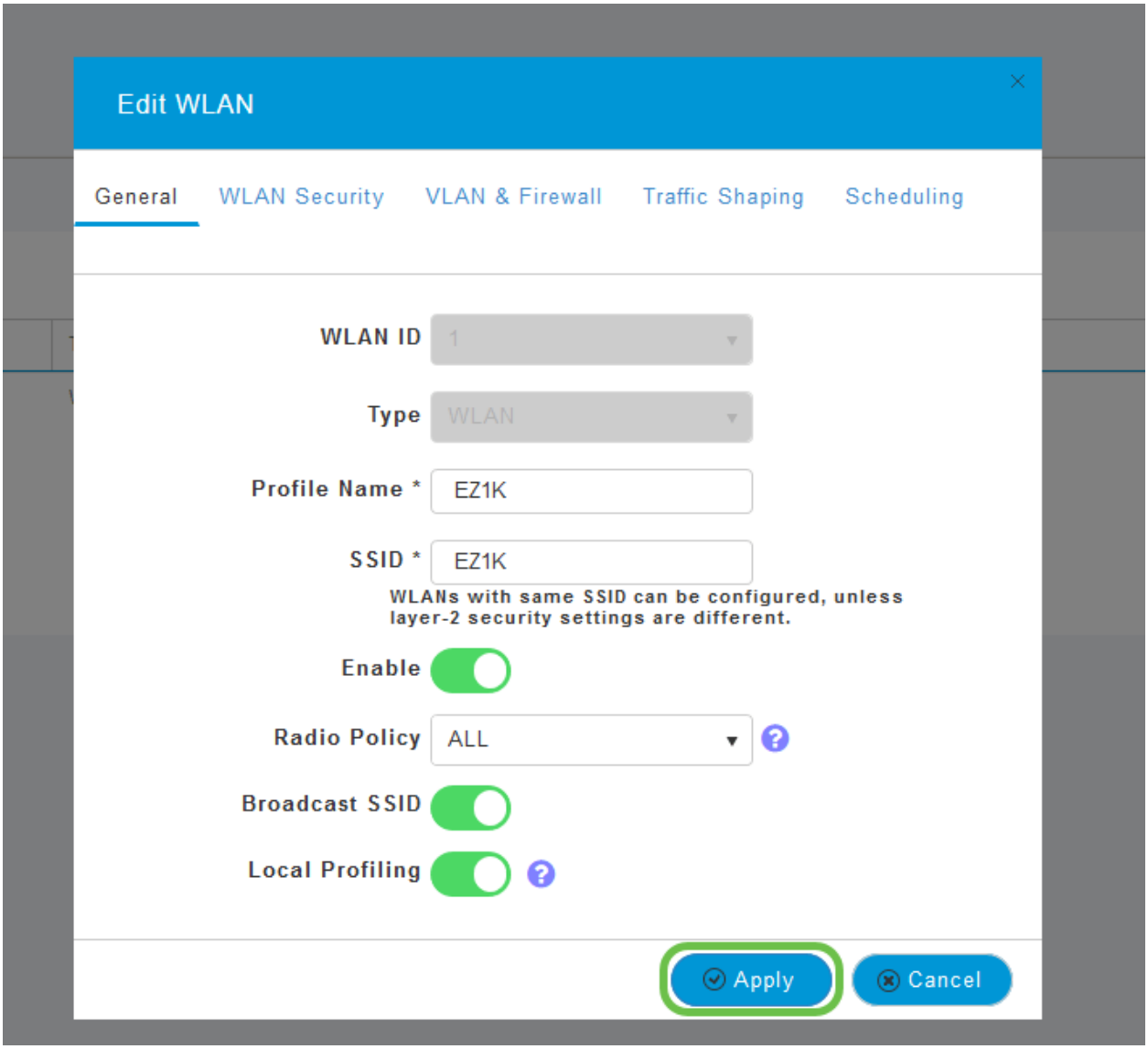


4단계

Local Profiling(로컬 프로파일링) 토글 버튼을 클릭하여 클라이언트 프로파일링을 전환합니다.

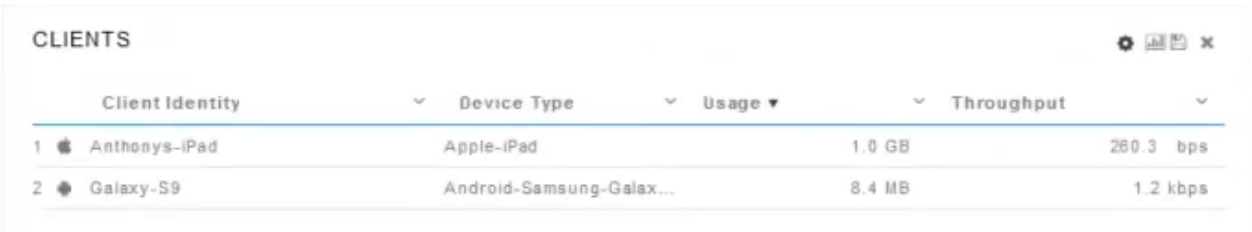
5단계

Apply를 **클릭합니다**.



6단계

왼쪽에서 **Monitoring** 섹션 메뉴 항목을 클릭합니다.클라이언트 데이터가 Monitoring(모니터링) 탭의 Dashboard(대시보드)에 *나타나며,*



결론

이제 보안 네트워크 설정을 완료했습니다.정말 기분이 좋군요, 이제 축하하고 일을 시작하겠습니다!

Cisco는 고객에게 최상의 서비스를 제공하기 원하므로 이 주제에 대한 의견 또는 제안 사항이 있으면 Cisco 콘텐츠 팀에 이메일을 보내 주십시오.

다른 문서 및 문서를 읽으려면 하드웨어에 대한 지원 페이지를 확인하십시오.

- Cisco RV260P VPN Router with PoE
- Cisco Business 140AC Access Point
- Cisco Business 142ACM Mesh Extender