총 네트워크 구성:웹 UI를 사용하는 RV345P 및 Cisco Business Wireless

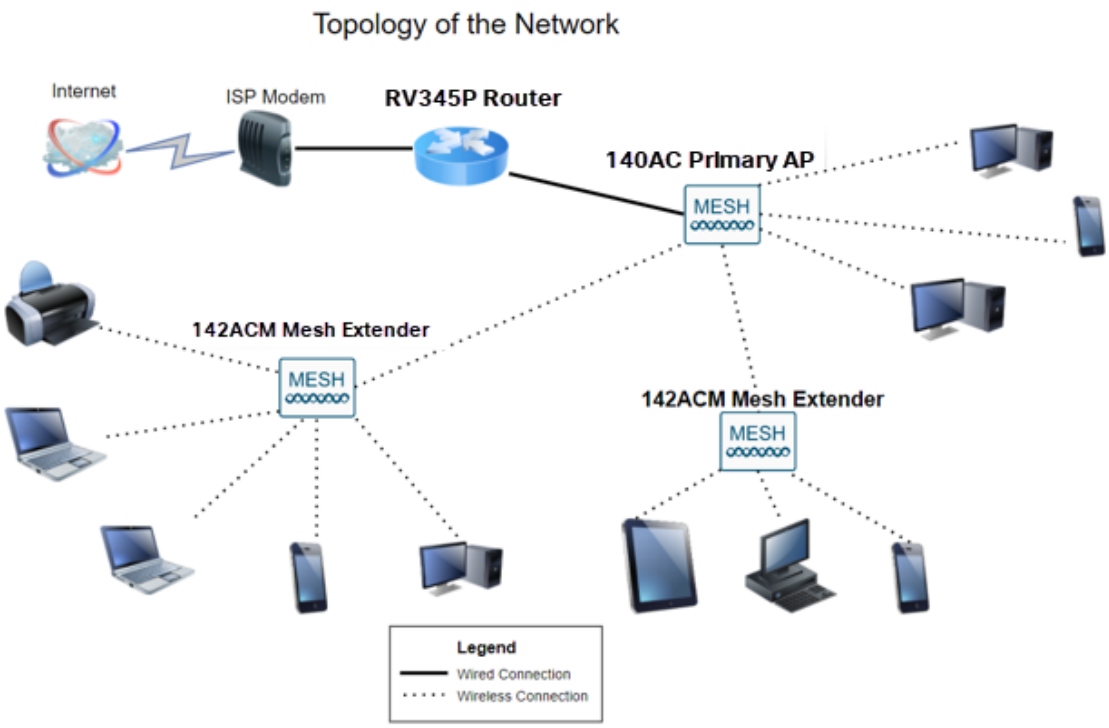
목표

이 설명서에서는 RV345P 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.

목차

토폴로지



소개

모든 연구 결과가 함께 제공되었으며 Cisco 장비를 구입하셨습니다. 정말 흥미롭습니다!이 시나리오에서는 RV345P 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 고급 라우터는 추가 기능을 위한 옵션도 제공합니다.

1. 애플리케이션 제어를 통해 트래픽을 제어할 수 있습니다.이 기능은 트래픽을 허용하되 로깅하거나, 트래픽을 차단하여 로깅하거나, 단순히 트래픽을 차단하도록 구성할 수 있습니다.
2. 웹 필터링은 웹 트래픽이 보안되지 않거나 부적절한 웹 사이트로 이동하는 것을 방지하는 데 사용됩니다.이 기능에 대한 로깅이 없습니다.
3. AnyConnect는 Cisco에서 제공하는 SSL(Secure Sockets Layer) VPN(Virtual Private Network)입니다.VPN을 사용하면 인터넷을 통해 안전한 터널을 만들어 원격 사용자와 사이트가 회사 사무실 또는 데이터 센터에 연결할 수 있습니다.

이러한 기능을 사용하려면 라이센스를 구입해야 합니다.라우터와 라이센스는 온라인으로 등록되며, 본 설명서에서 다룹니다.

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)

적용 가능한 디바이스 | 소프트웨어 버전

- RV345P | 1.0.03.21
- CBW140AC | 10.4.1.0
- CBW142ACM | 10.4.1.0(메시 네트워크에 하나 이상의 메시 익스텐더가 필요함)

사전 요구 사항

라우터 준비

1. 설치할 현재 인터넷 연결이 있는지 확인하십시오.
2. RV345P 라우터를 사용할 때 제공되는 특별 지침을 확인하려면 ISP(인터넷 서비스 공급자)에 문의하십시오.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.

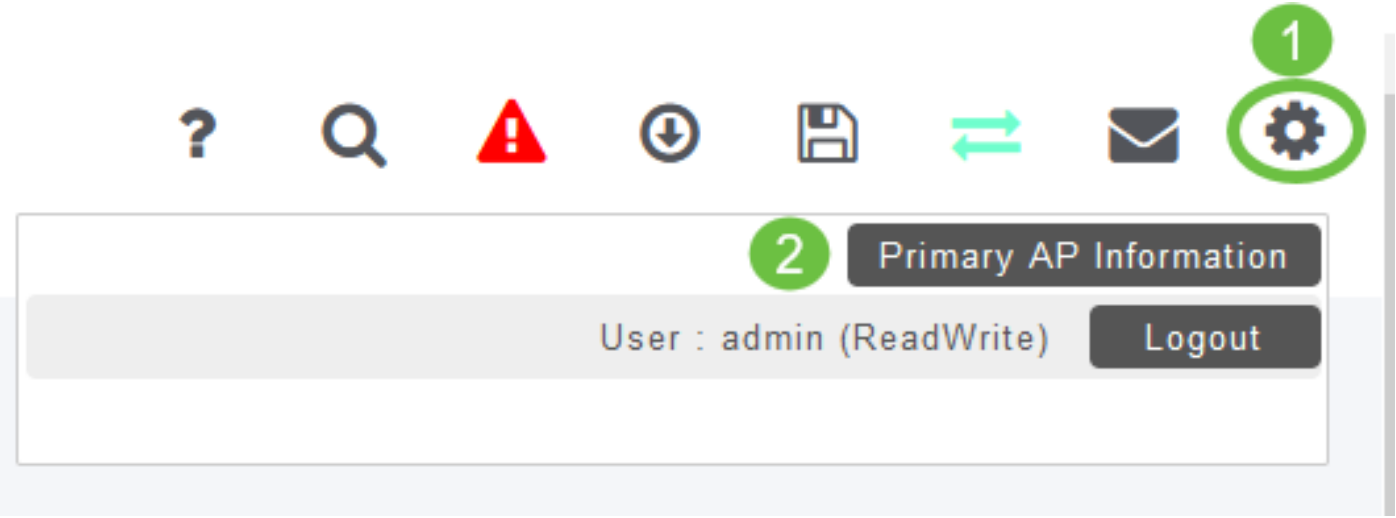
Cisco.com 계정 가져오기

이제 Cisco 장비를 소유하고 있으므로 Cisco.com 계정(CCO ID(Cisco Connection Online Identification)이라고도 함)을 얻어야 합니다. 계좌는 무료입니다.

이미 계정이 있는 경우 이 문서의 다음 섹션으로 이동할 수 있습니다.

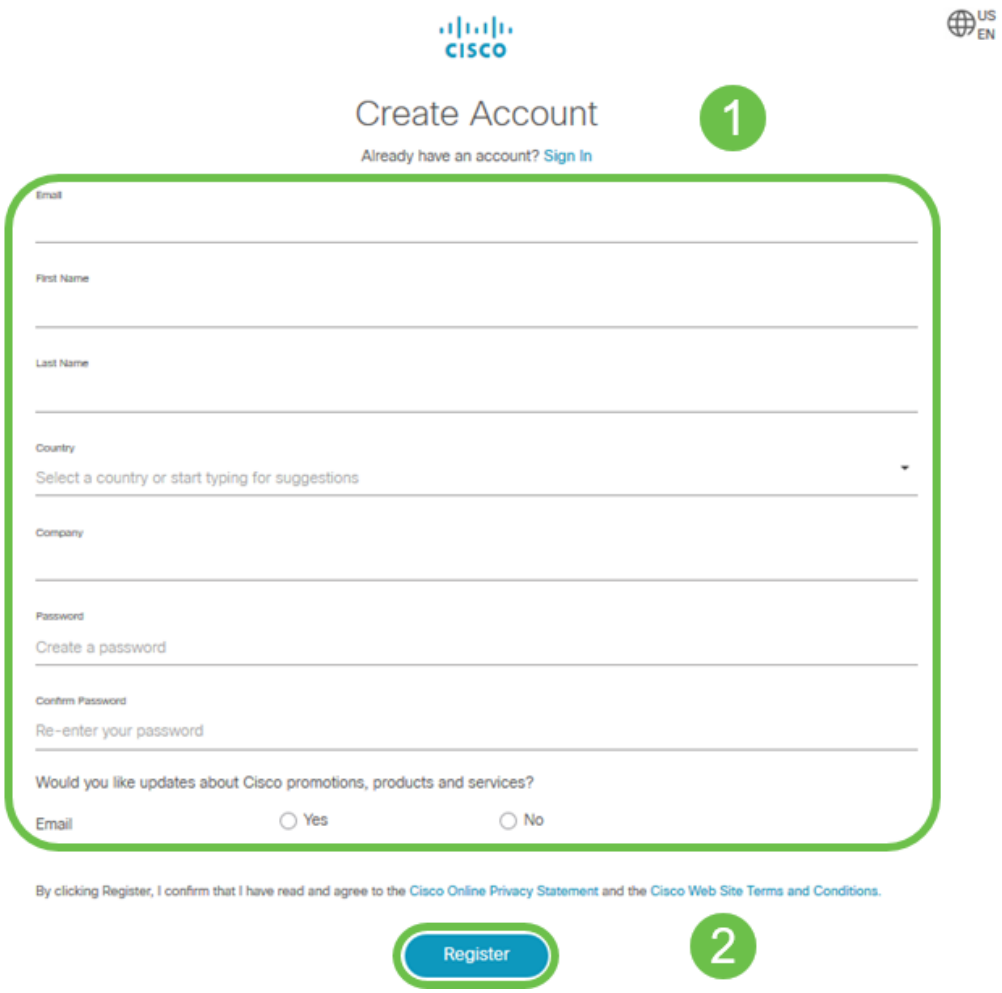
1단계

Cisco.com으로 이동합니다.**사람 아이콘**을 클릭한 다음 **계정 만들기를 클릭합니다**.



2단계

필요한 세부 정보를 입력하여 계정을 생성하고 Register(**등록**)를 클릭합니다.지침에 따라 등록 프로세스를 완료합니다.



문제가 있으면 [클릭하여 Cisco.com Account Registration Help 페이지로 이동합니다](#).

RV345P 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 나

열됩니다.특정 대상에 패킷을 가져오기 위해 라우팅 테이블에 정적 및 동적 컨피그레이션을 모두 나열할 수 있습니다.

RV345P에는 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.

준비됐어요?빨리 가자!

RV345P Out of the Box

1단계

RV345P LAN(이더넷) 포트 중 하나에서 컴퓨터의 이더넷 포트에 이더넷 케이블을 연결합니다.컴퓨터에 이더넷 포트가 없는 경우 어댑터가 필요합니다.초기 컨피그레이션을 수행하려면 터미널이 RV345P와 동일한 유선 하위 네트워크에 있어야 합니다.

2단계

RV345P와 함께 제공되는 전원 어댑터를 사용해야 합니다.다른 전원 어댑터를 사용하면 RV345P가 손상되거나 USB 동글이 손상될 수 있습니다.전원 스위치는 기본적으로 켜져 있습니다.

전원 어댑터를 RV345P의 12VDC 포트에 연결하되 아직 전원을 연결하지 마십시오.

3단계

모뎀이 꺼져 있는지 확인합니다.

4단계

이더넷 케이블을 사용하여 케이블 또는 DSL 모뎀을 RV345P의 WAN 포트에 연결합니다.

5단계

RV345P 어댑터의 반대쪽 끝을 전기 콘센트에 꽂습니다.이렇게 하면 RV345P의 전원이 켜집니다.모뎀을 다시 연결하여 전원을 켜도 됩니다.전원 어댑터가 제대로 연결되어 있고 RV345P 부팅이 완료되면 전면 패널의 전원 표시등이 녹색으로 켜집니다.

라우터 설정

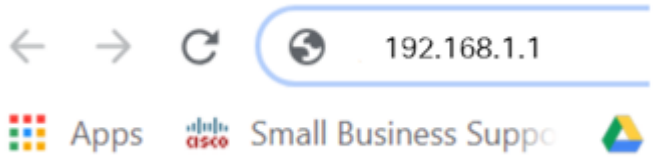
준비 작업이 완료되었습니다. 이제 몇 가지 구성을 시작할 때입니다!웹 UI를 시작하려면 다음 단계를 수행합니다.

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.

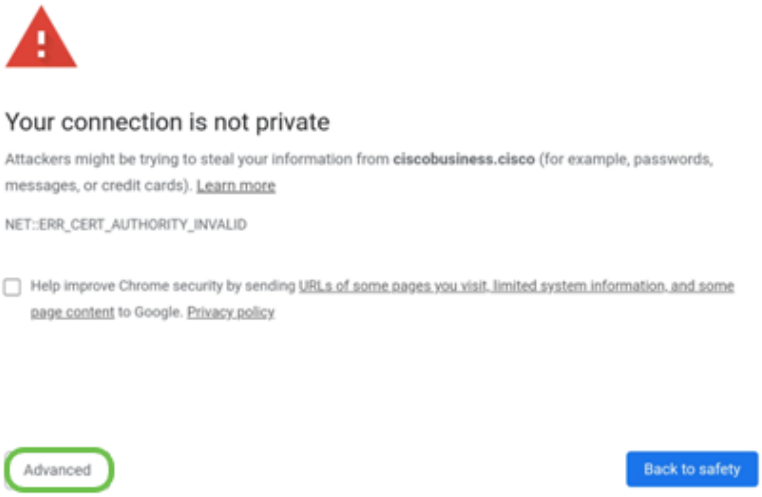
2단계

Safari, Internet Explorer 또는 Firefox와 같은 웹 브라우저를 엽니다.주소 표시줄에 RV345P, 192.168.1.1의 기본 IP 주소를 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.

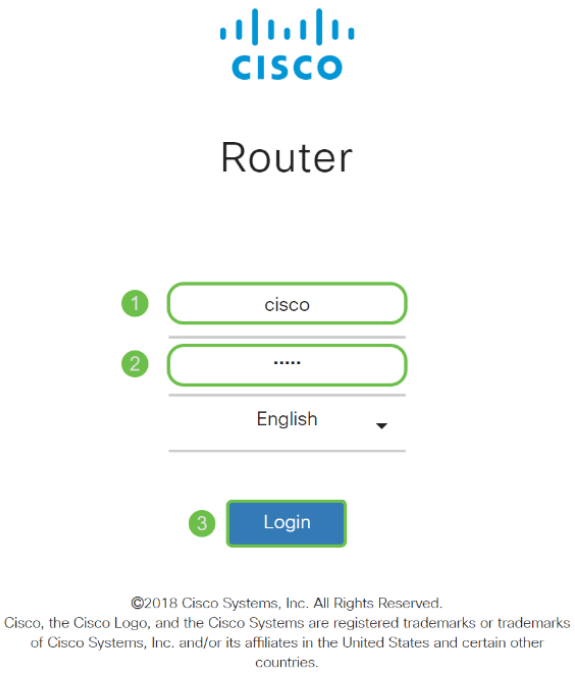


4단계

로그인 페이지가 나타나면 기본 사용자 이름 *cisco*와 기본 비밀번호 *cisco*를 *입력합니다*.

Login(**로그인)을 클릭합니다**.

자세한 내용은 Cisco RV340 Series VPN 라우터의 웹 기반 설정 페이지에 액세스하는 방법을 클릭하십시오.



5단계

Login(**로그인)을 클릭합니다**.Getting *Started* 페이지가 나타납니다.탐색 창이 열려 있지 않으면 **메뉴 아이콘**을 클릭하여 열 수 있습니다.

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)을 입력합니다. 요청이 시간 초과되면 라우터와 통신할 수 없습니다.

연결이 이루어지지 않을 경우 이 문제 해결 문서를 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(RV345P의 기본 IP 주소)로 설정된 192.168.1.x 범위의 고정 IP 주소가 있을 수 있습니다. 연결하려면 RV345P의 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 충돌

을 해결해야 합니다.이 섹션의 끝에서 자세히 알아보거나 **여기를 클릭하여 직접 이동하십시오**.

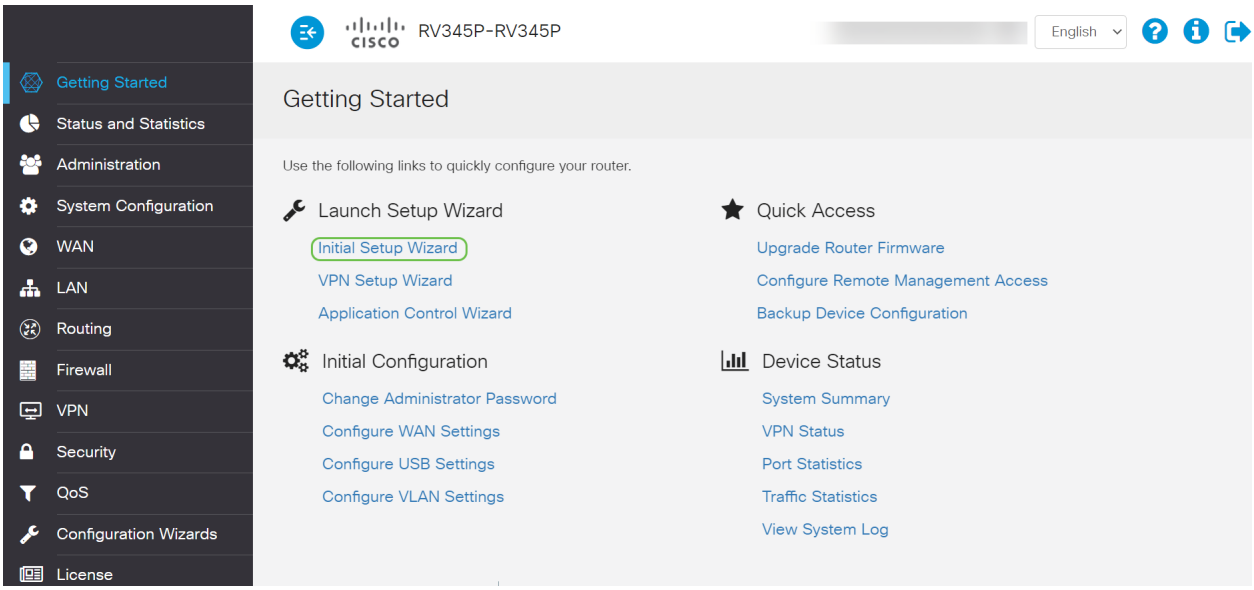
4. 두 장치의 전원을 끄면 모뎀과 RV345P를 재설정합니다.그런 다음 모뎀을 켜고 약 2분 동안 유휴 상태로 둡니다.그런 다음 RV345P의 전원을 켜십시오.이제 WAN IP 주소를 받아야 합니다.
5. DSL 모뎀이 있는 경우 ISP에 DSL 모뎀을 브리지 모드로 설정하도록 요청합니다.

초기 컨피그레이션

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

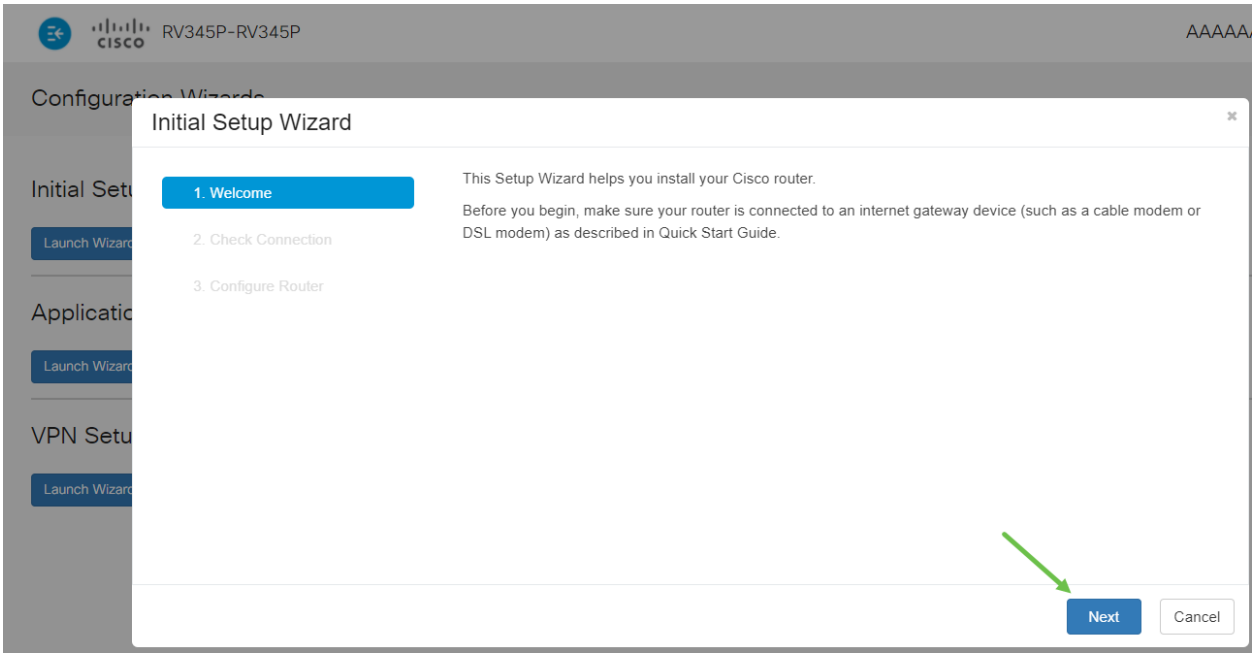
1단계

시작 *페이지*에서 **초기 설정 마법사**를 클릭합니다.



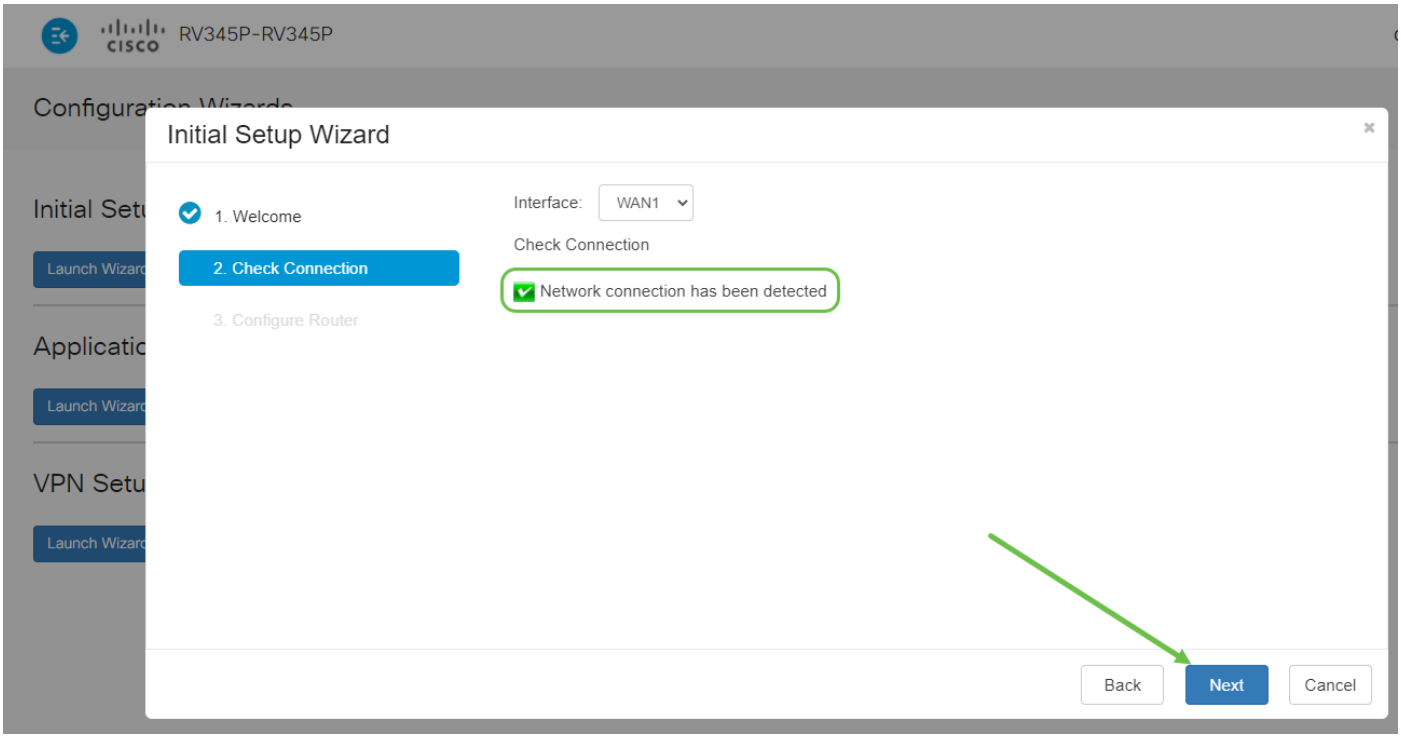
2단계

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



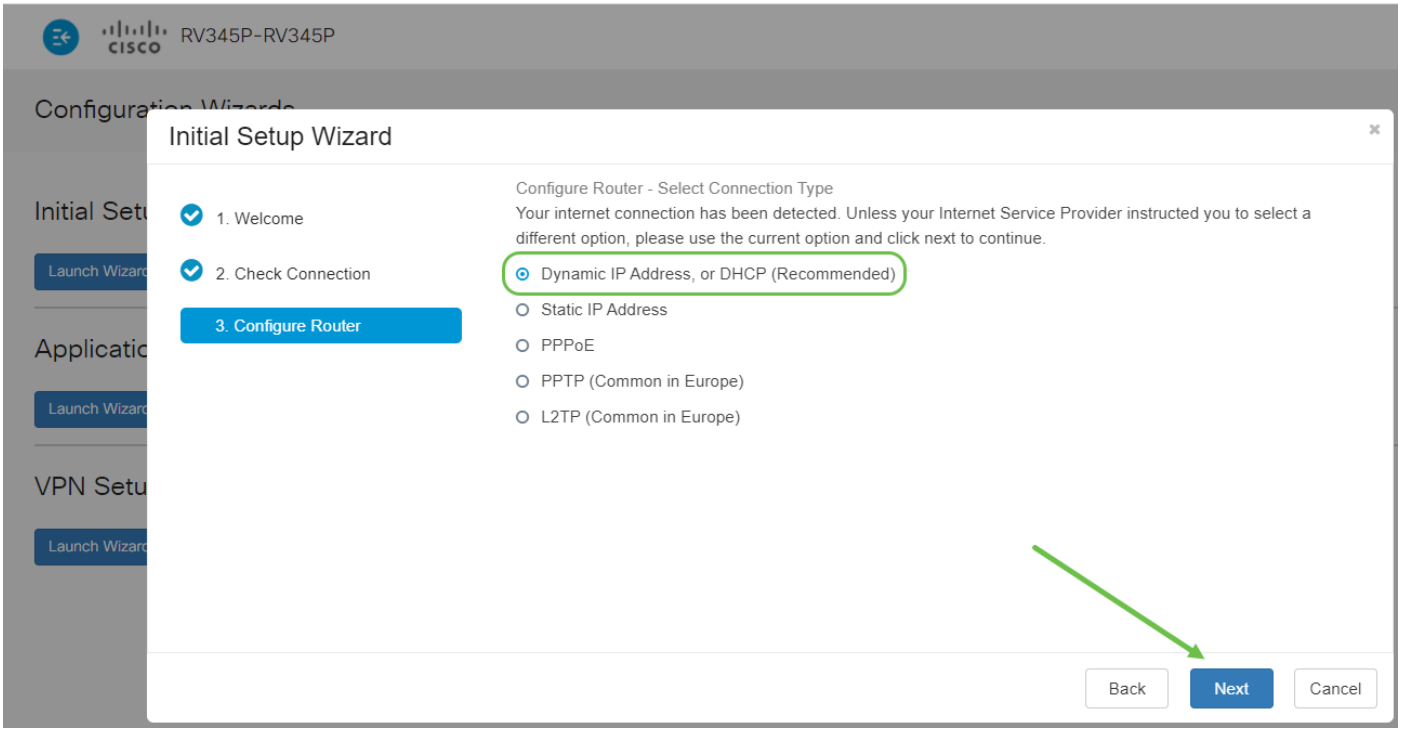
3단계

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



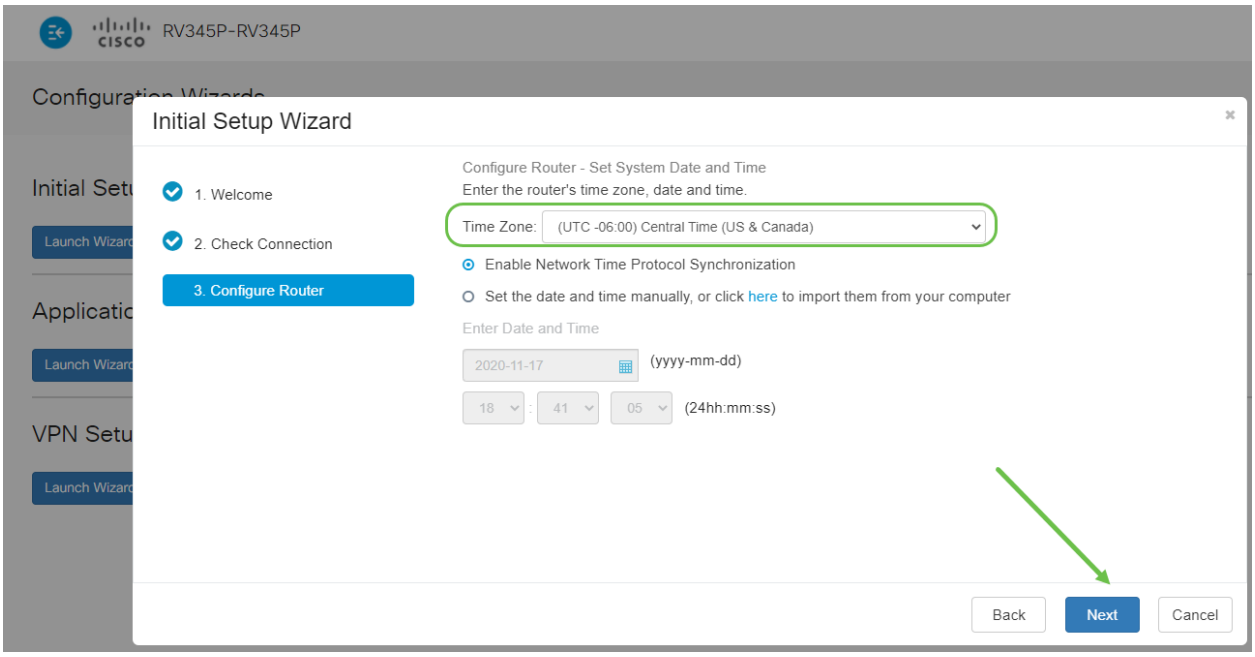
4단계

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



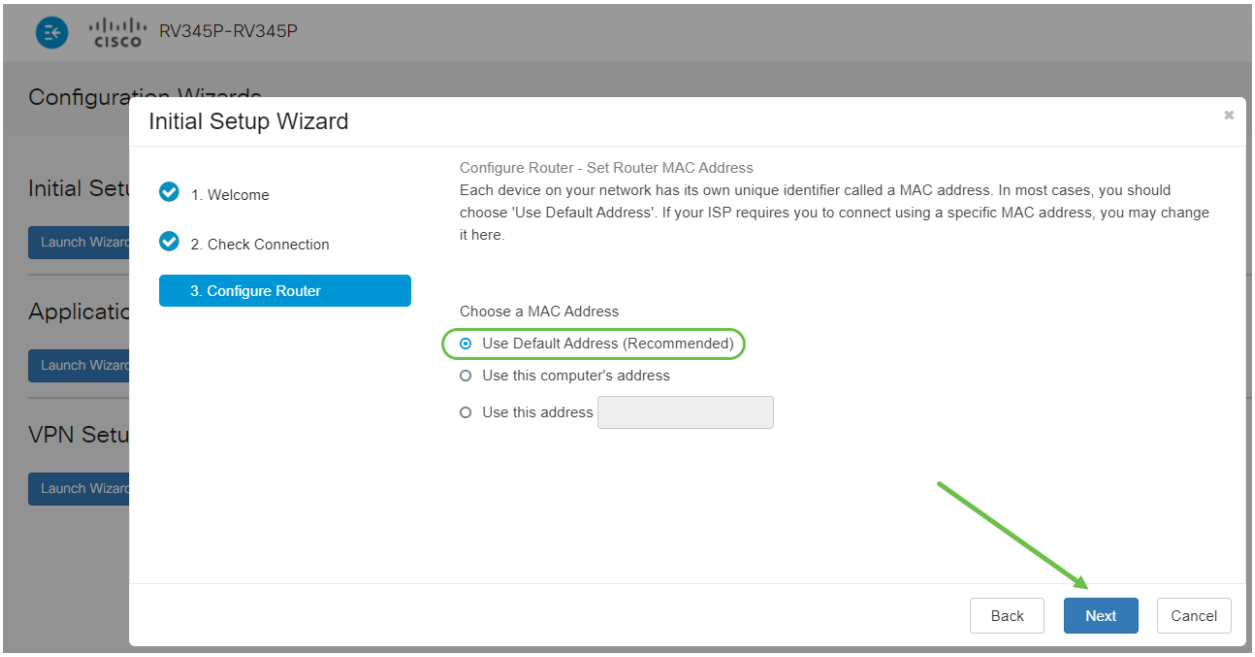
5단계

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.



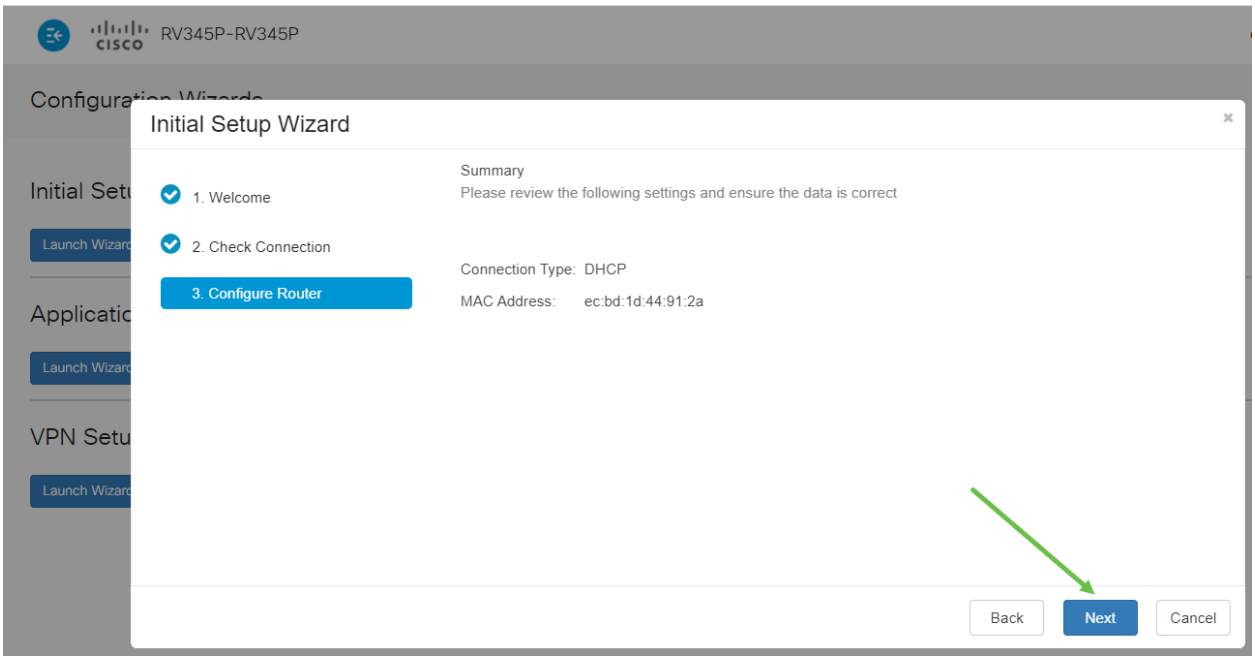
6단계

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



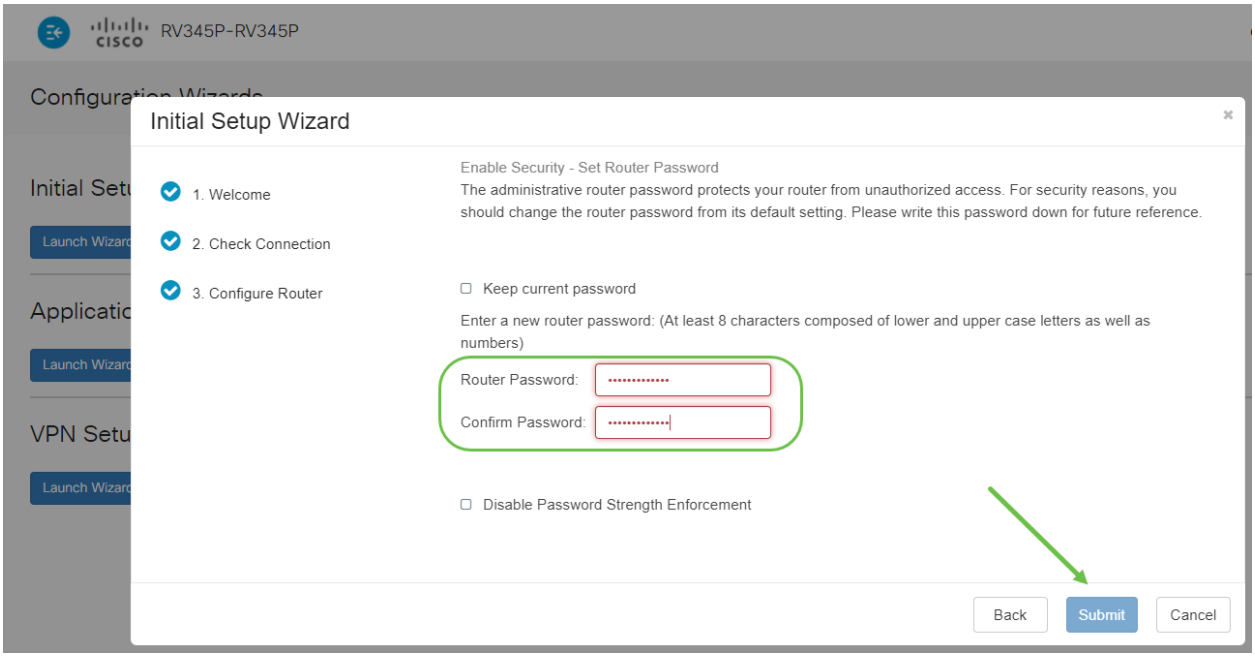
7단계

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 포함하고 숫자를 포함하는 것입니다. **강도** 요구 사항을 준수하는 **비밀번호를** 입력하십시오.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**.

이러한 설정에 대한 자세한 내용을 보려면 RV34x 라우터에서 DHCP WAN 설정 구성을 읽을 수 있습니다.

RV345P는 기본적으로 PoE(Power over Ethernet)가 활성화되어 있지만 일부 조정 기능을 사용할 수 있습니다.설정을 사용자 지정해야 하는 경우 RV345P 라우터에서 Configure Power over Ethernet (PoE) Settings(PoE 설정 구성)를 확인하십시오.

필요한 경우 IP 주소 수정(선택 사항)

*초기 설정 마법사*를 완료한 후 VLAN 설정을 편집하여 라우터에 고정 IP 주소를 설정할 수 있습니다.

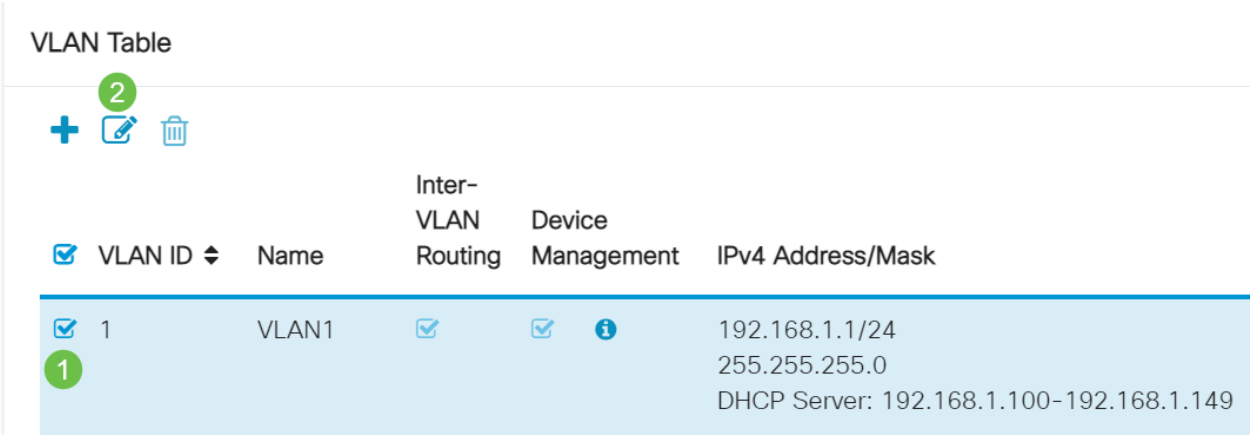
이 프로세스는 라우터 IP 주소에 기존 네트워크의 특정 주소를 할당해야 하는 경우에만 필요합니다.IP 주소를 편집할 필요가 없는 경우 이 문서의 다음 섹션으로 이동할 수 있습니다.

1단계

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

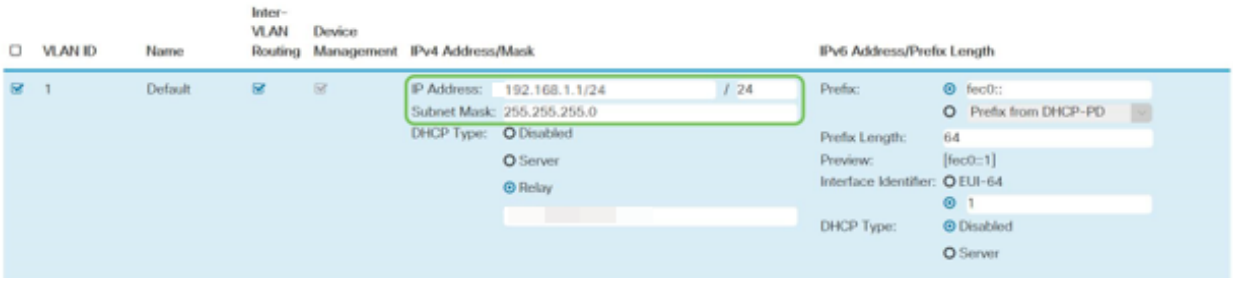
2단계

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



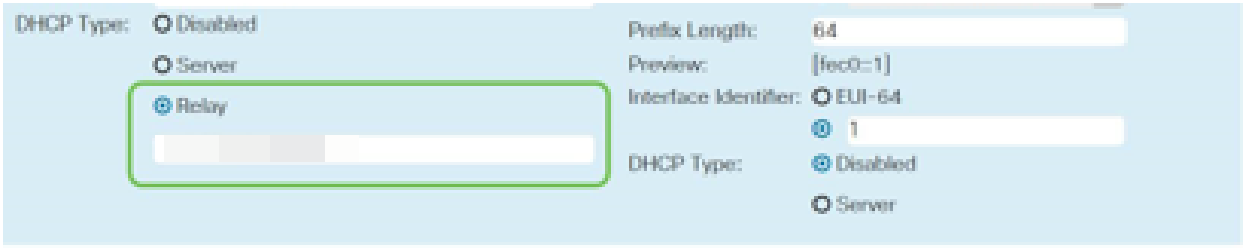
3단계

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.

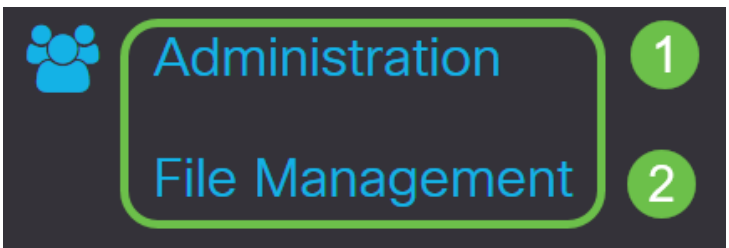


필요한 경우 펌웨어 업그레이드

이것은 중요한 단계입니다. 건너뛰지 마십시오!

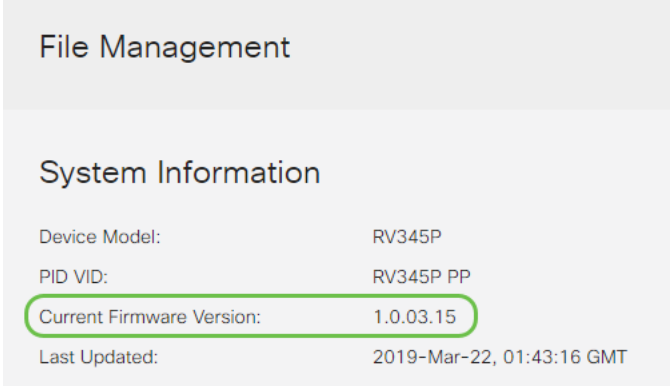
1단계

관리 > **파일 관리를 선택합니다**.



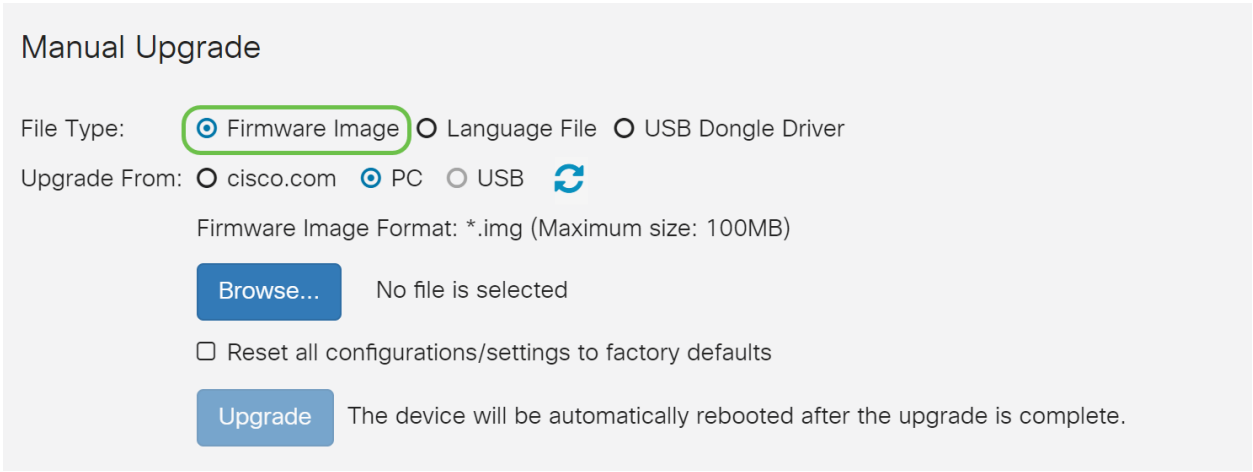
시스템 정보 영역에서 다음 하위 영역에 대해 설명합니다.

- 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.com*을 선택합니다.다른 몇 가지 옵션도 있지만 업그레이드를 수행하는 가장 쉬운 방법입니다.이 프로세스에서는 Cisco Software Downloads 웹 페이지에서 직접 최신 업그레이드 파일을 설치합니다.

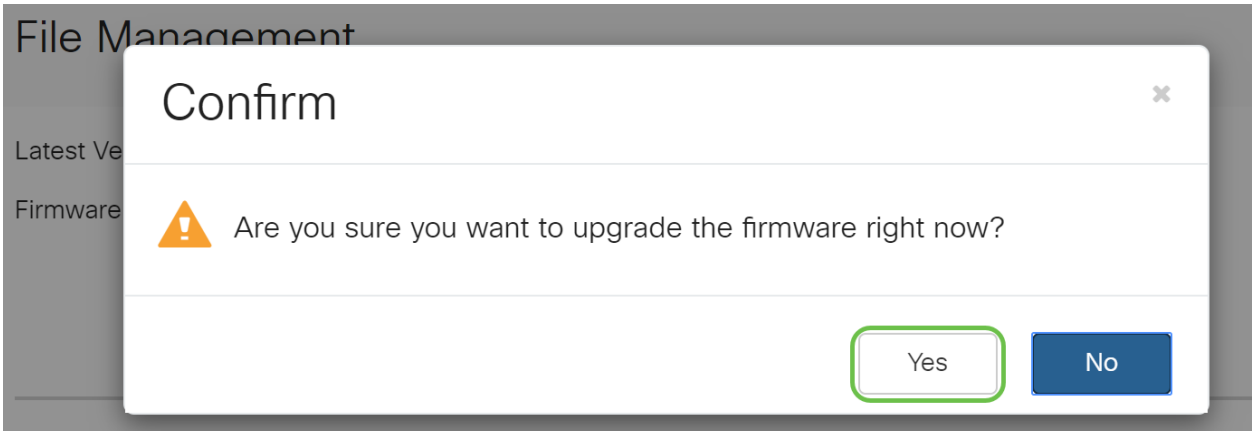
디바이스가 인터넷에 연결되어 있지 않거나 인터넷 연결이 끊어진 경우 cisco.com에서 업그레이드할 수 없습니다.이 옵션이 귀하와 관련된 경우 여기에서 다른 옵션을 찾을 수 있습니다.

4단계

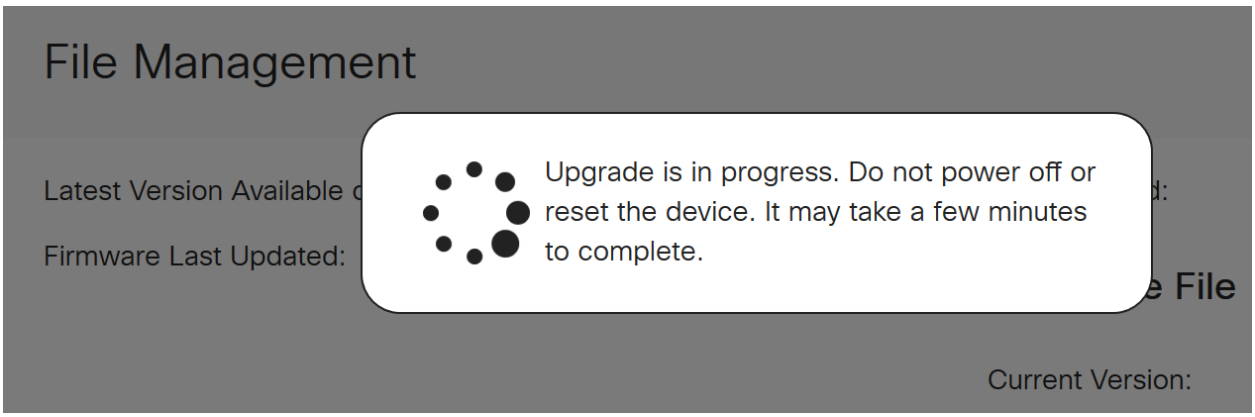
Upgrade를 **클릭합니다**.

5단계

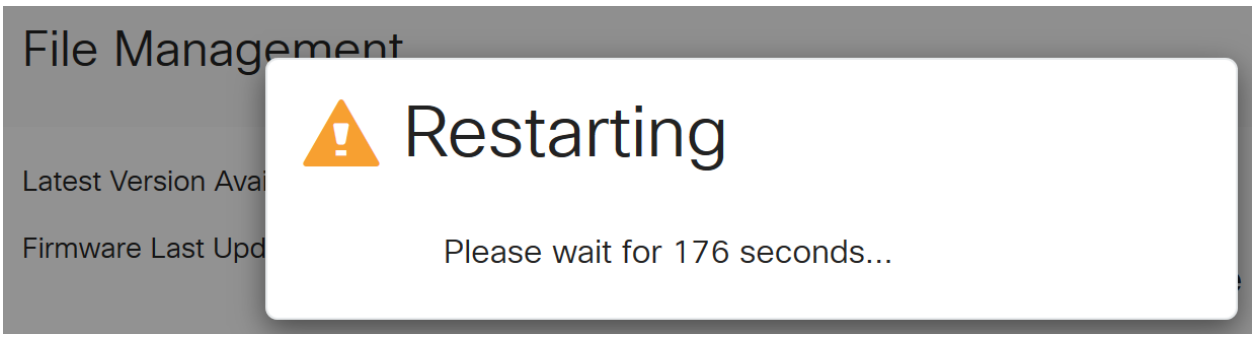
확인 창에서 **예**를 클릭하여 계속합니다.



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

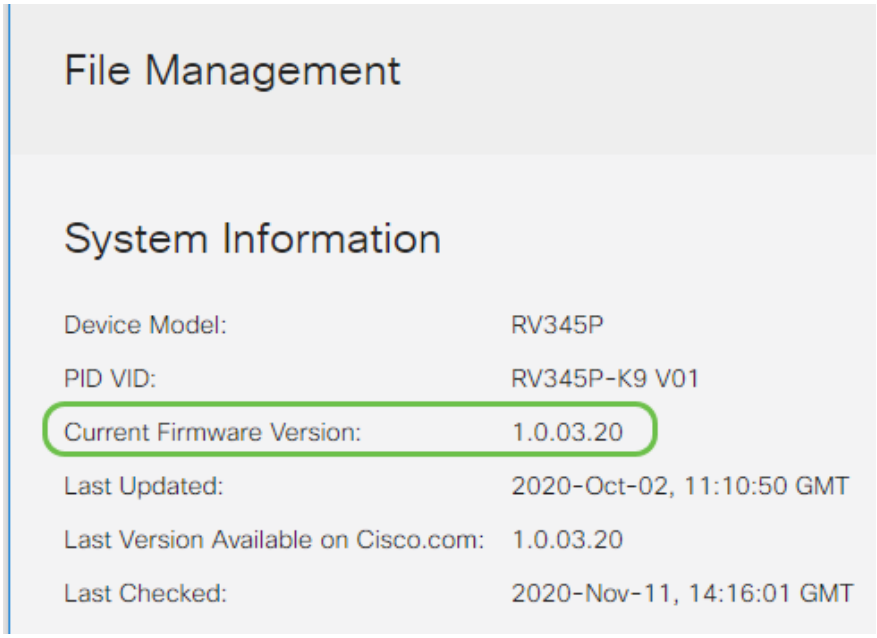


업그레이드가 완료되면 알림 창이 팝업되어 라우터가 프로세스가 완료되는 예상 시간을 카운트다운하여 *다시* 시작됨을 알립니다.이렇게 하면 로그아웃됩니다.



6단계

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

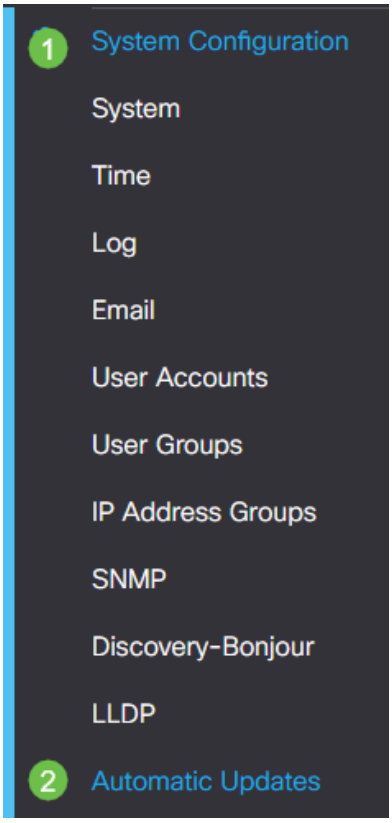


RV345P Series 라우터에서 자동 업데이트 구성

업데이트가 매우 중요하며 바쁜 사용자이므로 여기에서 자동 업데이트를 구성하는 것이 좋습니다!

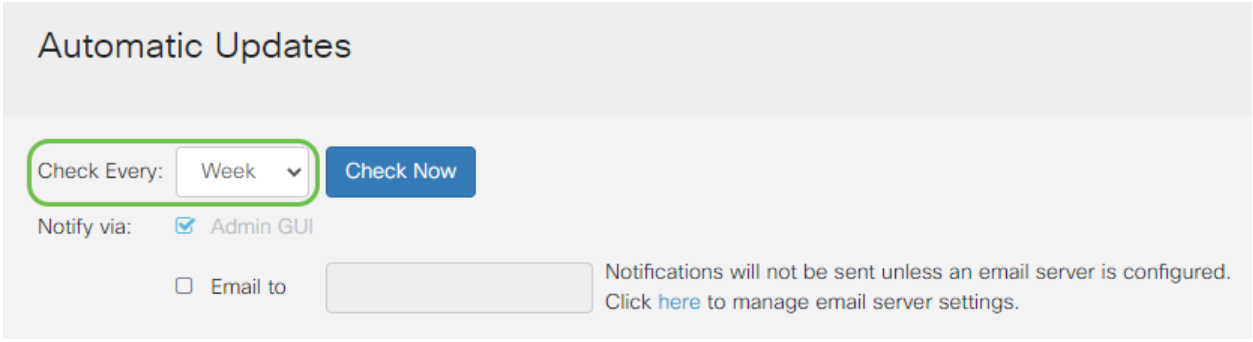
1단계

웹 기반 유틸리티에 로그인하고 System Configuration(시스템 컨피그레이션) > **Automatic Updates(자동 업데이트)**를 선택합니다.



2단계

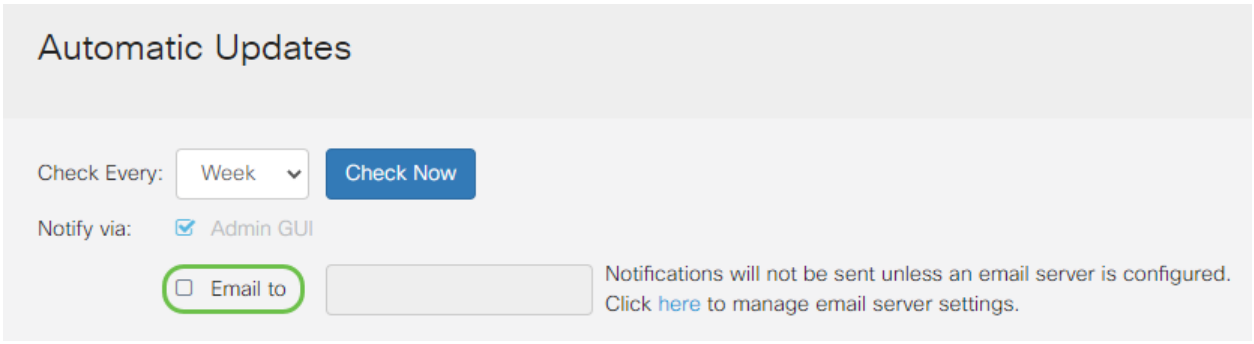
Check *Every* 드롭다운 목록에서 라우터가 업데이트를 확인하는 빈도를 선택합니다.



3단계

Notify *via(알림)* 영역에서 Email to(**이메일 수신**) 확인란을 선택하여 이메일을 통해 업데이트를 수신합니다.관리 *GUI* 확인란은 기본적으로 활성화되어 있으며 비활성화할 수 없습니다.업데이트가 제공되면 웹 기반 컨피그레이션에 알림이 표시됩니다.

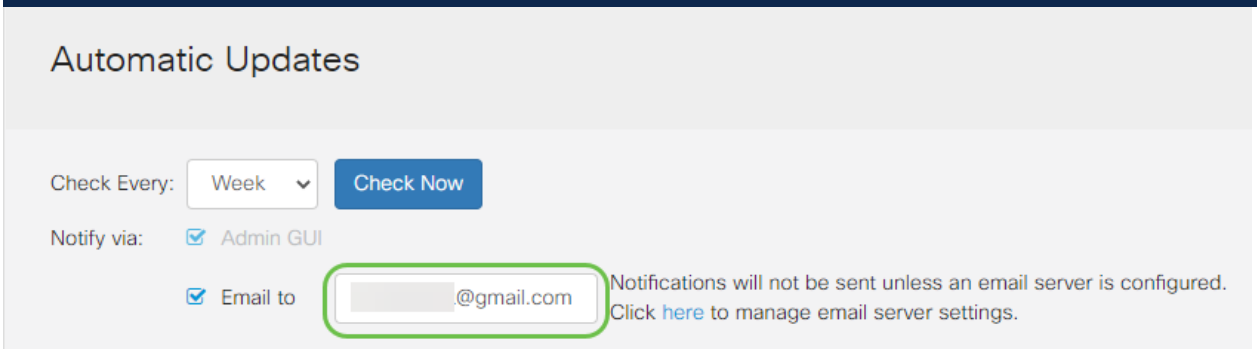
이메일 서버 설정을 설정하려면 여기를 클릭하여 방법을 알아보십시오.



4단계

Email to address 필드에 이메일 주소를 입력합니다.

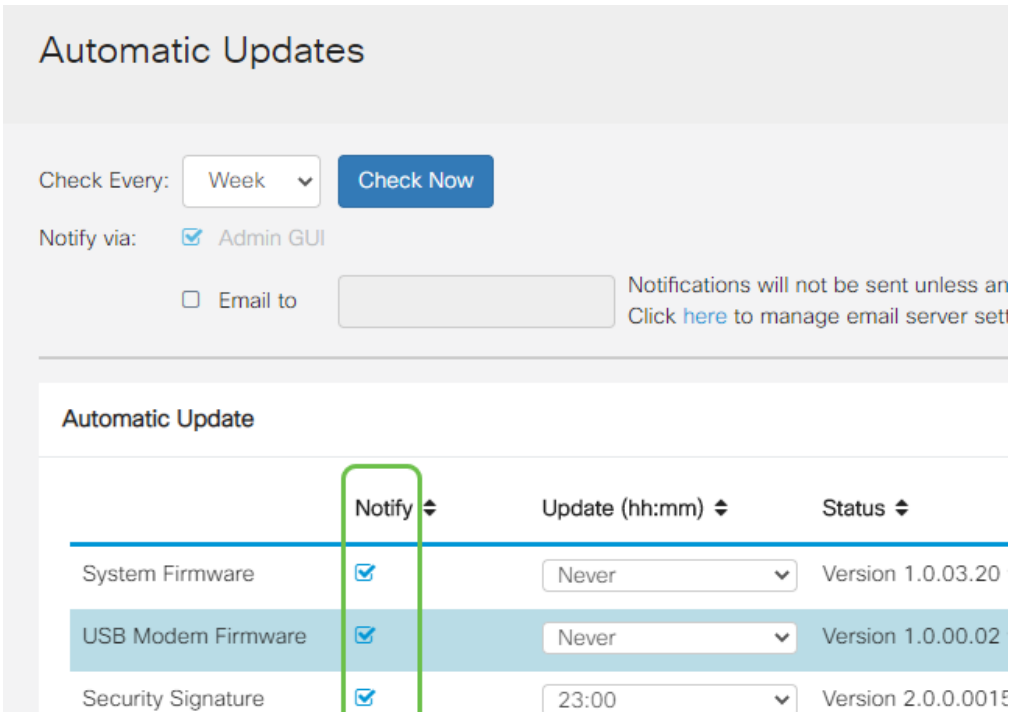
개인 전자 메일을 사용하여 개인 정보를 유지하는 대신 별도의 전자 메일 계정을 사용하는 것이 좋습니다.



5단계

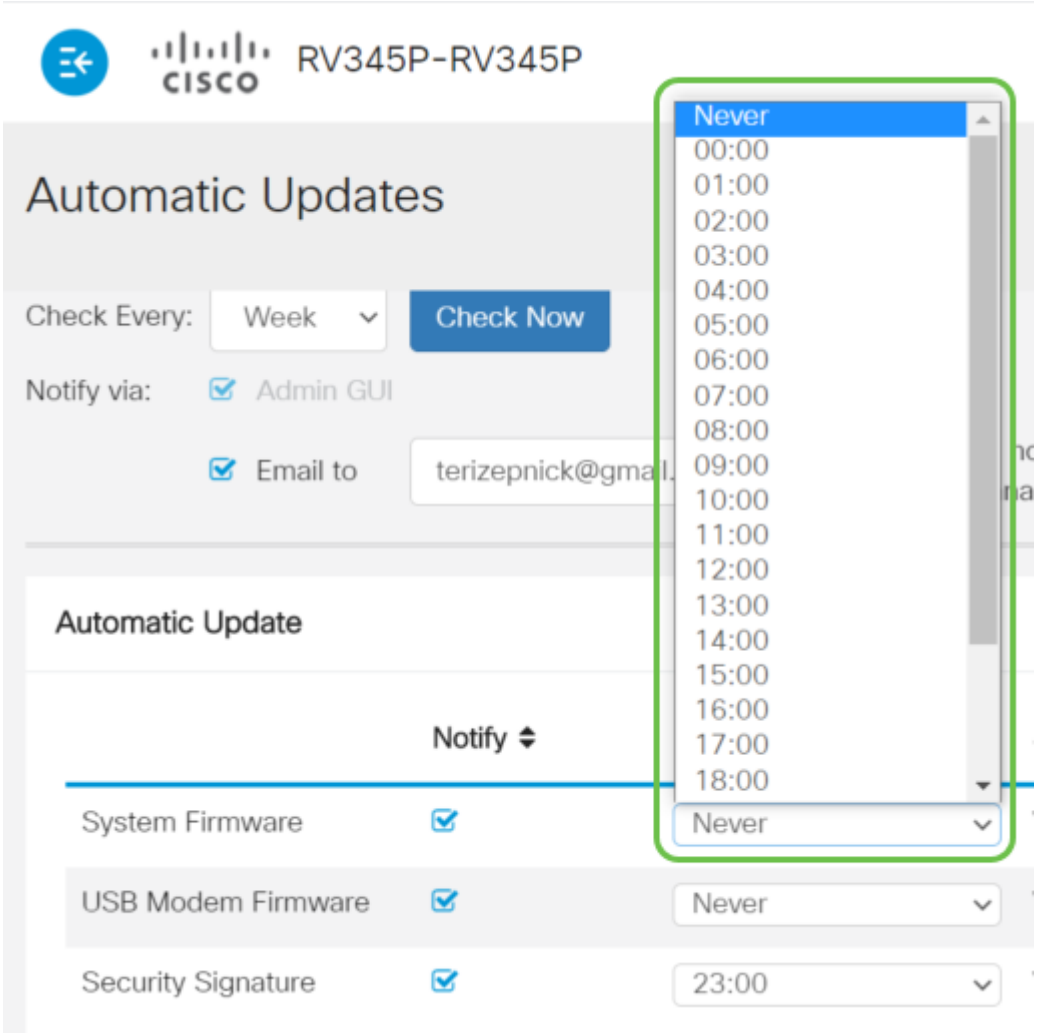
Automatically *Update(자동 업데이트)* 영역에서 **Notify(알림)** 확인란을 선택하여 알림을 받을 업데이트 종류를 확인합니다.옵션은 다음과 같습니다.

- 시스템 펌웨어 — 디바이스의 기본 제어 프로그램입니다.
- USB 모뎀 펌웨어 — USB 포트의 제어 프로그램 또는 드라이버입니다.
- 보안 서명 — 애플리케이션, 디바이스 유형, 운영 체제 등을 식별하기 위한 애플리케이션 제어에 대한 시그니처가 포함됩니다.



6단계

자동 업데이트 드롭다운 목록에서 자동 업데이트를 수행할 시간을 선택합니다.일부 옵션은 선택한 업데이트 유형에 따라 달라질 수 있습니다.보안 시그니처만이 즉시 업데이트를 받을 수 있는 유일한 옵션입니다.불편한 시간에 서비스가 중단되지 않도록 사무실 종료 시간을 설정하는 것이 좋습니다.



상태는 현재 실행 중인 펌웨어 또는 보안 서명 버전을 표시합니다.

7단계

Apply를 **클릭합니다**.

8단계

컨피그레이션을 영구적으로 저장하려면 Copy/Save Configuration(컨피그레이션 복사/저장) 페이지로 이동하거나 페이지 상단에서 **저장 아이콘**을 클릭합니다.

좋습니다. 라우터의 기본 설정이 완료되었습니다!이제 몇 가지 컨피그레이션 옵션을 살

펴볼 수 있습니다.

보안 옵션

물론 네트워크가 안전하길 원합니다.복잡한 비밀번호를 사용하는 것과 같은 몇 가지 간단한 옵션이 있지만, 더 안전한 네트워크를 위한 단계를 수행하려면 보안에 대한 이 섹션을 확인하십시오.

RV 보안 라이센스(선택 사항)

이 RV Security License 기능은 인터넷을 통한 공격으로부터 네트워크를 보호합니다.

- IPS(Intrusion Prevention System):네트워크 패킷, 로그 및/또는 광범위한 네트워크 공격을 검사합니다.네트워크 가용성 향상, 신속한 치료, 포괄적인 위협 차단 기능을 제공합니다.
- 안티바이러스:애플리케이션을 검사하여 라우터를 통과하는 HTTP, FTP, SMTP 이메일 첨부 파일, POP3 이메일 첨부 파일, IMAP 이메일 첨부 파일 등의 다양한 프로토콜을 검사하여 바이러스를 차단합니다.
- 웹 보안:인터넷에 연결하면서 비즈니스 효율성과 보안을 실현하며, 최종 장치와 인터넷 애플리케이션에 대한 인터넷 액세스 정책을 통해 성능과 보안을 보장합니다.클라우드 기반이며, 분류된 4억 5천만 개 이상의 도메인을 포함하는 80개 이상의 카테고리를 포함합니다.
- 애플리케이션 식별:인터넷 애플리케이션에 정책을 식별하고 할당합니다.500개의 고유한 애플리케이션이 자동으로 식별됩니다.
- 클라이언트 식별:클라이언트를 동적으로 식별하고 분류합니다.최종 디바이스 카테고리 및 운영 체제에 따라 정책을 할당하는 기능.

RV 보안 라이센스는 웹 필터링을 제공합니다.웹 필터링은 부적절한 웹 사이트에 대한 액세스를 관리할 수 있는 기능입니다.클라이언트의 웹 액세스 요청을 확인하여 해당 웹 사이트를 허용할지 거부할지를 결정할 수 있습니다.

라이센스 보안 기능은 90일 동안 무료로 시험해 볼 수 있습니다.평가 기간 후에 라우터에서 고급 보안 기능을 계속 사용하려면 라이센스를 취득하여 활성화해야 합니다.

또 다른 보안 옵션은 Cisco Umbrella입니다.대신 Umbrella 섹션으로 이동하려면 여기를 클릭하십시오.

보안 라이센스를 원하지 않는 경우 이 문서의 VPN 섹션으로 이동하려면 클릭하십시오.

Smart Account 소개

RV 보안 라이센스를 구매하려면 Smart Account가 필요합니다.

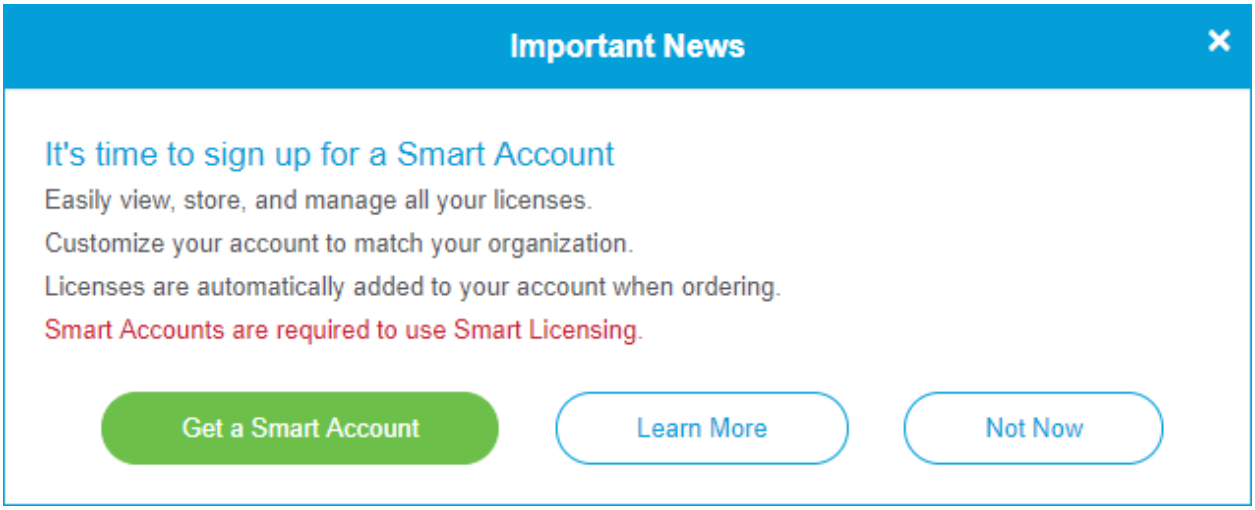
이 Smart Account의 활성화를 승인하면, 귀사는 조직을 대신하여 계정을 생성하고 제품 및 서비스 자격, 라이센스 계약 및 계정에 대한 사용자 액세스를 관리할 수 있는 권한이

부여된다는 데 동의합니다.Cisco 파트너는 고객을 대신하여 계정 생성을 승인할 수 없습니다.

새로운 Smart Account를 생성하는 것은 일회성 이벤트로, 그 시점부터 관리 기능은 툴을 통해 제공됩니다.

Smart Account 생성

Cisco.com 어카운트 또는 CCO ID(이 문서의 시작 부분에 생성한 ID)를 사용하여 일반 Cisco 어카운트에 액세스하면 Smart Account를 생성하는 메시지를 받을 수 있습니다.



이 팝업을 보지 못한 경우 클릭하여 Smart Account 생성 페이지로 이동할 수 있습니다.Cisco.com 계정 자격 증명으로 로그인해야 할 수 있습니다.

Smart Account 요청과 관련된 단계에 대한 자세한 내용을 보려면 여기를 클릭하십시오.

계정 이름과 기타 등록 세부 정보를 기록해 두십시오.

빠른 팁: 도메인을 입력해야 하는데 도메인이 없으면 name@domain.com 형식으로 이메일 주소를 입력할 수 *있습니다*.공통 도메인은 회사 또는 제공자에 따라 gmail, yahoo 등이 됩니다.

RV 보안 라이센스를 구매하기 전에 Cisco.com(CCO ID) 어카운트와 Cisco Smart Account가 있어야 합니다.

RV 보안 라이센스 구입

Cisco 총판사 또는 Cisco 파트너로부터 라이센스를 구매해야 합니다.Cisco 파트너를 찾으려면 여기를 클릭하십시오.

아래 표에는 라이센스의 부품 번호가 나와 있습니다.

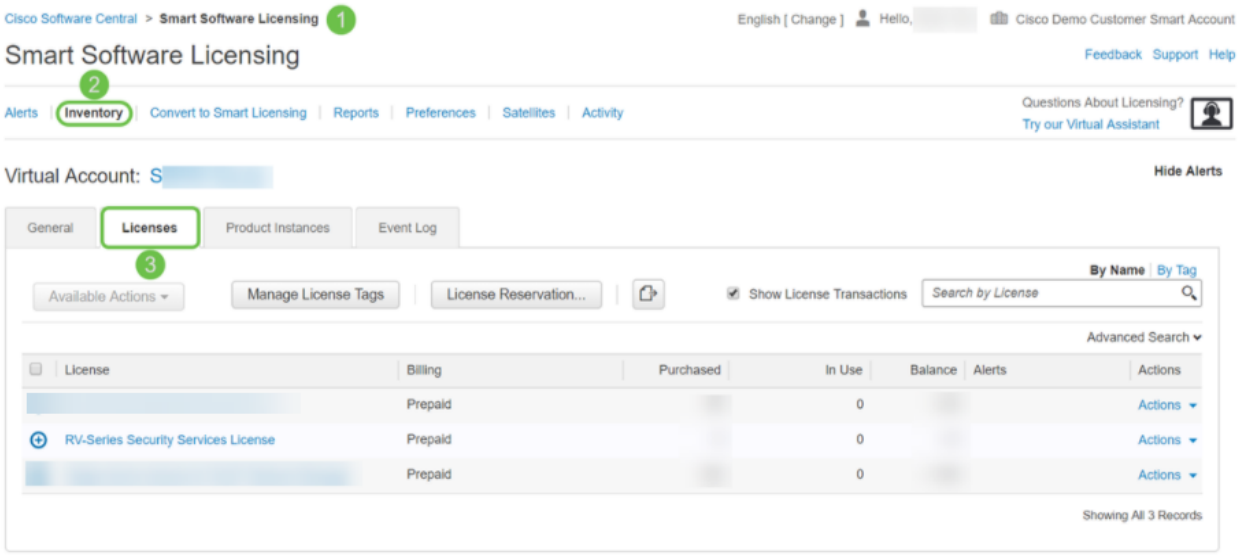
유형	제품 ID	설명
RV 보안 라이센스	LS-RV34X-SEC-1년=	RV 보안:1년:동적 웹 필터, 애플리케이션 가시성, 클라이언트 식별 및 통계, 게이트

웨이 안티바이러스 및 침입 방지 시스템
IPS.

라이센스 키는 라우터에 직접 입력되지는 않지만 라이센스를 주문하면 Cisco Smart Account에 할당됩니다.라이선스가 계정에 표시되는 데 걸리는 시간은 파트너가 주문을 수락하는 시기와 리셀러가 라이센스를 계정에 연결하는 시기(일반적으로 24-48시간)에 따라 달라집니다.

라이센스가 Smart Account에 있는지 확인

Smart License 어카운트 페이지로 이동한 다음 Smart **Software License 페이지 > Inventory > Licenses**를 클릭합니다.

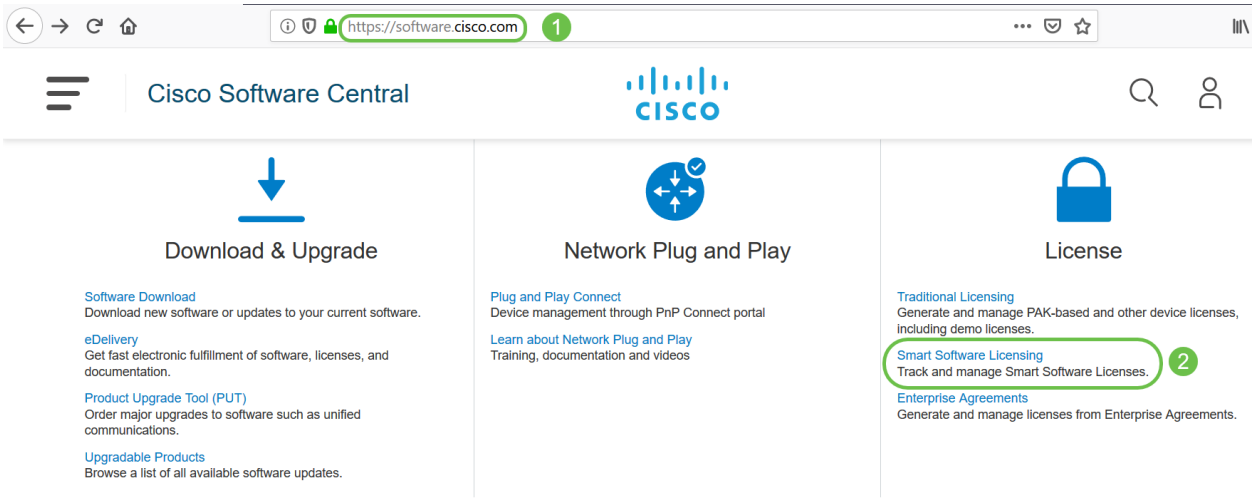


Smart Account에 라이센스가 표시되지 않으면 Cisco 파트너에게 문의하십시오.

RV345P Series 라우터에서 RV 보안 라이센스 구성

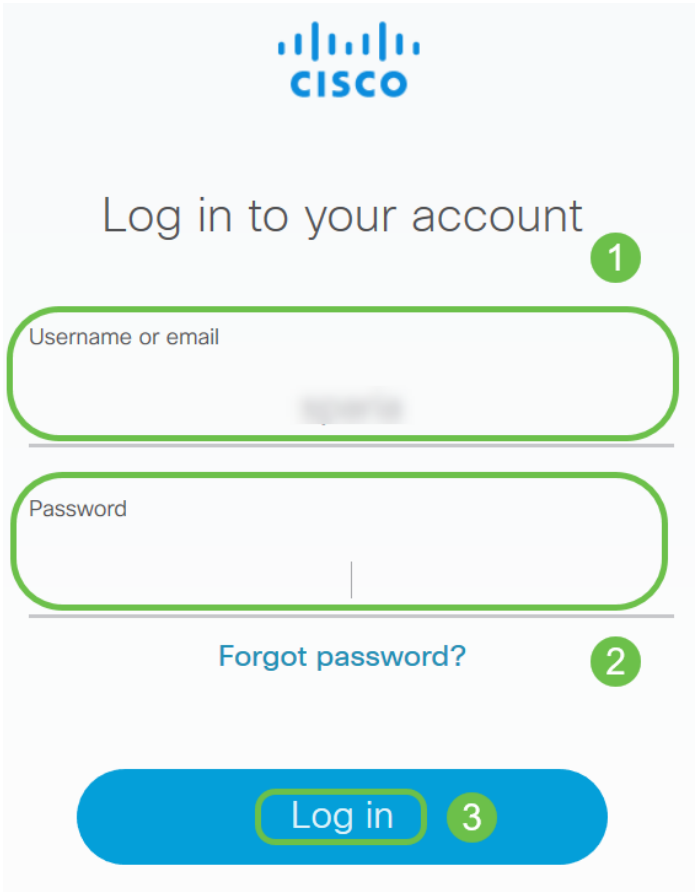
1단계

Cisco Software에 액세스하고 **Smart Software Licensing으로 이동합니다**.



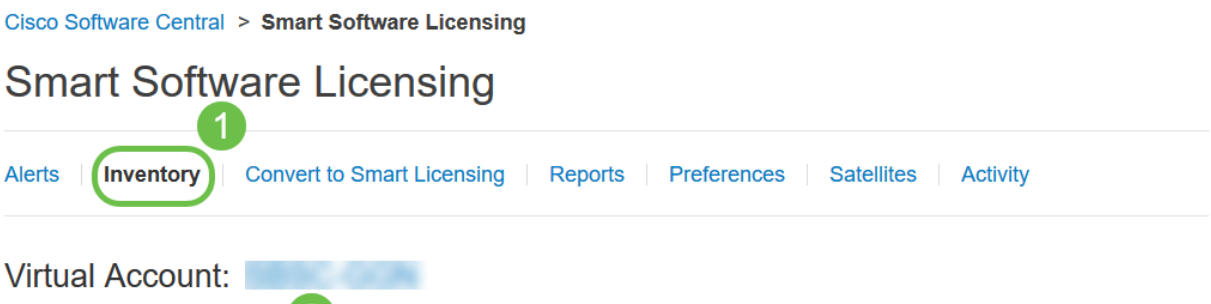
2단계

사용자 *이름 또는 이메일* 및 *비밀번호*를 입력하여 Smart Account에 로그인합니다.Log in(**로그인)을 클릭합니다**.



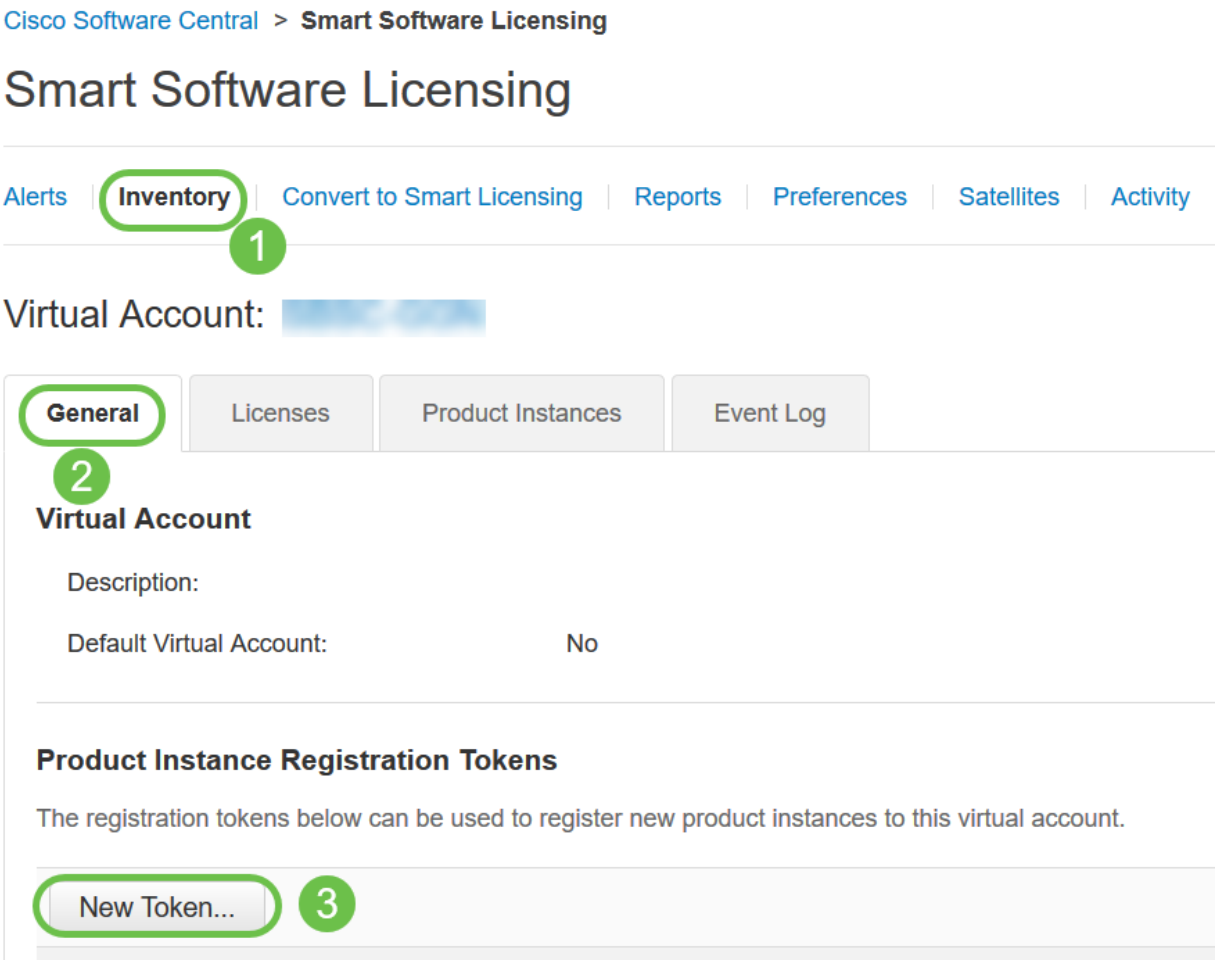
3단계

Inventory(**인벤토리) > Licenses(라이센스)**로 이동하고 *RV-Series Security Services License*가 Smart Account에 나열되는지 확인합니다.나열된 라이센스가 표시되지 않으면 Cisco 파트너에게 문의하십시오.



4단계

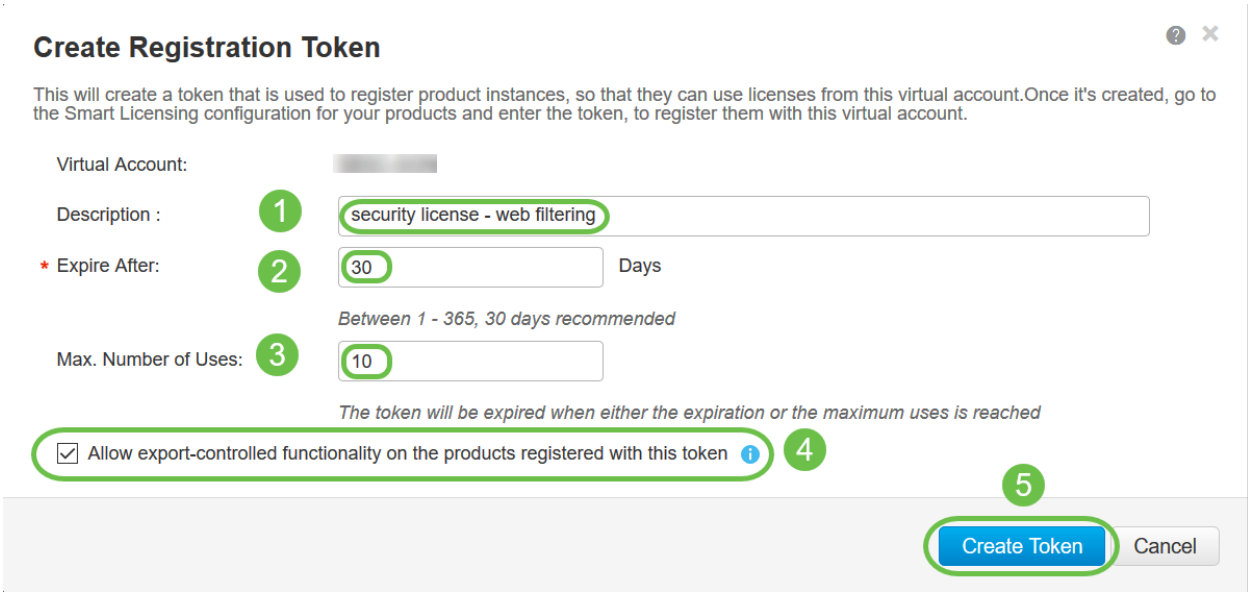
Inventory(**인벤토리**) > **General(일반)으로 이동합니다**.Product Instance *Registration Tokens(제품 인스턴스 등록 토큰)*에서 New Token(**새 토큰)을 클릭합니다**.



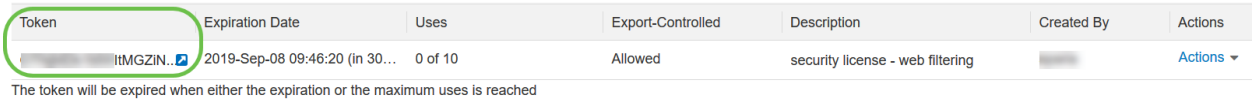
5단계

등록 토큰 생성 창이 나타납니다.Virtual *Account(가상* 어카운트) 영역에는 등록 토큰을 생성할 가상 어카운트가 표시됩니다.*Create Registration Token(등록 토큰 생성*) 페이지에서 다음을 완료합니다.

- Description 필드에 토큰에 대한 고유한 설명을 입력합니다.이 예에서는 보안 라이센스 - 웹 필터링이 입력됩니다.
- Expire After(만료 후) 필드에 1~365일 사이의 값을 입력합니다.Cisco에서는 이 필드에 대해 30일 값을 권장합니다.그러나 필요에 맞게 값을 수정할 수 있습니다.
- 최대Number of Uses 필드에 값을 입력하여 해당 토큰을 사용할 횟수를 정의합니다.토큰은 일 또는 최대 사용 수에 도달하면 만료됩니다.
- Allow export-controlled functionality on the products registered with this token(이 토큰에 등록된 제품의 내보내기 제어 기능 허용) 확인란을 선택하여 가상 어카운트의 제품 인스턴스 토큰에 대한 내보내기 제어 기능을 활성화합니다.내보내기 제어 기능을 이 토큰과 함께 사용할 수 있도록 허용하지 않으려면 확인란의 선택을 취소합니다.내보내기 제어 기능을 준수하는 경우에만 이 옵션을 사용합니다.일부 수출 통제 기능은 미국 상무부에 의해 제한됩니다.이 기능은 확인란의 선택을 취소하면 이 토큰을 사용하여 등록된 제품에 대해 제한됩니다.위반은 모두 벌금과 행정의 영향을 받는다.
- 토큰 **생성**을 클릭하여 토큰을 생성합니다.

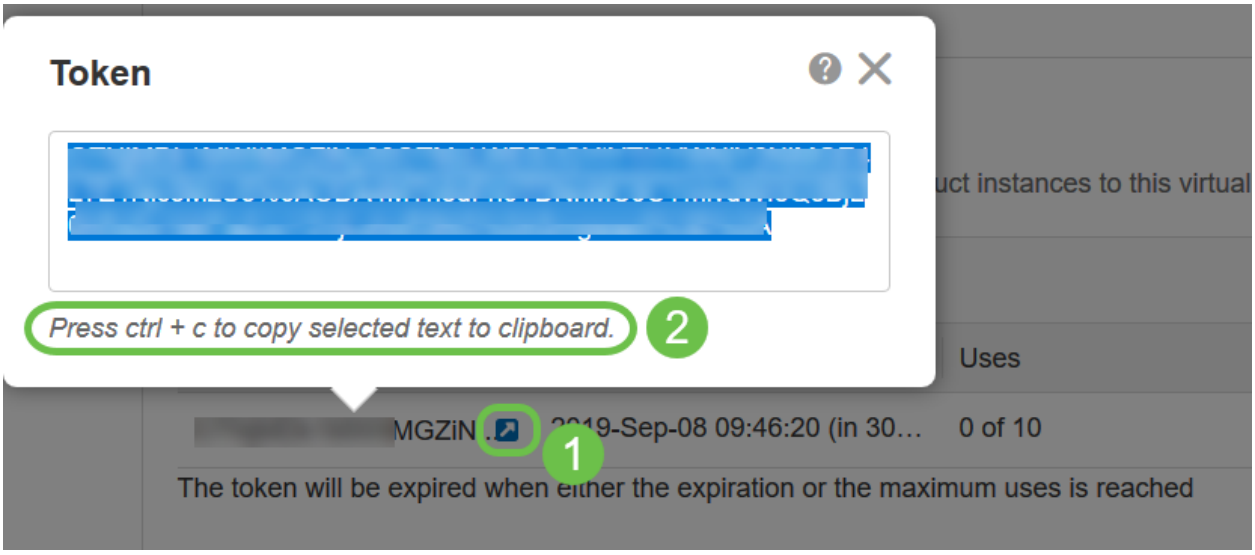


제품 인스턴스 등록 토큰을 생성했습니다.



6단계

토큰 열의 **화살표 아이콘**을 *클릭하여* 토큰을 클립보드로 복사하려면 키보드에서 **<ctrl+c>를** 누릅니다.

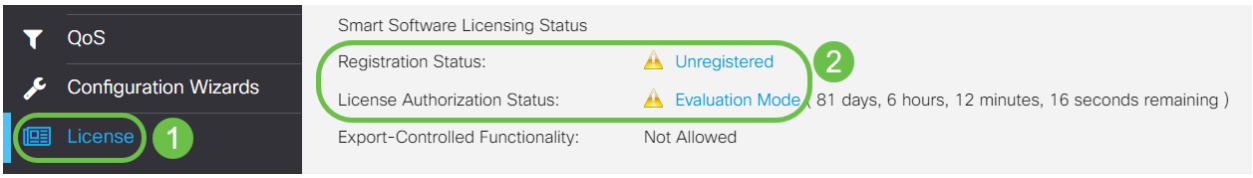


7단계(선택 사항)

Actions(작업) 드롭다운 메뉴를 클릭하고 **Copy(복사)**를 선택하여 토큰을 클립보드로 복사하거나 **Download...**를 선택하여 복사할 수 있는 토큰의 텍스트 파일 복사본을 다운로드합니다.

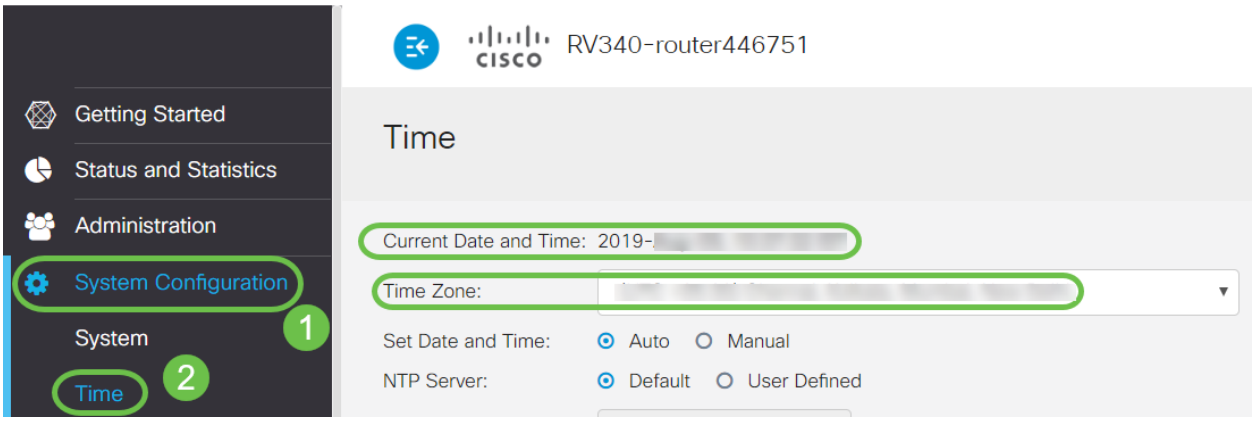
8단계

License(**라이센스**)로 이동하고 *Registration Status(등록 상태)*가 Unregistered(등록되지 않음)로 표시되고 *License Authorization Status(라이센스 권한 부여 상태)가 Evaluation Mode(평가 모드)*로 표시되는지 *확인합니다.*



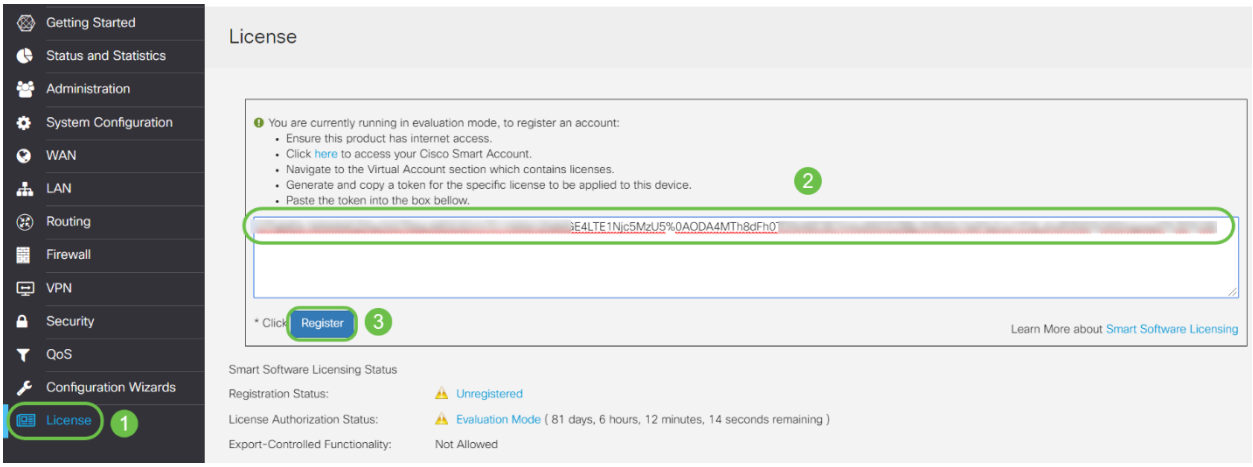
9단계

System Configuration(**시스템 컨피그레이션) > Time(시간)**으로 이동하고 *Current Date and Time* and *Time Zone(현재 날짜 및 시간* 및 *표준 시간대)*이 표준 시간대별로 올바르게 반영되었는지 확인합니다.



10단계

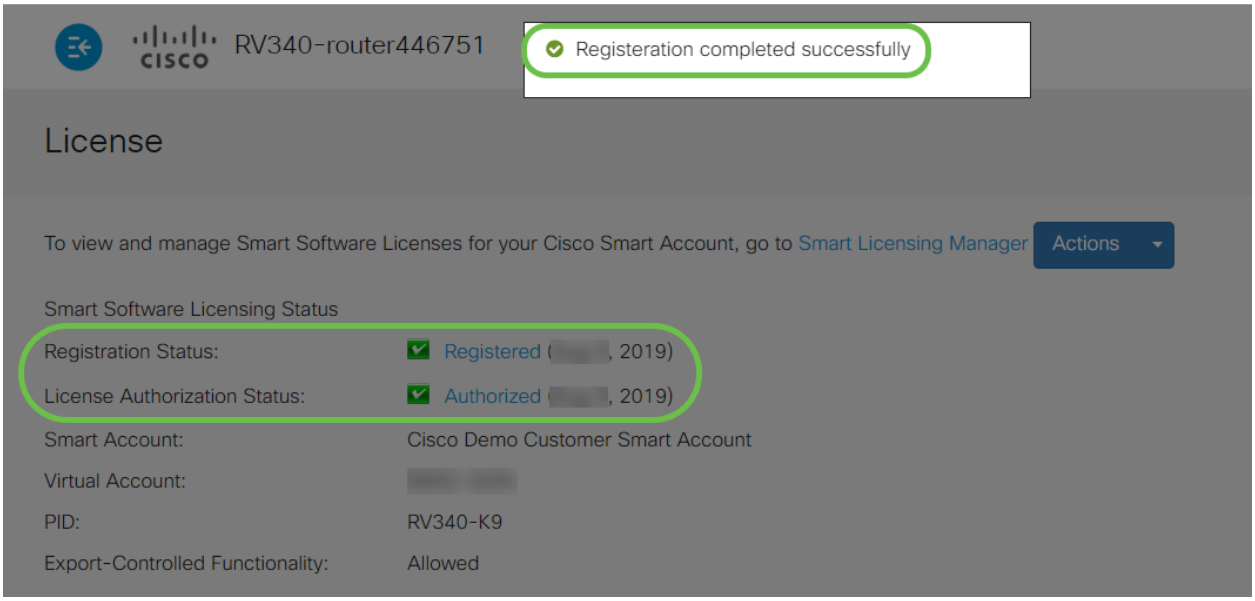
License로 **이동합니다**.복사한 토큰을 6단계에서 *License* 탭 아래의 텍스트 상자에 붙여 넣습니다. 키보드**에서 ctrl + v를** 선택합니다.Register(**등록)를 클릭합니다**.



등록에는 몇 분 정도 걸릴 수 있습니다.라우터가 라이센스 서버에 연결을 시도하므로 페이지를 벗어나지 마십시오.

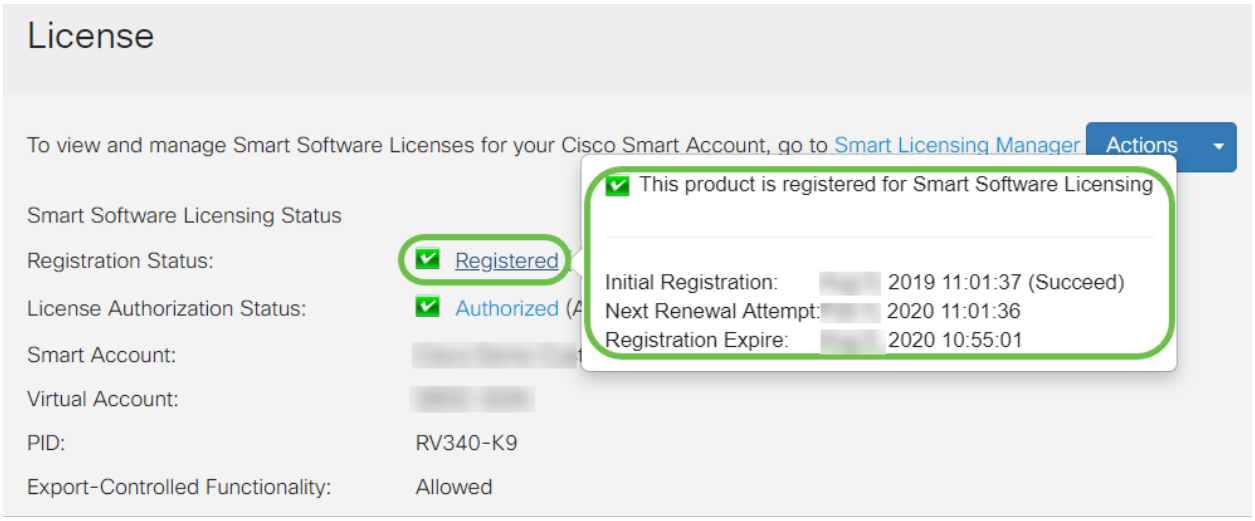
11단계

이제 Smart License를 사용하여 RV345P Series 라우터를 성공적으로 등록하고 인증해야 합니다.화면 *등록*이 *성공적으로 완료되었다는* 알림*이 표시됩니다*.또한 Registration Status(*등록 상태*)가 Registered(등록됨)로 표시되고 License Authorization Status(라이센스 *권한 부여 상태)가 Authorized(권한*)로 *표시됩니다*.



12단계(선택 사항)

라이센스의 *Registration Status(등록 상태)*에 대한 자세한 내용을 보려면 마우스 포인터를 *Registered* 상태 위로 이동합니다.다음 정보가 포함된 대화 상자 메시지가 나타납니다.

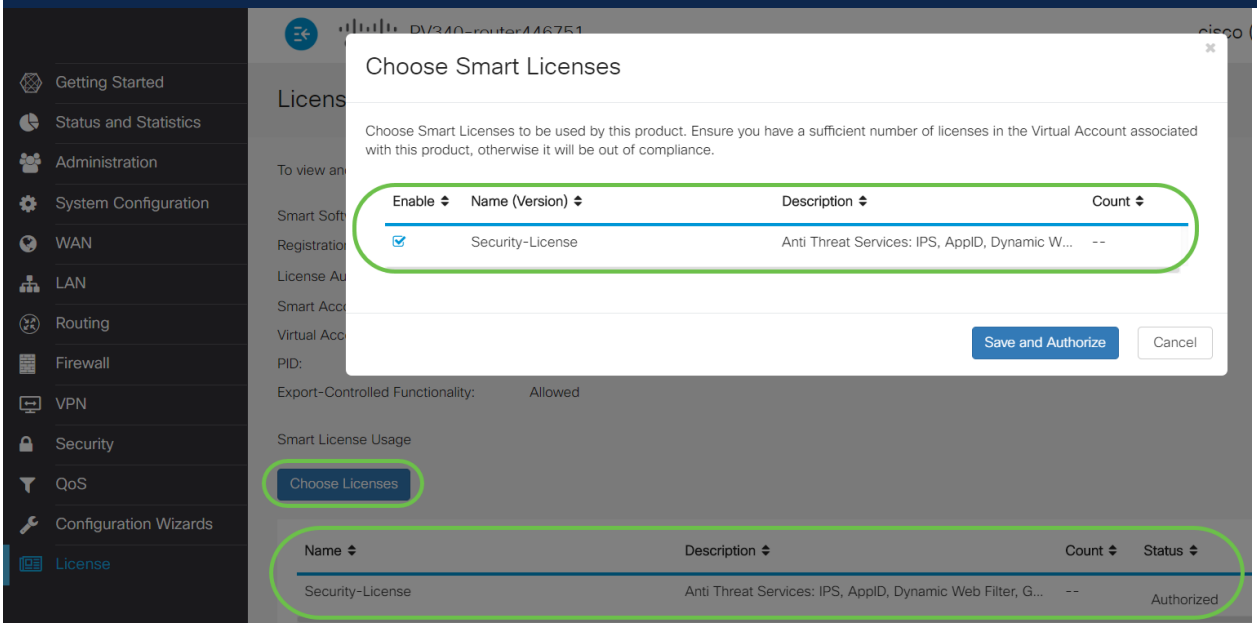


- 초기 등록 — 이 영역은 라이센스가 등록된 날짜와 시간을 나타냅니다.
- Next Renewal Attempt — 이 영역은 라우터가 라이센스를 갱신하려고 시도하는 날짜와 시간을 나타냅니다.
- 등록 만료 — 이 영역은 등록이 만료되는 날짜와 시간을 나타냅니다.

13단계

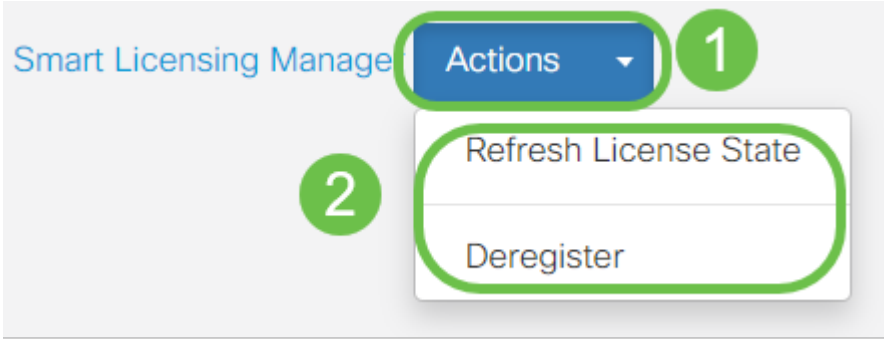
License 페이지에서 *Security-License 상태가 Authorized(승인됨)*로 표시되는지 *확인합니다*.Choose License(라이센스 **선택)** 버튼을 클릭하여 *Security-License(보안 라이센스)가 활성화되었는지* 확인할 수도 있습니다.

이 단계에서 문제가 발생하면 라우터를 재부팅해야 할 수 있습니다.



14단계(선택 사항)

License *State(라이센스 상태)*를 새로 고치거나 라우터에서 라이센스를 등록 취소하려면 *Smart Licensing Manager***Actions**(작업) 드롭다운 메뉴를 클릭하고 작업 항목을 선택합니다.



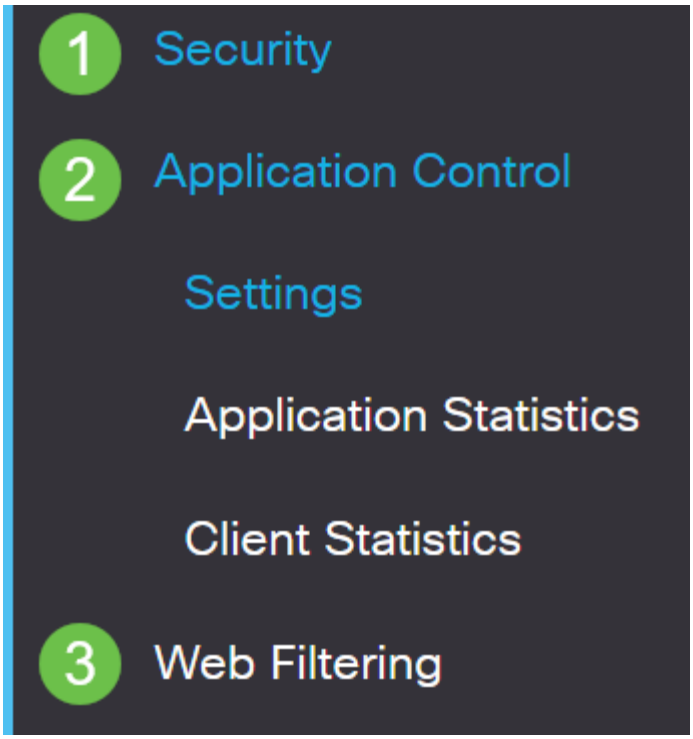
라우터에 라이센스가 있으므로 다음 섹션의 단계를 완료해야 합니다.

RV345P 라우터의 웹 필터링

활성화 후 90일 이내에 무료로 웹 필터링을 사용할 수 있습니다.무료 평가 후 이 기능을 계속 사용하려면 라이센스를 구입해야 합니다.클릭하여 해당 섹션으로 돌아갑니다.

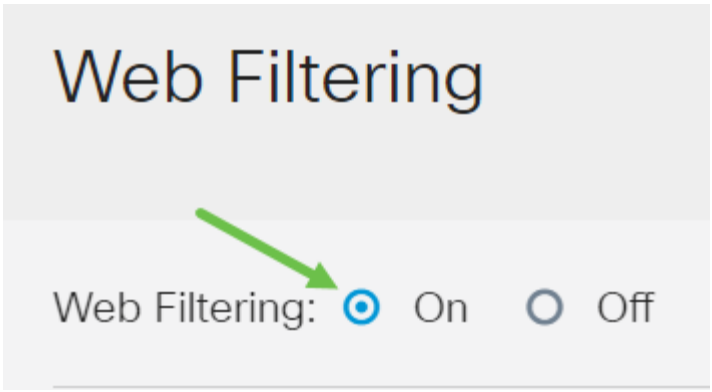
1단계

웹 기반 유틸리티에 로그인하고 **보안 > 애플리케이션 제어 > 웹 필터링을** 선택합니다.



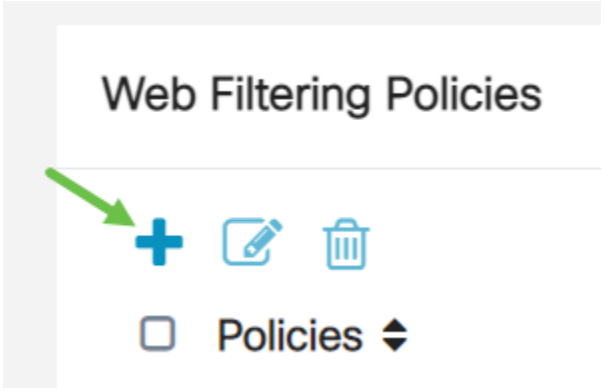
2단계

켜기 라디오 버튼**을** 선택합니다.



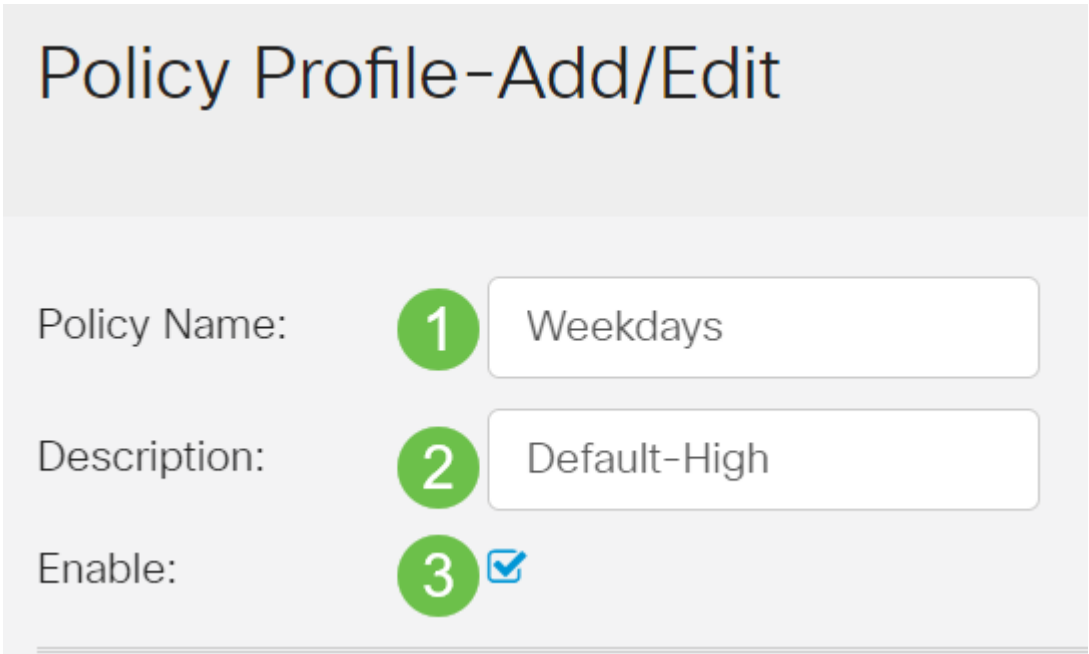
3단계

추가 아이콘을 클릭합니다.



4단계

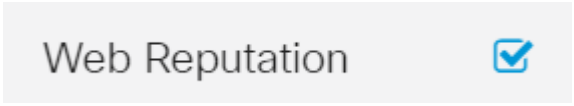
Policy Name(*정책 이름*), *Description(설명)* 및 Enable(*활성화*) 확인란을 입력합니다.



라우터에서 Content Filtering(콘텐츠 필터링)이 활성화된 경우 콘텐츠 필터링이 비활성화되었고 두 기능을 동시에 활성화할 수 없다는 알림이 표시됩니다.Apply(**적용**)를 클릭하여 컨피그레이션을 진행합니다.

5단계

웹 평판 인덱스를 기반으로 필터링을 활성화하려면 Web Reputation(웹 평판) 확인란을 선택합니다.

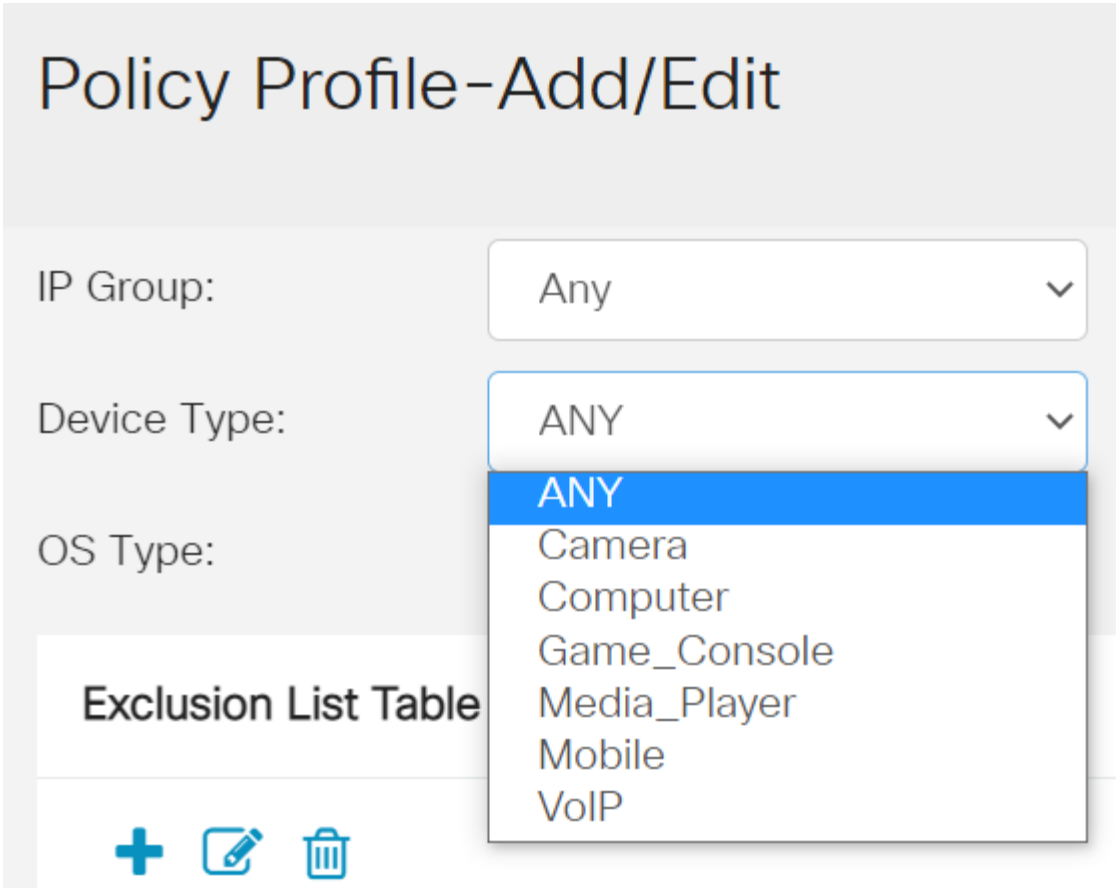


웹 평판 지수에 따라 웹 사이트 또는 URL의 악명성에 따라 콘텐츠가 필터링됩니다.점수가 40 미만인 경우 웹 사이트가 차단됩니다.웹 평판 기술에 대한 자세한 내용을 보려면 여기를 클릭하십시오.

6단계

Device *Type* 드롭다운 목록에서 필터링할 패킷의 소스/대상을 선택합니다.한 번에 하나의 옵션만 선택할 수 있습니다.옵션은 다음과 같습니다.

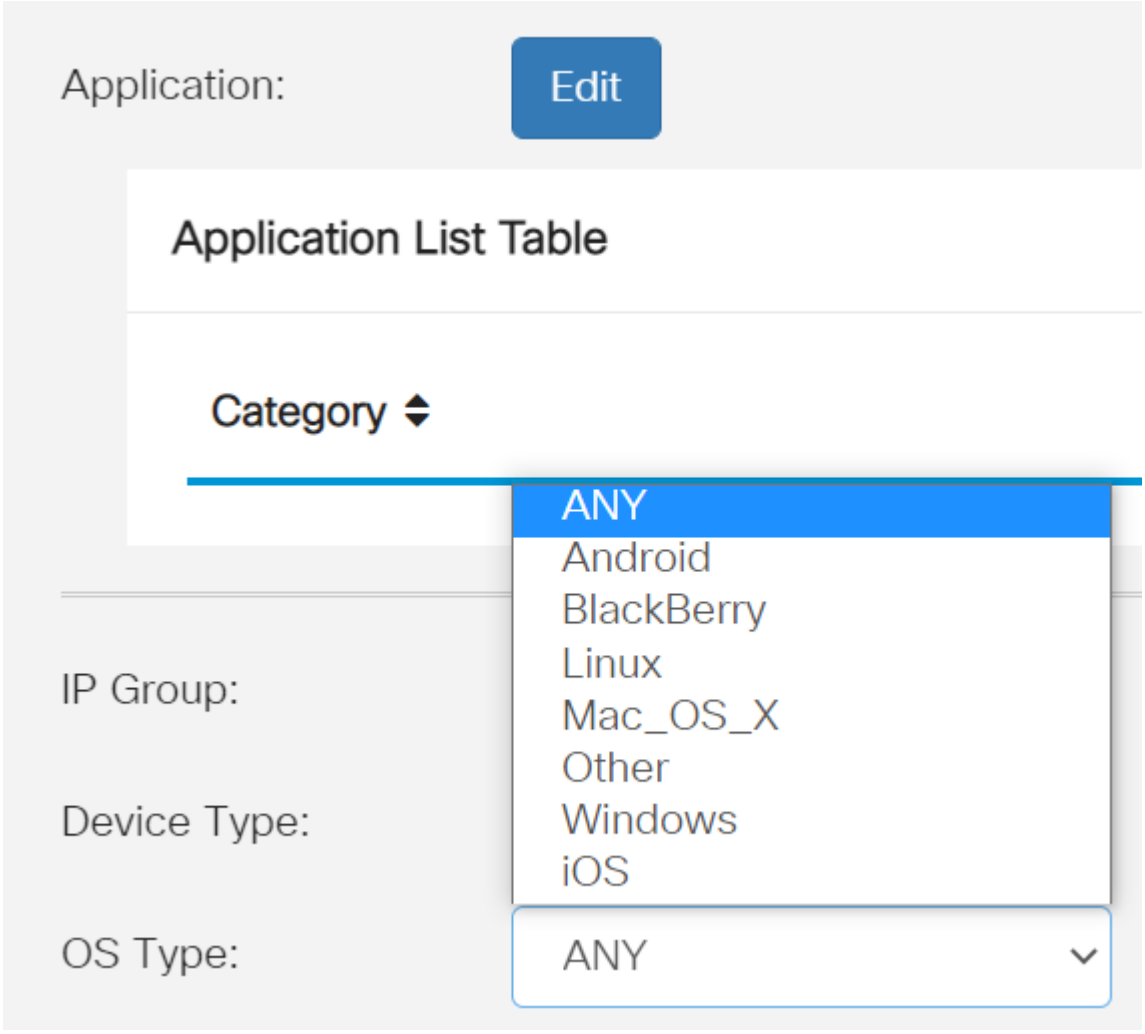
- ANY — 모든 디바이스에 정책을 적용하려면 이 옵션을 선택합니다.
- 카메라 — 카메라(예: IP 보안 카메라)에 정책을 적용하려면 이 옵션을 선택합니다.
- 컴퓨터 — 컴퓨터에 정책을 적용하려면 이 옵션을 선택합니다.
- Game_Console — 게임 콘솔에 정책을 적용하려면 이 옵션을 선택합니다.
- Media_Player — 미디어 플레이어에 정책을 적용하려면 이 옵션을 선택합니다.
- 모바일 — 모바일 디바이스에 정책을 적용하려면 이 옵션을 선택합니다.
- VoIP — Voice over Internet Protocol 디바이스에 정책을 적용하려면 이 옵션을 선택합니다.



7단계

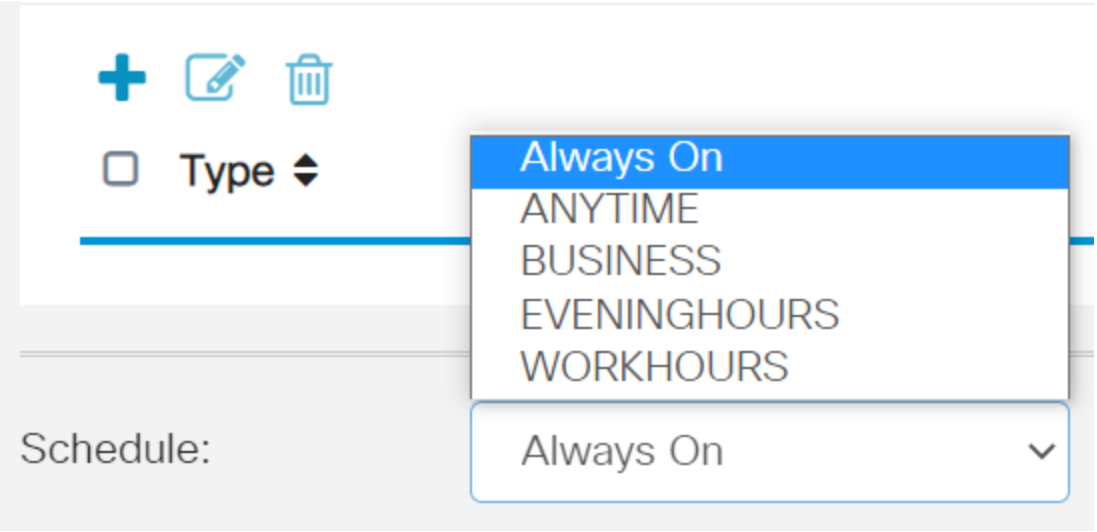
OS Type 드롭다운 목록에서 정책을 적용할 운영 체제(OS)를 선택합니다.한 번에 하나의 옵션만 선택할 수 있습니다.옵션은 다음과 같습니다.

- ANY — 모든 유형의 OS에 정책을 적용합니다.이것이 기본값입니다.
- Android — Android OS에만 정책을 적용합니다.
- BlackBerry — Blackberry OS에만 정책을 적용합니다.
- Linux — Linux OS에만 정책을 적용합니다.
- Mac_OS_X — Mac OS에만 정책을 적용합니다.
- 기타 — 나열되지 않은 OS에 정책을 적용합니다.
- Windows — Windows OS에 정책을 적용합니다.
- iOS — iOS OS에만 정책을 적용합니다.



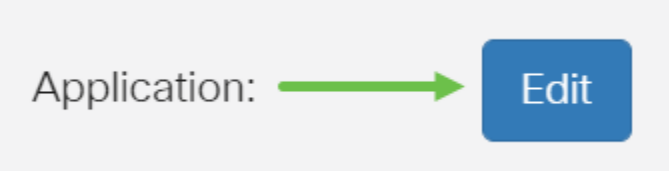
8단계

아래로 스크롤하여 *Schedule(예약)* 섹션으로 이동하고 필요에 가장 적합한 옵션을 선택합니다.



9단계

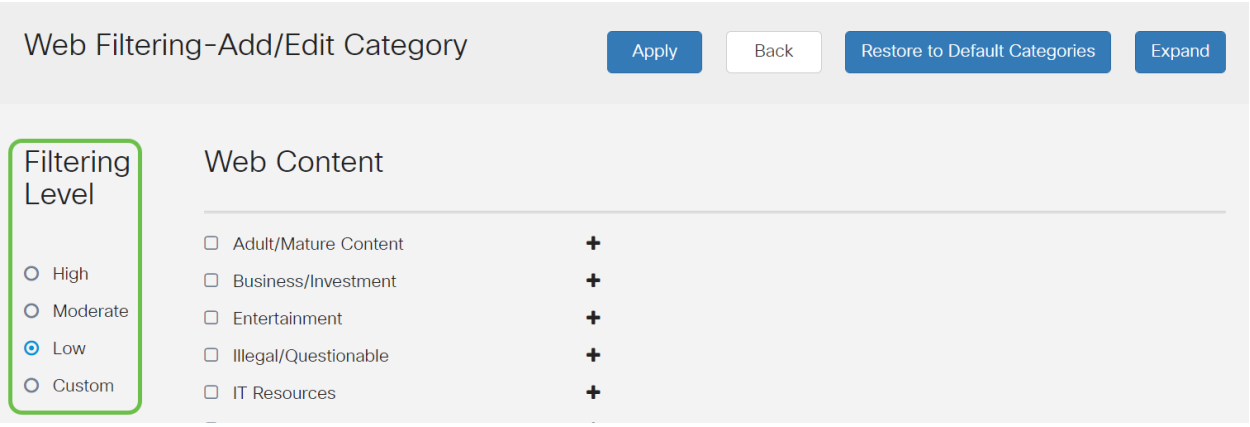
수정 아이콘을 클릭합니다.



10단계

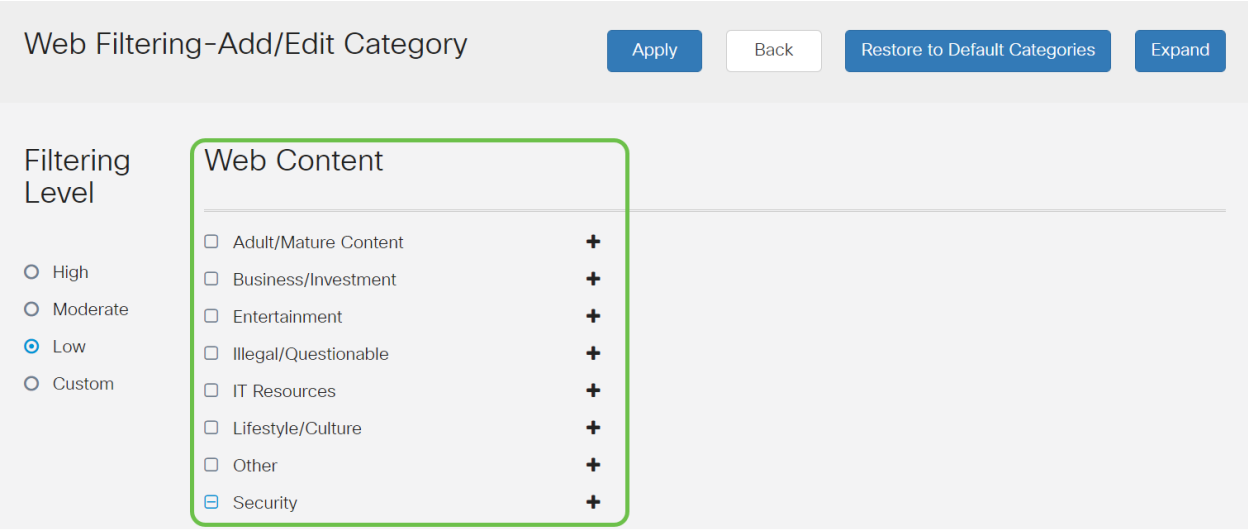
Filtering Level(필터링 레벨) 열에서 라디오 버튼을 클릭하여 네트워크 정책에 가장 적합한 필터링 범위를 빠르게 정의합니다.옵션은 High, Moderate, Low 및 Custom입니다.활성화된 각 웹 콘텐츠 카테고리로 필터링된 특정 사전 정의된 하위 카테고리를 확인하려면 아래의 필터링 레벨을 클릭하십시오.미리 정의된 필터는 더 이상 변경할 수 없으며 회색으로 표시됩니다.

- **낮음** — 기본 옵션입니다.이 옵션을 사용하여 보안이 활성화됩니다.
- **보통** — 성인/성인 콘텐츠, 불법/미심쩍은 내용 및 보안이 이 옵션으로 활성화됩니다.
- **높음** — 성인/성인 콘텐츠, 비즈니스/투자, 불법/미심쩍은, IT 리소스 및 보안은 이 옵션을 통해 활성화됩니다.
- **사용자** 정의 — 사용자 정의 필터를 허용하도록 설정된 기본값이 없습니다.



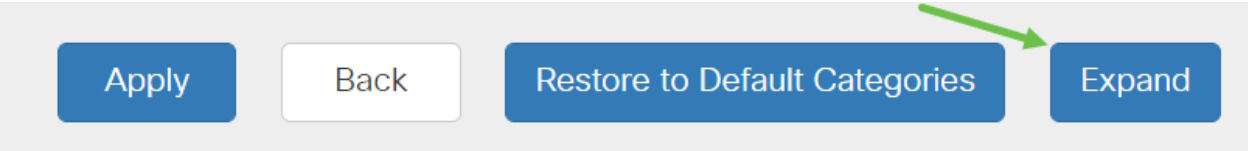
11단계

필터링할 웹 콘텐츠를 입력합니다.한 섹션에 대한 자세한 내용을 보려면 **더하기 아이콘**을 클릭합니다.



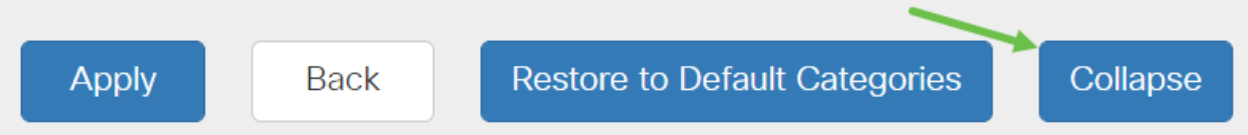
12단계(선택 사항)

모든 웹 콘텐츠 하위 범주 및 설명을 보려면 **확장** 단추를 클릭할 수 있습니다.



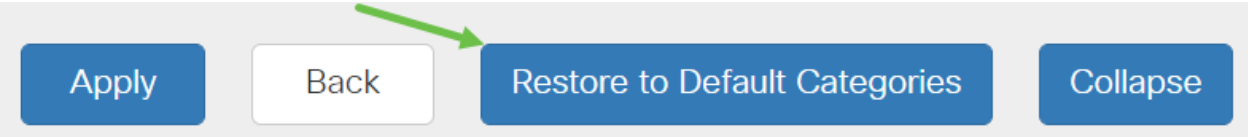
13단계(선택 사항)

축소를 클릭하여 하위 범주 및 설명을 축소합니다.



14단계(선택 사항)

기본 범주로 돌아가려면 Restore to **Default Categories**를 클릭합니다.



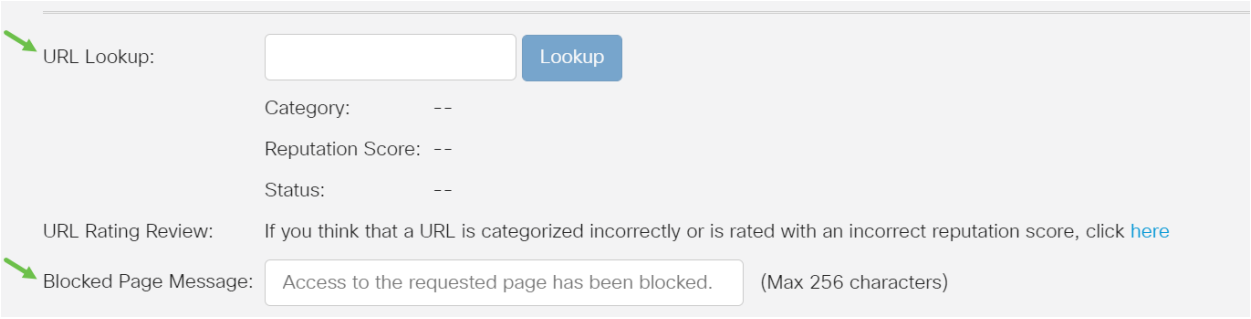
15단계

Apply(**적용**)를 클릭하여 컨피그레이션을 저장하고 Filter(필터) 페이지로 돌아가서 설정을 계속합니다.

Application List Table(애플리케이션 목록 테이블)에서 선택한 필터링 레벨을 기반으로 하는 해당 하위 범주가 테이블에 채워집니다.

16단계(선택 사항)

다른 옵션으로는 URL 조회 및 요청된 페이지가 차단된 시기를 표시하는 메시지가 있습니다.



17단계(선택 사항)

Apply를 **클릭합니다**.

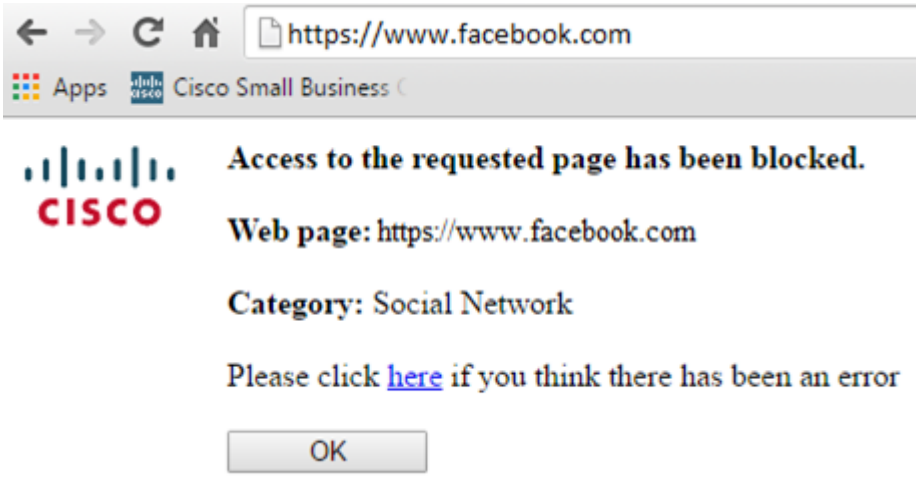
18단계

컨피그레이션을 영구적으로 저장하려면 *Copy/Save Configuration(컨피그레이션 복사/저장)* 페이지로 이동하거나 페이지 상단에서 **저장 아이콘**을 클릭합니다.

19단계(선택 사항)

웹 사이트 또는 URL이 필터링되거나 차단되었는지 확인하려면 웹 브라우저를 시작하거나 브라우저에서 새 탭을 엽니다.차단 목록에 있거나 차단 또는 거부되도록 필터링한 도메인 이름을 입력합니다.

이 예제에서는 www.facebook.com을 사용했습니다.



이제 RV345P 라우터에서 웹 필터링을 성공적으로 구성했어야 합니다.웹 필터링에 RV Security License를 사용하므로 Umbrella가 필요하지 않을 수 있습니다.Umbrella도 원한다면 여기를 클릭하십시오.보안이 충분한 경우 다음 섹션으로 건너뛰려면 클릭합니다.

문제 해결

라이센스를 구매했지만 가상 어카운트에 표시되지 않는 경우 두 가지 옵션이 있습니다.

1. 리셀러에게 연락하여 전송을 요청합니다.
2. Cisco에 연락하면 리셀러와 연락하겠습니다.

이상적으로는, 당신도 그렇게 할 필요는 없지만, 이 교차로에 도착하면 기꺼이 도와 드리겠습니다!이 프로세스를 최대한 효율적으로 진행하려면 아래 설명된 자격 증명과 함께 위의 표에 자격 증명이 필요합니다.

필요한 정보	정보 찾기
라이센스 송장	라이센스 구매를 완료한 후 이메일로 전송해야 합니다.
Cisco 판매 주문 번호	리셀러에게 다시 연락하여 구매해야 할 수도 있습니다.
Smart Account 라이센스 페이지의 스크린샷	스크린샷을 찍으면 Cisco 팀과 공유할 수 있는 화면 내용이 캡처됩니다.스크린샷에 익숙하지 않은 경우 아래 방법을 사용할 수 있습니다.

스크린샷

토큰이 있거나 문제 해결 중인 경우 스크린샷을 찍어 화면의 내용을 캡처하는 것이 좋습니다.

스크린샷을 캡처하는 데 필요한 절차의 차이점이 있는 경우 운영 체제에 해당하는 링크는 아래를 참조하십시오.

- 윈도우
- MAC
- iPhone/iPad
- Android

Umbrella RV Branch 라이센스(선택 사항)

Umbrella는 Cisco의 간단하면서도 매우 효과적인 클라우드 보안 플랫폼입니다.

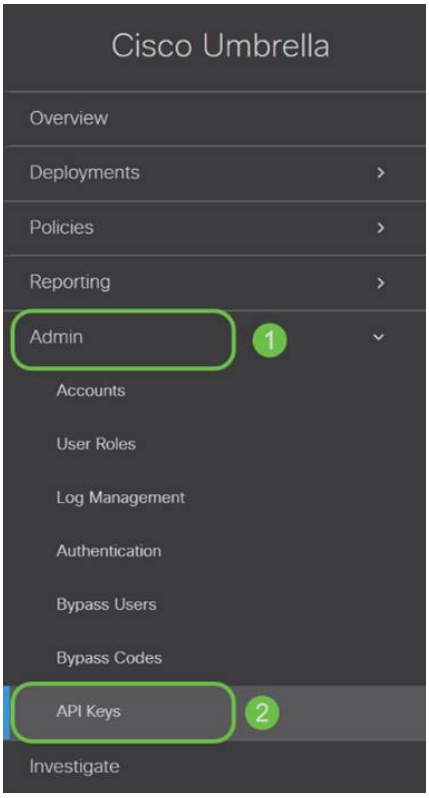
Umbrella는 클라우드에서 작동하며 많은 보안 관련 서비스를 수행합니다.긴급 위협에서 사후 조사에 이르기까지Umbrella는 모든 포트 및 프로토콜에서 공격을 검색하고 차단합니다.

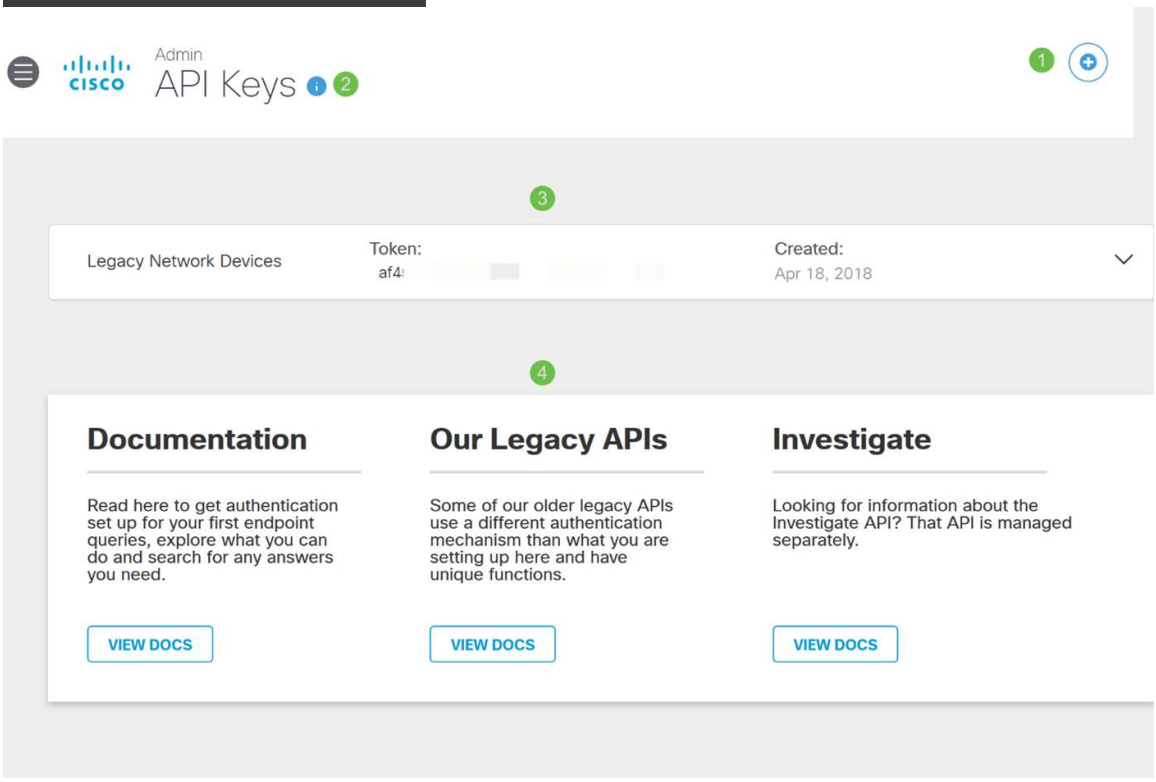
Umbrella는 DNS를 방어의 주 벡터로 사용합니다.사용자가 브라우저 표시줄에 URL을 입력하고 *Enter*를 누르면 Umbrella가 전송에 참여합니다.이 URL은 Umbrella의 DNS 확인자에 전달되며, 보안 경고가 도메인과 연결된 경우 요청이 차단됩니다.이 텔레메트리 데이터는 전송되고 마이크로초 단위로 분석되므로 레이턴시가 거의 발생하지 않습니다.텔레메트리 데이터는 전 세계 수십억 개의 DNS 요청을 추적하는 로그 및 기기를 사용합니다.이 데이터가 널리 보급될 때 전 세계적으로 데이터를 상호 연결하여 공격이 시작될 때 신속하게 대응할 수 있습니다.전체 정책, 요약 버전에 대한 자세한 내용은 Cisco의 개인 정보 보호 정책을 참조하십시오.텔레메트리 데이터를 툴과 로그에서 파생된 데이터로 간주합니다.

Cisco Umbrella를 방문하여 자세히 알아보고 계정을 만드십시오.문제가 발생한 경우 여기에서 설명서를 확인하고 여기에서 Umbrella Support 옵션을 확인하십시오.

1단계

Umbrella Account에 로그인한 후 *Dashboard* 화면에서 **Admin > API Keys를 클릭합니다**.



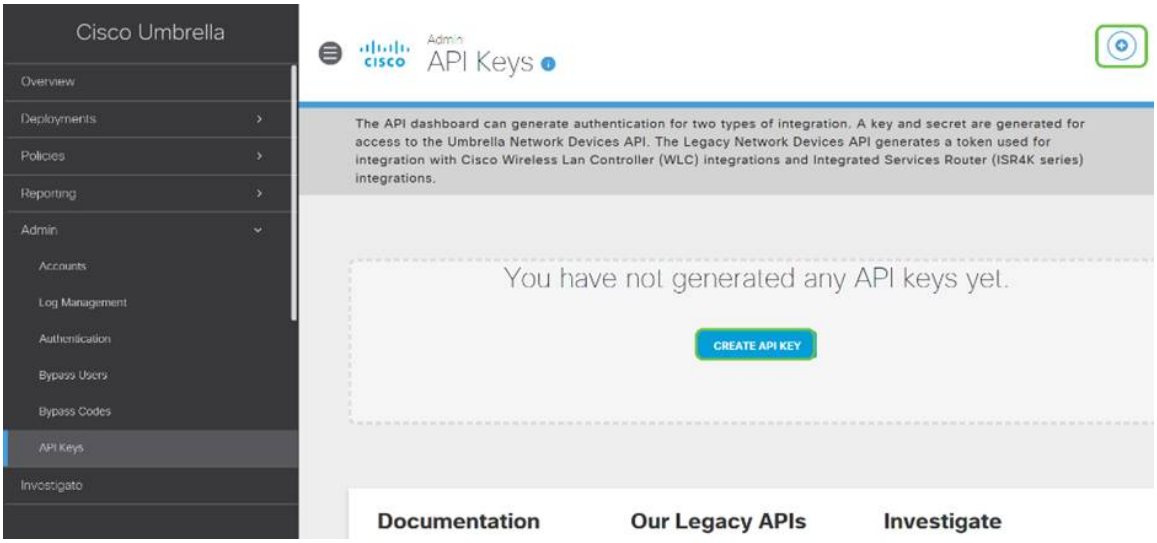


API 키 화면 분석(기존 API 키 포함)

1. API 키 추가 - Umbrella API와 함께 사용할 새 키 생성을 시작합니다.
2. Additional Info(추가 정보) - 이 화면의 설명자를 사용하여 아래로/위로 이동합니다.
3. Token Well(토큰 웰) - 이 계정에서 만든 모든 키와 토큰이 포함됩니다.(키가 생성되면 입력됨)
4. 지원 문서 - 각 섹션의 항목과 관련된 Umbrella 사이트의 설명서에 대한 링크입니다.

2단계

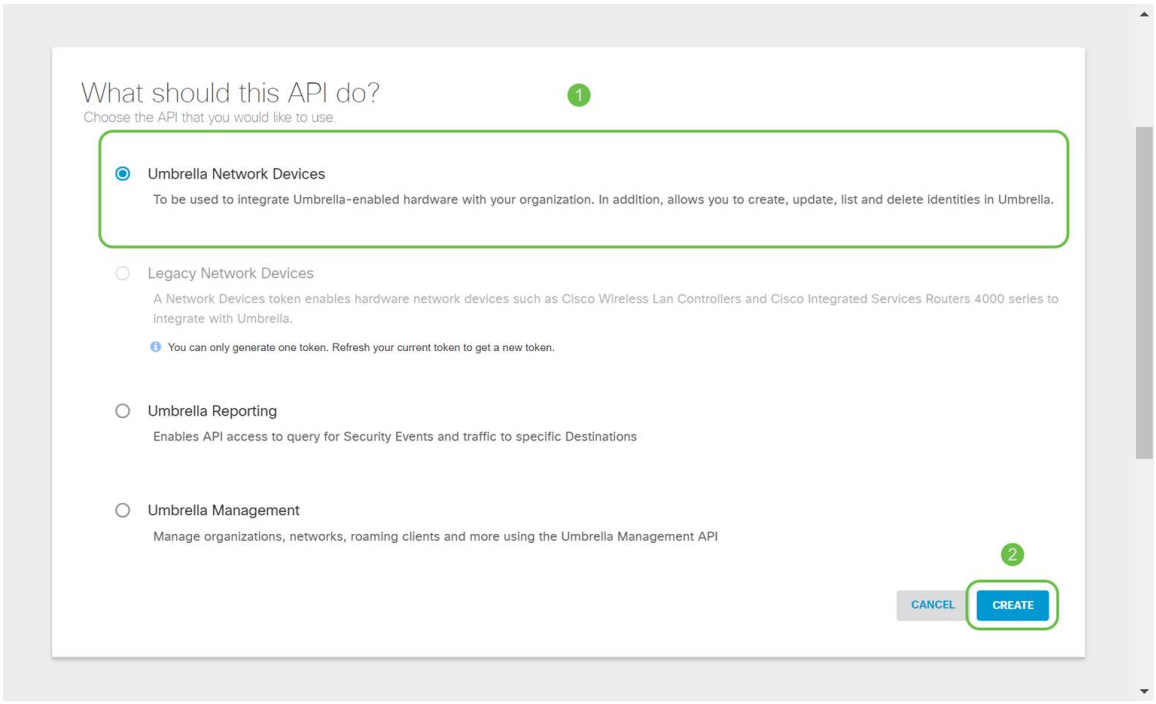
오른쪽 상단 모서리에서 **Add API Key(API 키 추가)** 버튼을 클릭하거나 Create API Key(**API 키 생성**) 버튼을 클릭합니다.둘 다 같은 기능을 합니다.



위 스크린샷은 이 메뉴를 처음으로 여는 것과 유사합니다.

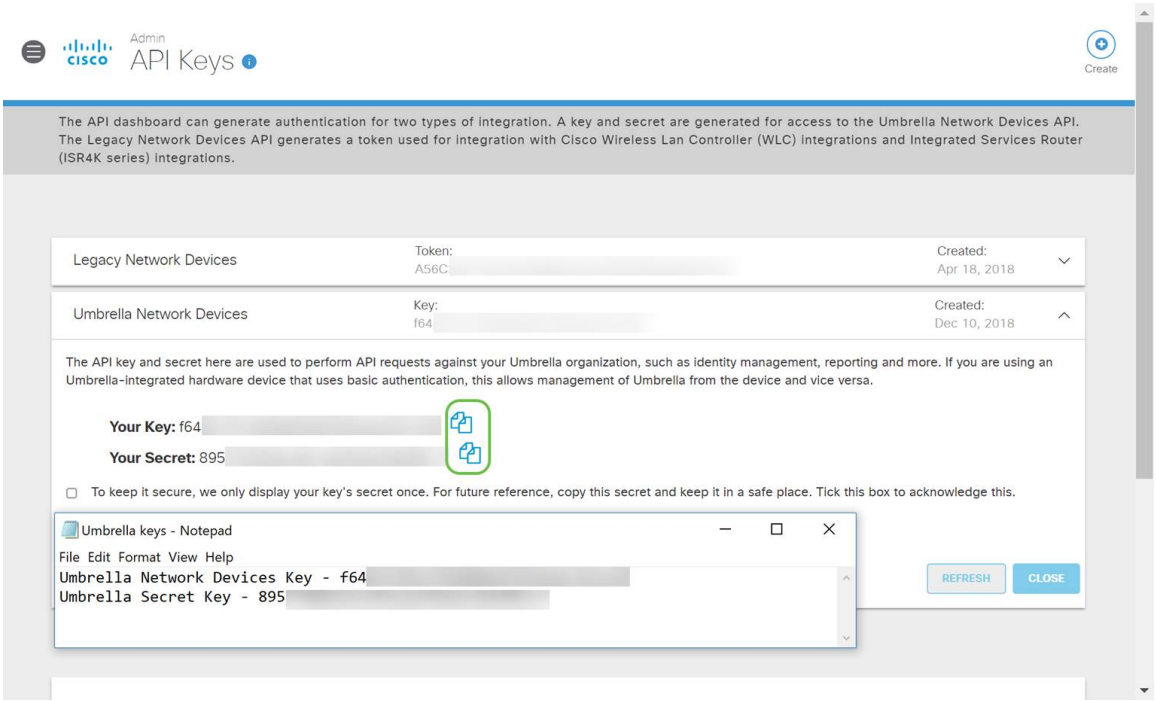
3단계

Umbrella **Network Devices(Umbrella 네트워크 디바이스)**를 선택한 다음 Create(생성) 버튼을 클릭합니다.



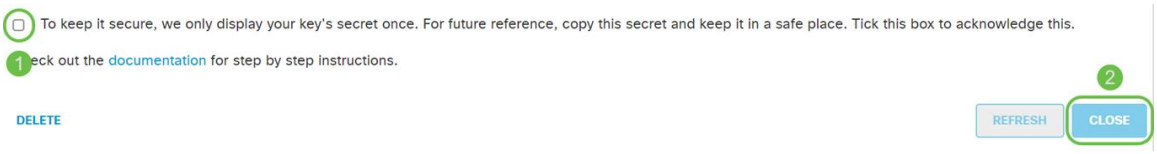
4단계

메모장과 같은 텍스트 편집기를 열고 API 및 API *Secret Key*의 오른쪽에 있는 **복사 아이콘**을 클릭하면 팝업 알림이 키를 클립보드에 복사했음을 확인합니다.한 번에 하나씩 비밀번호와 API 키를 문서에 붙여넣어 나중에 참조할 수 있도록 레이블을 지정합니다.이 경우 레이블은 "Umbrella network devices key"입니다.그런 다음 나중에 쉽게 액세스할 수 있는 안전한 위치에 텍스트 파일을 저장합니다.



5단계

키와 비밀 키를 안전한 위치에 복사한 후 Umbrella *API 화면*에서 **확인란**을 클릭하여 비밀 키의 임시 보기 승인을 완료한 다음 **Close** 버튼을 클릭합니다.



비밀 키를 분실하거나 실수로 삭제하면 이 키를 검색하기 위해 호출할 기능 또는 지원 번호가 없습니다.분실된 경우 키를 삭제하고 Umbrella로 보호하려는 각 디바이스로 새 API 키를 다시 인증해야 합니다.

RV345P에서 Umbrella 구성

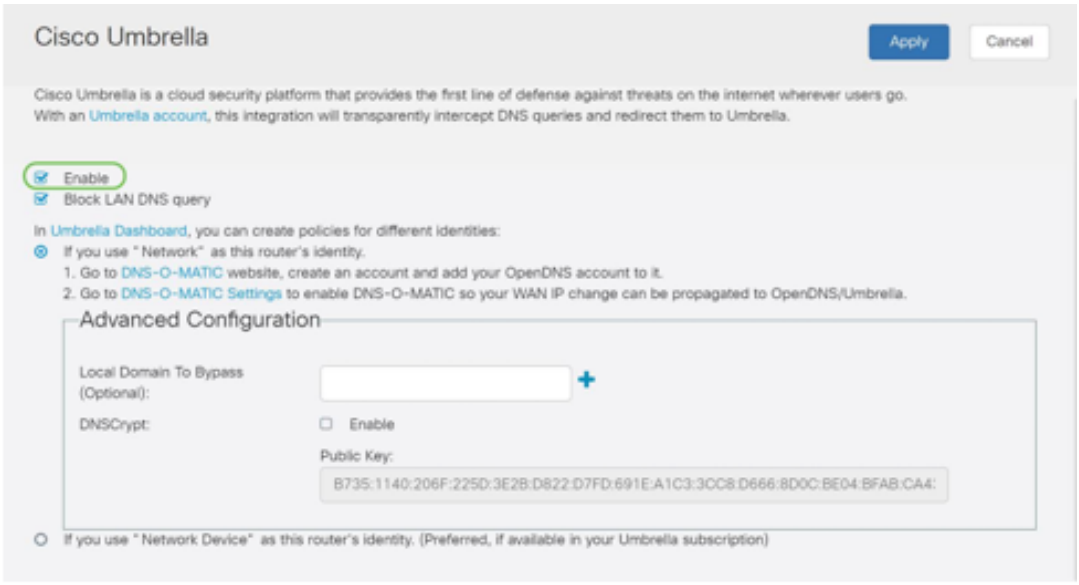
이제 Umbrella에서 API 키를 생성했으므로 해당 키를 가져와 RV345P에 설치할 수 있습니다.

1단계

RV345P 라우터에 로그인한 후 사이드바 메뉴에서 **Security(보안) >Umbrella**를 클릭합니다.

2단계

Umbrella API 화면에는 다양한 옵션이 있습니다. Enable(활성화) 확인란을 클릭하여 Umbrella를 활성화하기 시작합니다.

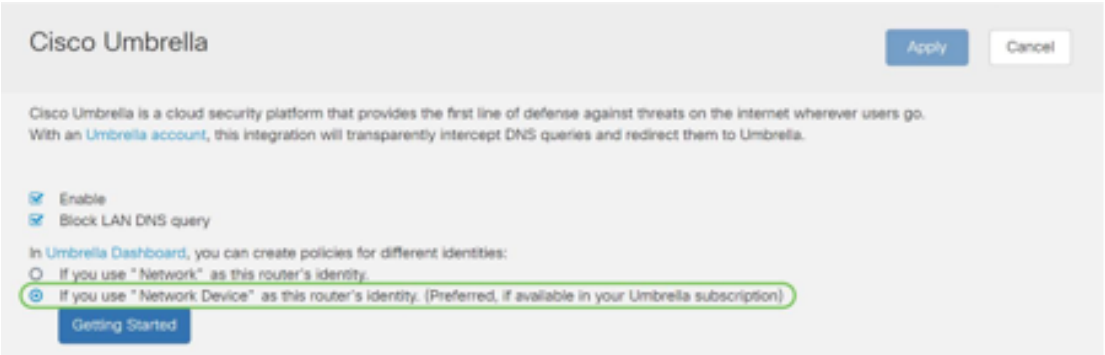


3단계(선택 사항)

기본적으로 Block *LAN DNS Queries*(*LAN DNS 쿼리 차단) 상자*가 선택됩니다.이 깔끔한 기능은 라우터에 액세스 제어 목록을 자동으로 생성하여 DNS 트래픽이 인터넷으로 유출되는 것을 방지합니다.이 기능은 모든 도메인 변환 요청을 RV345P를 통해 전달하도록 강제하며 대부분의 사용자에게 좋은 방법입니다.

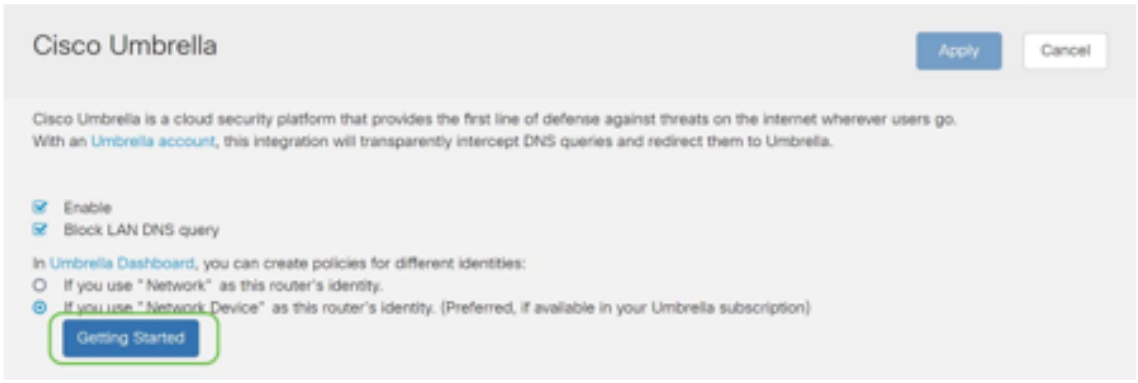
4단계

다음 단계는 두 가지 방법으로 진행됩니다.둘 다 네트워크 설정에 따라 달라집니다.DynDNS 또는 NoIP와 같은 서비스를 사용하는 경우 기본 이름 지정 체계를 "Network"로 둡니다.Umbrella가 보호를 제공할 때 해당 서비스와 Umbrella 인터페이스를 보장하려면 해당 어카운트에 로그인해야 합니다."네트워크 디바이스"에 의존하므로 하단 라디오 버튼을 클릭하겠습니다.



5단계

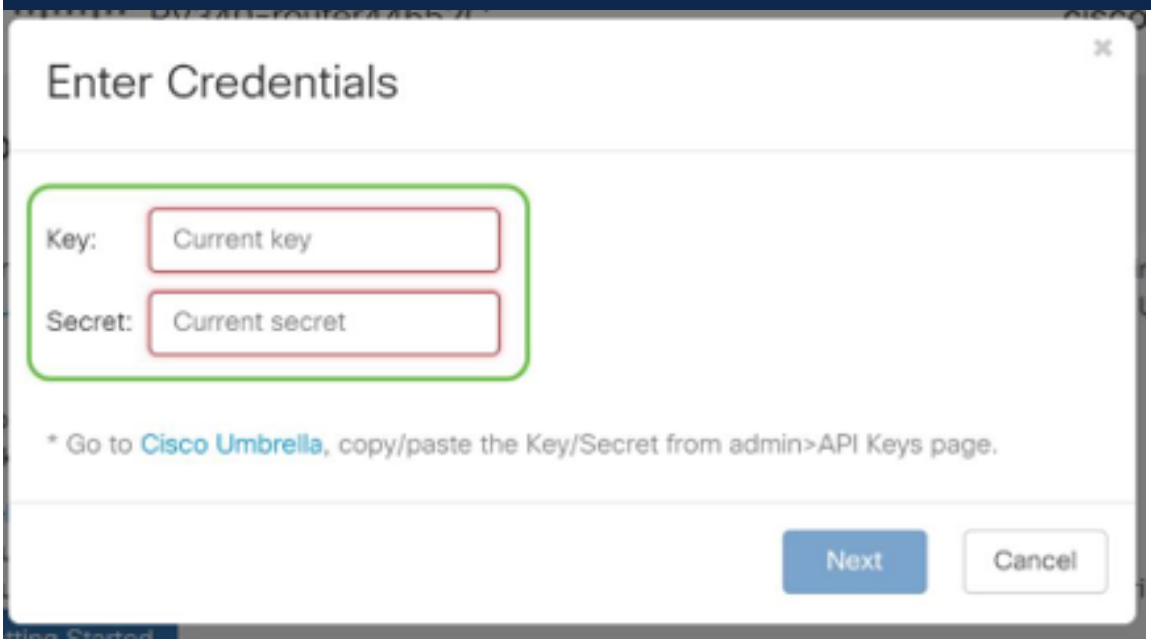
Getting **Started를 클릭합니다**.



6단계

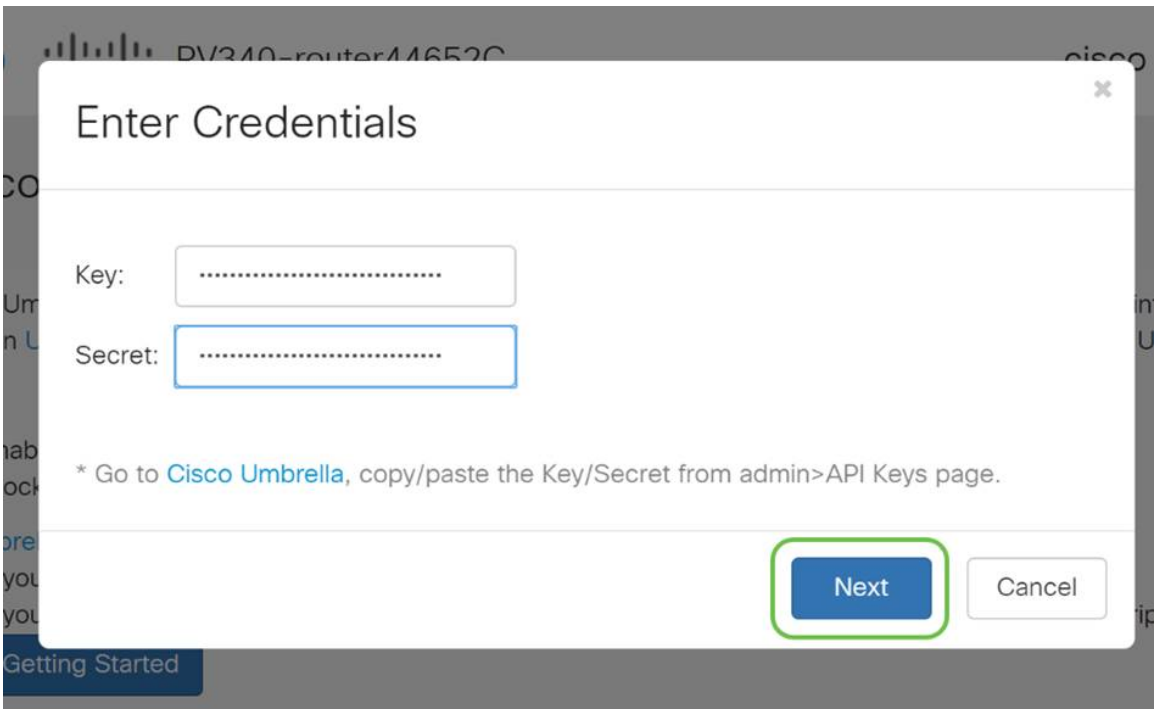
텍스트 상자에 **API 키** 및 **암호 키**를 입력합니다.

그걸 두 번 불러서 중요한 걸 알거야!비밀 키를 분실하거나 실수로 삭제하면 이 키를 검색하기 위해 호출할 기능 또는 지원 번호가 없습니다. 비밀 유지 및 보안을 유지하십시오.분실된 경우 키를 삭제하고 Umbrella로 보호하려는 각 디바이스로 새 API 키를 다시 인증해야 합니다.



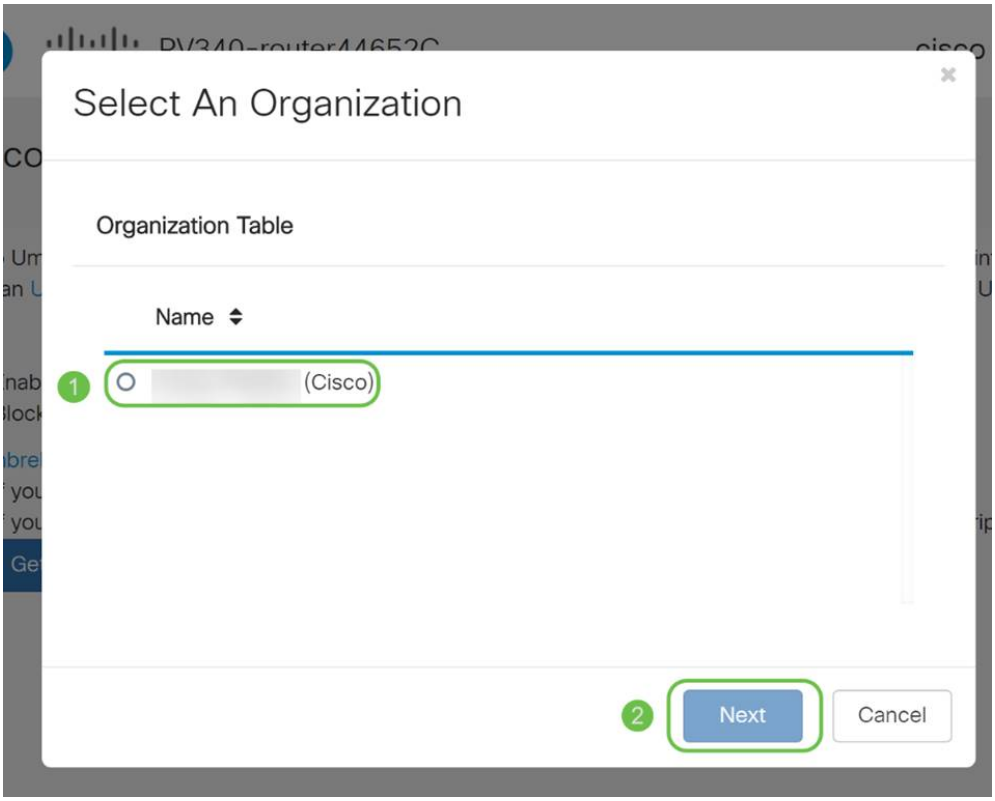
7단계

API 및 암호 키를 입력한 후 **Next** 버튼을 클릭합니다.



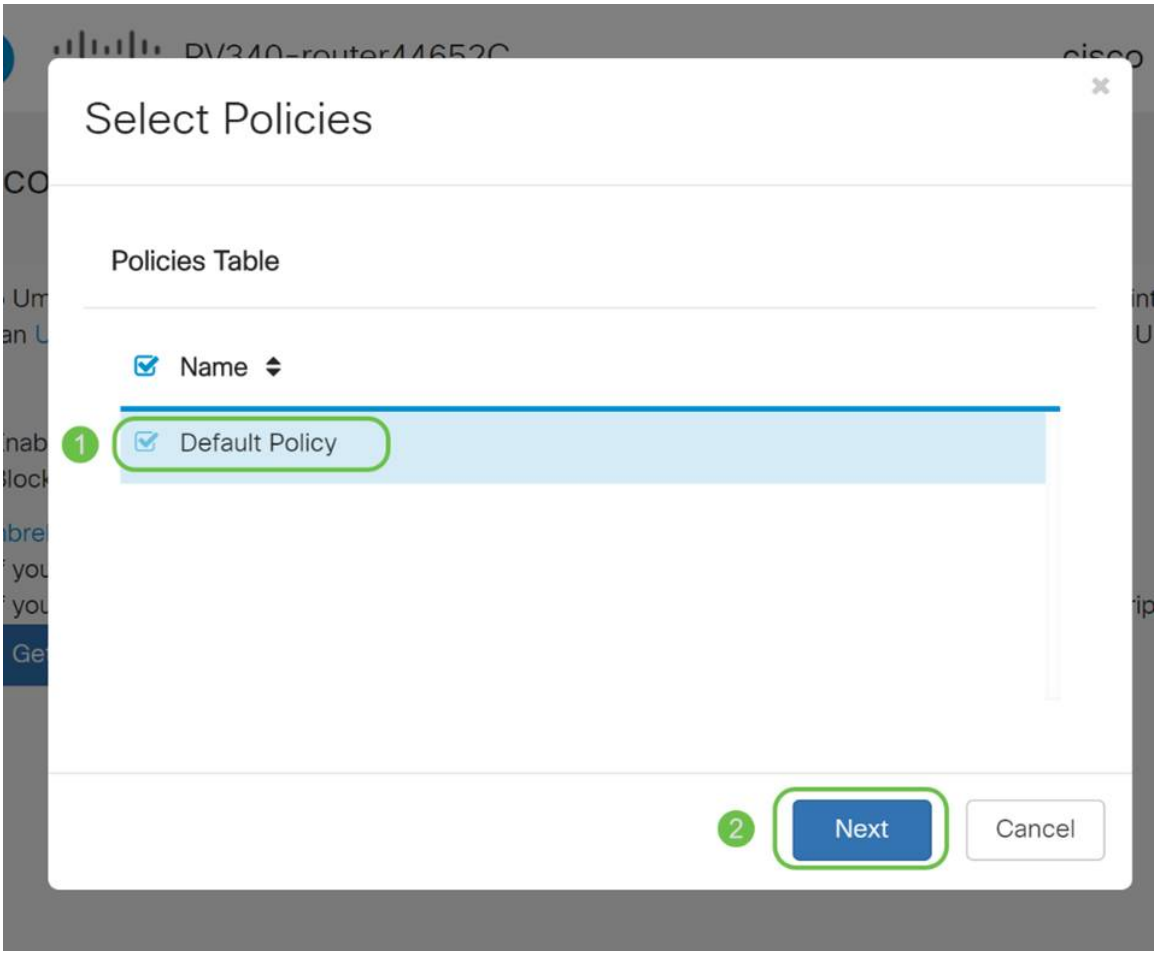
8단계

다음 화면에서 라우터와 연결할 **조직**을 선택합니다.Next(**다음)를 클릭합니다**.



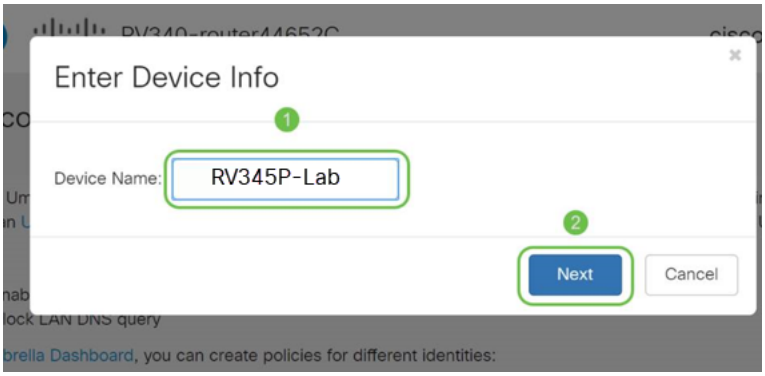
9단계

RV345P에서 라우팅한 트래픽에 적용할 정책을 선택합니다.대부분의 사용자에게 기본 정책은 충분한 커버리지를 제공합니다.



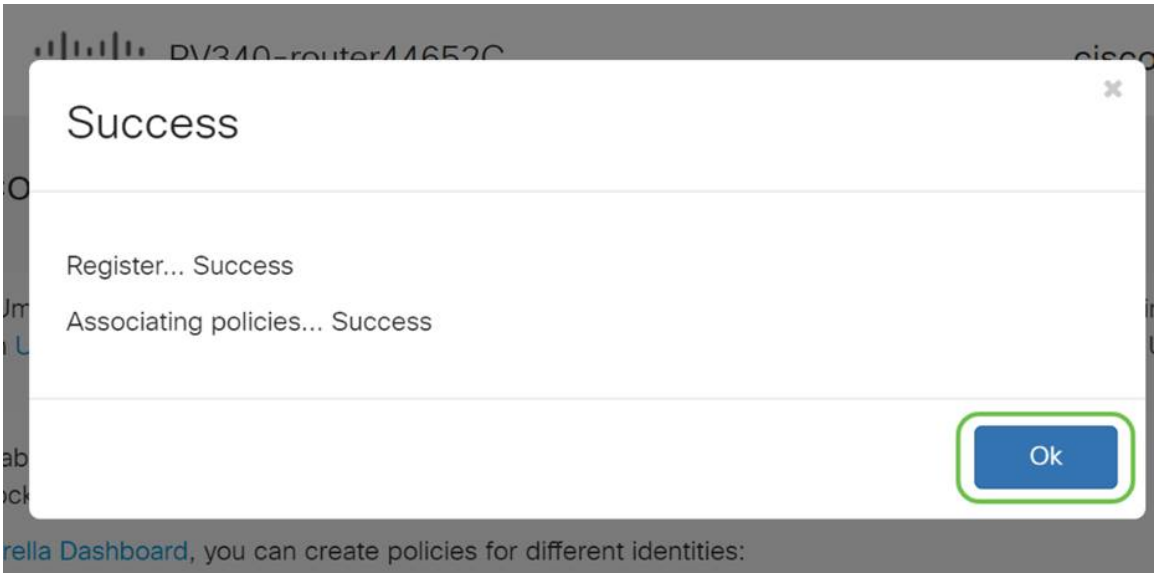
10단계

장치에 이름을 할당하여 Umbrella 보고에서 지정할 수 있습니다.설치 프로그램에서 RV *345P-Lab*이라는 이름을 *지정했습니다*.



11단계

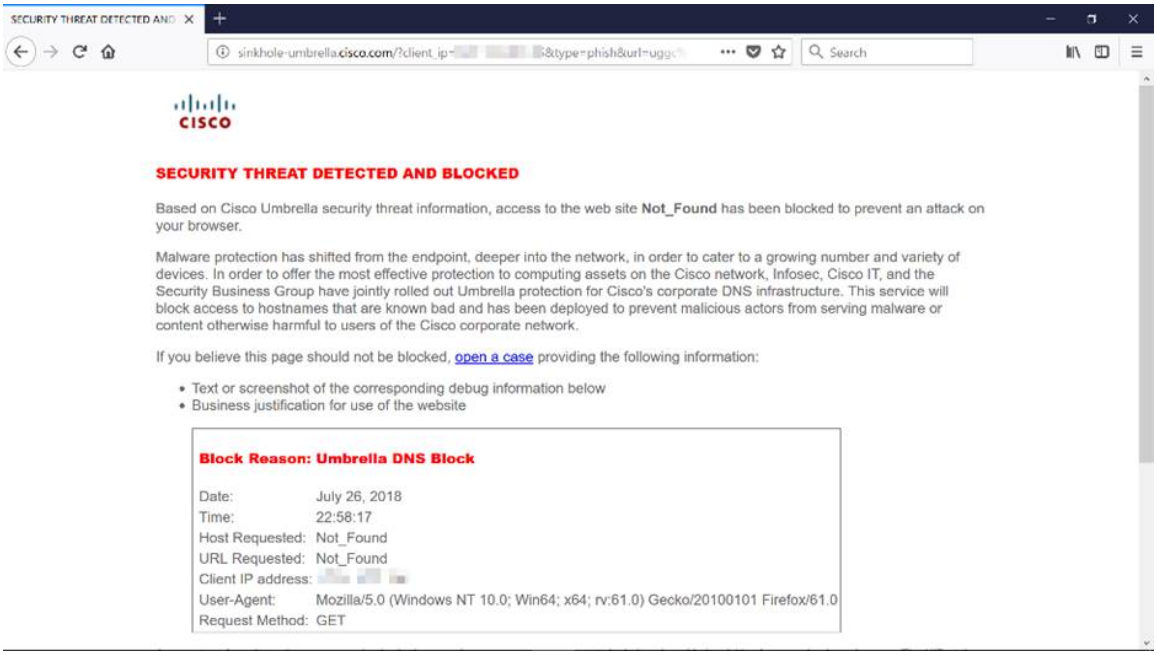
다음 화면에서는 선택한 설정을 확인하고 성공적으로 연결되면 업데이트를 제공합니다. **확인**을 **클릭합니다**.



확인

축하합니다. 이제 Cisco Umbrella로 보호됩니다.아니면 당신은?라이브 예제를 다시 확인해보면 Cisco는 페이지가 로드되는 즉시 이를 확인하는 데 필요한 전용 웹 사이트를 만들었습니다. 여기를 클릭하거나 브라우저 바에 https://InternetBadGuys.com를 입력합니다.

Umbrella가 올바르게 구성된 경우 이와 유사한 화면이 표시됩니다.



기타 보안 옵션

네트워크 장치에서 이더넷 케이블을 뽑았다가 네트워크에 연결하여 누군가가 네트워크에 무단 액세스를 시도하는 것이 염려되십니까?이 경우 각 IP 및 MAC 주소를 사용하여 라우터에 직접 연결할 수 있는 호스트 목록을 등록해야 합니다.지침은 RV34x Series Router의 IP Source Guard 구성 문서에서 찾을 수 있습니다.

VPN 옵션

VPN(Virtual Private Network) 연결을 통해 사용자는 인터넷과 같은 공용 또는 공유 네트워크를 통해 데이터를 액세스, 전송 및 수신할 수 있지만 사설 네트워크와 해당 리소스를 보호하기 위해 기본 네트워크 인프라에 안전하게 연결할 수 있습니다.

VPN 터널은 암호화 및 인증을 사용하여 데이터를 안전하게 전송할 수 있는 사설 네트워크를 설정합니다.회사 사무실은 직원들이 사무실 외부에 있더라도 개인 네트워크에 액세스할 수 있도록 하는 것이 유용하고 필요하기 때문에 VPN 연결을 주로 사용합니다.

VPN을 사용하면 원격 호스트가 동일한 로컬 네트워크에 있는 것처럼 작동할 수 있습니다.라우터는 최대 50개의 터널을 지원합니다.라우터가 인터넷 연결을 위해 구성된 후 라우터와 엔드포인트 간에 VPN 연결을 설정할 수 있습니다.VPN 클라이언트는 연결을 설정할 수 있도록 VPN 라우터의 설정에 전적으로 의존합니다.

어떤 VPN이 사용자의 요구에 가장 잘 부합하는지 잘 모르겠으면 **Cisco Business VPN 개요 및 모범 사례를 확인하십시오**.

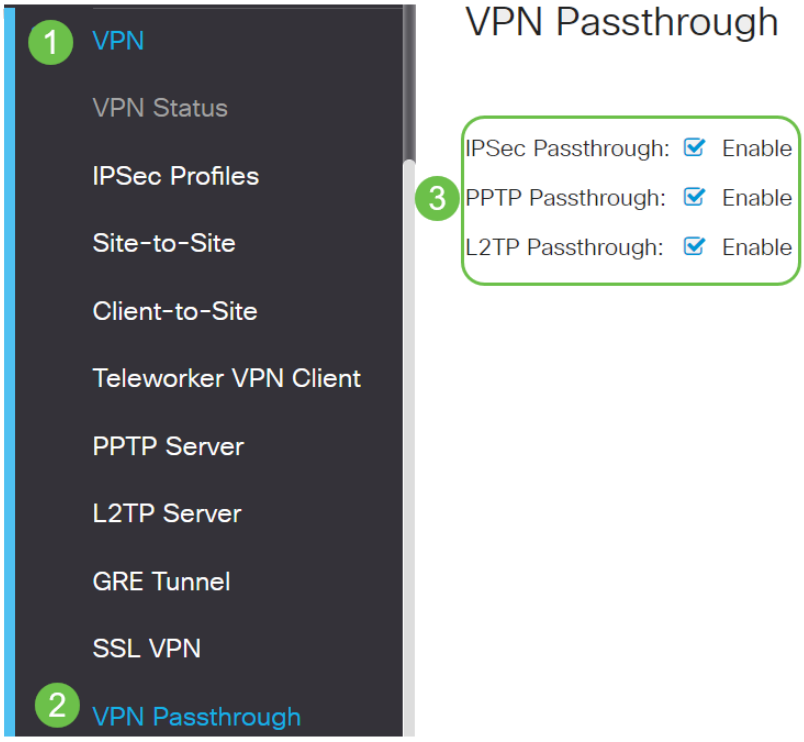
AnyConnect VPN은 이 컨피그레이션 가이드에 나열된 유일한 Cisco VPN 지원 제품입니다.TheGreenBow 및 Shrew Soft를 비롯한 타사 타사 타사 제품은 Cisco에서 지원하지 않습니다.그것들은 지침 용도로 엄격히 포함되어 있다.기사 이외의 항목에 대한 지원이 필요한 경우 해당 서드파티에 지원을 문의해야 합니다.

VPN 설정을 계획하지 않을 경우 **클릭하여 다음 섹션으로 이동할** 수 있습니다.

VPN 통과

일반적으로 모든 라우터는 동일한 인터넷 연결을 통해 여러 클라이언트를 지원하려는 경우 IP 주소를 보존하기 위해 NAT(Network Address Translation)를 지원합니다.그러나 PPTP(Point-to-Point Tunneling Protocol) 및 IPsec(Internet Protocol Security) VPN은 NAT를 지원하지 않습니다.여기서 VPN 패스스루가 시작됩니다.VPN Passthrough는 이 라우터에 연결된 VPN 클라이언트에서 생성된 VPN 트래픽이 이 라우터를 통과하고 VPN 엔드포인트에 연결할 수 있도록 하는 기능입니다.VPN Passthrough를 사용하면 VPN 클라이언트에서 시작된 인터넷으로 PPTP 및 IPsec VPN을 통과하고 원격 VPN 게이트웨이에 연결할 수 있습니다.이 기능은 NAT를 지원하는 홈 라우터에서 일반적으로 찾아볼 수 있습니다.

기본적으로 IPsec, PPTP 및 L2TP Passthrough가 활성화됩니다.이러한 설정을 보거나 조정하려면 **VPN > VPN Passthrough**를 선택합니다.필요에 따라 보거나 조정합니다.



AnyConnect VPN

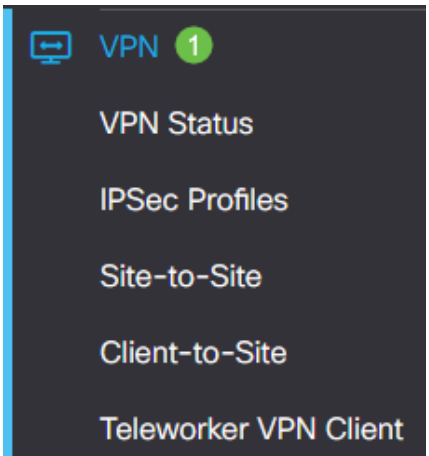
Cisco AnyConnect를 사용하면 다음과 같은 여러 가지 이점이 있습니다.

1. 안전하고 지속적인 연결
2. 지속적인 보안 및 정책 시행
3. ASA(Adaptive Security Appliance) 또는 엔터프라이즈 소프트웨어 구축 시스템에서 구축 가능
4. 맞춤형 및 번역 가능
5. 쉽게 구성
6. IPsec(Internet Protocol Security) 및 SSL(Secure Sockets Layer) 모두 지원
7. IKEv2.0(Internet Key Exchange version 2.0) 프로토콜 지원

RV345P에서 AnyConnect SSL VPN 구성

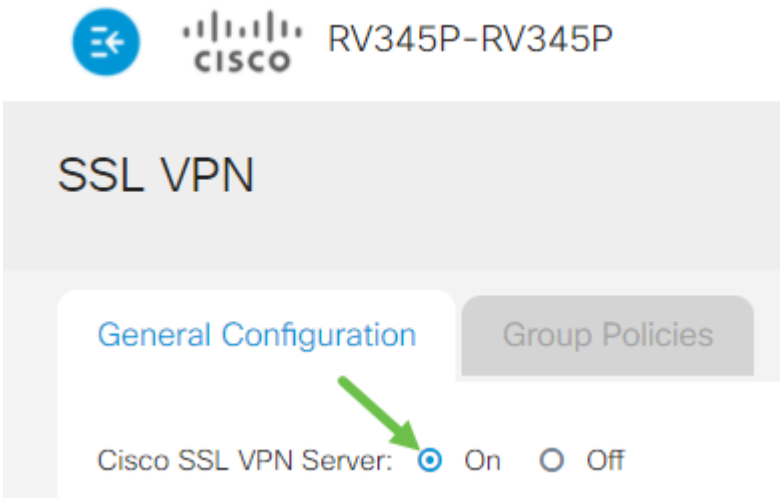
1단계

라우터 웹 기반 유틸리티에 액세스하고 **VPN > SSL VPN**을 선택합니다.



2단계

Cisco SSL VPN Server를 활성화하려면 On(**켜기**) 라디오 버튼을 클릭합니다.



필수 게이트웨이 설정

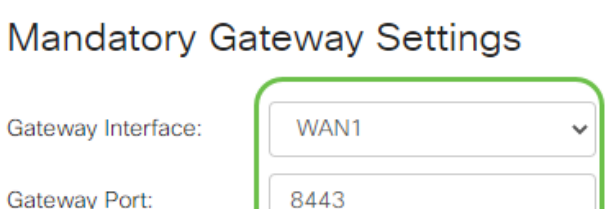
1단계

다음 컨피그레이션 설정은 필수입니다.

1. 드롭다운 목록에서 Gateway Interface(게이트웨이 인터페이스)를 선택합니다.이 포트는 SSL VPN 터널을 통해 트래픽을 전달하는 데 사용됩니다.옵션은 다음과 같습니다 .WAN1, WAN2, USB1, USB2
2. Gateway Port(게이트웨이 포트) 필드에 SSL VPN 게이트웨이에 사용되는 포트 번호를 1~65535의 범위에서 입력합니다.
3. 드롭다운 목록에서 Certificate File(인증서 파일)을 선택합니다.이 인증서는 SSL VPN 터널을 통해 네트워크 리소스에 액세스하려는 사용자를 인증합니다.드롭다운 목록에는 기본 인증서 및 가져온 인증서가 포함됩니다.
4. Client *Address Pool* 필드에 클라이언트 주소 풀의 IP 주소를 입력합니다.이 풀은 원격 VPN 클라이언트에 할당될 IP 주소의 범위가 됩니다.

   IP 주소 범위가 로컬 네트워크의 IP 주소와 겹치지 않는지 확인합니다.

6. 드롭다운 목록에서 Client Netmask(클라이언트 넷마스크)를 선택합니다.
7. *Client Domain* 필드에 클라이언트 도메인 이름을 입력합니다.SSL VPN 클라이언트에 푸시해야 하는 도메인 이름입니다.
8. 로그인 배너 필드에 로그인 배너로 표시될 텍스트를 *입력합니다*.클라이언트가 로그인할 때마다 표시되는 배너입니다.



2단계

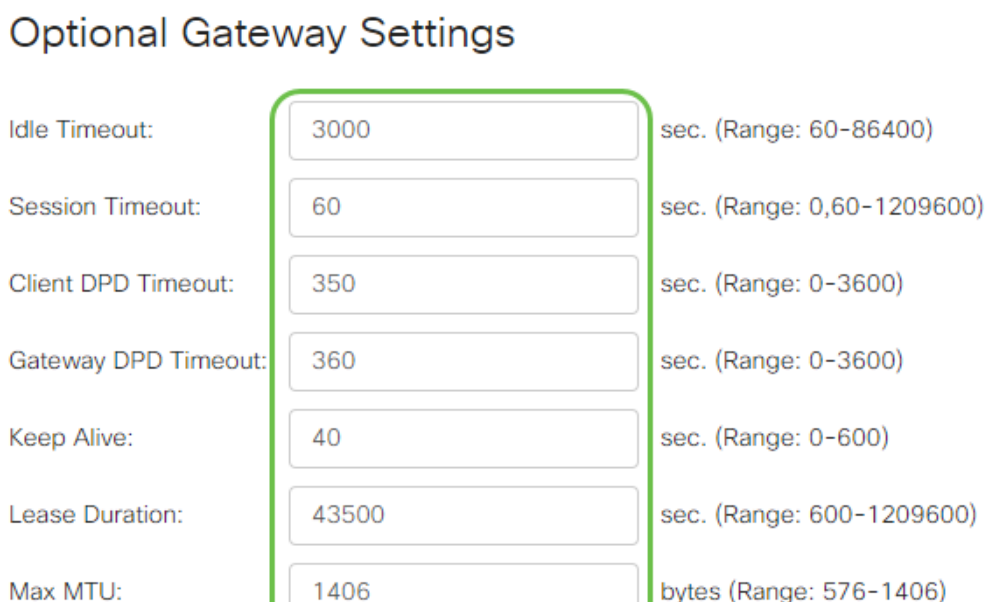
Apply를 **클릭합니다**.

선택적 게이트웨이 설정

1단계

다음 컨피그레이션 설정은 선택 사항입니다.

1. 60~86400 사이의 유휴 시간 제한 값을 초 단위로 입력합니다. 이 기간은 SSL VPN 세션이 유휴 상태로 유지되는 시간이 됩니다.
2. *Session Timeout* 필드에 값을 초 단위로 입력합니다.지정된 유휴 시간 이후 TCP(Transmission Control Protocol) 또는 UDP(User Datagram Protocol) 세션이 시간 초과되는 시간입니다.범위는 60~1209600입니다.
3. ClientDPD Timeout(ClientDPD 시간 제한) 필드에 0~3600의 값을 초 단위로 입력합니다.이 값은 VPN 터널의 상태를 확인하기 위해 HELLO/ACK 메시지를 주기적으로 전송하도록 지정합니다.이 기능은 VPN 터널의 양쪽 끝에서 활성화되어야 합니다.
4. GatewayDPD Timeout(게이트웨이DPD 시간 제한) 필드에 0~3600의 값을 초 단위로 입력합니다.이 값은 VPN 터널의 상태를 확인하기 위해 HELLO/ACK 메시지를 주기적으로 전송하도록 지정합니다.이 기능은 VPN 터널의 양쪽 끝에서 활성화되어야 합니다.
5. *Keep Alive* 필드에 0~600의 값을 초 단위로 입력합니다. 이 기능을 사용하면 라우터가 항상 인터넷에 연결되어 있습니다.VPN 연결이 끊어진 경우 다시 설정하려고 시도합니다.
6. Lease Duration(*리스 기간*) 필드에 연결할 터널의 지속 시간(초)에 대한 값을 *입력합니다*.범위는 600~1209600입니다.
7. 네트워크를 통해 전송할 수 있는 패킷 크기를 바이트 단위로 입력합니다.범위는 576~1406입니다.
8. Rekey Interval(키 재설정 간격) 필드에 릴레이 간격 시간을 입력합니다.키 재설정 기능을 사용하면 세션이 설정된 후 SSL 키를 재협상할 수 있습니다.범위는 0~43200입니다.



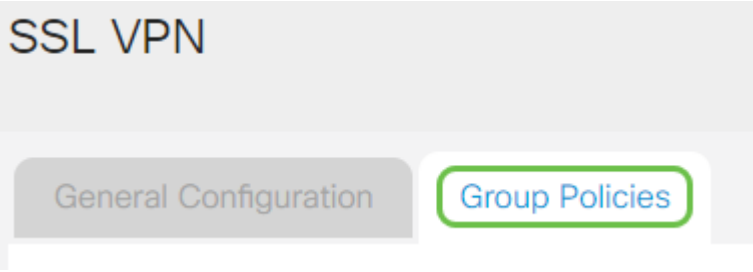
2단계

Apply를 **클릭합니다**.

그룹 정책 구성

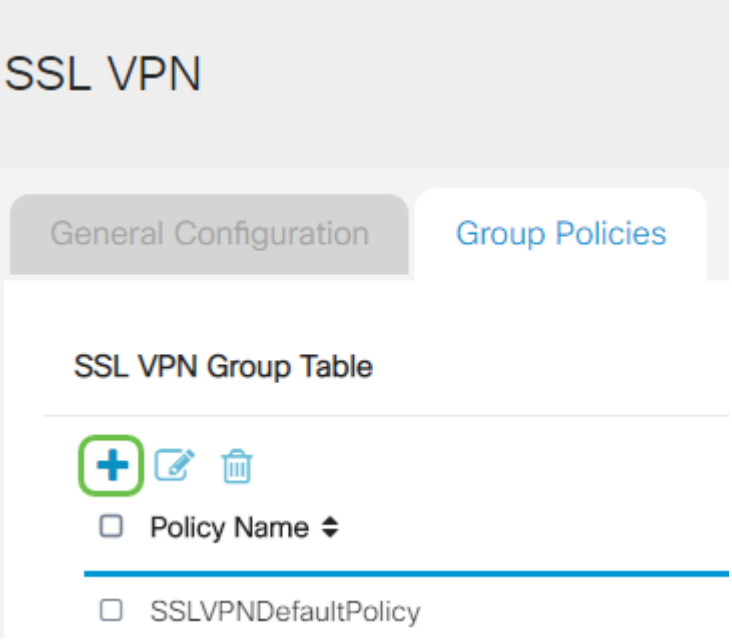
1단계

Group Policies 탭을 클릭합니다.



2단계

SSL VPN Group Table(SSL VPN 그룹 테이블) 아래에서 **추가 아이콘**을 클릭하여 그룹 정책을 추가합니다.

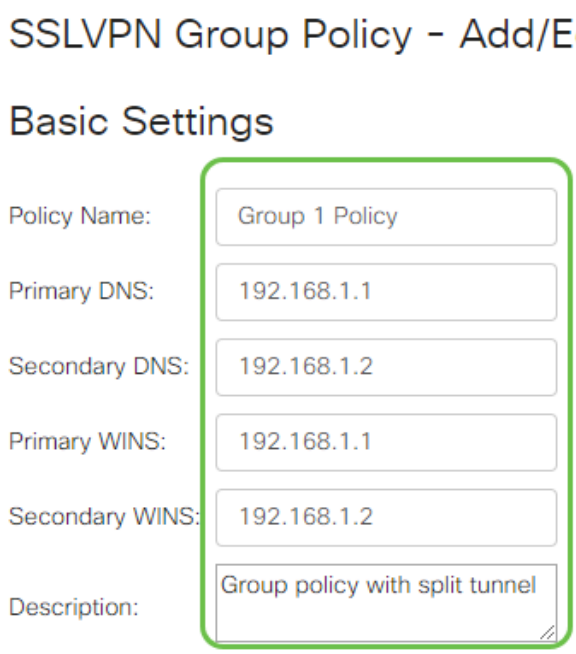


SSL VPN Group(SSL VPN 그룹) 테이블에는 디바이스의 그룹 정책 목록이 표시됩니다.목록에서 SSLVPNDefaultPolicy라는 이름의 첫 번째 그룹 정책을 편집할 수도 있습니다.디바이스에서 제공하는 기본 정책입니다.

3단계

1. *Policy Name* 필드에 기본 설정 정책 이름을 입력합니다.

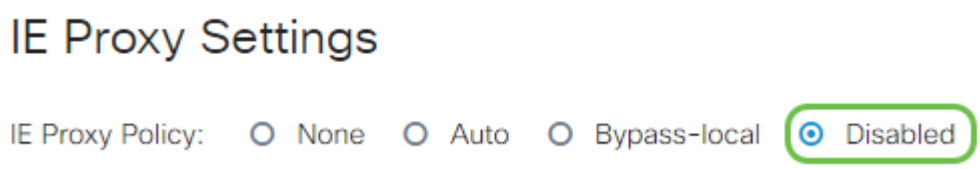
2. 제공된 필드에 기본 DNS의 IP 주소를 입력합니다.기본적으로 이 IP 주소는 이미 제공됩니다.
3. *(선택 사항) 제공된 필드에 보조 DNS의 IP 주소를 입력합니다.이는 기본 DNS가 실패할 경우 백업 역할을 합니다.*
4. (선택 사항) 제공된 필드에 기본 WINS의 IP 주소를 입력합니다.
5. (선택 사항) 제공된 필드에 보조 WINS의 IP 주소를 입력합니다.
6. (선택 사항) Description(설명) 필드에 정책에 대한 설명을 *입력합니다*.



4단계(선택 사항)

VPN 터널을 설정하기 위해 Microsoft MSIE(Internet Explorer) 프록시 설정을 활성화하려면 라디오 버튼을 클릭하여 IE 프록시 정책을 선택합니다.옵션은 다음과 같습니다.

- None(없음) - 브라우저에서 프록시 설정을 사용하지 않도록 허용합니다.
- Auto(자동) - 브라우저에서 프록시 설정을 자동으로 탐지할 수 있습니다.
- Bypass-local - 브라우저에서 원격 사용자에 구성된 프록시 설정을 우회하도록 허용합니다.
- Disabled(비활성화됨) - MSIE 프록시 설정을 비활성화합니다.



5단계(선택 사항)

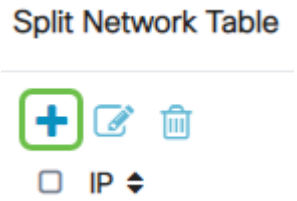
Split Tunneling Settings(스플릿 터널링 설정) 영역에서 Enable Split **Tunneling(스플릿 터널링 활성화**) 확인란을 선택하여 암호화되지 않은 인터넷 트래픽이 인터넷에 직접 전송되도록 허용합니다.Full Tunneling은 모든 트래픽을 최종 디바이스로 보낸 다음 목적지 리소스로 라우팅하여 웹 액세스 경로에서 회사 네트워크를 제거합니다.

6단계(선택 사항)

스플릿 터널링을 적용할 때 트래픽을 포함할지 제외할지를 선택하려면 라디오 버튼을 클릭합니다.

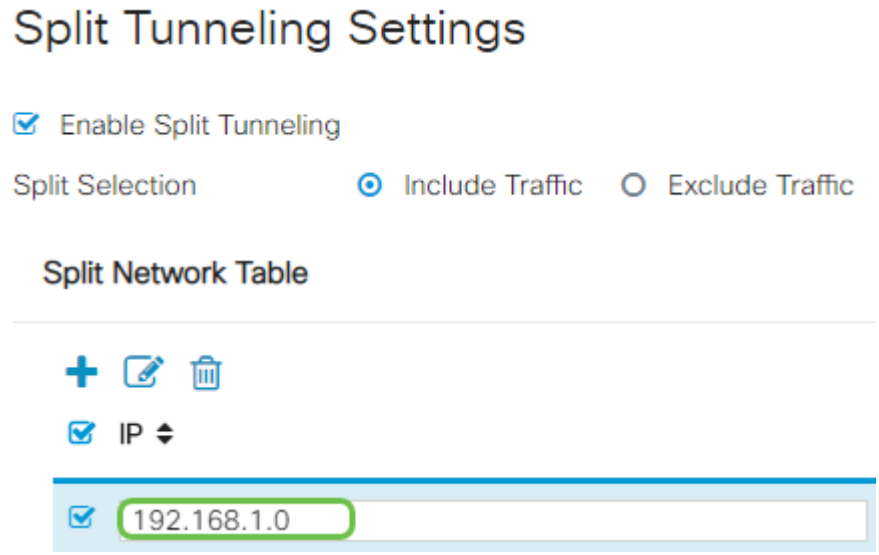
7단계

Split Network Table(네트워크 분할 테이블)에서 **추가 아이콘**을 클릭하여 분할 네트워크 예외를 추가합니다.



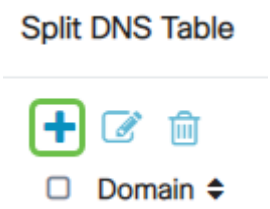
8단계

제공된 필드에 네트워크의 IP 주소를 입력합니다.



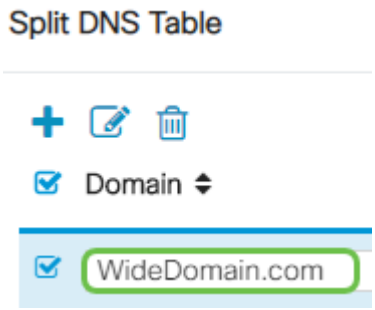
9단계

Split DNS Table(DNS 테이블 분할)에서 **추가 아이콘**을 클릭하여 스플릿 DNS 예외를 추가합니다.



10단계

제공된 필드에 도메인 이름을 입력한 다음 **적용**을 클릭합니다.



라우터는 기본적으로 2개의 AnyConnect 서버 라이센스와 함께 제공됩니다.즉, AnyConnect 클라이언트 라이센스가 있으면 다른 RV340 시리즈 라우터와 동시에 2개의 VPN 터널을 설정할 수 있습니다.

간단히 말해, RV345P 라우터에는 라이센스가 필요하지 않지만 모든 클라이언트에는 라이센스가 필요합니다.AnyConnect 클라이언트 라이센스를 사용하면 데스크톱 및 모바일 클라이언트가 VPN 네트워크에 원격으로 액세스할 수 있습니다.

다음 섹션에서는 클라이언트에 대한 라이센스를 가져오는 방법에 대해 자세히 설명합니다.

AnyConnect 모빌리티 클라이언트

VPN 클라이언트는 원격 네트워크에 연결하려는 컴퓨터에 설치 및 실행되는 소프트웨어입니다.이 클라이언트 소프트웨어는 IP 주소 및 인증 정보와 같은 VPN 서버의 구성과 동일한 구성으로 설정해야 합니다.이 인증 정보에는 데이터를 암호화하는 데 사용할 사용자 이름 및 사전 공유 키가 포함됩니다.연결할 네트워크의 물리적 위치에 따라 VPN 클라이언트는 하드웨어 디바이스일 수도 있습니다.이는 일반적으로 VPN 연결을 사용하여 별도의 위치에 있는 두 네트워크를 연결하는 경우에 발생합니다.

Cisco AnyConnect Secure Mobility Client는 다양한 운영 체제 및 하드웨어 구성에서 작동하는 VPN에 연결하기 위한 소프트웨어 애플리케이션입니다.이 소프트웨어 애플리케이션을 사용하면 다른 네트워크의 원격 리소스에 사용자가 네트워크에 직접 연결된 것처럼 안전하게 액세스할 수 있습니다.

라우터가 AnyConnect로 등록되고 구성되면 클라이언트는 구매한 라이센스 풀에서 라우터에 라이센스를 설치할 수 있습니다. 이 라이센스는 다음 섹션에 자세히 설명되어 있습니다.

구매 라이센스

Cisco 총판사 또는 Cisco 파트너로부터 라이센스를 구매해야 합니다.라이센스를 주문할 때는 Cisco Smart Account ID 또는 도메인 ID를 name@domain.com 형식으로 *제공해야* 합니다.

Cisco 총판사 또는 파트너가 없는 경우 여기에서 해당 총판사를 찾을 수 있습니다.

작성 시 다음 제품 SKU를 사용하여 25개의 번들로 구성된 추가 라이센스를 구매할 수 있습니다. Cisco AnyConnect 주문 가이드에 설명된 대로 AnyConnect 클라이언트 라이센스에 대한 다른 옵션이 있지만, 전체 기능에 대한 최소 요구 사항은 나열된 제품 ID입니다.

먼저 나열된 AnyConnect 클라이언트 라이센스 제품 SKU는 1년의 라이센스를 제공하며 최소 25개의 라이센스를 구매해야 합니다.RV340 시리즈 라우터에 적용되는 기타 제품 SKU는 다음과 같이 다양한 서브스크립션 레벨에서도 사용할 수 있습니다.

- **LS-AC-PLS-1Y-S1** — 1년 Cisco AnyConnect Plus 클라이언트 라이센스
- **LS-AC-PLS-3Y-S1** — 3년 Cisco AnyConnect Plus 클라이언트 라이센스
- **LS-AC-PLS-5Y-S1** — 5년 Cisco AnyConnect Plus 클라이언트 라이센스
- **LS-AC-PLS-P-25-S** — 25팩 Cisco AnyConnect Plus 영구 클라이언트 라이센스
- **LS-AC-PLS-P-50-S** — 50팩 Cisco AnyConnect Plus 영구 클라이언트 라이센스

클라이언트 정보

클라이언트가 다음 중 하나를 설정할 때 이러한 링크를 보내야 합니다.

- 창:Windows 컴퓨터의 AnyConnect
- Mac: Mac에 AnyConnect를 설치합니다.
- Ubuntu 데스크톱:Ubuntu 데스크톱에 AnyConnect 설치 및 사용
- 문제가 있는 경우 Cisco AnyConnect Secure Mobility Client Errors에 대한 기본 문제 해결을 위한 정보 수집으로 이동할 수 있습니다.

AnyConnect VPN 연결 확인

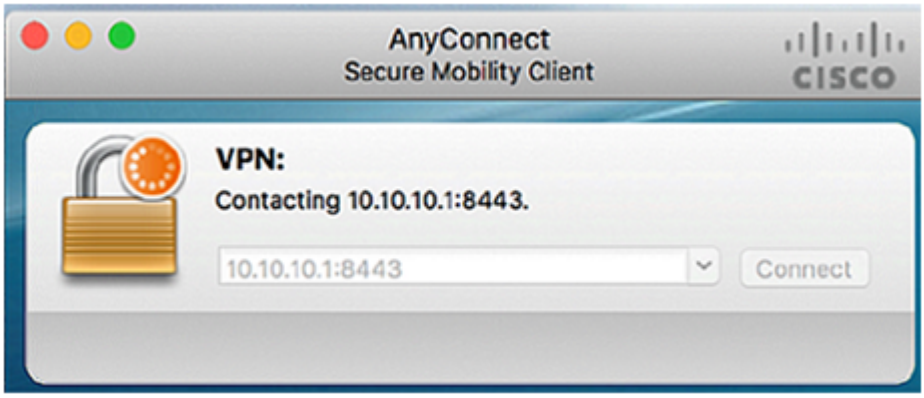
1단계

AnyConnect **Secure Mobility Client 아이콘을 클릭합니다**.

2단계

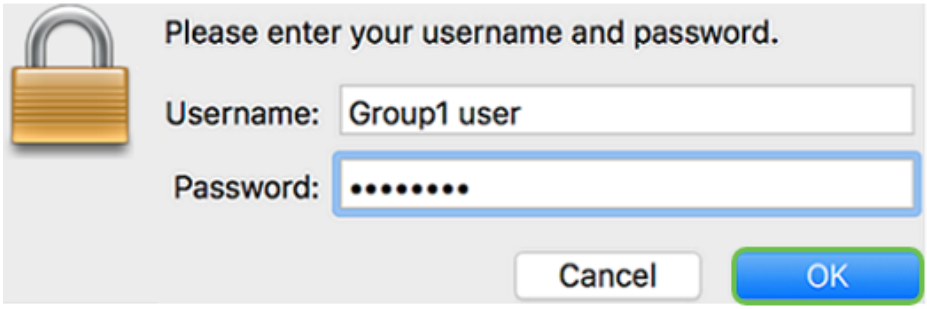
AnyConnect Secure Mobility Client(AnyConnect 보안 모빌리티 클라이언트) 창에서 게이트웨이 IP 주소 및 콜론(:)으로 구분된 게이트웨이 포트 번호를 입력한 다음 **연결**을 클릭합니다.

이제 소프트웨어가 원격 네트워크에 연결되어 있음을 표시합니다.



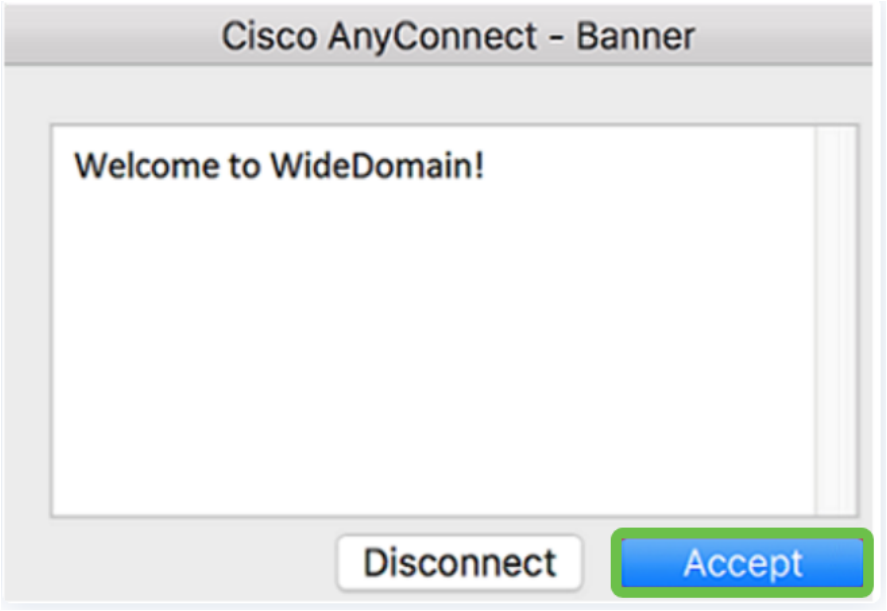
3단계

각 필드에 서버 사용자 이름과 비밀번호를 입력한 다음 **OK**(확인)를 클릭합니다.

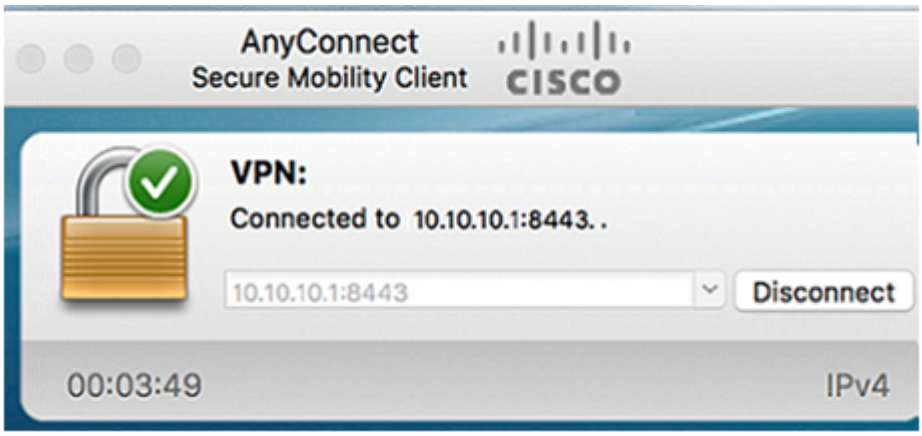


4단계

연결이 설정되면 로그인 배너가 나타납니다.Accept(수락)**를 클릭합니다**.



이제 AnyConnect 창에 네트워크에 대한 VPN 연결 성공 여부가 표시됩니다.



지금 AnyConnect VPN을 사용 중인 경우 다른 VPN 옵션을 건너뛰고 다음 섹션으로 이동할 수 있습니다.

Shrew 소프트 VPN

IPsec VPN을 사용하면 인터넷을 통해 암호화된 터널을 설정하여 원격 리소스를 안전하게 확보할 수 있습니다.RV34X 시리즈 라우터는 IPsec VPN 서버로 작동하며 Shrew Soft VPN Client를 지원합니다.이 섹션에서는 라우터와 Shrew 소프트 클라이언트를 구성하여 VPN에 대한 연결을 보호하는 방법을 보여줍니다.

Cisco는 Shrew Soft를 지원하지 않습니다.이 예는 데모용으로만 제공됩니다.shrew Soft에 문제가 있는 경우 해당 담당자에게 지원을 요청하십시오.

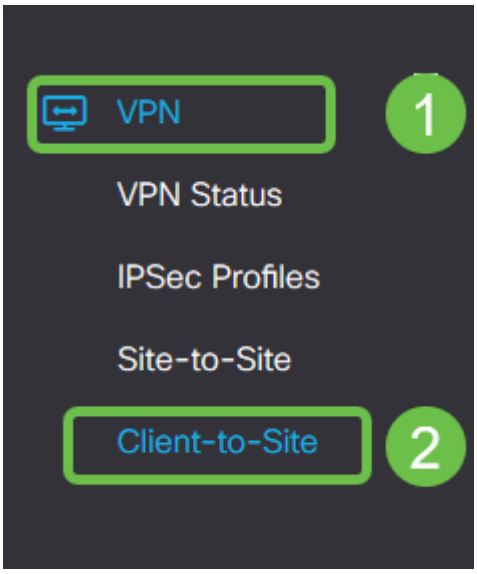
shrew Soft VPN 클라이언트 소프트웨어의 최신 버전을 여기에서 다운로드할 수 있습니다.https://www.shrew.net/download/vpn

RV345P Series 라우터에서 Shrew 소프트 구성

먼저 RV345P에서 **Client-to-Site VPN**을 구성합니다.

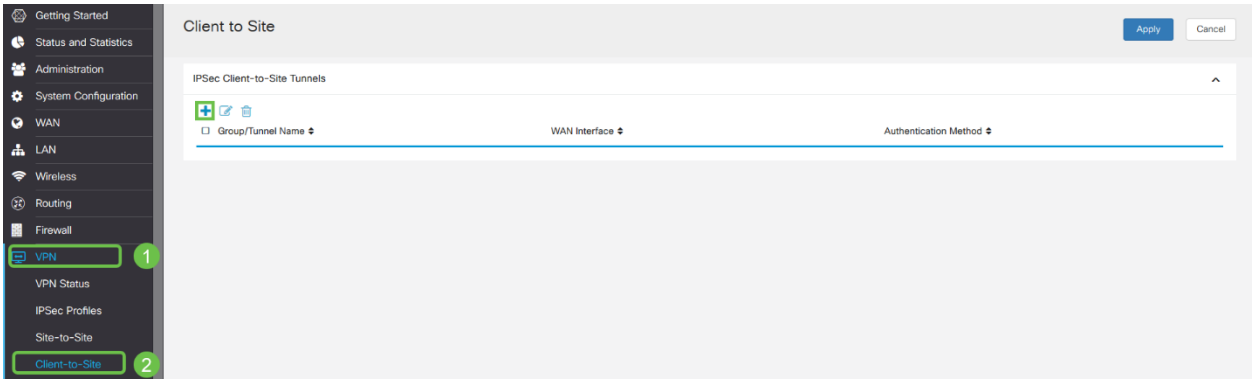
1단계

VPN > Client-to-Site로 이동합니다.



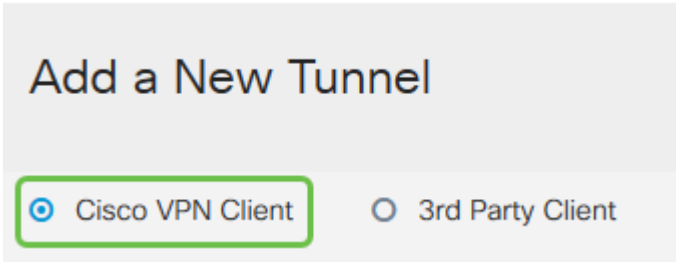
2단계

Client-**to-Site** VPN 프로필을 추가합니다.



3단계

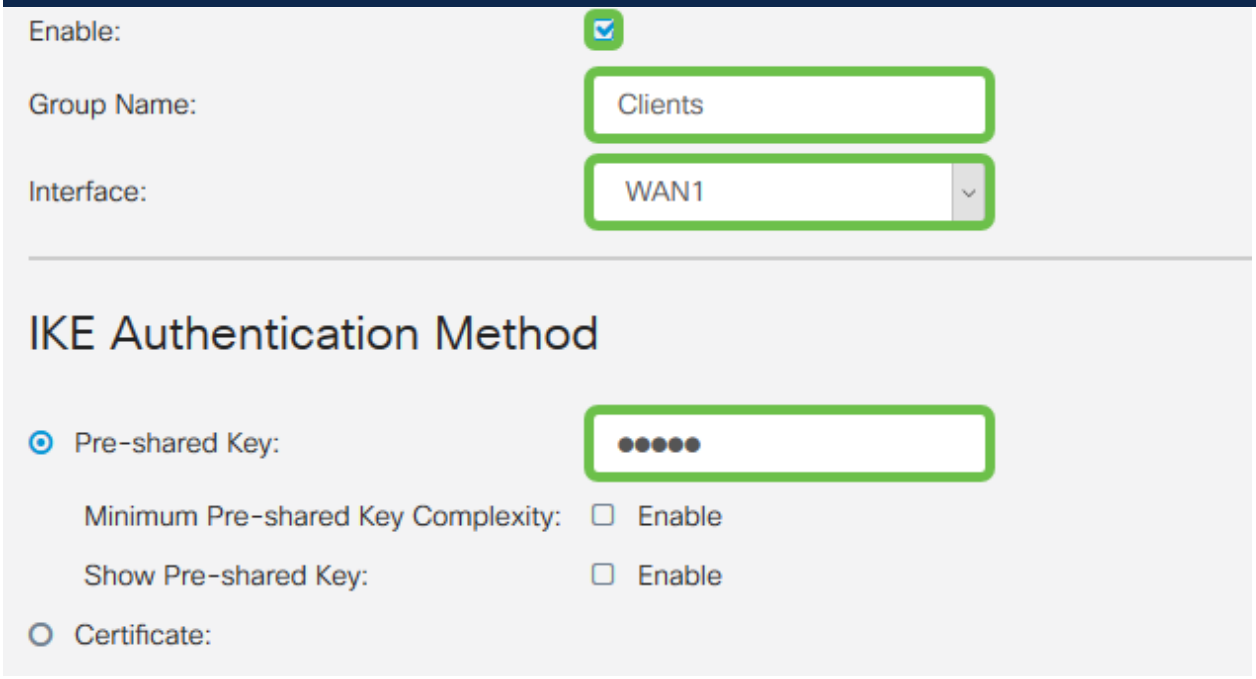
Cisco VPN Client 옵션을 선택합니다.



4단계

Enable(활성화) 확인란을 선택하여 VPN 클라이언트 프로파일을 활성화합니다.또한 *그룹 이름*을 구성하고 **WAN 인터페이스**를 선택한 다음 **사전 공유 키를 입력하겠습니다**.

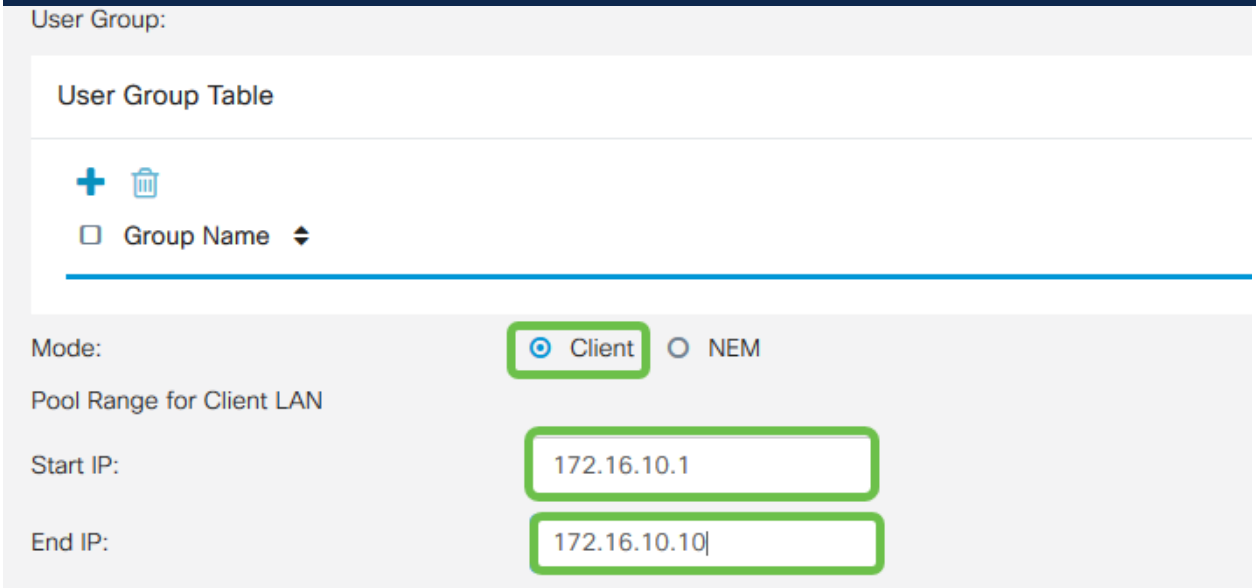
그룹 이름 및 *사전 공유 키는* 나중에 클라이언트를 구성할 때 사용되므로 주의하십시오.



5단계

사용자 **그룹 테이블**을 비워둡니다.라우터의 *사용자 그룹*에 대한 것이지만 아직 구성하지 않았습니다.Mode(**모드**)가 Client(클라이언트)로 **설정되었는지 확인합니다**.클라이언트 **LAN 풀 범위를 입력합니다**.172.16.10.1~172.16.10.10을 사용하겠습니다

풀 범위는 네트워크의 다른 곳에서 사용되지 않는 고유한 서브넷을 사용해야 합니다.



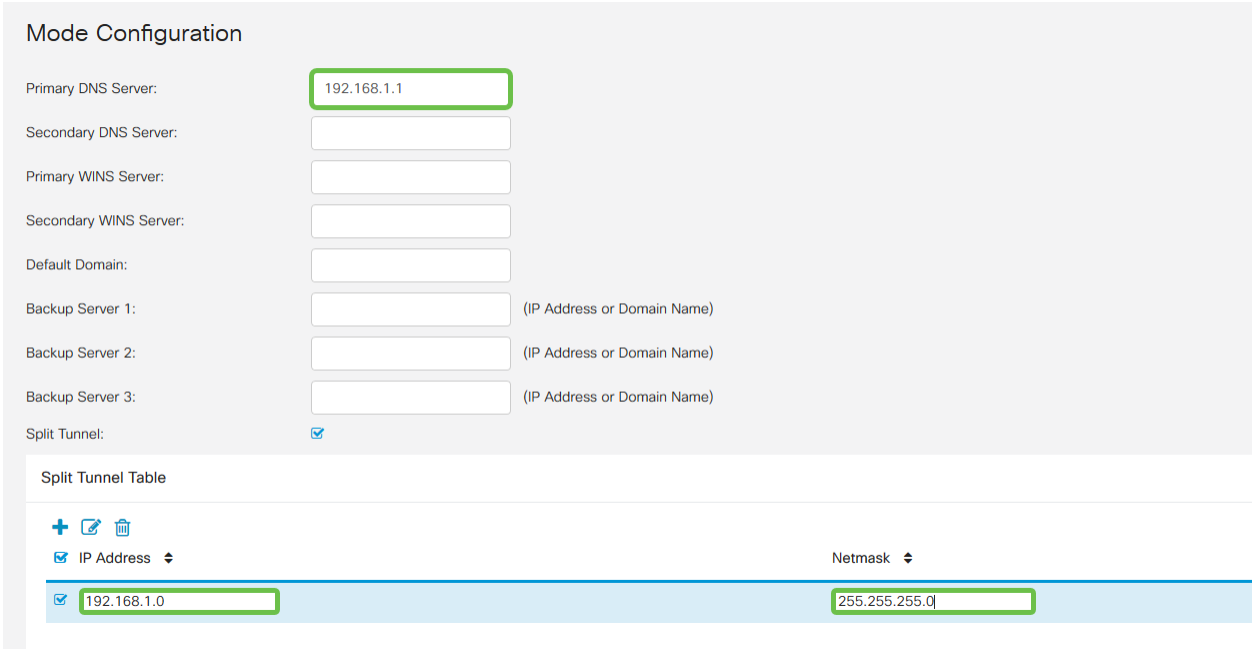
6단계

여기서 **모드 컨피그레이션** 설정을 구성합니다.사용할 설정은 다음과 같습니다.

- **기본 DNS 서버**:내부 DNS 서버가 있거나 외부 DNS 서버를 사용하려는 경우 여기에 입력할 수 있습니다.그렇지 않으면 기본값은 RV345P LAN IP 주소로 설정됩니다.여기서는

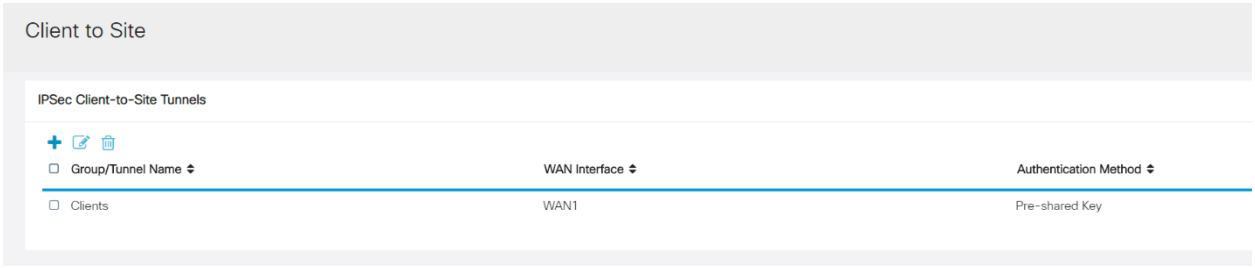
기본값을 사용합니다.

- **스플릿 터널:** 스플릿 터널링을 활성화하려면 선택합니다.VPN 터널을 통해 이동할 트래픽을 지정하는 데 사용됩니다.여기서는 스플릿 터널을 사용합니다.
- **Split Tunnel Table(터널 분할 테이블):**VPN 클라이언트에서 VPN을 통해 액세스할 수 있는 네트워크를 입력합니다.이 예에서는 RV345P LAN 네트워크를 사용합니다.



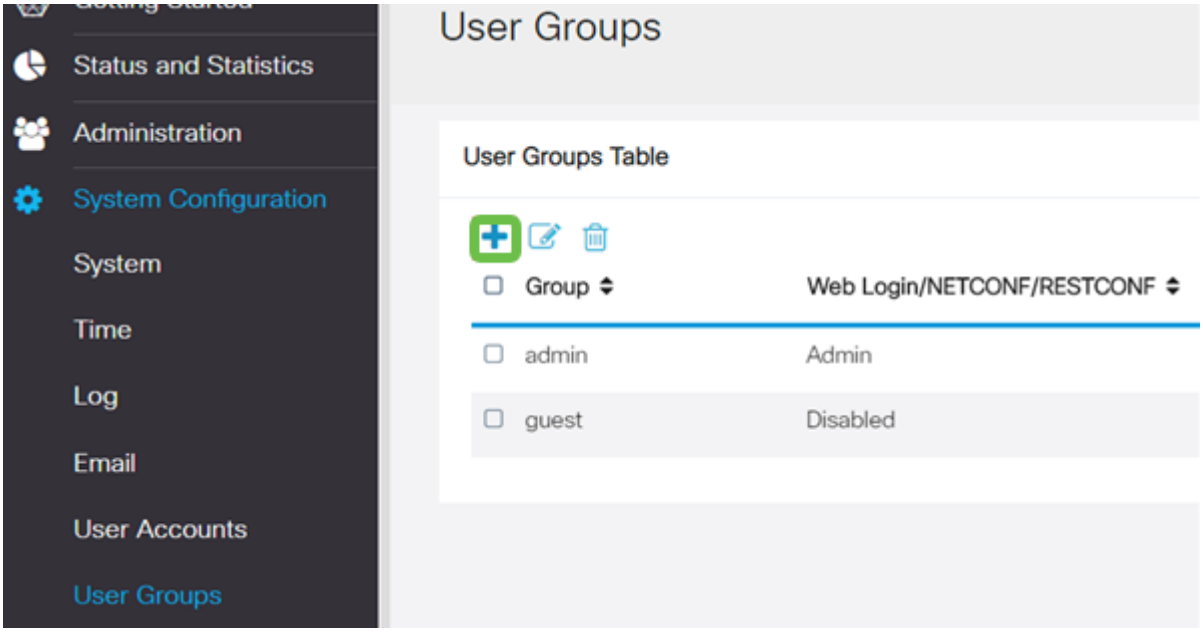
7단계

Save(**저장**)를 클릭한 후 IPsec Client-to-**Site Groups(IPsec 클라이언트-사이트 그룹**) 목록**에서 Profile(프로필)을 볼 수 있습니다**.



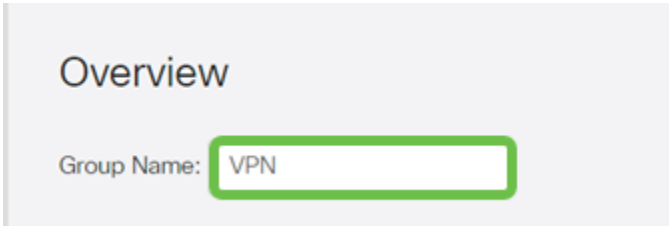
8단계

VPN **클라이언트** 사용자 인증에 사용할 사용자 그룹을 구성합니다.System **Configuration(시스템 컨피그레이션) > User Groups(사용자 그룹**)에서 **더하기 아이콘**을 클릭하여 사용자 그룹을 추가합니다.



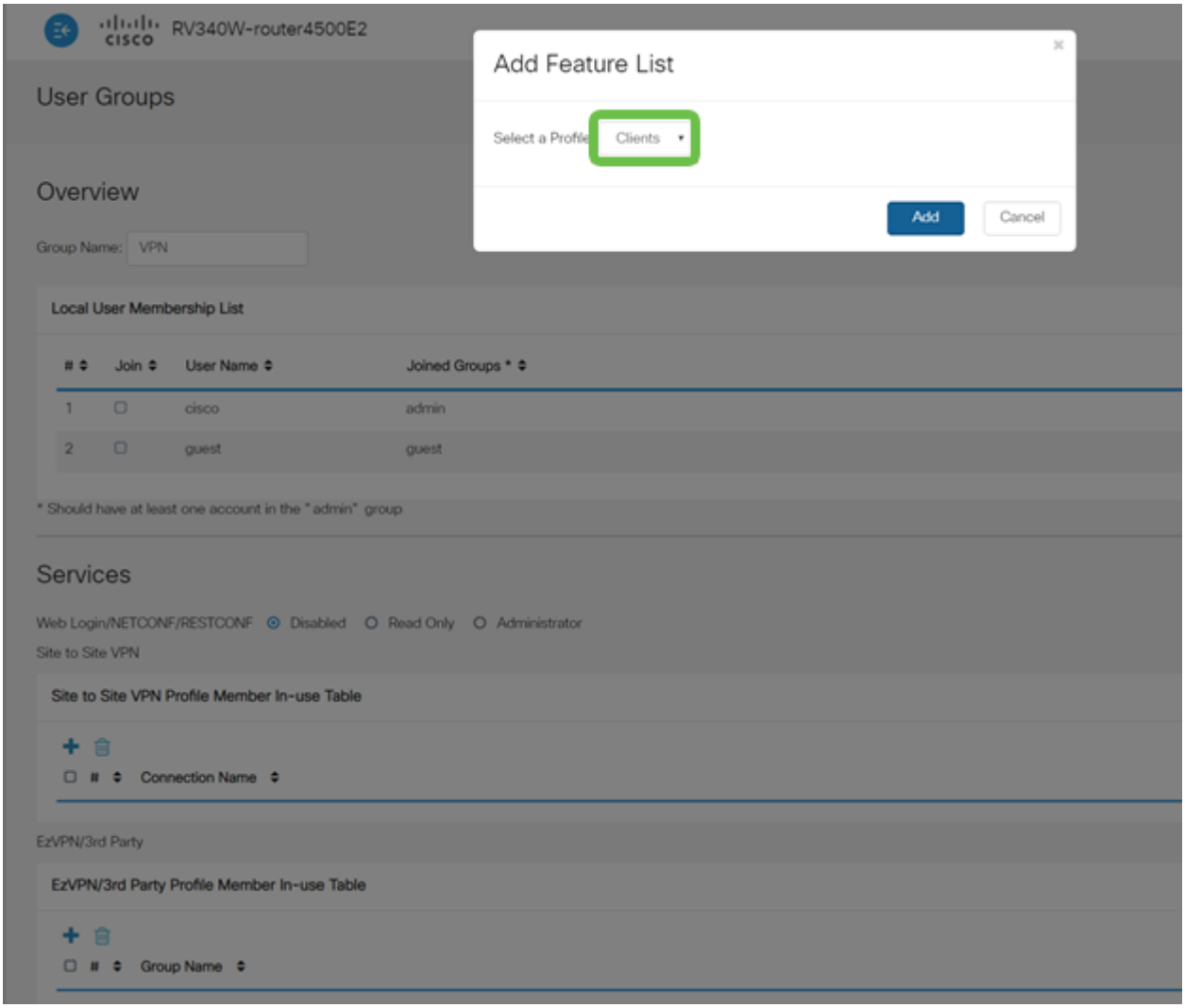
9단계

그룹 이름을 **입력합니다**.



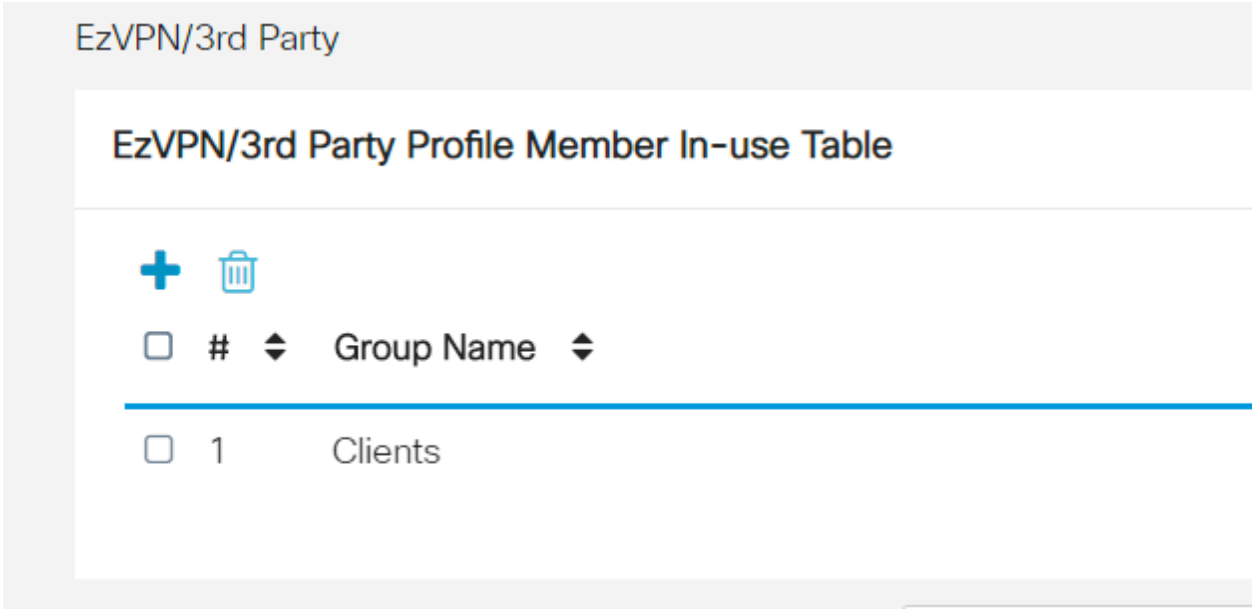
10단계

Services(**서비스**) > EzVPN/**제3자**에서 Add(**추가**)**를** 클릭하여 이 사용자 그룹을 이전에 구성된 **Client-to-Site** Profile(클라이언트-사이트 간 프로필)에 연결합니다.



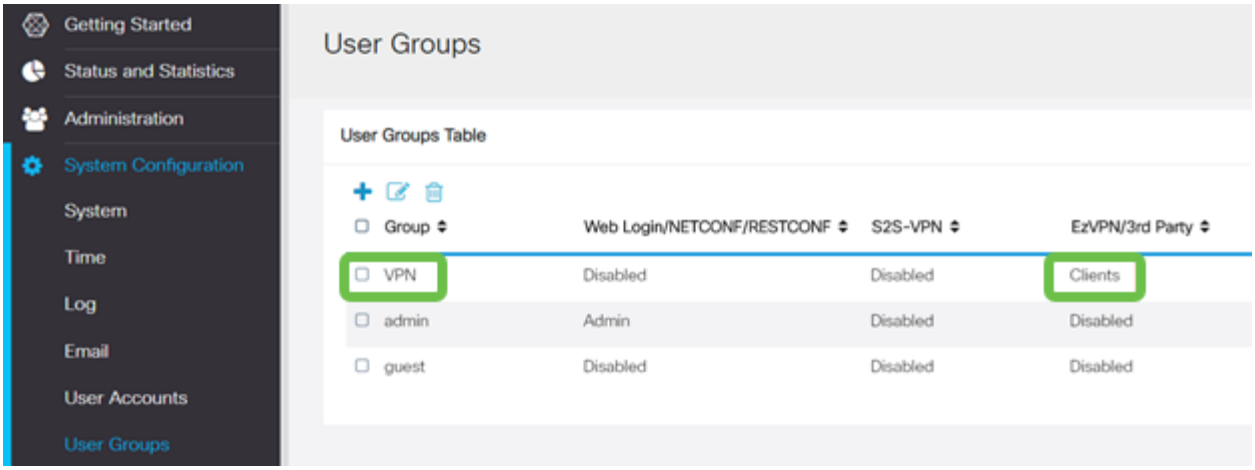
11단계

이제 EzVPN/**타사의** 목록에 Client-to-Site 그룹 이름**이 표시됩니다.**



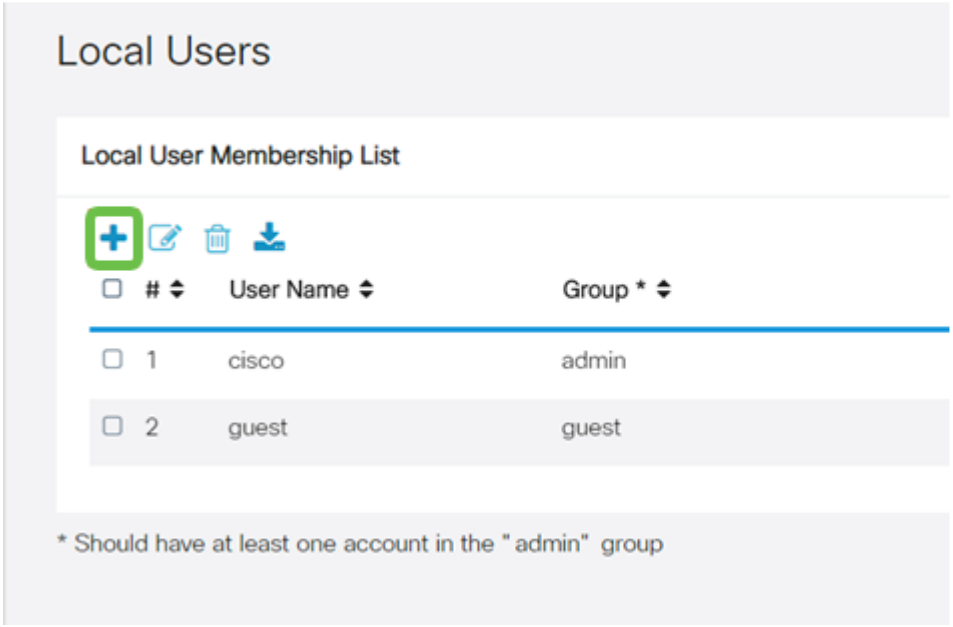
12단계

사용자 그룹 컨피그레이션**을 적용한** 후 **사용자 그룹** 목록에 이 컨피그레이션이 표시되고 새 사용자 그룹이 이전에 생성한 클라이언트-사이트 프로필과 함께 사용됩니다.



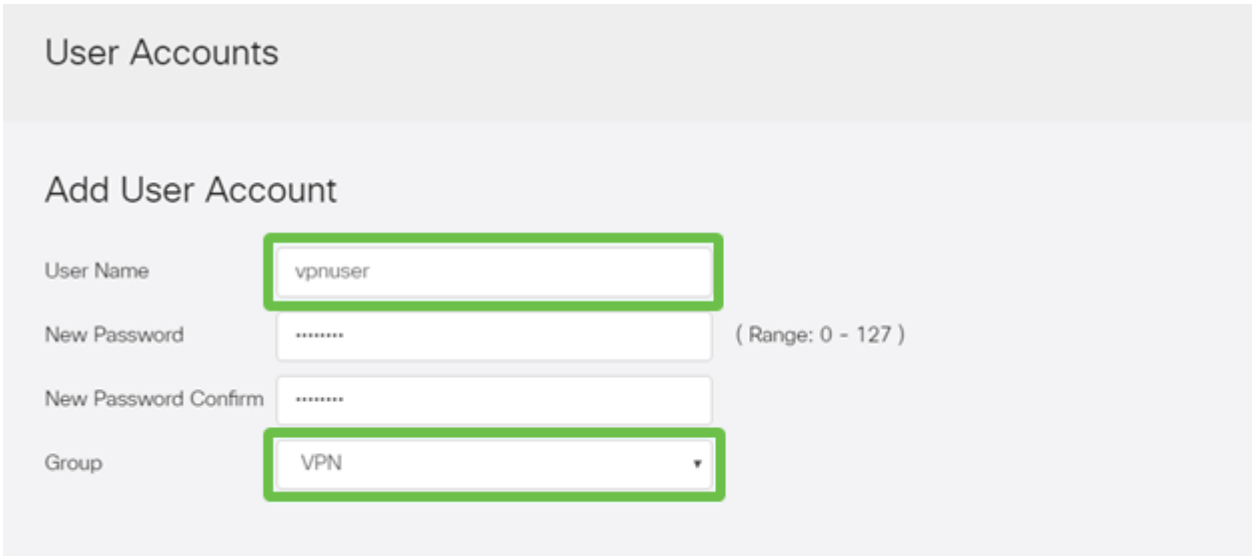
13단계

System Configuration(시스템 컨피그레이션) **> User Accounts(사용자 계정)**에서 새 사용자**를 구성합니다.더하기 아이콘**을 클릭하여 새 사용자를 생성합니다.



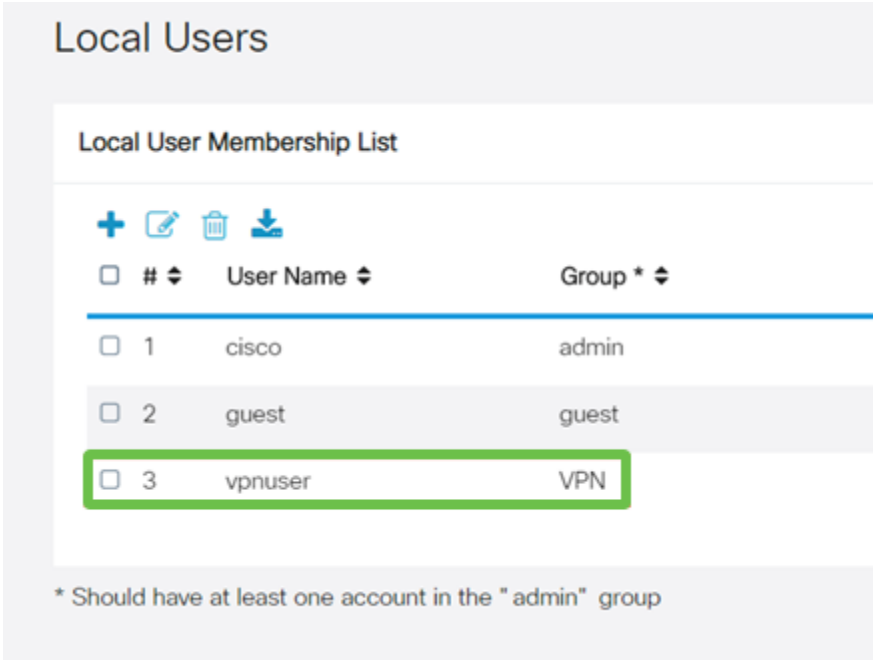
14단계

새 **사용자 이름**과 **새 비밀번호를 입력합니다.그룹**이 방금 구성한 새 **사용자 그룹**으로 설정되어 있는지 확인합니다.완료되면 **Apply**를 클릭합니다.



15단계

새 **사용자**가 **로컬 사용자** 목록에 **표시됩니다**.



이렇게 하면 RV345P Series 라우터의 컨피그레이션이 완료됩니다.다음으로 Shrew Soft VPN 클라이언트를 구성합니다.

shrew Soft VPN 클라이언트 구성

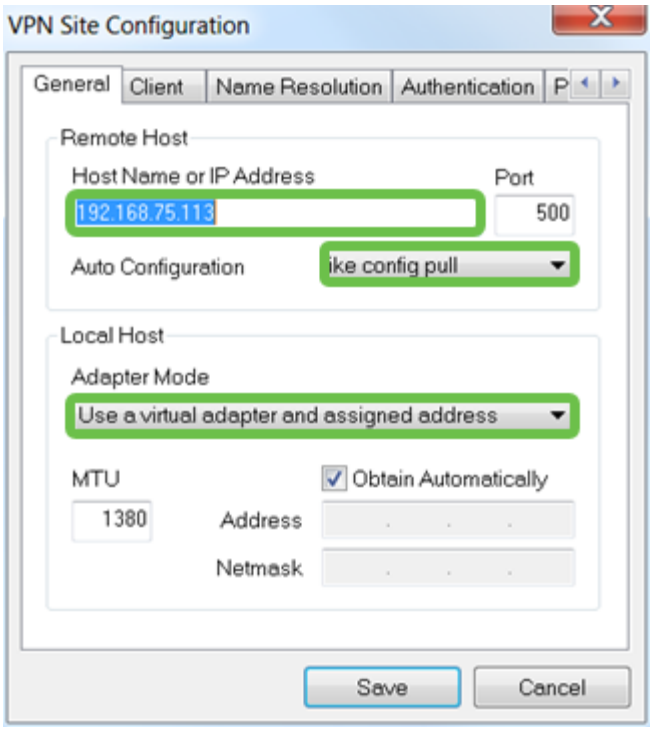
다음 단계를 수행합니다.

1단계

Shrew Soft *VPN Access Manager*를 열고 **Add**(**추가**)를 클릭하여 프로필을 추가합니다.나타나는 *VPN Site Configuration(VPN 사이트 컨피그레이션*) 창에서 General(**일반**) 탭을 구성합니다.

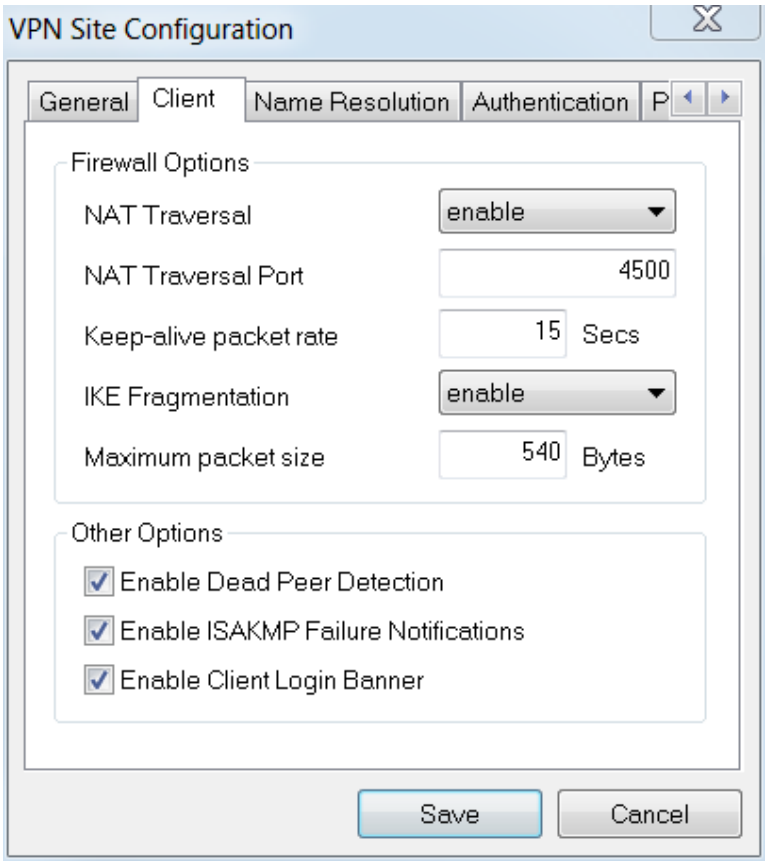
- **호스트 이름 또는 IP 주소**:WAN IP 주소(또는 RV345P의 호스트 이름)를 사용합니다.
- **자동 구성**:ike config pull 선택

- 어댑터 모드:가상 어댑터 및 할당된 주소 사용을 선택합니다.



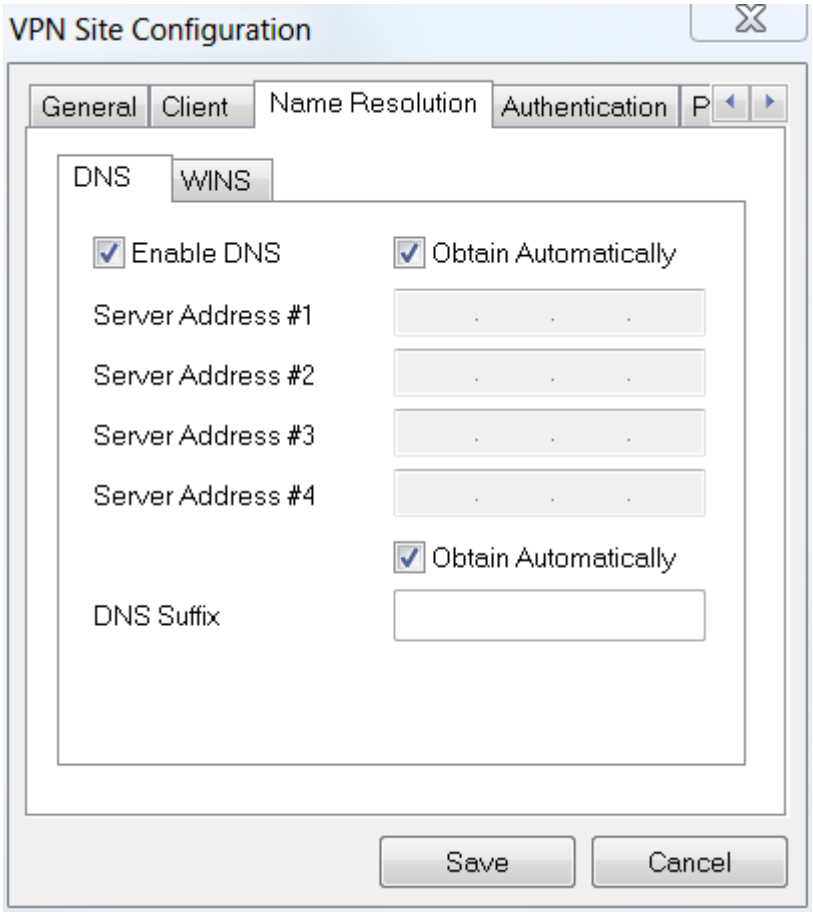
2단계

Client(클라이언트) 탭을 **구성합니다**.이 예제에서는 기본 설정을 유지했습니다.



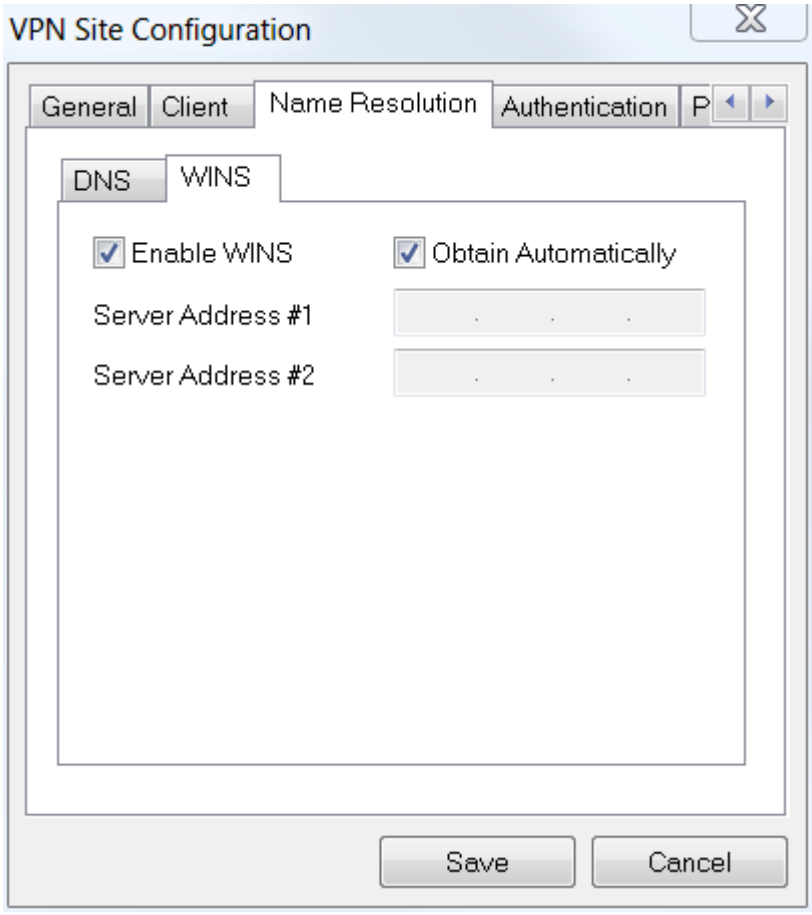
3단계

Name **Resolution(이름 확인) > DNS**에서 **Enable DNS(DNS 활성화)** 확인란을 선택하고 Obtain Automatically(**자동 가져오기**) 확인란을 선택한 상태로 둡니다.



4단계

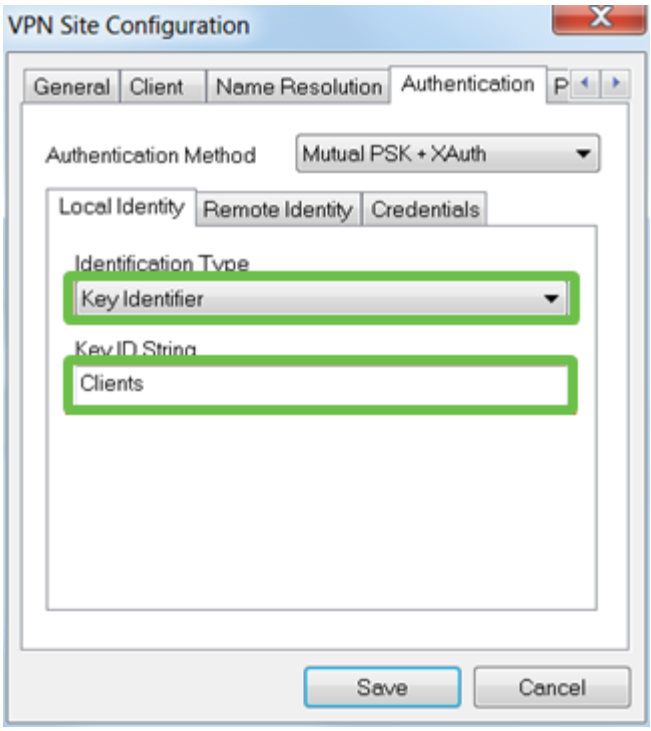
Name Resolution(**이름 확인**) > **WINS 탭에서 Enable WINS(WINS 활성화**) 상자를 선택하고 Obtain Automatically(자동 가져오기) 확인란을 선택한 상태로 둡니다.



5단계

Authentication **> Local Identity를 클릭합니다**.

- **식별 유형**:키 **식별자 선택**
- **키 ID 문자열**:RV345P에 구성된 **그룹 이름**을 입력합니다.

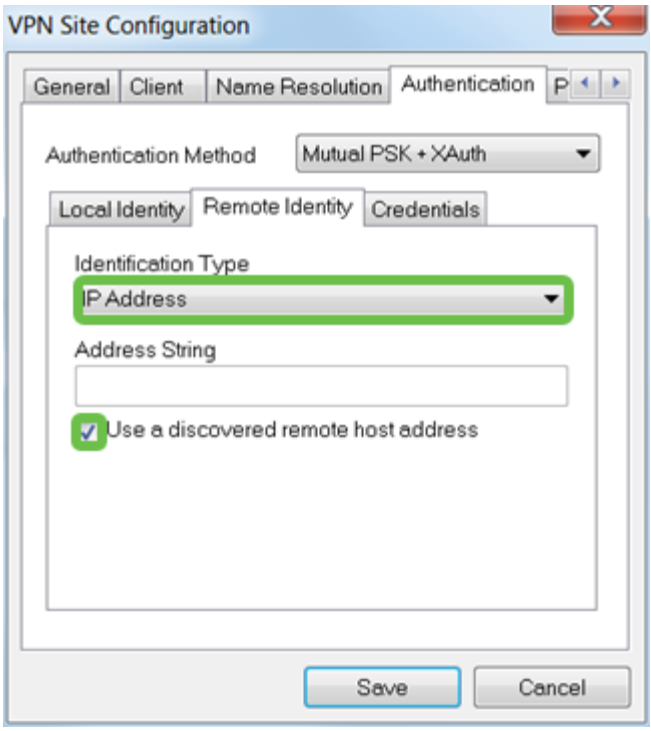


6단계

Authentication(**인증**) **> Remote Identity(원격 ID)에서**.이 예제에서는 기본 설정을 유지했

습니다.

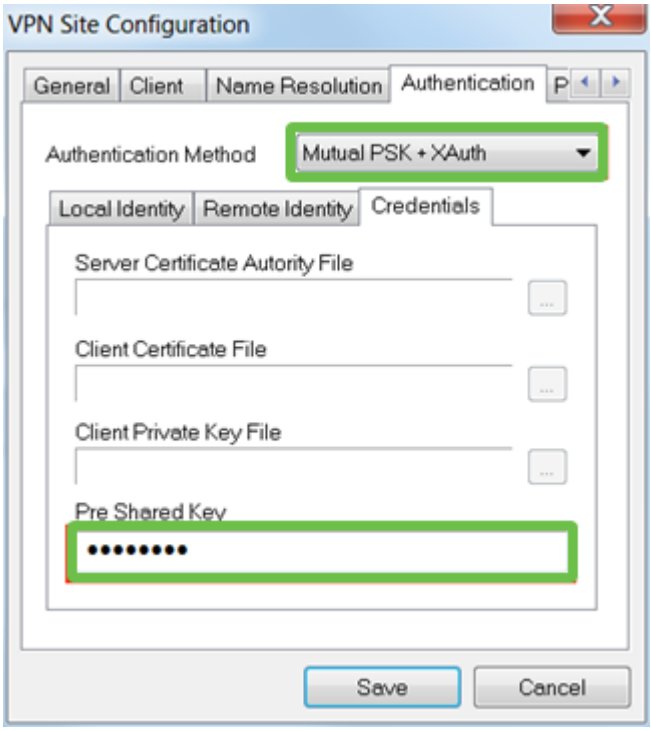
- **식별 유형**:IP 주소
- **주소 문자열**:<공백>
- **검색된 원격 호스트 주소** 상자 사용:선택



7단계

Authentication(**인증**) > **Credentials(자격 증명**)에서 다음을 구성합니다.

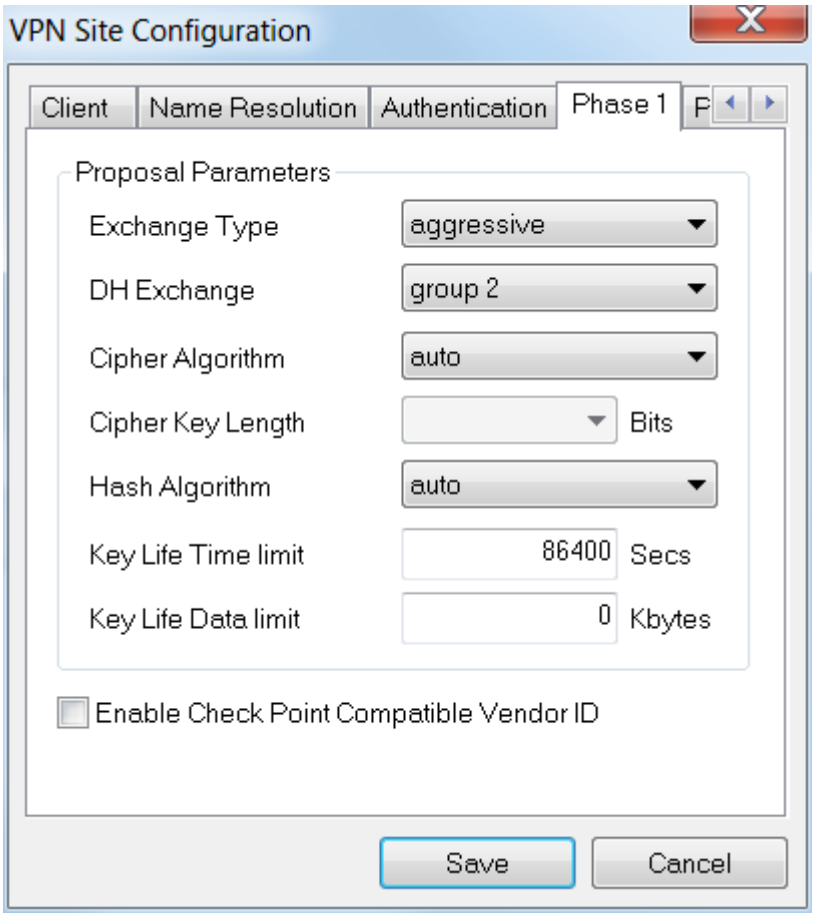
- **인증 방법**:상호 **PSK + XAuth 선택**
- **사전 공유 키**:RV345P 클라이언트 프로파일**에** 구성된 사전 공유 키를 입력합니다.



8단계

Phase 1 탭이 예에서는 기본 설정이 유지되었습니다.

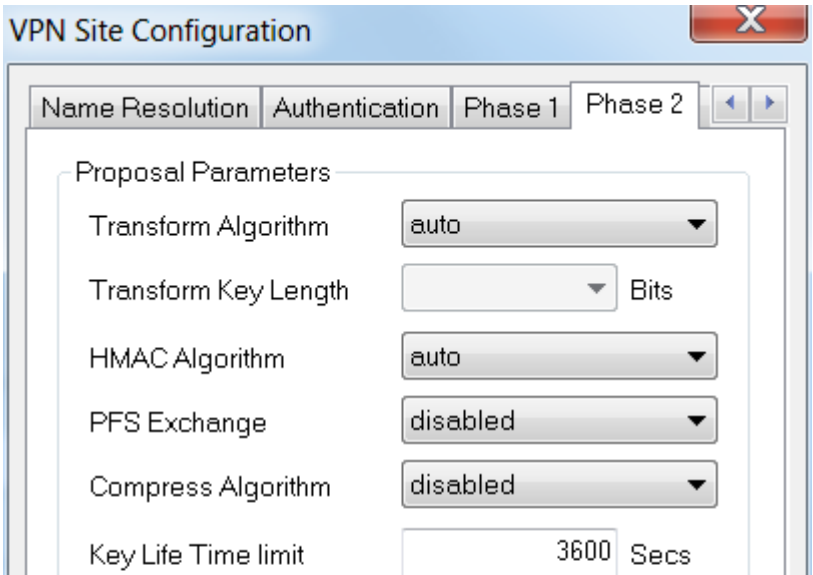
- **Exchange 유형:** 적극적인
- **DH Exchange:** 그룹 2
- **암호 알고리즘:** 자동
- **해시 알고리즘:** 자동



9단계

이 예에서 **단계 2** 탭의 기본값은 동일하게 유지되었습니다.

- **변환 알고리즘:** 자동
- **HMAC 알고리즘:** 자동
- **PFS Exchange:** 사용 안 함
- **압축 알고리즘:** 사용 안 함

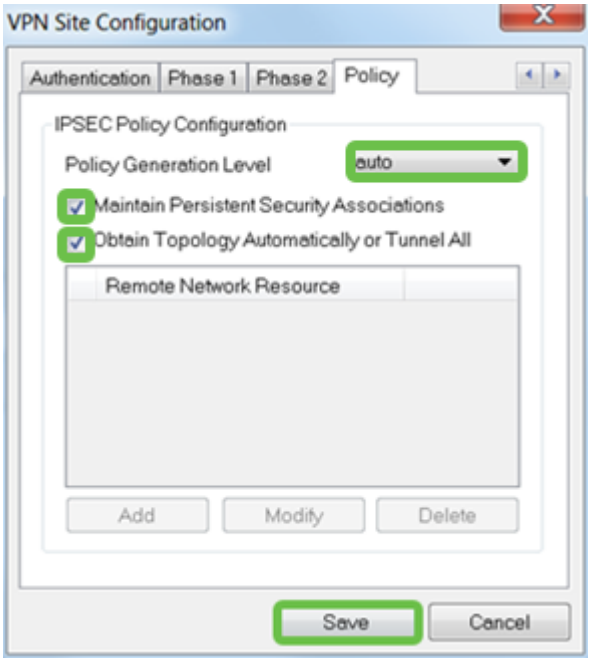


10단계

Policy 탭 예에 다음 설정을 사용했습니다.

- **정책 생성 레벨:** 자동
- **영구 보안 연결 유지:** 선택
- **토폴로지 자동 가져오기 또는 모두 터널:** 선택

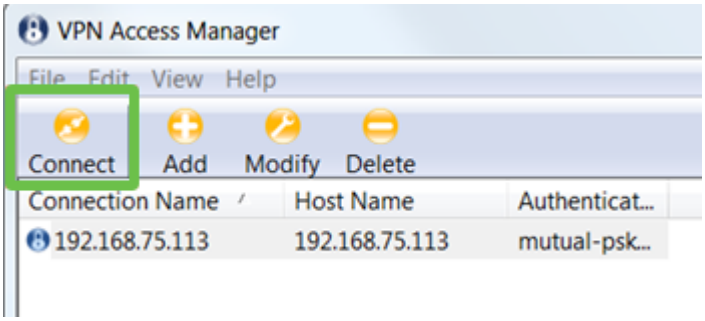
RV345P에서 **스플릿 터널링**을 구성했으므로 여기서 구성할 필요가 없습니다.



완료되면 **저장**을 클릭합니다.

11단계

이제 연결을 테스트할 준비가 되었습니다.*VPN Access Manager*에서 연결 프로파일을 강조 표시하고 Connect(**연결**) 버튼을 클릭합니다.

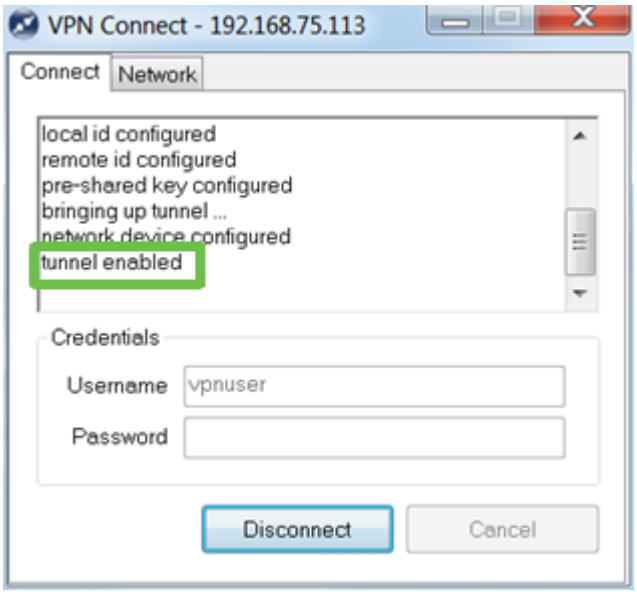


12단계

표시되는 **VPN Connect** 창에서 RV345P(13 및 14단계)에서 생성한 **User Account**의 자격 증명을 사용하여 **Username** 및 **Password**(사용자 이름 및 비밀번호)를 입력합니다. 완료되면 **연결**을 클릭합니다.

13단계

터널이 연결되어 있는지 확인합니다.**터널**이 **활성화되었음을** 확인해야 합니다.



Shrew Soft가 이 컨피그레이션의 예로 사용되었습니다.shrew Soft는 Cisco 제품이 아니므로 기술 지원이 필요한 경우 이 서드파티에 문의하십시오.

기타 VPN 옵션

VPN을 사용하기 위한 다른 옵션이 있습니다.자세한 내용을 보려면 다음 링크를 클릭하십시오.

- GreenBow VPN 클라이언트를 사용하여 RV34x Series 라우터와 연결
- RV34x Series 라우터에서 Teleworker VPN 클라이언트 구성
- Rv34x Series 라우터에서 PPTP(Point-to-Point Tunneling Protocol) 서버 구성
- RV34x Series 라우터에서 IPsec(Internet Protocol Security) 프로파일 구성
- RV34x 라우터에서 L2TP WAN 설정 구성

- RV34x에서 Site-to-Site VPN 구성

RV345P 라우터의 보충 구성

VLAN 구성(선택 사항)

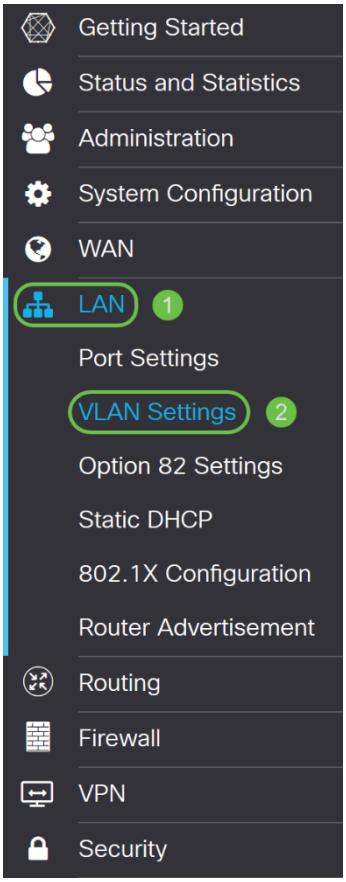
VLAN(Virtual Local Area Network)을 사용하면 LAN(Local Area Network)을 서로 다른 브로드캐스트 도메인으로 논리적으로 분할할 수 있습니다.네트워크에서 민감한 데이터를 브로드캐스트할 수 있는 시나리오에서는 특정 VLAN에 브로드캐스트를 지정하여 보안을 강화하기 위해 VLAN을 생성할 수 있습니다.또한 VLAN을 사용하여 불필요한 대상으로 브로드캐스트 및 멀티캐스트를 보낼 필요가 없으므로 성능을 높일 수 있습니다.VLAN을 생성할 수 있지만, VLAN이 하나 이상의 포트에 수동으로 또는 동적으로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

추가 지침을 보려면 VLAN 모범 사례 및 보안 팁을 참조하십시오.

VLAN을 생성하지 않으려면 다음 섹션으로 건너뛸 수 있습니다.

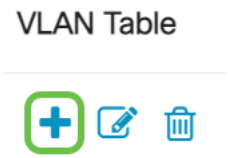
1단계

LAN > VLAN Settings(VLAN 설정)로 이동합니다.



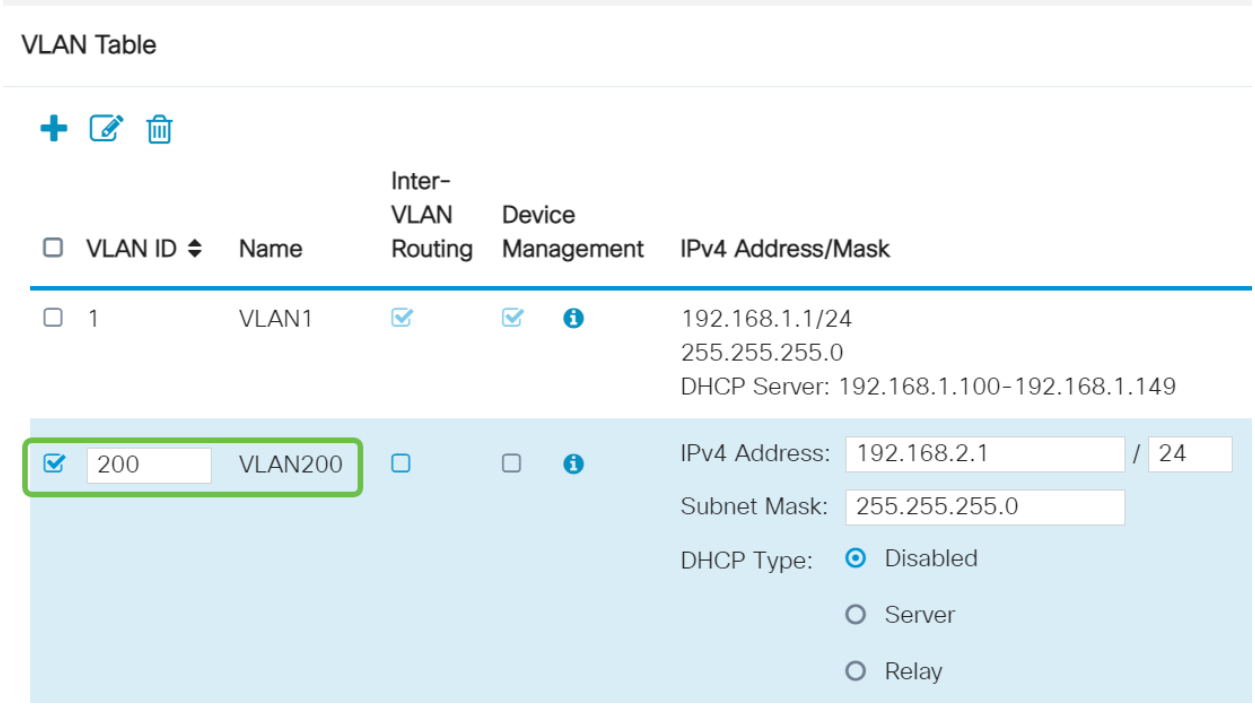
2단계

추가 **아이콘**을 클릭하여 새 VLAN을 생성합니다.



3단계

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



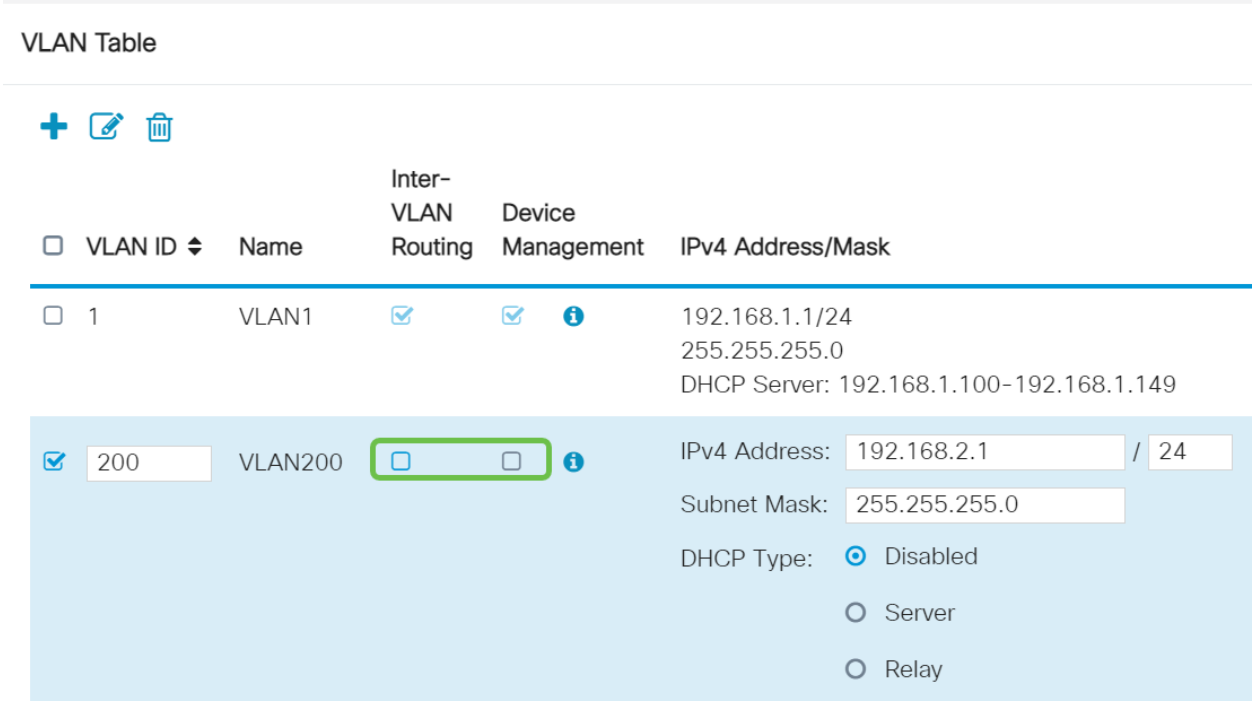
4단계

Inter-VLAN Routing 및 *Device Management* 모두에 대해 Enabled(활성화됨) *상자*를 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.

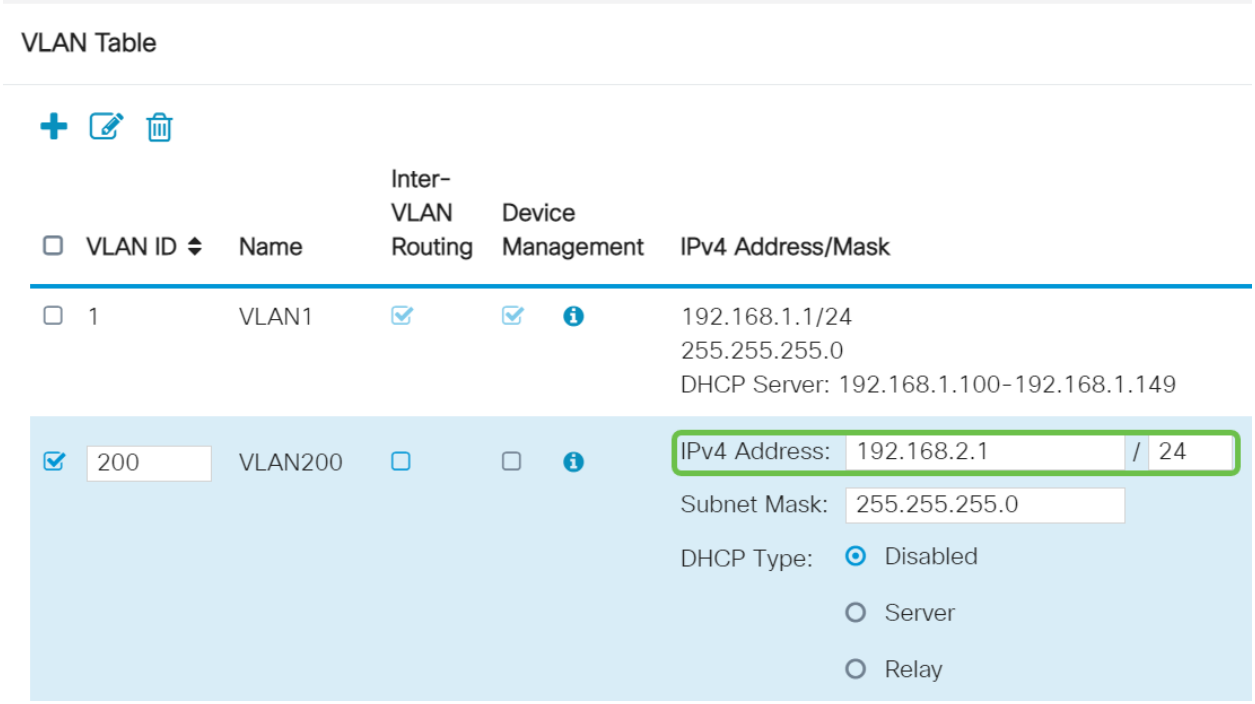
Device Management는 브라우저를 사용하여 VLAN에서 RV345P의 웹 UI에 로그인하고 RV345P를 관리할 수 있는 소프트웨어입니다.게스트 네트워크에서도 비활성화되어야 합니다.

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



5단계

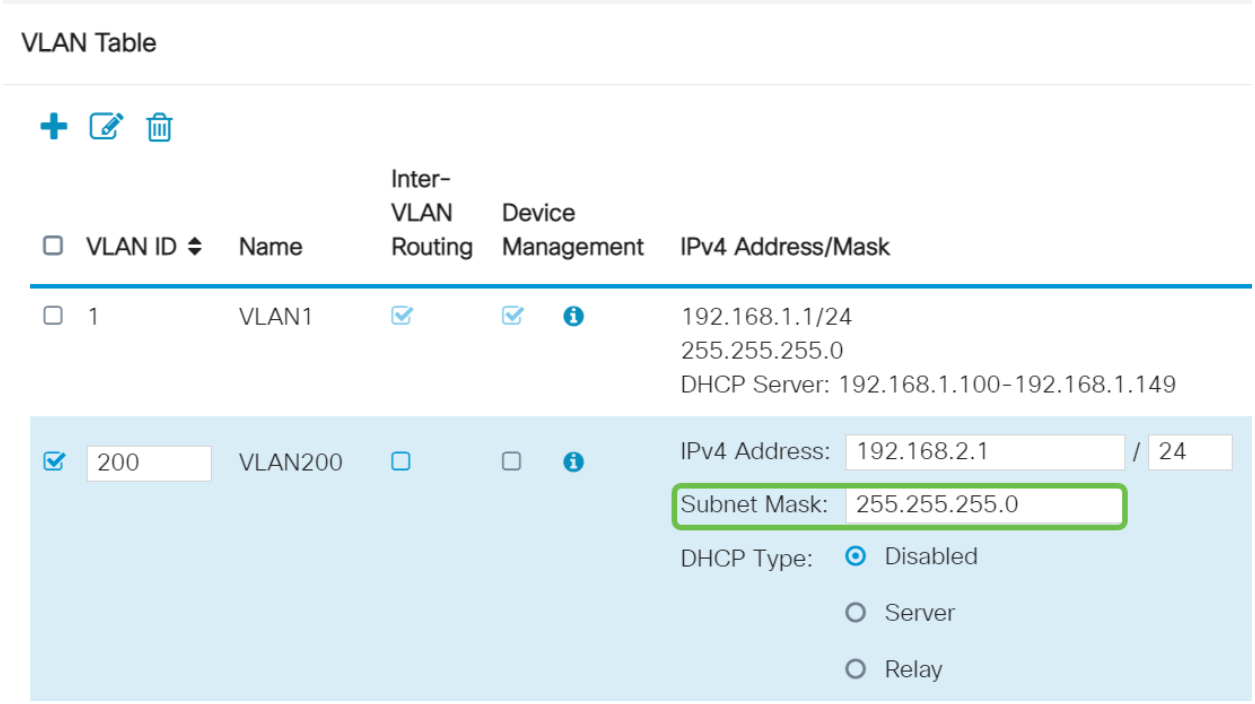
프라이빗 IPv4 주소가 *IP Address* 필드에 자동으로 채워집니다.이 옵션을 선택하면 조정할 수 있습니다.이 예에서는 서브넷에 DHCP에 사용할 수 있는 192.168.2.100-192.168.2.149 IP 주소가 있습니다.192.168.2.1-192.168.2.99 및 192.168.2.150-192.168.2.254은 고정 IP 주소에 사용할 수 있습니다.



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**.



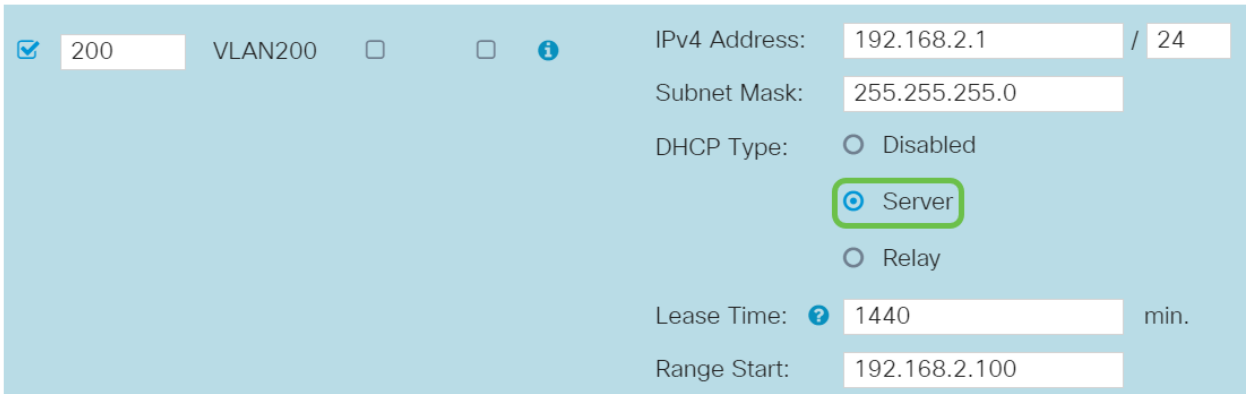
7단계

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.

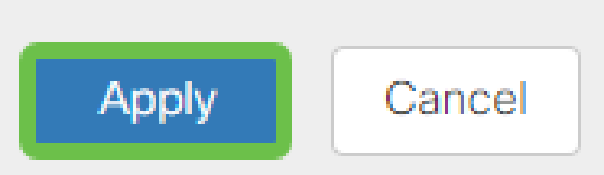
서버 - 가장 자주 사용하는 옵션입니다.

- 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(선택 사항)

16개의 VLAN은 RV345P에서 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 해제될 수 있습니다.트렁크에서 원하지 않는 VLAN은 제외해야 합니다.

하나의 VLAN에 고유한 포트가 할당되었습니다.

- 액세스 포트로 간주됩니다.
- 이 포트에 할당된 VLAN에는 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:

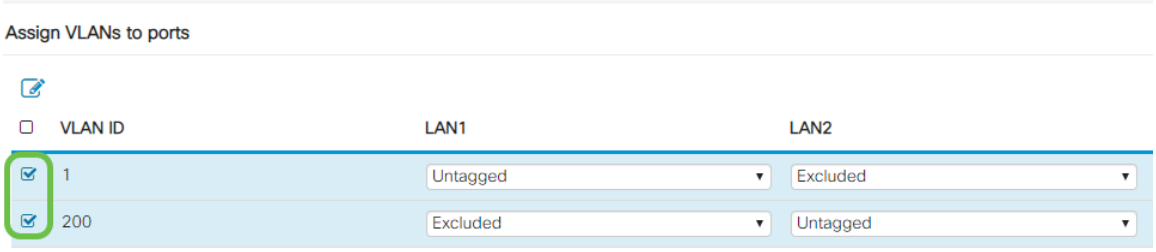
- 트렁크 포트로 간주됨
- VLAN 중 하나에 Untagged(태그 없음)라는 레이블이 지정될 수 있습니다.
- 트렁크 포트의 일부인 나머지 VLAN에 Tagged라는 레이블이 지정되어야 합니다.
- 트렁크 포트에 속하지 않은 VLAN은 해당 포트에 대해 Excluded(제외) 레이블이 지정되어야 합니다.

이 예에서는 트렁크가 없습니다.

1단계

수정할 *VLAN ID*를 선택합니다.

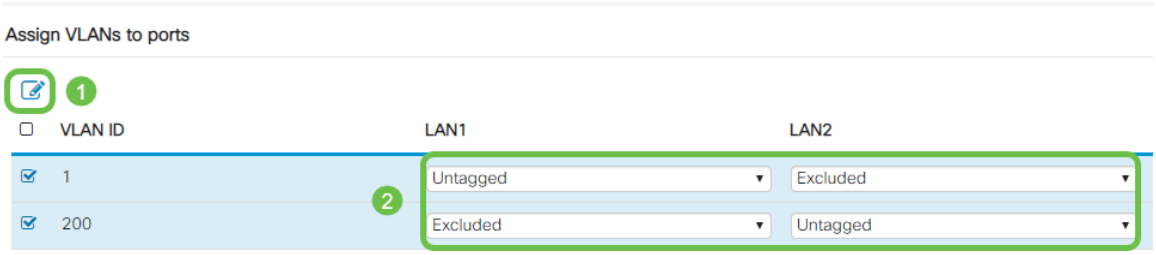
이 예에서는 *VLAN 1*과 VLAN *200을* 선택했습니다.



2단계

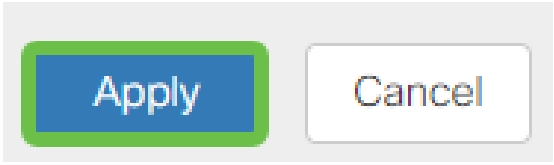
Edit(**수정**)를 클릭하여 LAN 포트에 VLAN을 할당하고 각 설정을 Tagged(태그), Untagged(태그 *없음*) 또는 Excluded(*제외됨*)로 *지정합니다*.

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**.



3단계

Apply(**적용**)를 클릭하여 컨피그레이션을 저장합니다.



이제 새 VLAN을 생성하고 RV345P의 포트에 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.

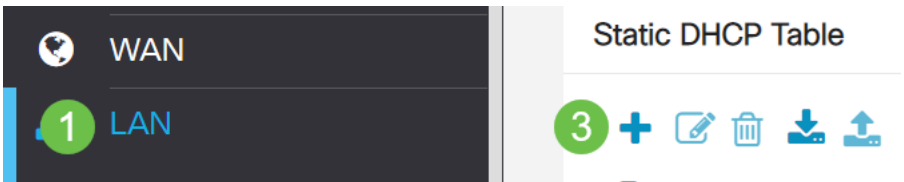
고정 IP 추가(선택 사항)

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 이동할 수 있습니다.

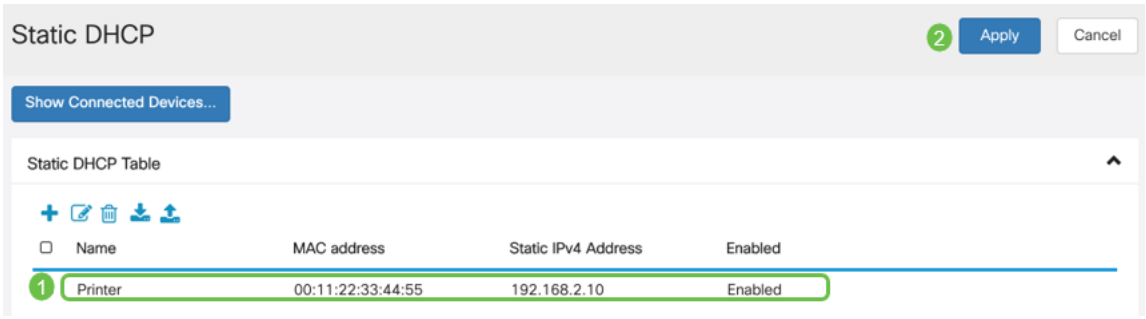
1단계

LAN > Static DHCP로 이동합니다.더하기 아이콘을 클릭합니다.



2단계

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



인증서 관리(선택 사항)

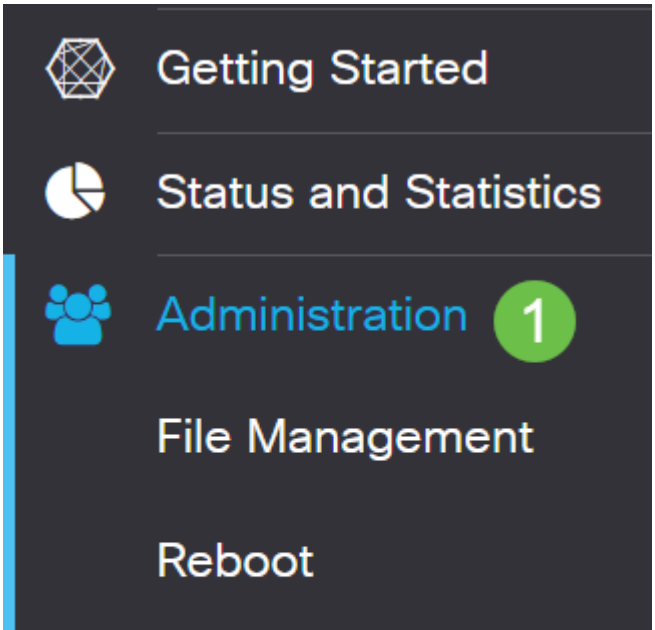
디지털 인증서는 인증서의 명명된 주체에 의해 공개 키의 소유권을 인증합니다.이렇게 하면 신뢰 당사자가 인증된 공개 키에 해당하는 개인 키가 만든 서명 또는 어설션에 의존할 수 있습니다.라우터는 네트워크 관리자가 생성한 인증서인 자체 서명 인증서를 생성할 수 있습니다.또한 디지털 ID 인증서를 신청하기 위해 CA(Certificate Authority)에 요청을 보낼 수 있습니다.타사 애플리케이션의 합법적인 인증서를 보유하는 것이 중요합니다.

인증에 CA(Certificate Authority)가 사용됩니다.인증서는 다양한 서드파티 사이트에서 구매할 수 있습니다.이는 귀하의 사이트가 안전하다는 것을 증명하는 공식적인 방법입니다.기본적으로 CA는 신뢰할 수 있는 소스이며, 사용자가 합법적인 비즈니스인지 확인하고 신뢰할 수 있는지 확인합니다.필요에 따라 최소한의 비용으로 인증서를 생성합니다.CA에서 체크 아웃한 후, 해당 정보가 확인되면 사용자에게 인증서를 발급합니다.이 인증서는 컴퓨터에서 파일로 다운로드할 수 있습니다.그런 다음 라우터(또는 VPN 서버)로 이동하여 업로드할 수 있습니다.

CSR/인증서 생성

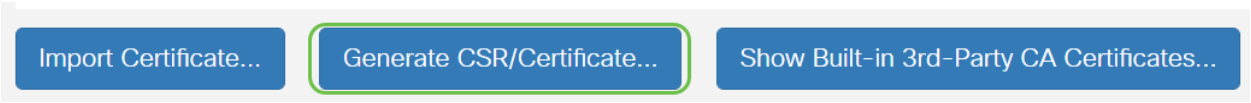
1단계

라우터의 웹 기반 유틸리티에 로그인하고 Administration(관리) **> Certificate(인증서)를** 선택합니다.



2단계

Generate **CSR/Certificate를 클릭합니다**.CSR/인증서 생성 페이지로 이동합니다.

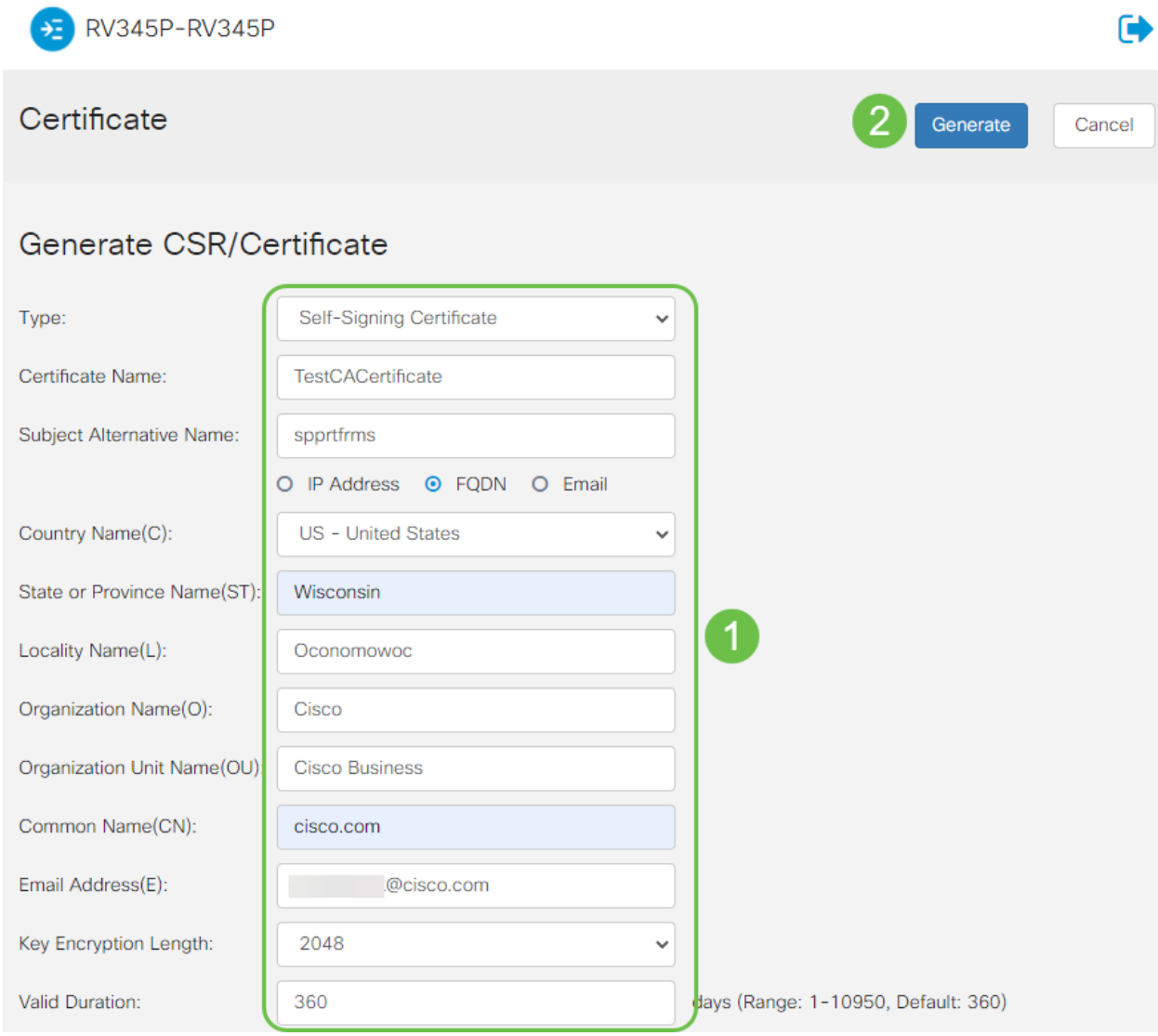


3단계

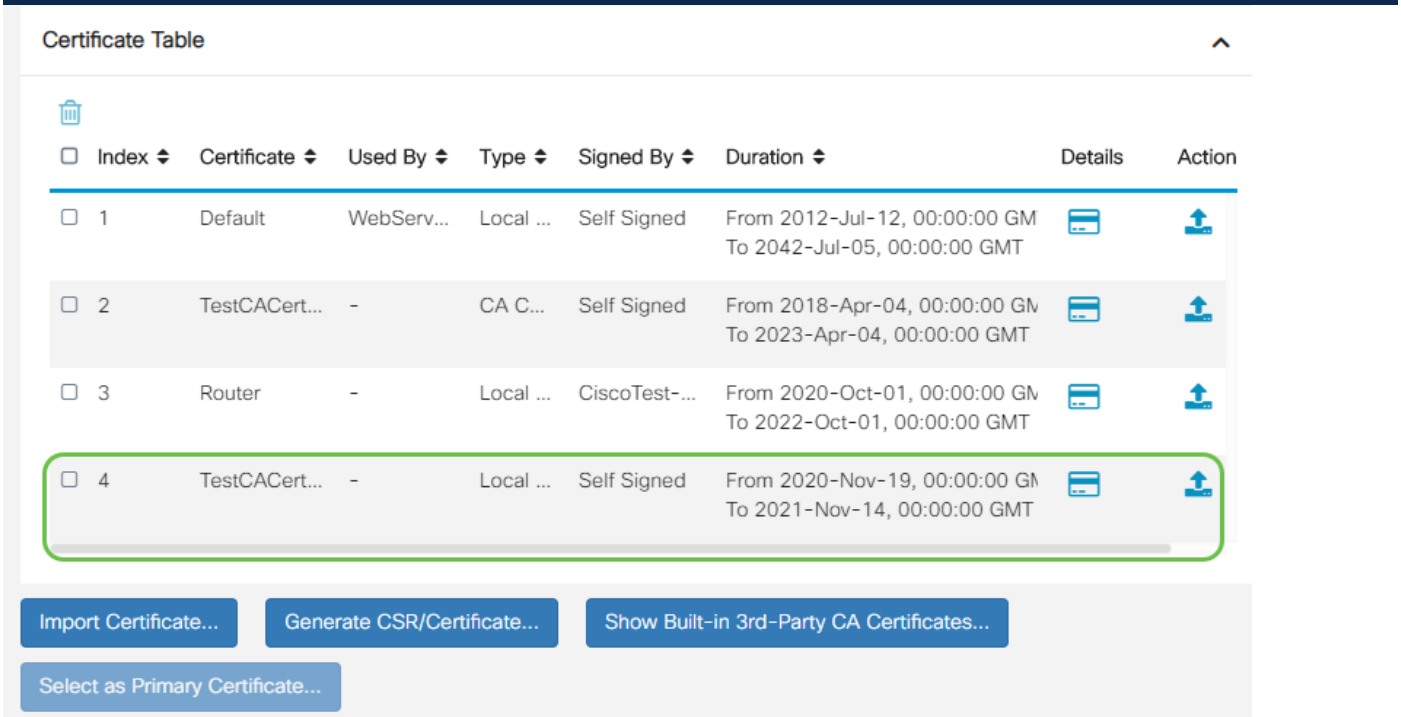
상자에 다음을 입력합니다.

- 적절한 인증서 유형 선택
  - 자체 서명 인증서 — 자체 작성자가 서명한 SSL(Secure Socket Layer) 인증서입니다.이 인증서는 신뢰할 수 없습니다. 개인 키가 공격자에 의해 보안된 경우 취소할 수 없습니다.
  - Certified Signing Request — PKI(Public Key Infrastructure)로서 디지털 ID 인증서를 신청하기 위해 인증 기관에 전송됩니다.개인 키가 비밀로 유지되므로 자체 서명보다 안전합니다.
- Certificate Name 필드에 인증서 이름을 입력하여 요청을 식별합니다.이 필드는 공백이거나 공백과 특수 문자를 포함할 수 없습니다.
- (선택 사항) Subject Alternative Name(주체 대체 이름) 영역에서 라디오 버튼을 클릭합니다.옵션은 다음과 같습니다.
  - IP 주소 — 인터넷 프로토콜(IP) 주소를 입력합니다.
  - FQDN — FQDN(정규화된 도메인 이름)을 입력합니다.
  - 이메일 — 이메일 주소를 입력합니다.

- Subject Alternative Name 필드에 FQDN을 입력합니다.
- Country Name(국가 이름) 드롭다운 목록에서 귀하의 조직이 합법적으로 등록된 국가 이름을 선택합니다.
- State or Province Name(ST) 필드에 조직이 있는 주, 도, 지역 또는 지역의 이름이나 약어를 입력합니다.
- 조직이 등록되거나 Locality Name(구/군/시) 필드에 있는 구/군/시의 이름을 입력합니다.
- 사업체가 법적으로 등록된 이름을 입력합니다.소기업 또는 단독 소유자로 등록하는 경우 Organization Name 필드에 인증서 요청자의 이름을 입력합니다.특수 문자는 사용할 수 없습니다.
- 조직 단위 이름 필드에 이름을 입력하여 조직 내의 부서를 구분합니다.
- Common Name 필드에 이름을 입력합니다.이 이름은 인증서를 사용하는 웹 사이트의 정규화된 도메인 이름이어야 합니다.
- 인증서를 생성하려는 사람의 이메일 주소를 입력합니다.
- Key Encryption Length 드롭다운 목록에서 키 길이를 선택합니다.옵션은 512, 1024 및 2048입니다.키 길이가 클수록 인증서의 보안이 강화됩니다.
- Valid Duration 필드에 인증서가 유효한 일 수를 입력합니다.기본값은 360입니다.
- Generate를 **클릭합니다**.



생성된 인증서가 이제 인증서 테이블에 나타납니다.

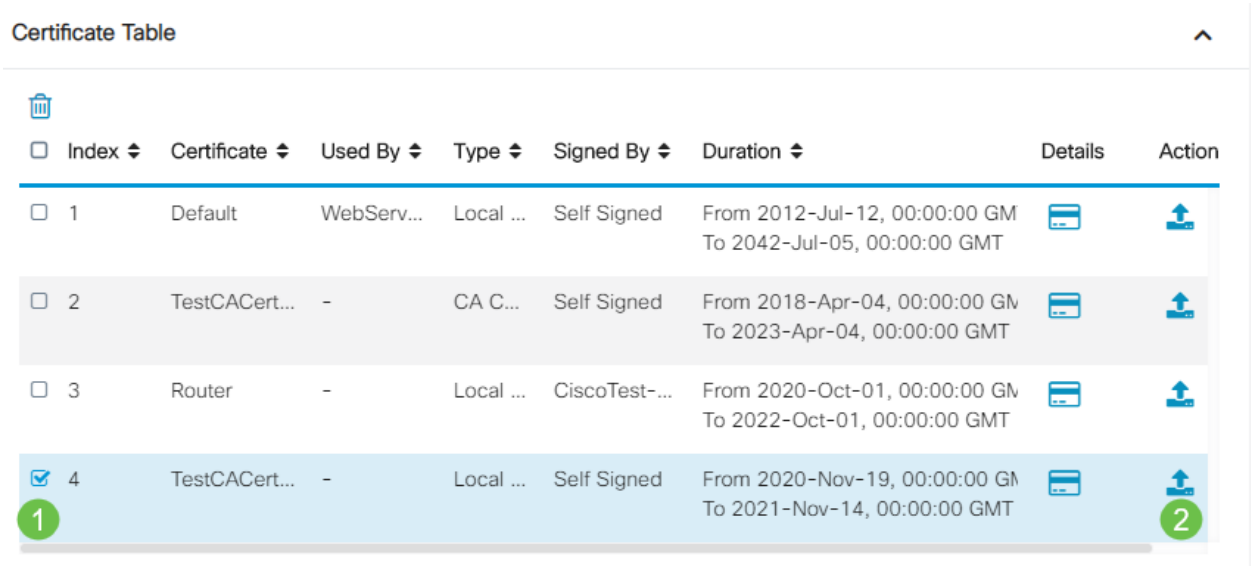


이제 RV345P 라우터에 인증서를 생성했습니다.

인증서 내보내기

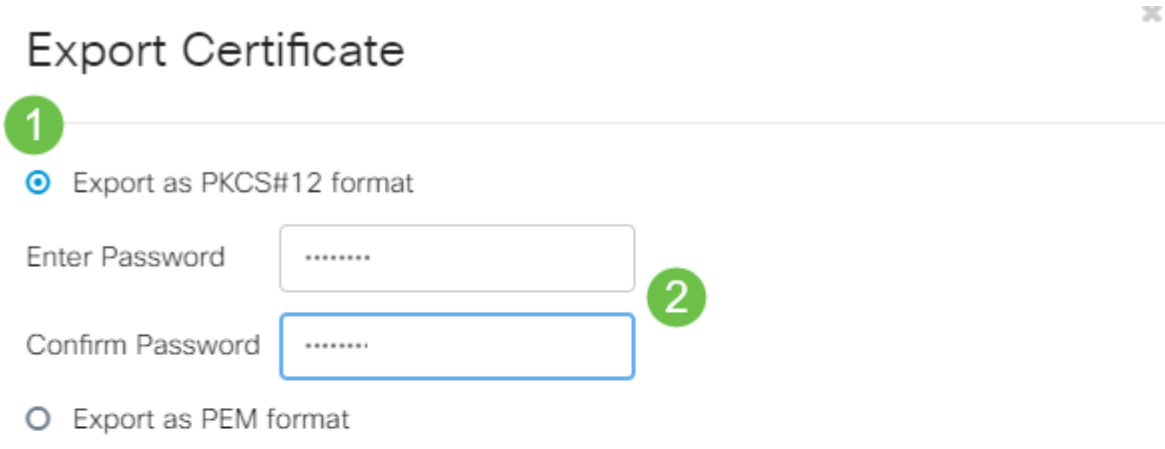
1단계

인증서 테이블에서 내보낼 인증서의 확인란을 선택하고 **내보내기 아이콘**을 클릭합니다.



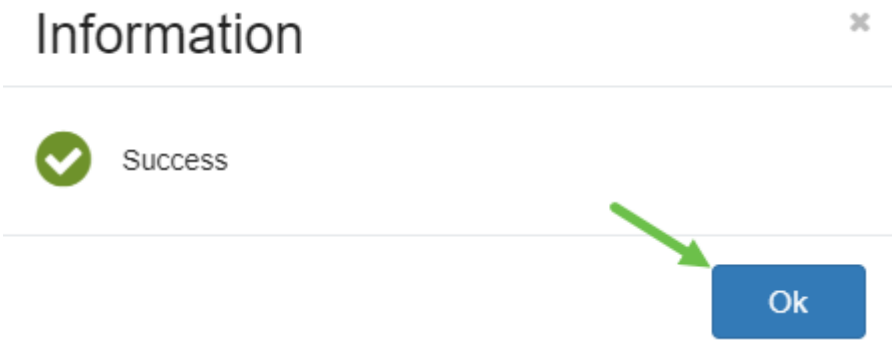
2단계

- 인증서를 내보내려면 형식을 클릭합니다.옵션은 다음과 같습니다.
  - PKCS #12 — PKCS(Public Key Cryptography Standards) #12은 .p12 확장자로 제공되는 내보낸 인증서입니다.내보내기, 가져오기 및 삭제되는 파일을 보호하기 위해 파일을 암호화하려면 암호가 필요합니다.
  - PEM — PEM(Privacy Enhanced Mail)은 메모장과 같은 간단한 텍스트 편집기를 사용하여 쉽게 읽을 수 있는 데이터로 변환할 수 있도록 웹 서버에 자주 사용됩니다.
- PEM을 선택한 경우 Export(내보내기)를 **클릭합니다**.
- Enter Password(비밀번호 입력) 필드에 내보낼 파일을 보호하기 위한 비밀번호를 입력합니다.
- Confirm Password 필드에 비밀번호를 다시 입력합니다.
- Select Destination(대상 선택) 영역에서 PC가 선택되었으며 현재 사용 가능한 유일한 옵션입니다.
- Export(내보내기)를 **클릭합니다**.



3단계

다운로드가 성공했음을 알리는 메시지가 다운로드 버튼 아래에 나타납니다.브라우저에서 파일이 다운로드되기 시작합니다.**확인**을 **클릭합니다**.

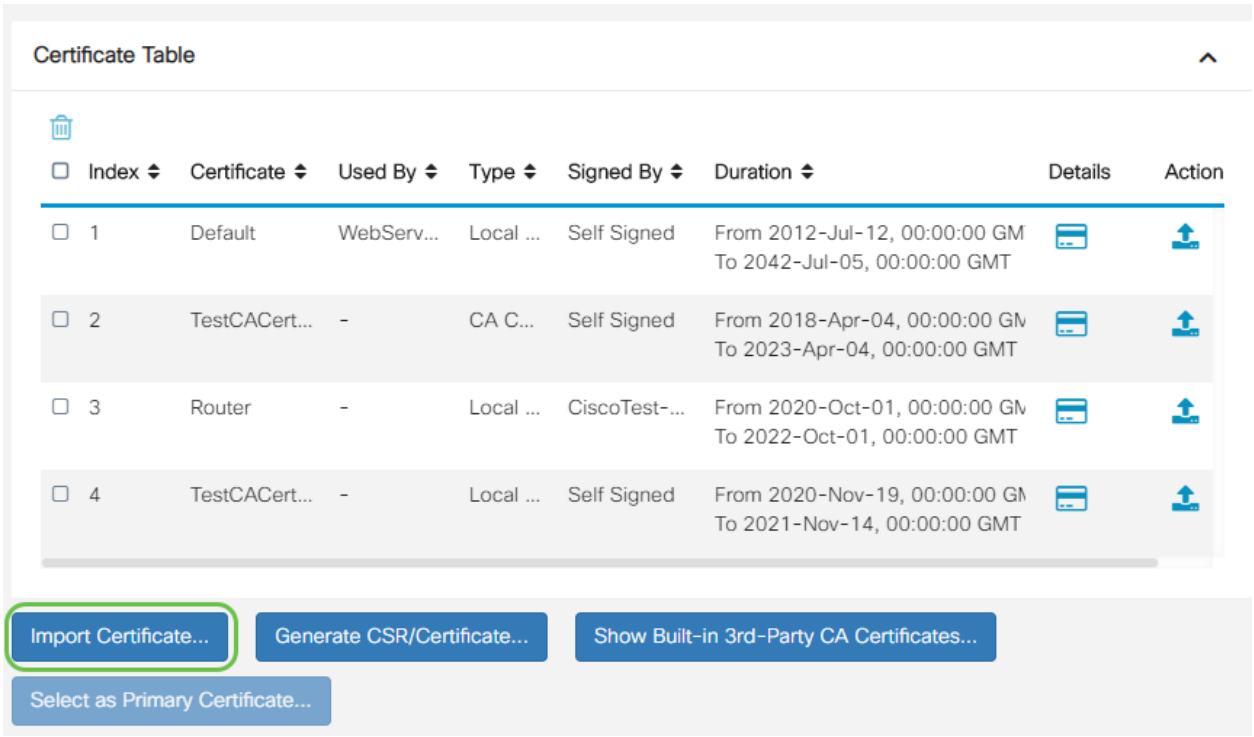


이제 RV345P Series 라우터에서 인증서를 성공적으로 내보냈어야 합니다.

인증서 가져오기

1단계

Import **Certificate..(인증서 가져오기...)를 클릭합니다**..



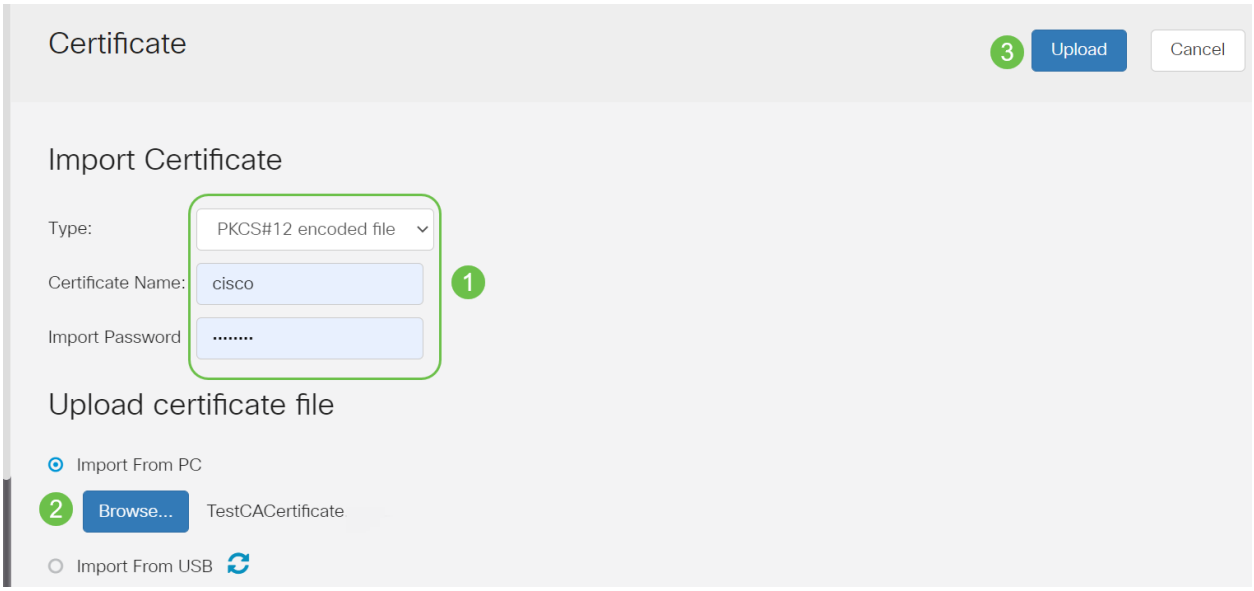
2단계

- 드롭다운 목록에서 가져올 인증서의 유형을 선택합니다.옵션은 다음과 같습니다.
  - 로컬 인증서 — 라우터에서 생성된 인증서.
  - CA 인증서 — 신뢰할 수 있는 서드파티 기관에서 인증한 인증서로서 인증서에 포함된 정보가 정확함을 확인했습니다.
  - PKCS #12 Encoded 파일 — PKCS(Public Key Cryptography Standards) #12은 서버 인증서를 저장하는 형식입니다.

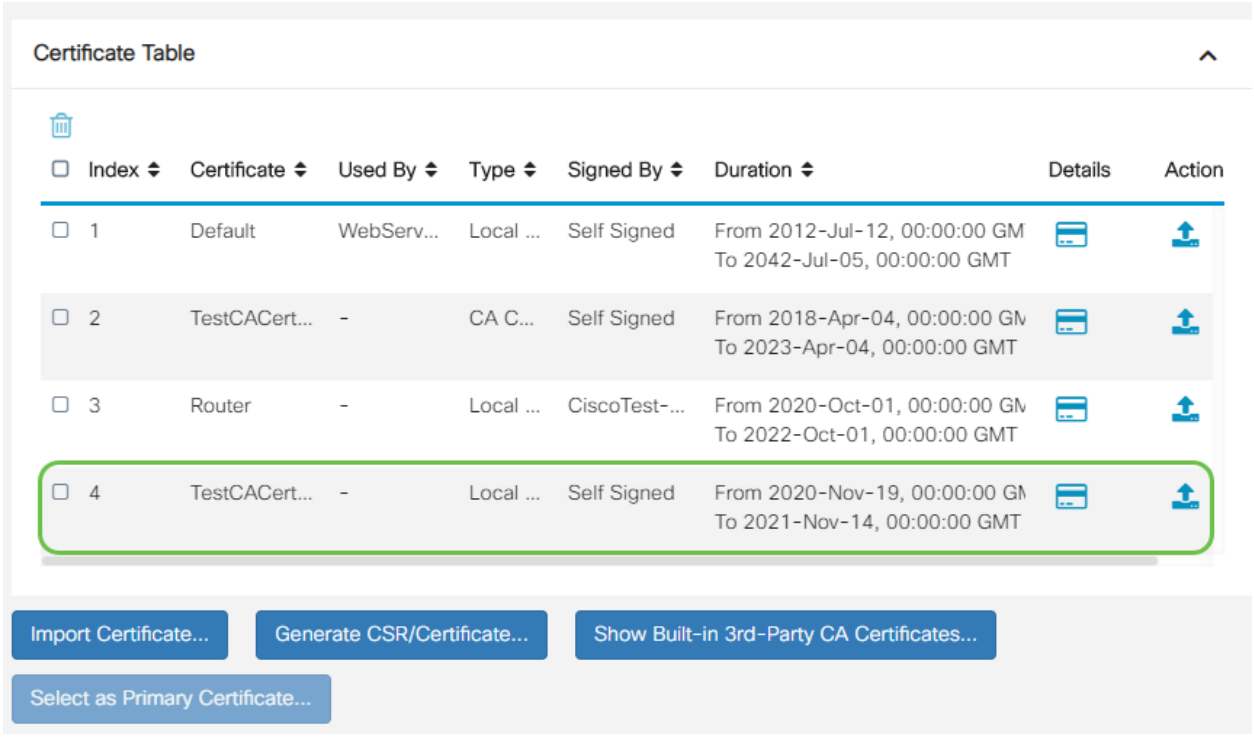
- Certificate Name(인증서 이름) 필드에 인증서 이름을 입력합니다.

- PKCS #12을 선택한 경우 Import Password 필드에 파일의 비밀번호를 입력합니다.그렇지 않으면 3단계로 건너뜁니다.
- 인증서를 가져오려면 소스를 클릭합니다.옵션은 다음과 같습니다.
    - PC에서 가져오기
    - USB에서 가져오기

- 라우터에서 USB 드라이브를 탐지하지 못하면 Import from USB(USB에서 가져오기) 옵션이 회색으로 표시됩니다.
- Import From USB(USB에서 가져오기)를 선택했는데 라우터에서 USB를 인식하지 못하는 경우 Refresh(새로 고침)를 클릭합니다.
- Choose File(파일 선택) 버튼을 클릭하고 적절한 파일을 선택합니다.
- Upload(**업로드)를 클릭합니다**.



성공하면 자동으로 기본 Certificate 페이지로 이동합니다.인증서 테이블이 최근에 가져온 인증서로 채워집니다.



이제 RV345P 라우터에서 인증서를 성공적으로 가져와야 합니다.

동글 및 RV345P Series 라우터를 사용하여 모바일 네트워크 구성(선택 사항)

동글 및 RV345P 라우터를 사용하여 백업 모바일 네트워크를 구성하려는 경우이 경우 동글을 사용하는 모바일 네트워크 구성 및 RV34x Series 라우터를 읽어야 합니다.

축하합니다. RV345P 라우터의 구성을 완료했습니다!이제 Cisco Business Wireless 디바이스를 구성합니다.

CBW140AC 구성

CBW140AC 발신

먼저 CBW140AC의 PoE 포트에서 RV345P의 PoE 포트에 이더넷 케이블을 연결합니다.RV345P의 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 RV345x 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.

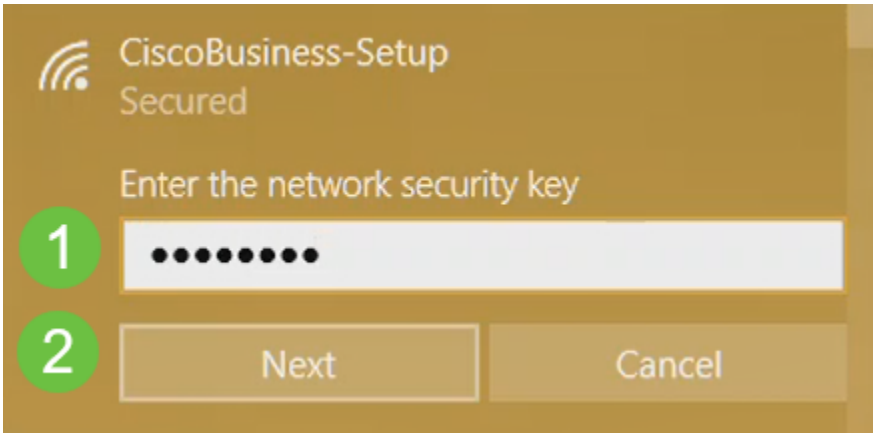
1단계

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.

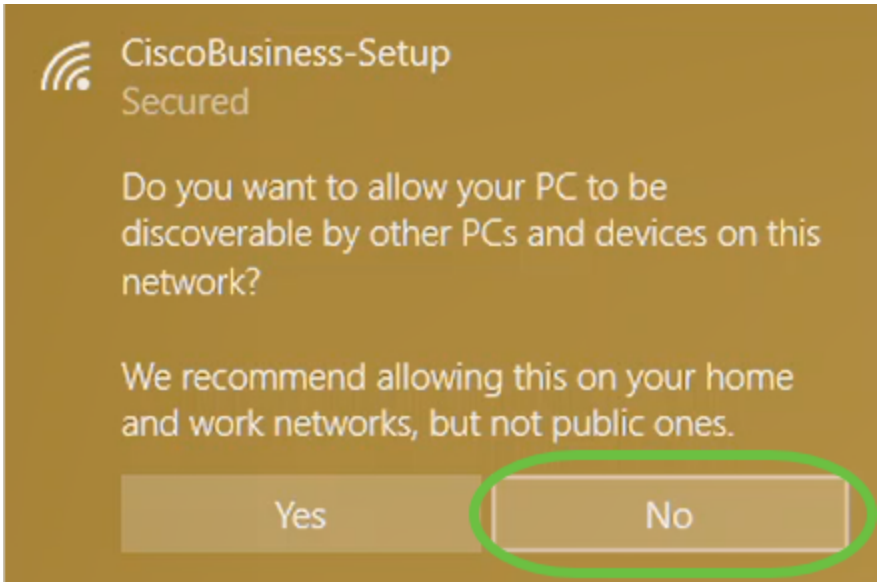
2단계

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



3단계

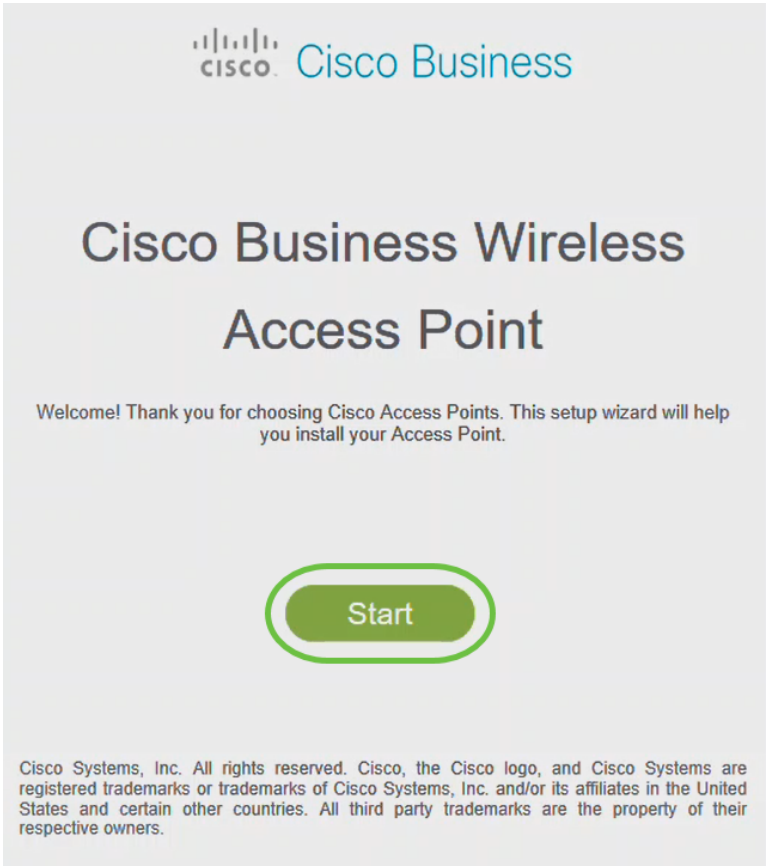
다음 화면이 표시됩니다.한 번에 하나의 디바이스만 구성할 수 있으므로 **No**를 클릭합니다.



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.

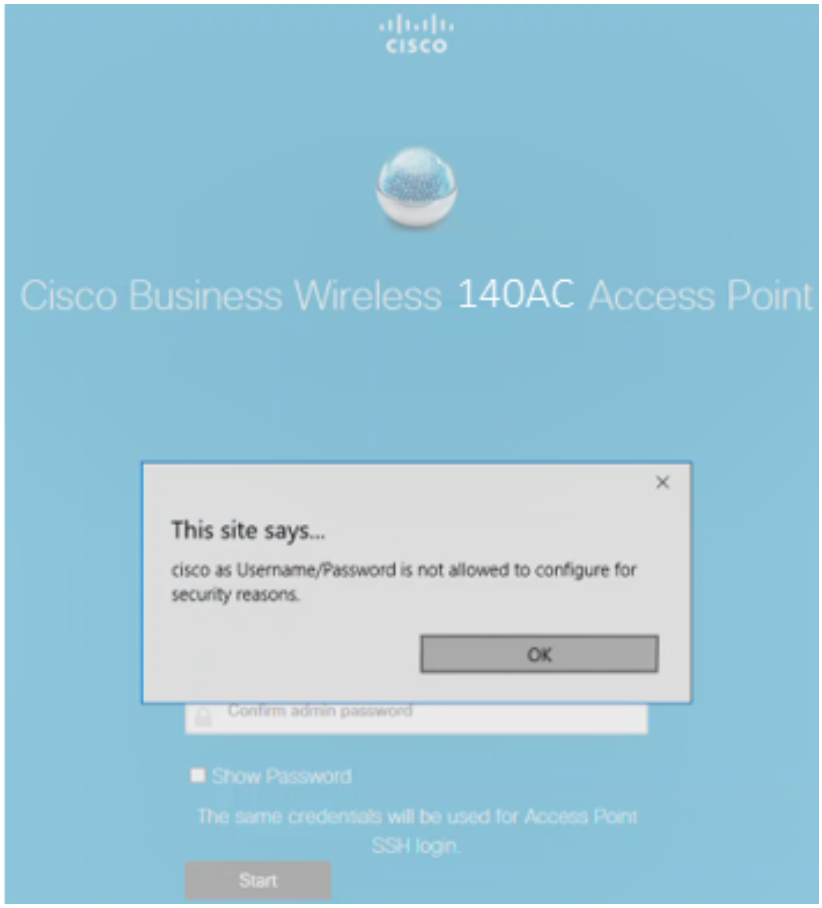
5단계

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**.

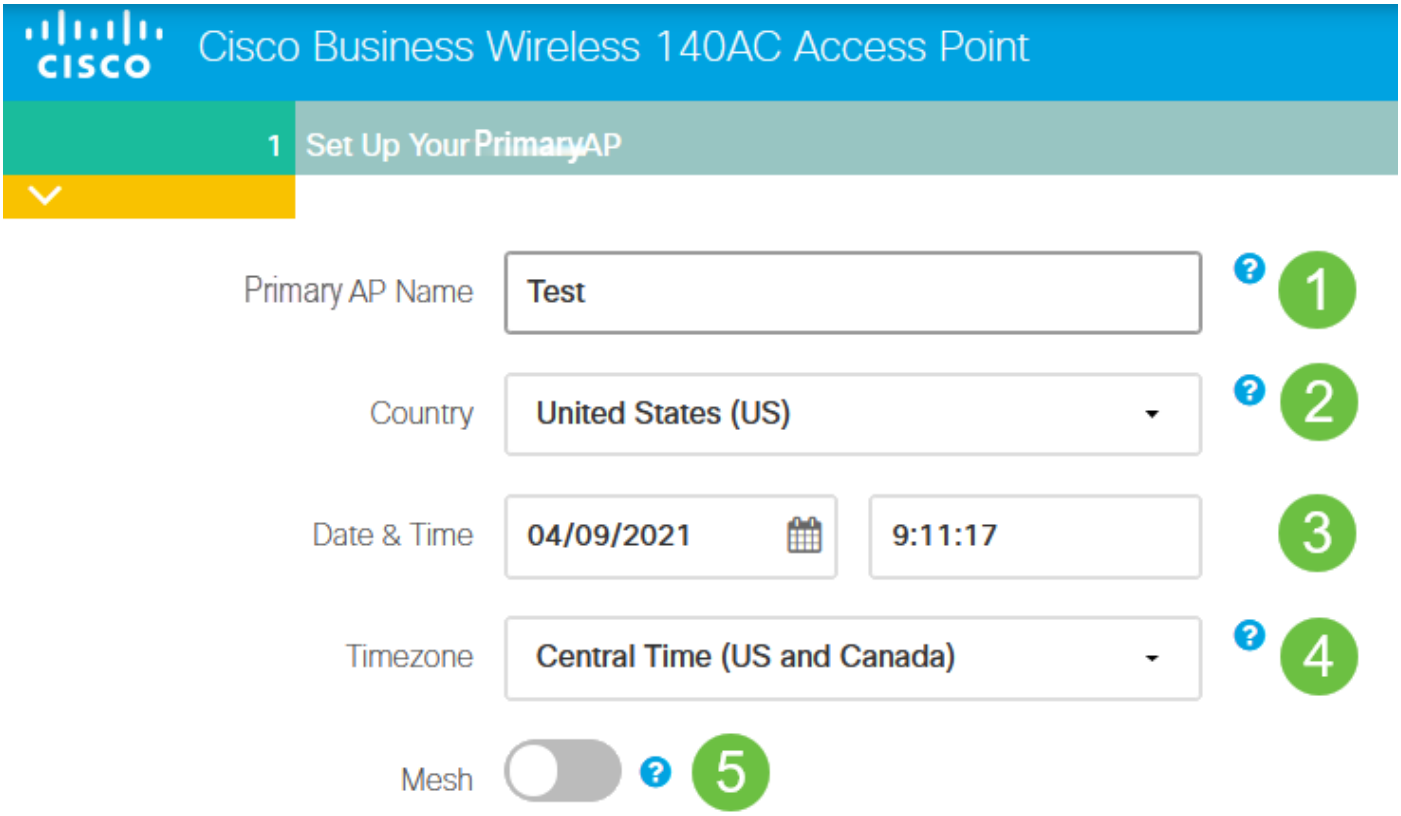
cisco 또는 사용자 이름 또는 비밀번호 필드에서 이를 사용하지 마십시오.이렇게 하면 아래와 같은 오류 메시지가 표시됩니다.



6단계

다음을 입력하여 *기본 AP*를 설정합니다.

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



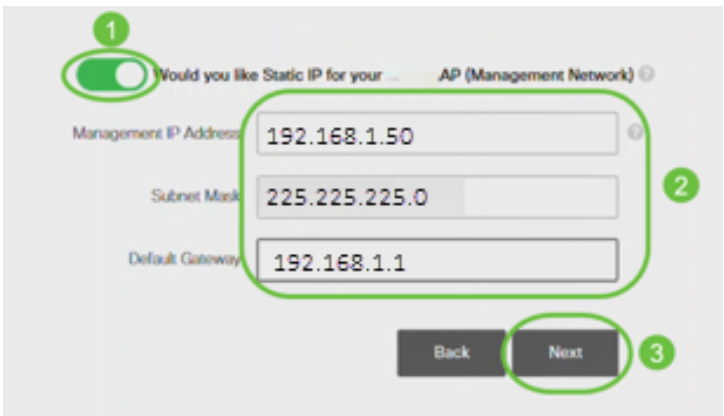
*메시*는 메시 네트워크를 생성하려는 경우에만 활성화해야 합니다.기본적으로 비활성화되어 있습니다.

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**.



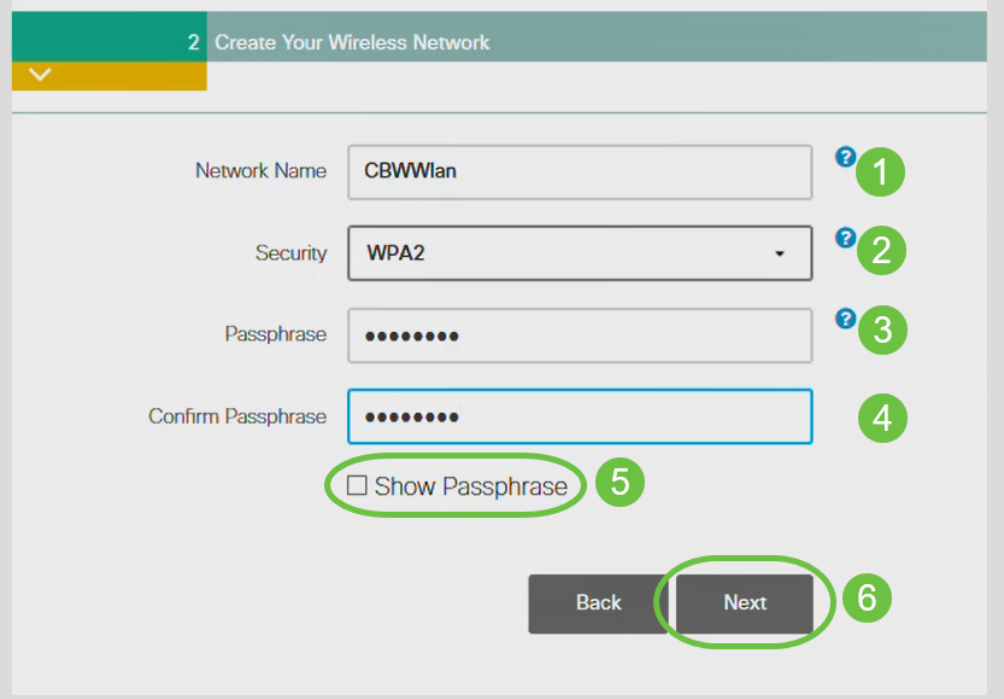
기본적으로 이 옵션은 비활성화되어 있습니다.

8단계

다음을 입력하여 *무선 네트워크*를 생성합니다.

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

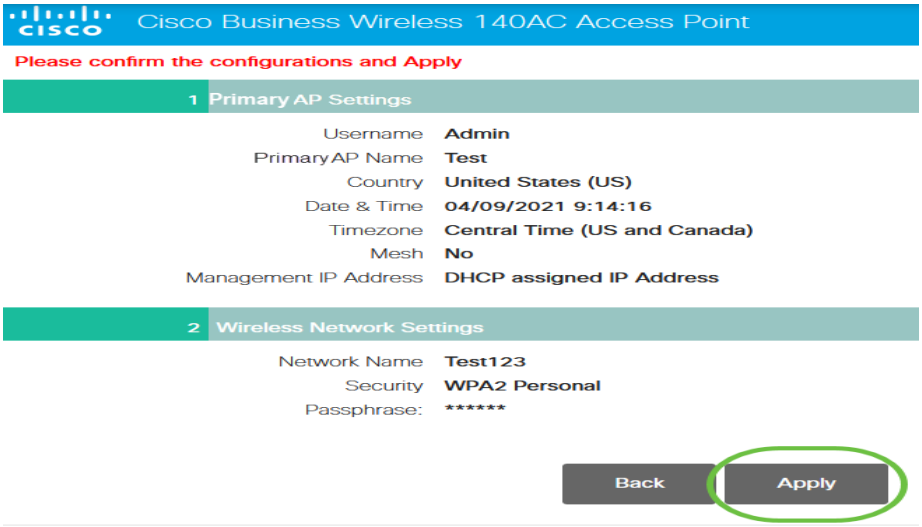
Next(**다음)를 클릭합니다**.



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

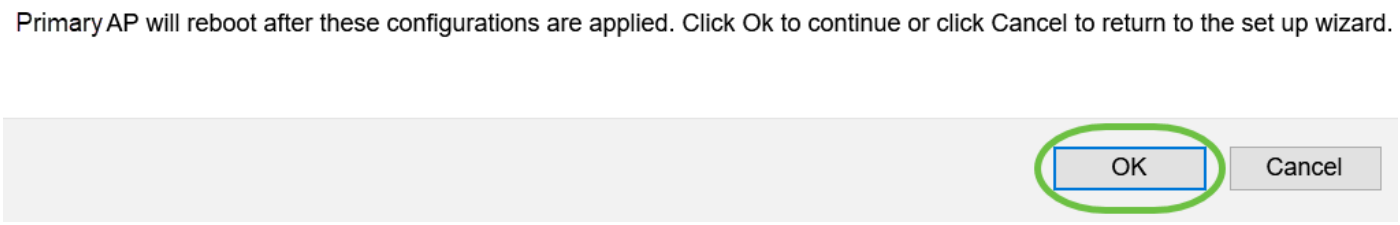
9단계

설정을 확인하고 Apply를 **클릭합니다**.

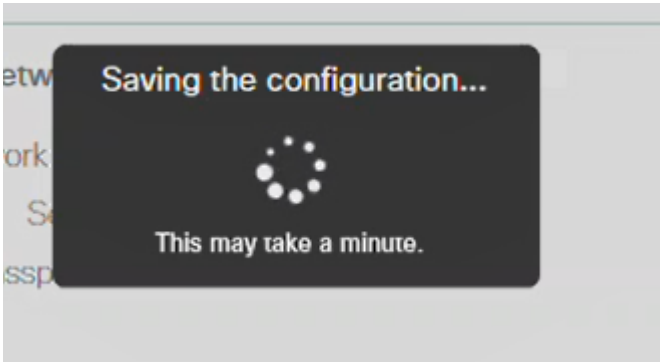


10단계

확인**을** 클릭하여 설정을 적용합니다.



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

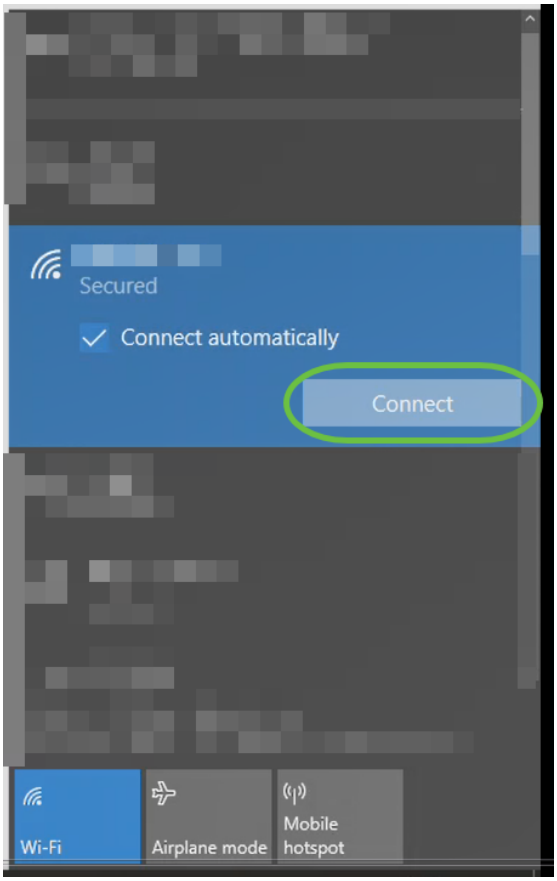


재부팅하는 동안 액세스 포인트의 LED가 여러 색상 패턴을 거칩니다.LED가 녹색으로 깜박이면 다음 단계로 진행합니다.LED가 빨간색 깜박임 패턴을 통과하지 못하면 네트워크에 DHCP 서버가 없음을 나타냅니다.AP가 스위치 또는 DHCP 서버가 있는 라우터에 연결되어 있는지 확인합니다.

11단계

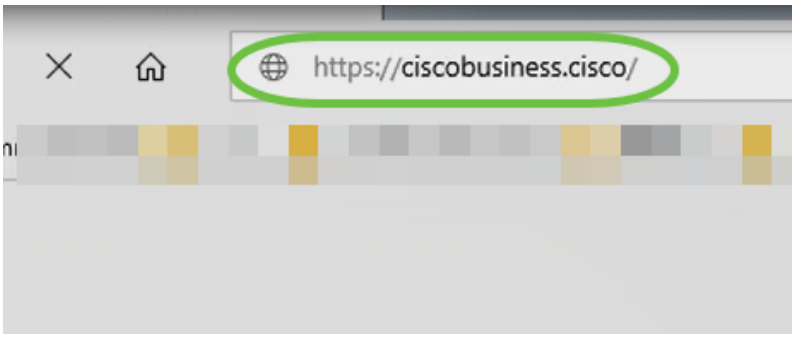
PC의 무선 옵션으로 이동하여 구성한 네트워크를 선택합니다.**연결**을 **클릭합니다**.

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.



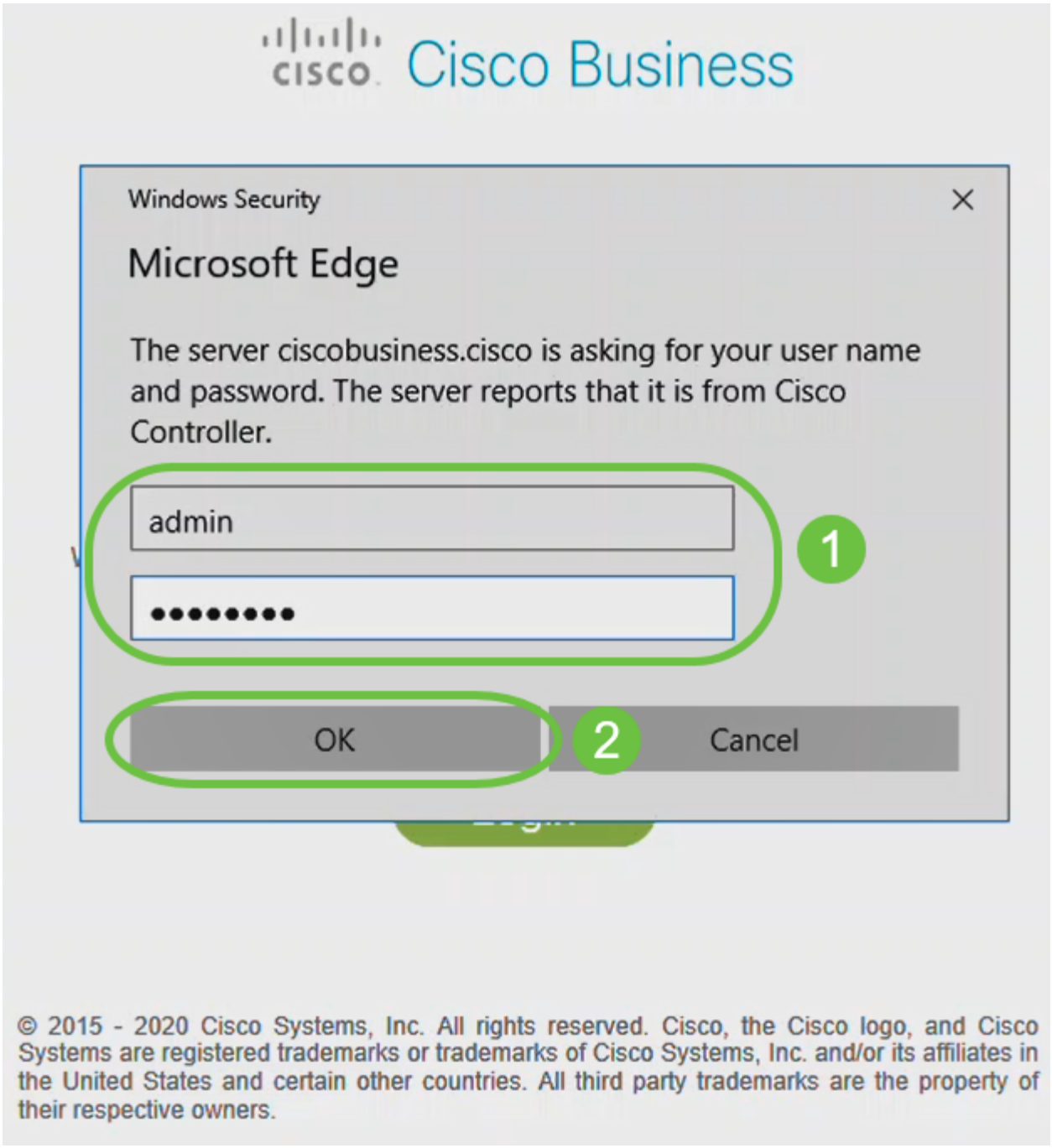
이 단계에서 https를 *입력하고 http*를 *입력하지* 마십시오.

13단계

Login(**로그인)을 클릭합니다**.

14단계

구성된 자격 증명을 사용하여 로그인합니다.**확인**을 **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

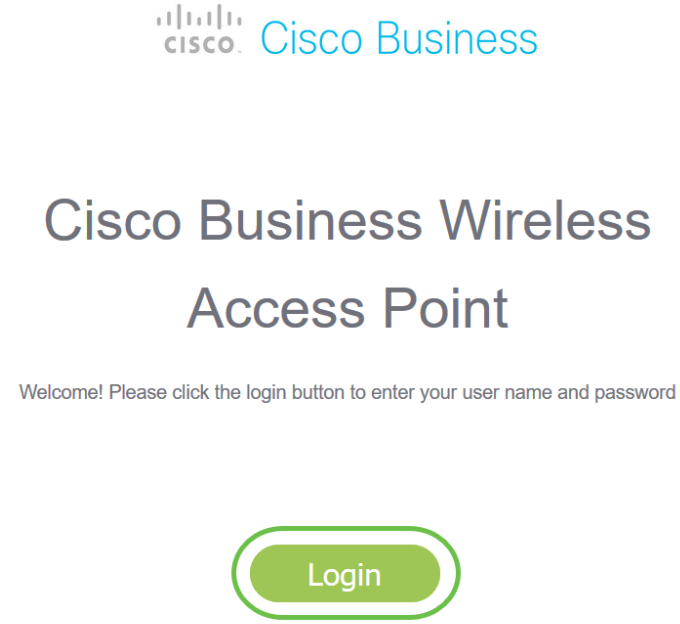
선택한 위치의 벽에 두 개의 메시 확장기를 연결합니다.각 메시 익스텐더의 MAC 주소를 기록합니다.

2단계

메시 익스텐더가 부팅될 때까지 10분 정도 기다립니다.

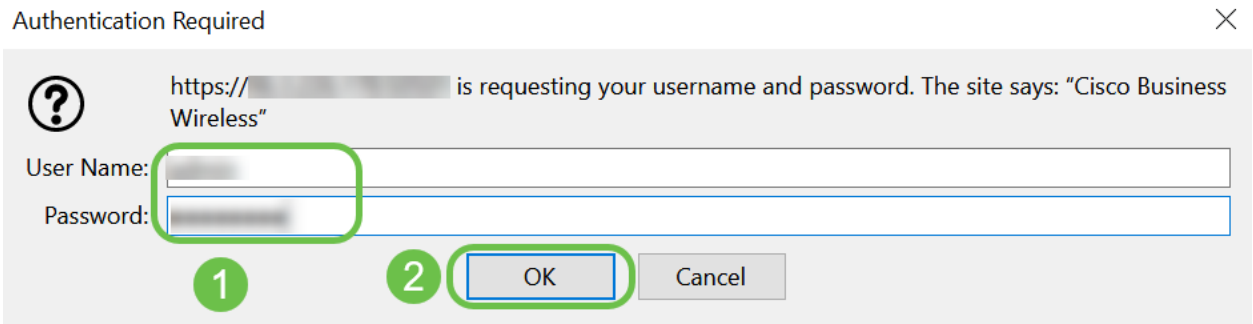
3단계

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



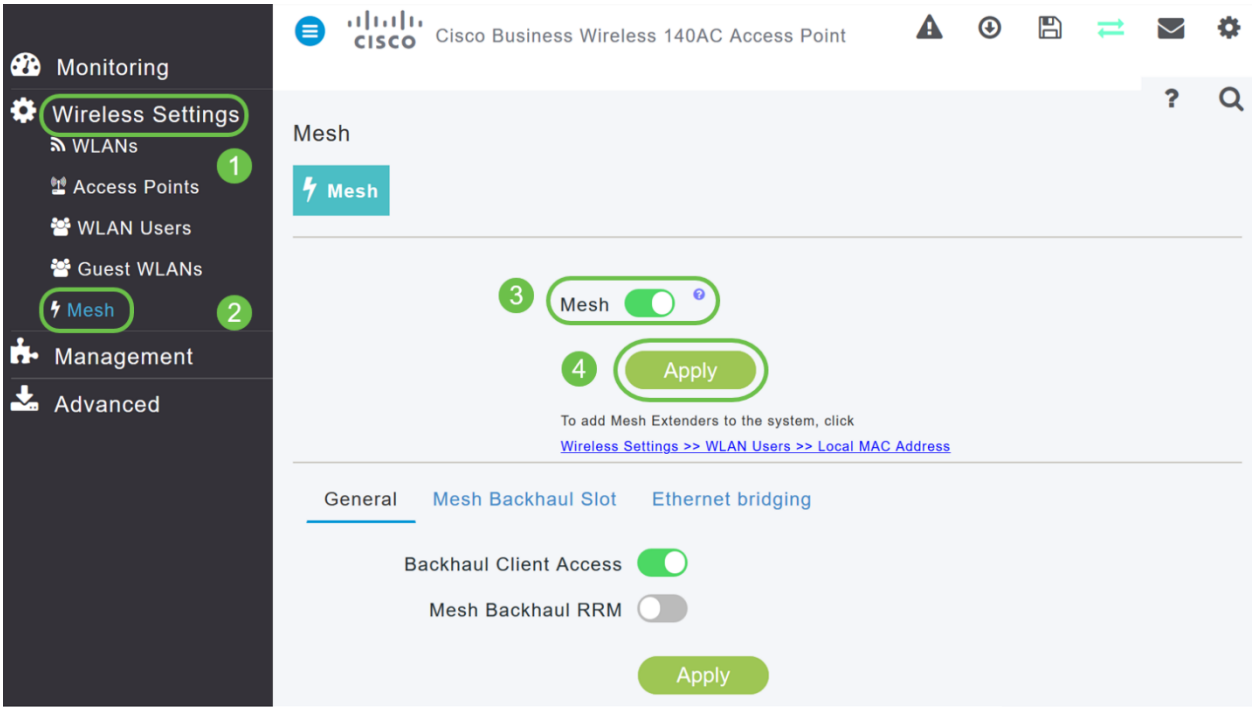
4단계

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**.

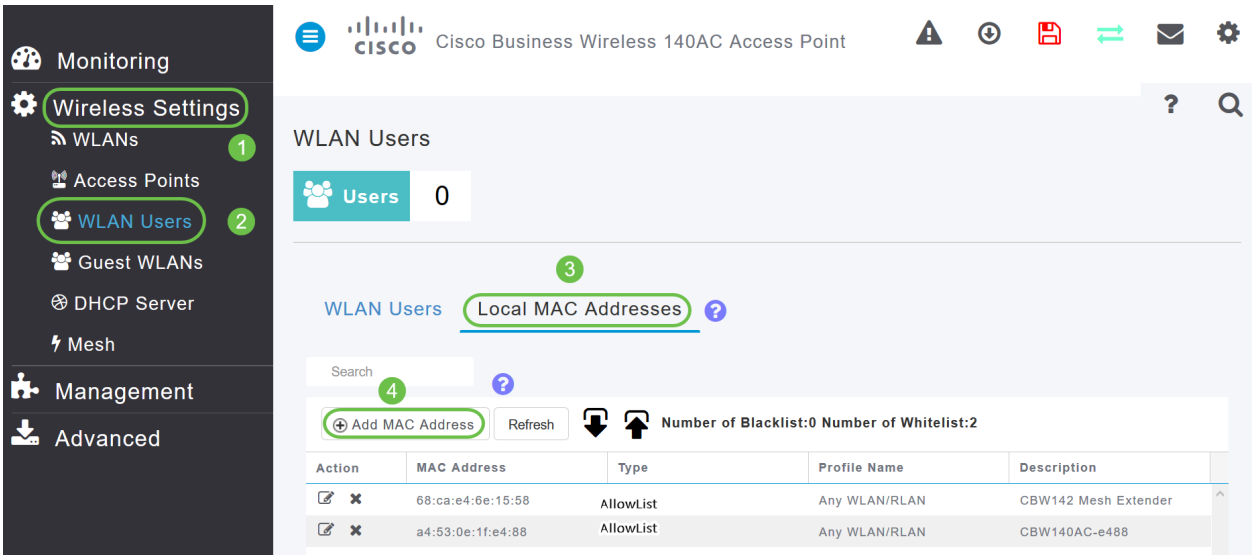


6단계

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.

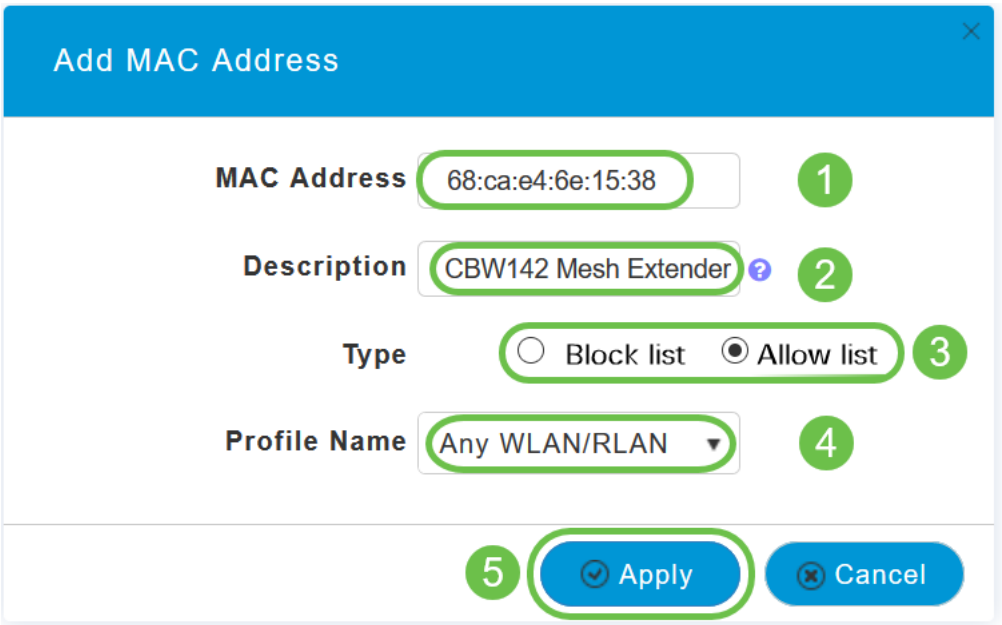
7단계

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.

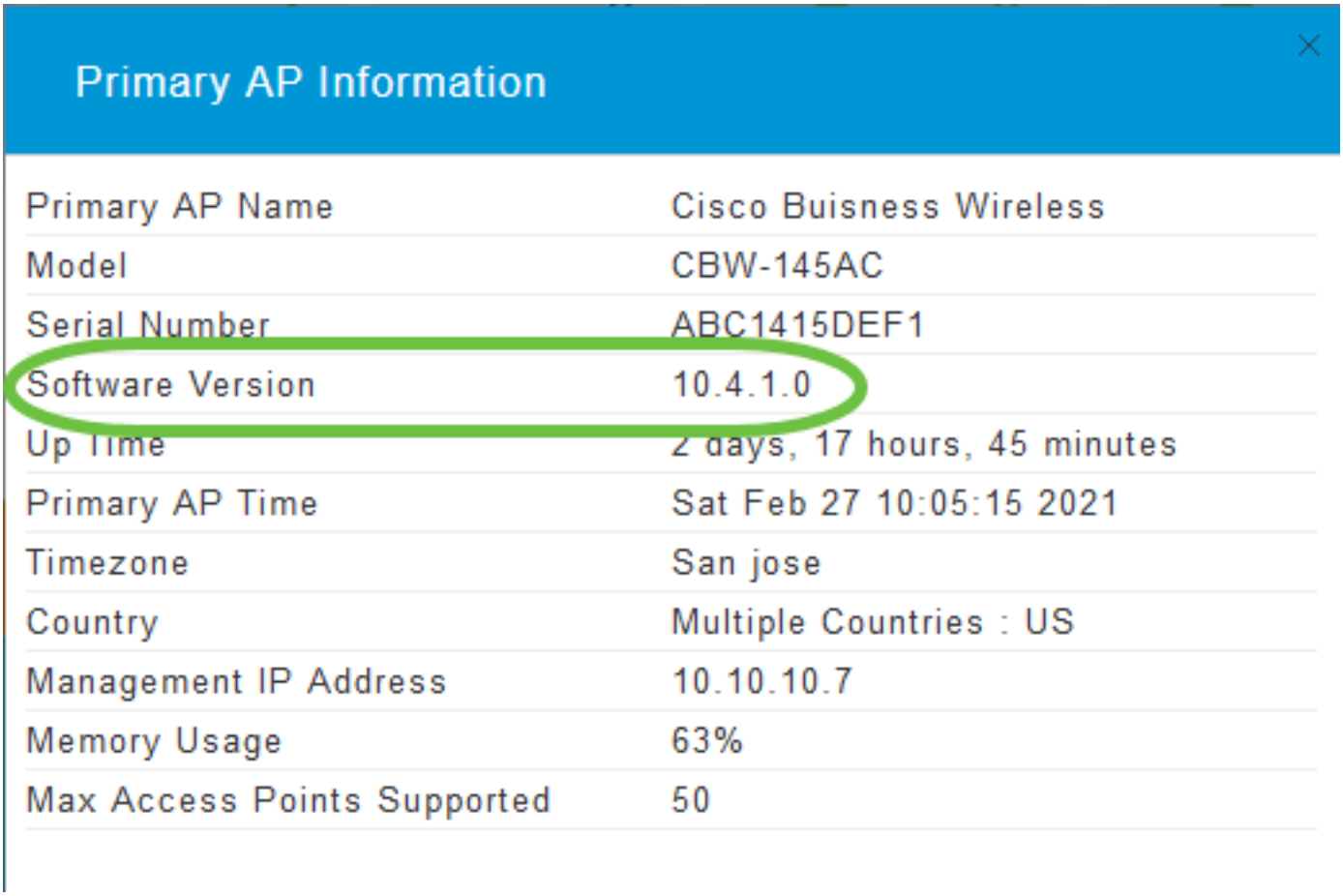
웹 UI를 사용하여 소프트웨어 확인 및 업데이트

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.

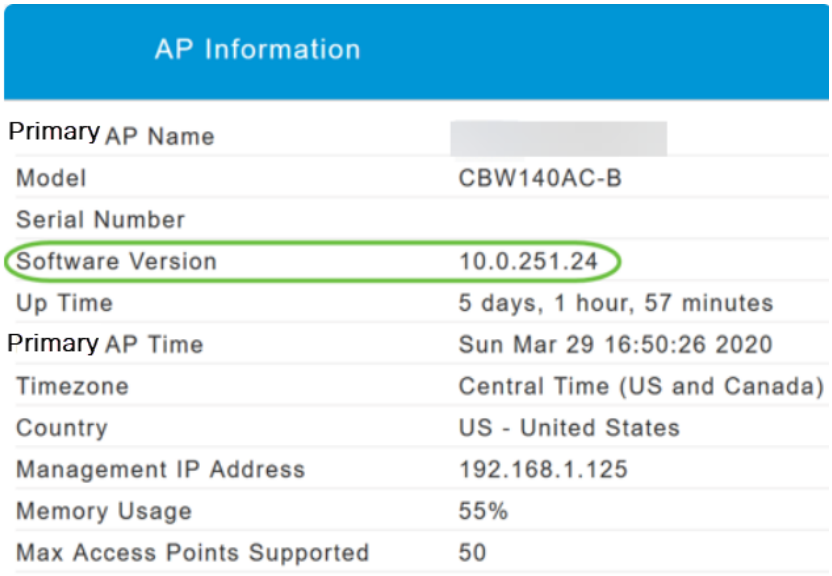
1단계

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.

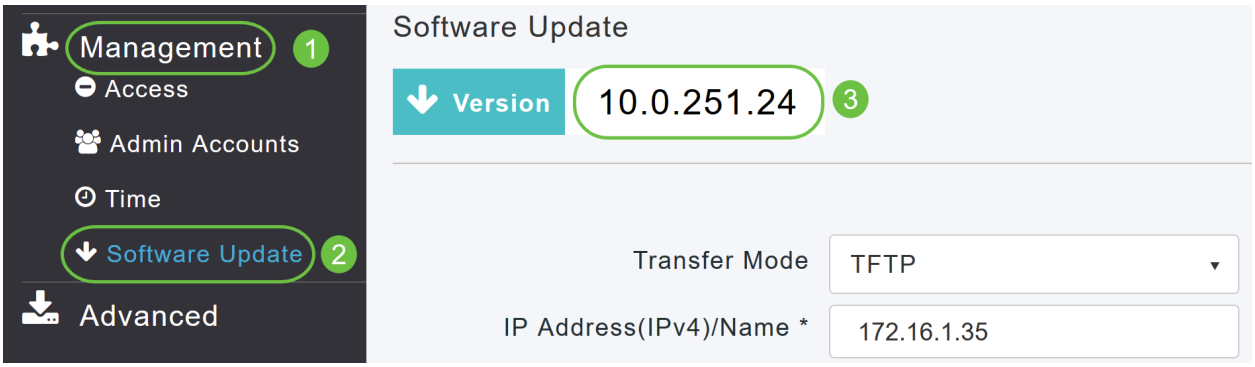


최신 버전의 소프트웨어를 실행 중인 경우 Create WLANs(WLAN 생성) 섹션으로 이동할 수 있습니다.

3단계

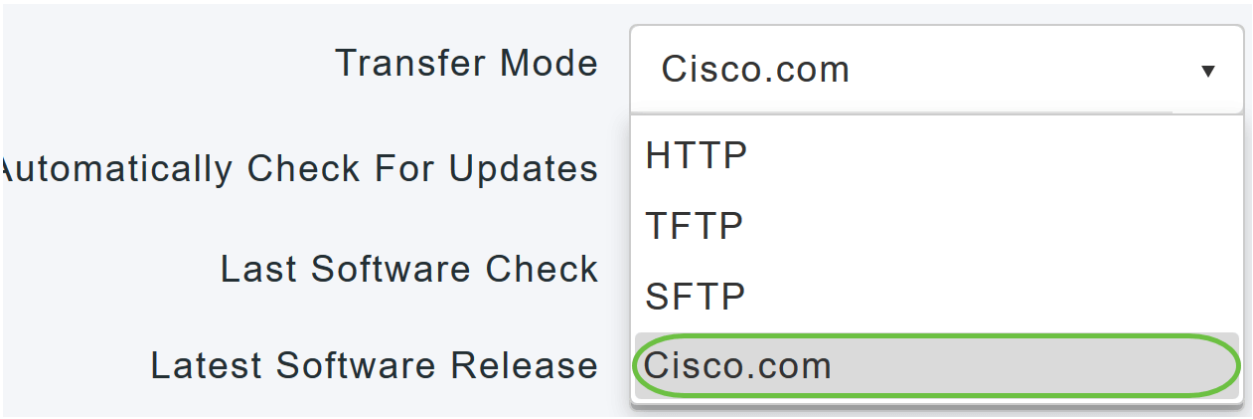
메뉴에서 **Management(관리) > Software Update(소프트웨어 업데이트)**를 선택합니다.

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



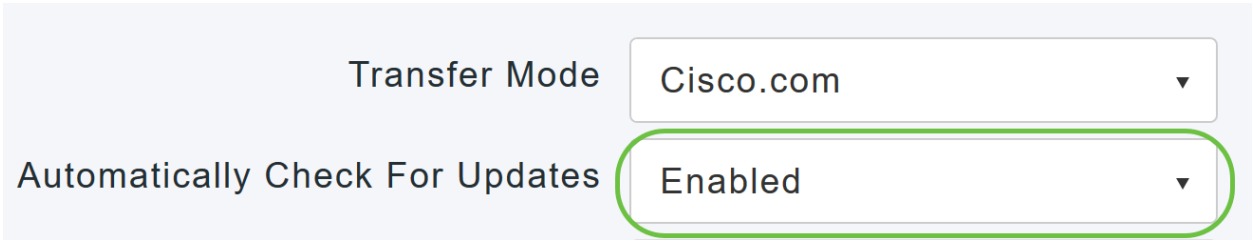
CBW AP 소프트웨어를 업데이트할 수 있으며 기본 AP의 현재 구성은 삭제되지 않습니다.

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



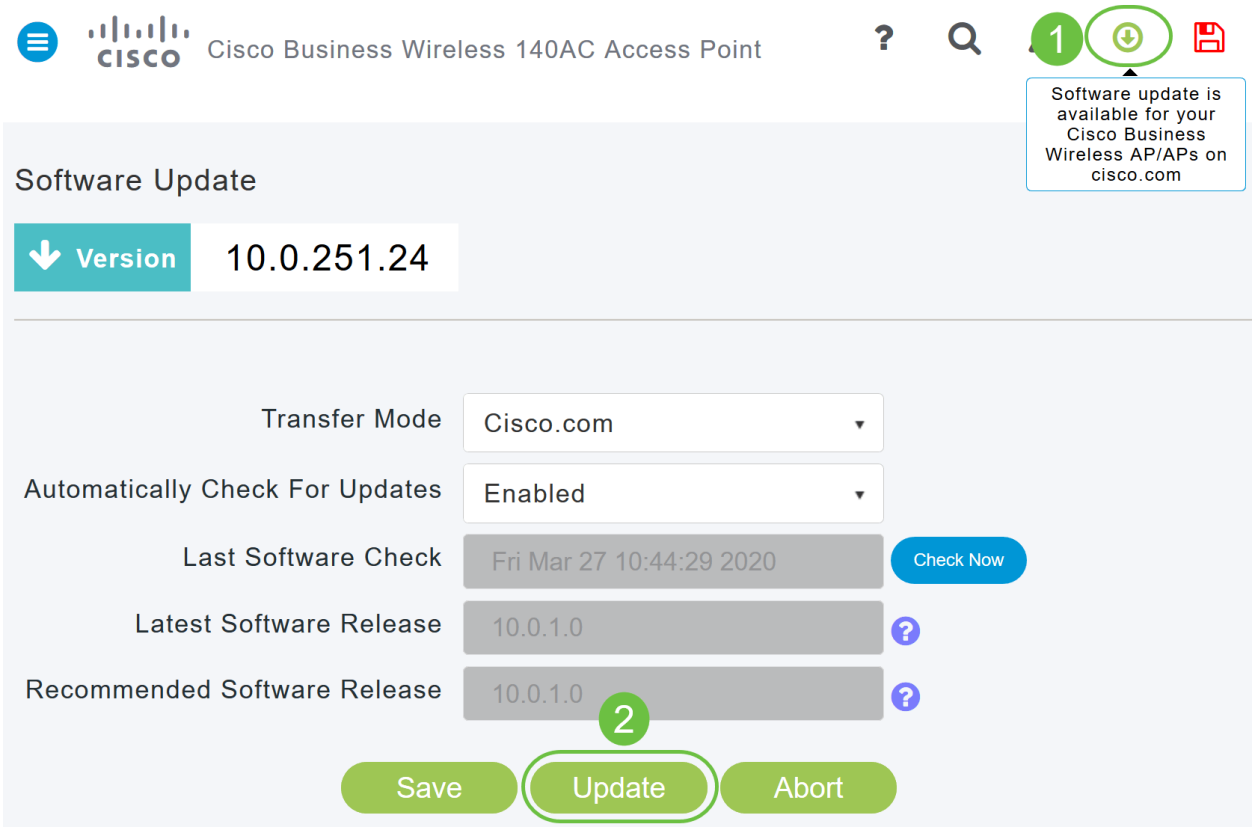
4단계

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



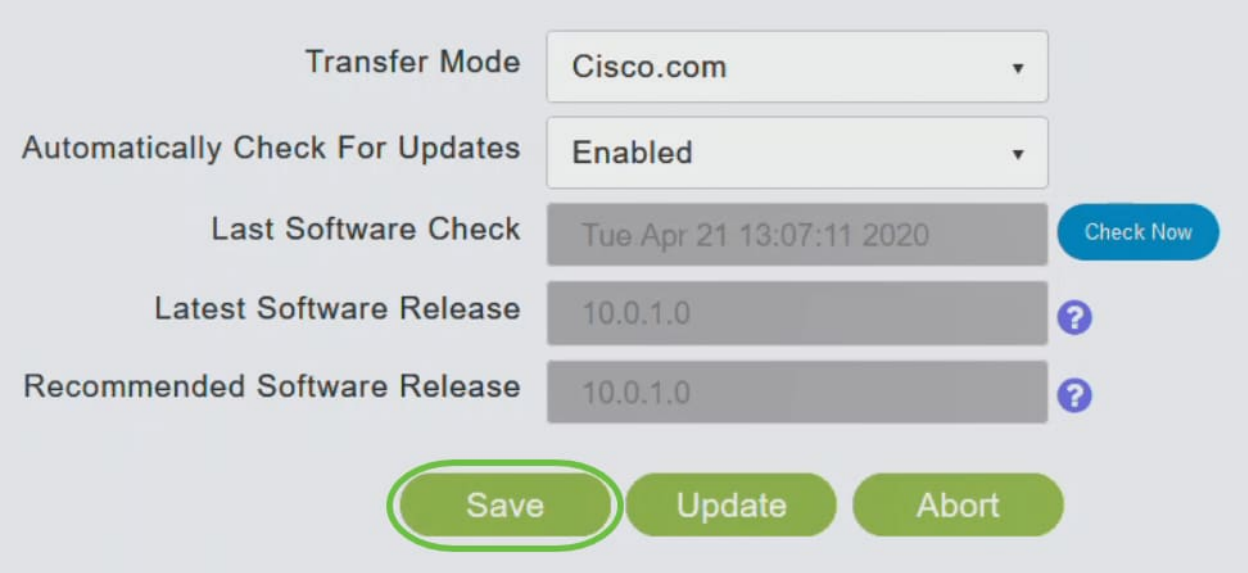
소프트웨어 확인이 완료되고 Cisco.com에서 최신 소프트웨어 업데이트 또는 권장 소프트웨어 업데이트가 제공되는 경우 다음을 수행합니다.

- 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.

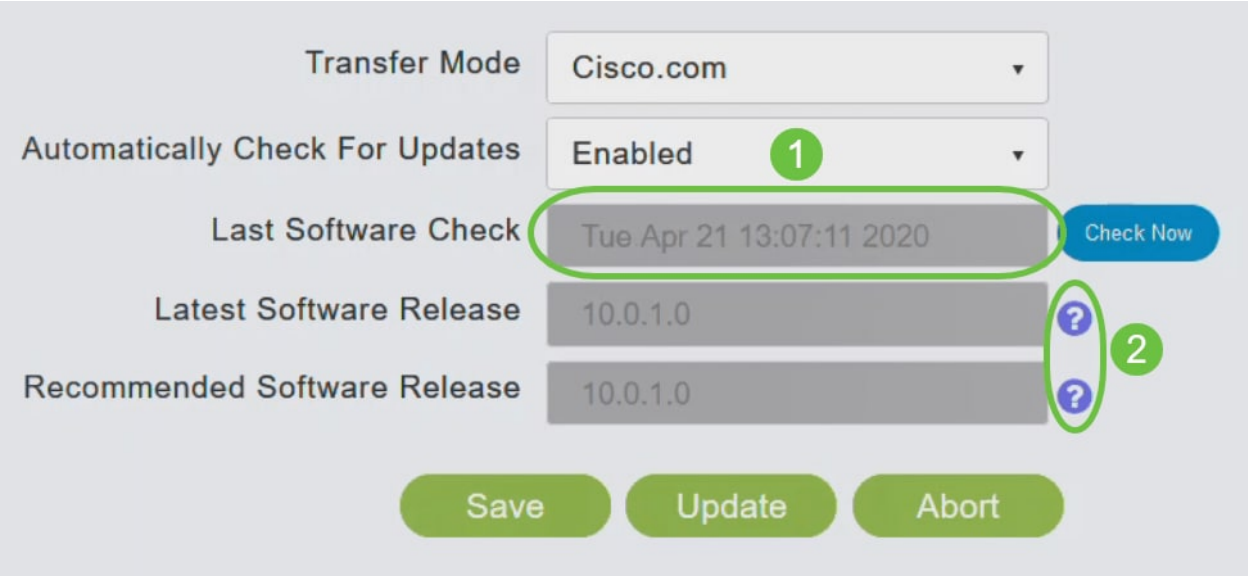


5단계

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

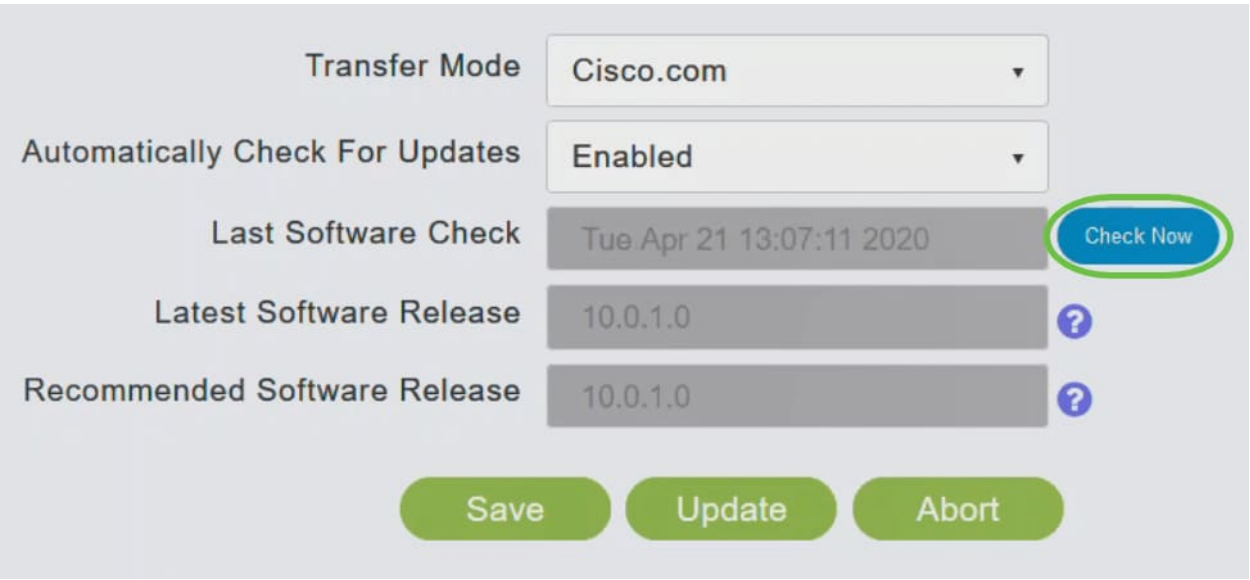


Last *Software Check*(마지막 소프트웨어 확인) 필드는 마지막 자동 또는 수동 소프트웨어 확인의 타임스탬프를 표시합니다.옆에 있는 **물음표 아이콘**을 클릭하여 표시된 릴리스의 노트를 볼 수 있습니다.



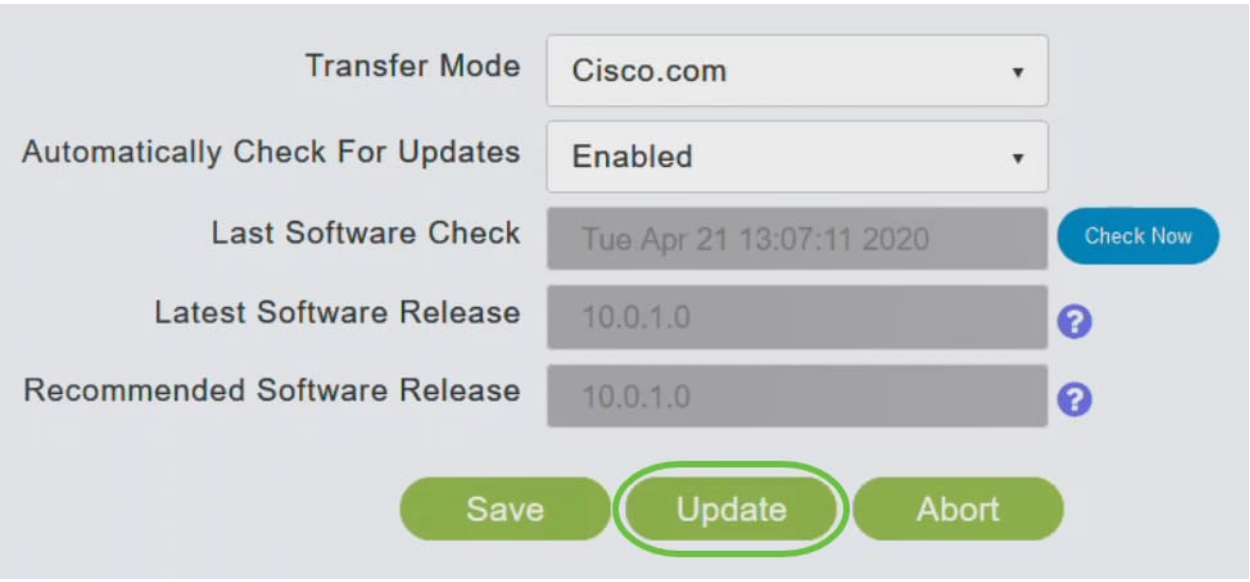
6단계

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



7단계

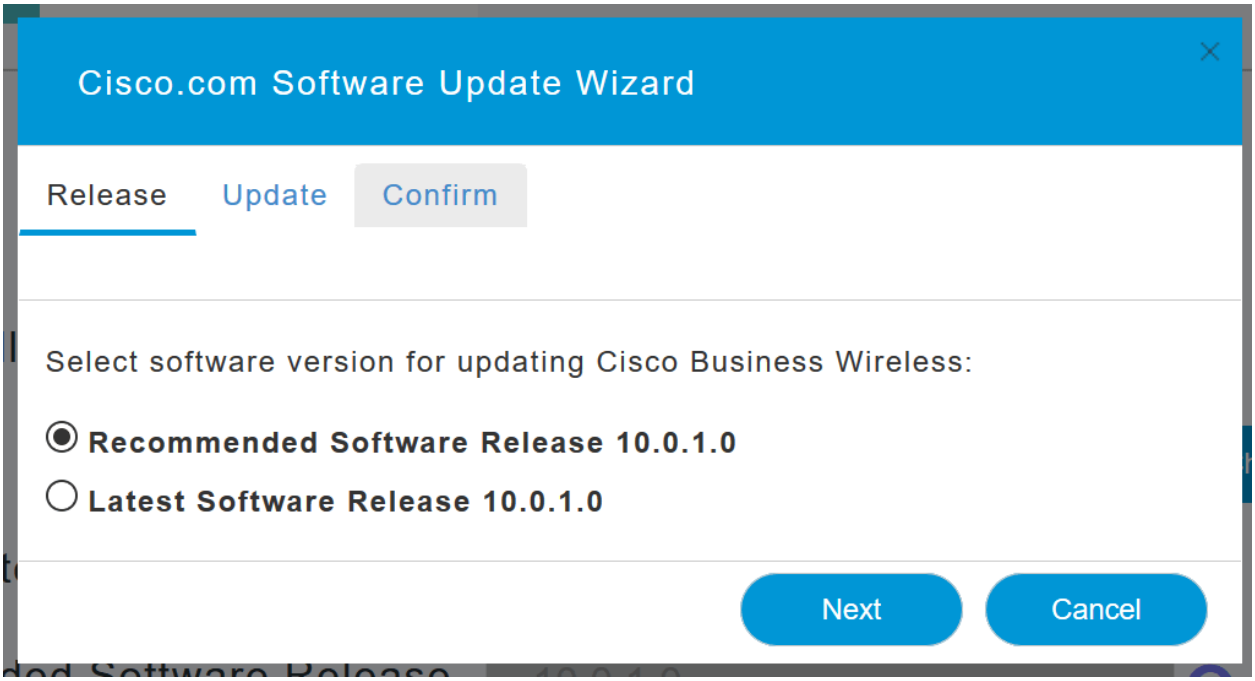
소프트웨어 업데이트를 계속하려면 Update(**업데이트**)를 클릭합니다.



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

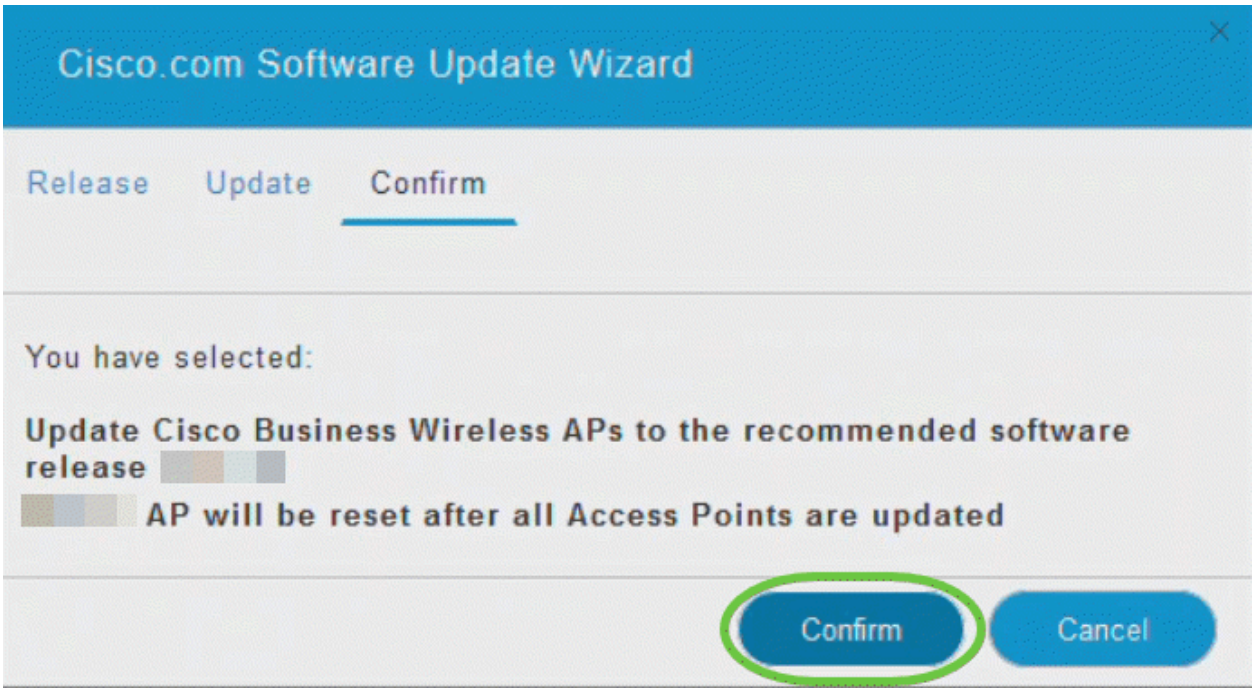
- Release(릴리스) 탭 - 권장 소프트웨어 릴리스 또는 최신 소프트웨어 릴리스로 업데이트할지 지정합니다.
- Update(업데이트) 탭 - AP를 재설정해야 하는 시기를 지정합니다.지금 바로 끝내거나 나중에 예약하도록 선택할 수 있습니다.이미지 사전 다운로드가 완료된 후 기본 AP가 자동으로 재부팅되도록 설정하려면 Auto Restart(자동 재시작) 확인란을 선택합니다.
- 확인 탭 - 선택 사항을 확인합니다.

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



8단계

확인을 **클릭합니다**.

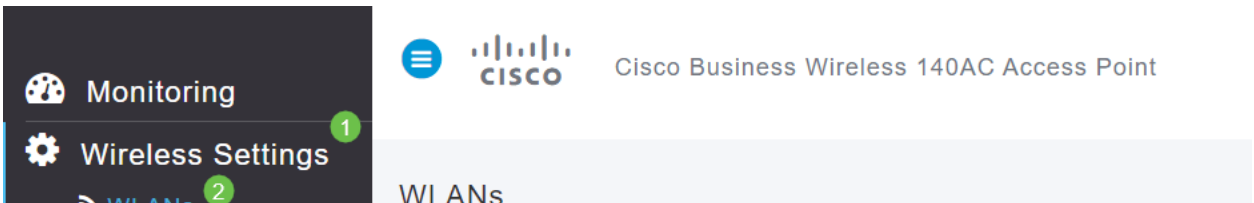


웹 UI에서 WLAN 생성

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

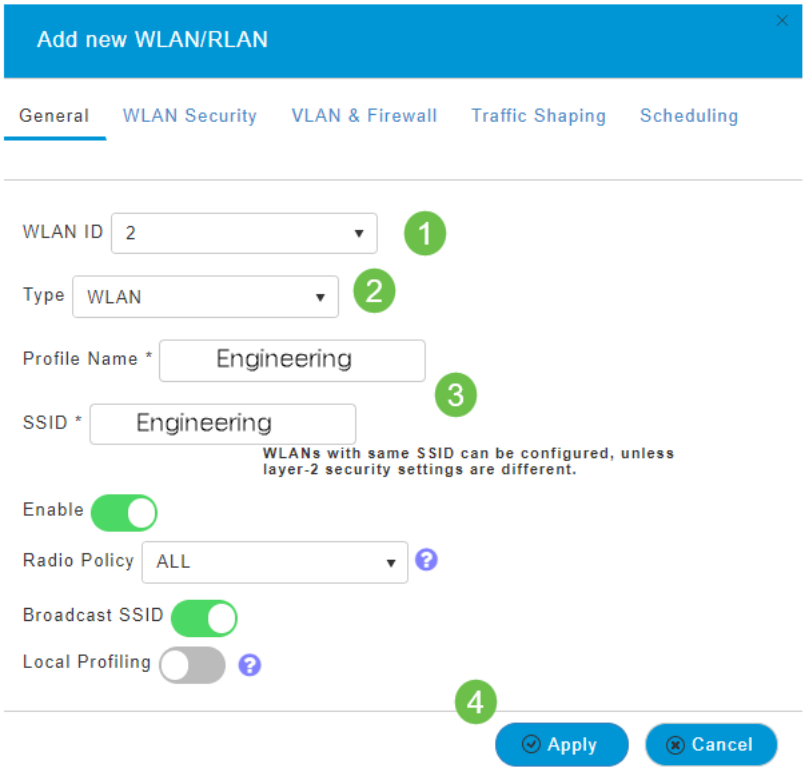
일반 탭에서 다음 정보를 입력합니다.

- 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.

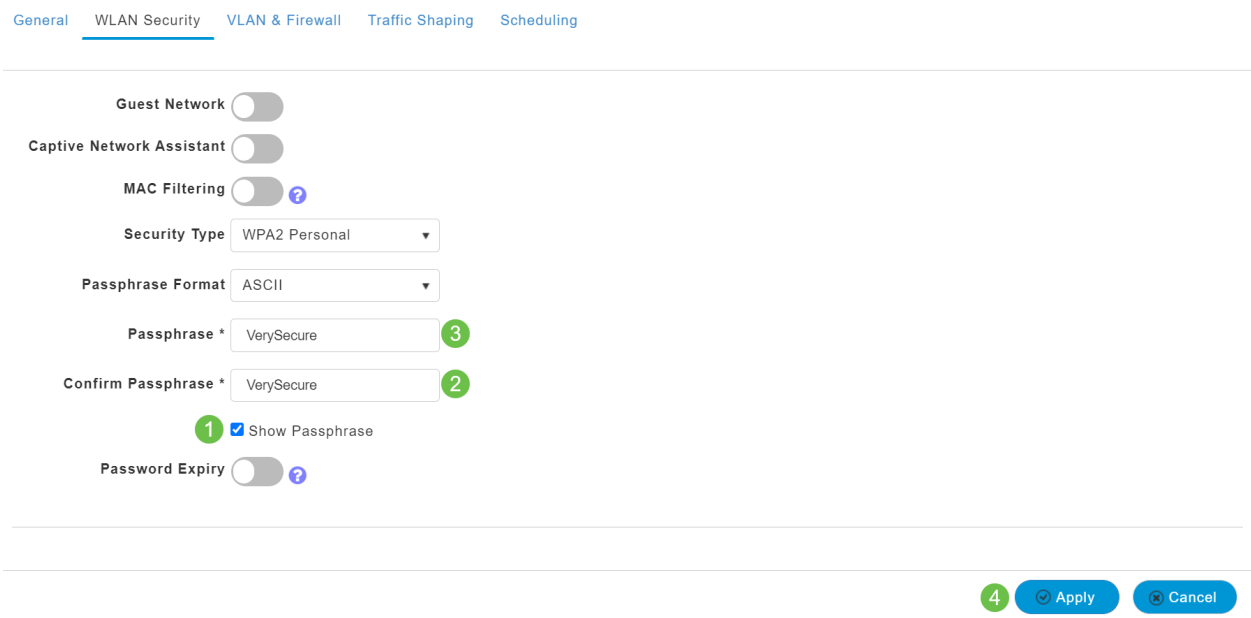
WPA2 Personal은 PSK 인증을 사용하여 네트워크를 보호하는 데 사용되는 방법입니다.PSK는 기본 AP, WLAN 보안 정책 및 클라이언트에서 각각 구성됩니다.WPA2 Personal은 네트워크에서 인증 서버를 사용하지 않습니다.

- 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.

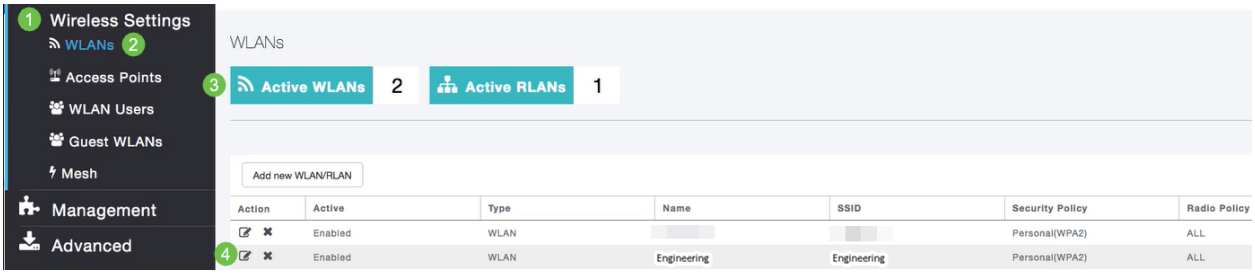


4단계

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

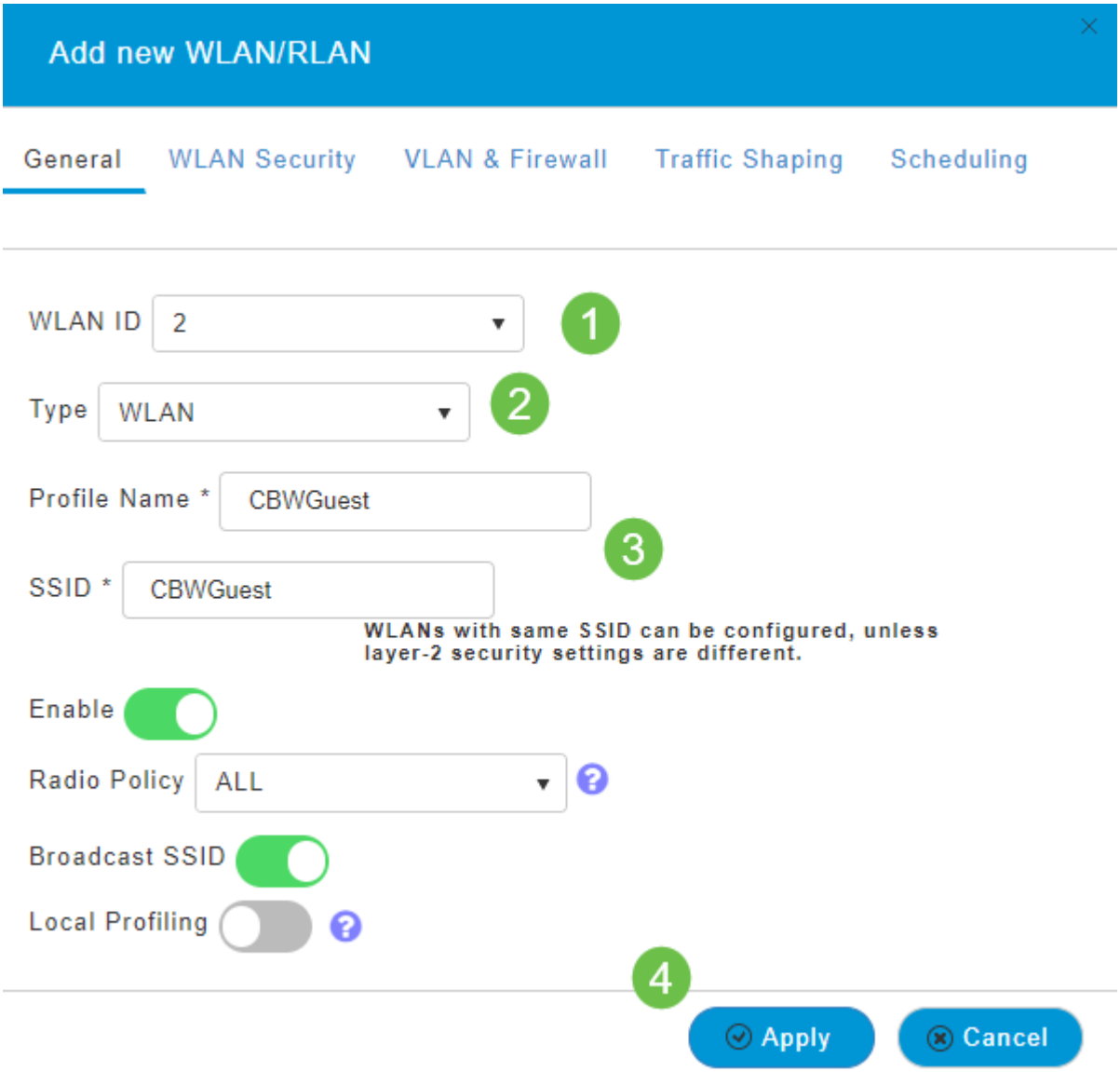
일반 탭에서 다음 정보를 입력합니다.

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.

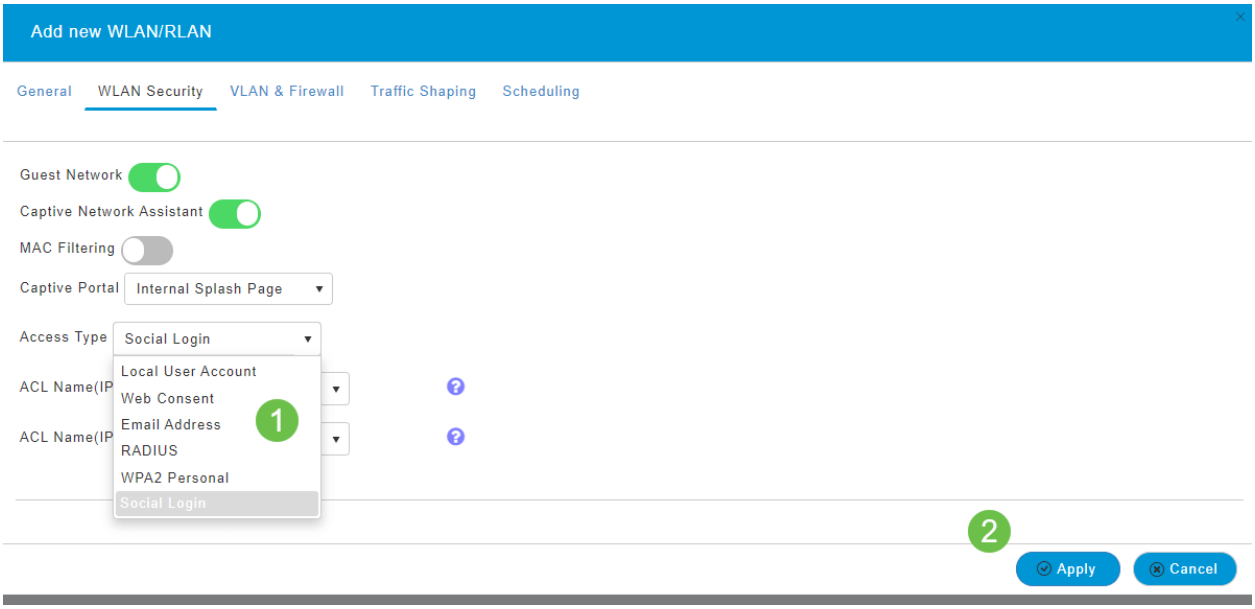
*액세스 유형*에 대한 기타 옵션은 다음과 같습니다.

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)

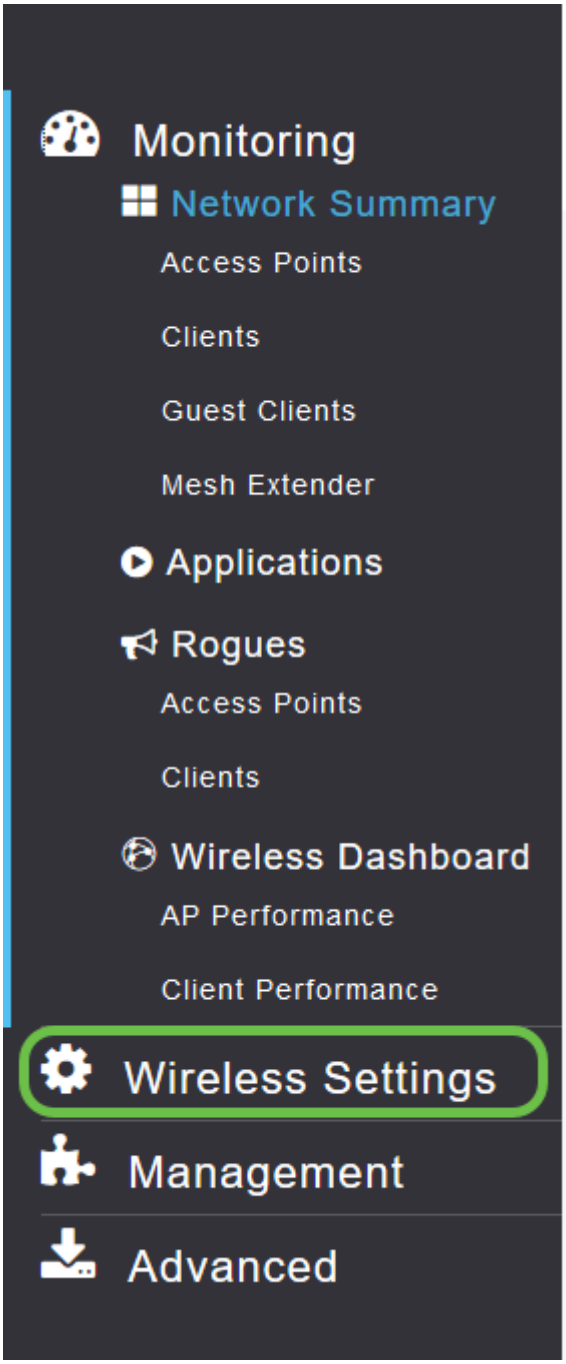
프로파일링은 조직 정책을 구체화하는 기능의 하위 집합입니다.트래픽 유형을 매칭하고 우선순위를 지정할 수 있습니다.유사 규칙에서는 트래픽의 순위를 매기거나 삭제하는 방법을 결정합니다.Cisco Business Mesh Wireless 시스템은 클라이언트 및 애플리케이션 프로파일링을 제공합니다.사용자가 네트워크에 액세스하는 작업은 많은 정보 교환에서 시작됩니다. 그 중 하나는 트래픽 유형입니다.정책은 플로우 차트와 마찬가지로 경로를 전달하기 위해 트래픽 흐름을 중단합니다.기타 정책 기능 유형에는 게스트 액세스, 액세스 제어 목록, QoS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

1단계

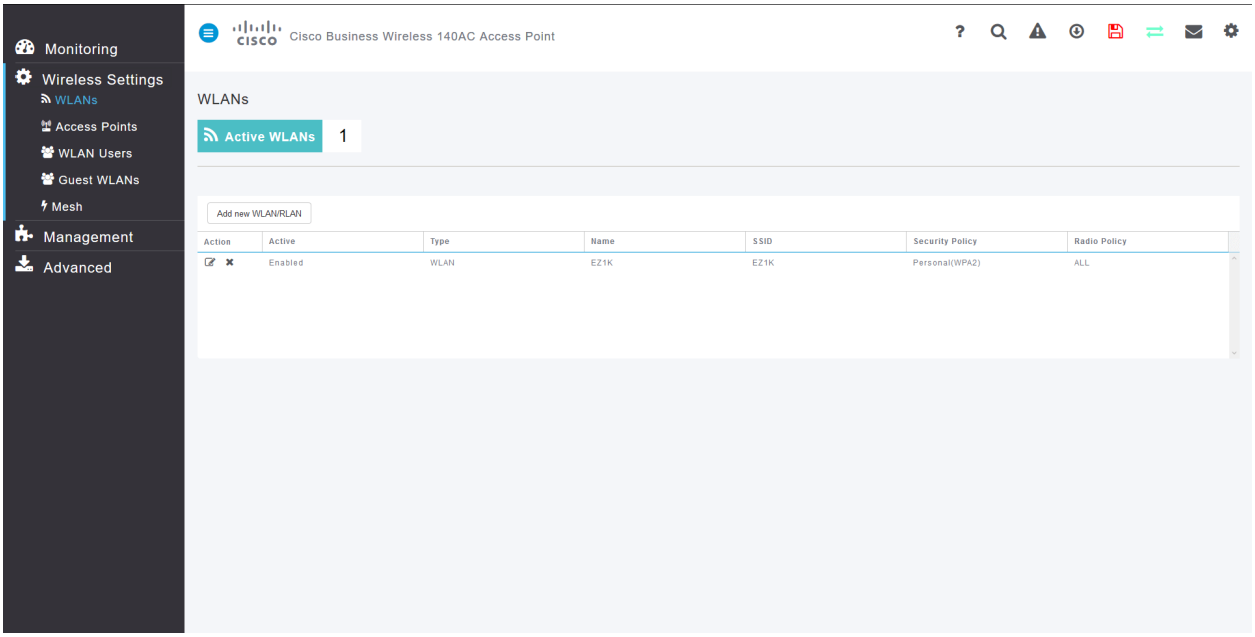
왼쪽 메뉴 모음이 표시되지 않으면 화면 왼쪽에 있는 메뉴로 이동합니다.

2단계

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

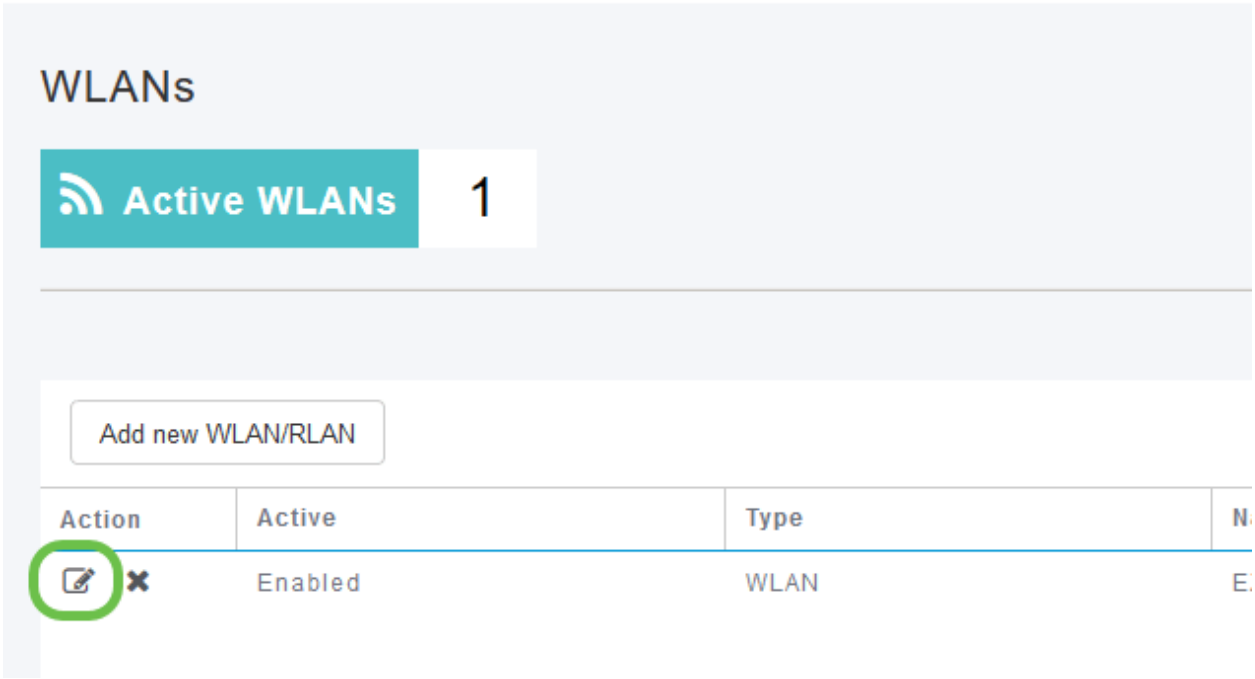


아래 이미지는 무선 설정 링크를 클릭할 때 표시되는 이미지와 유사합니다.

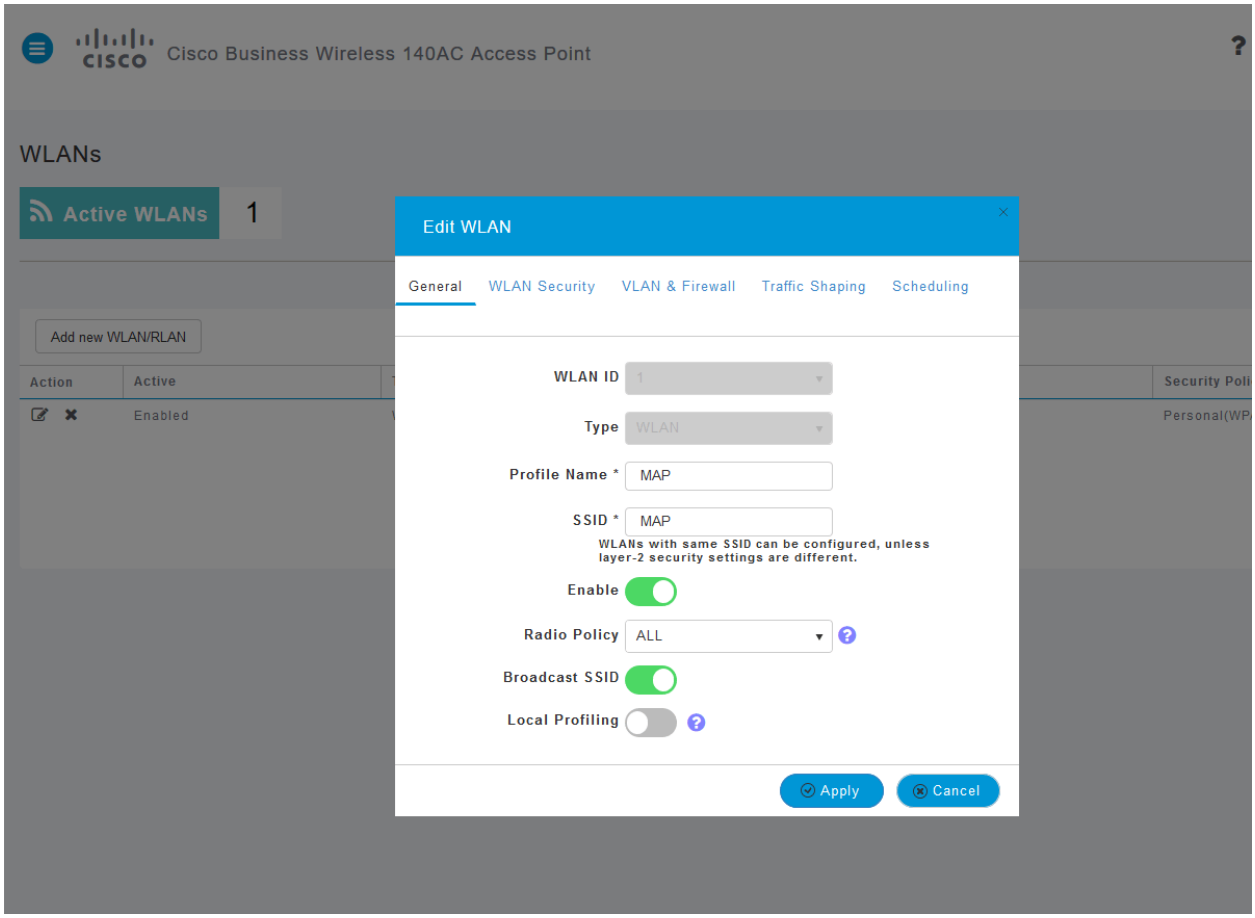


3단계

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

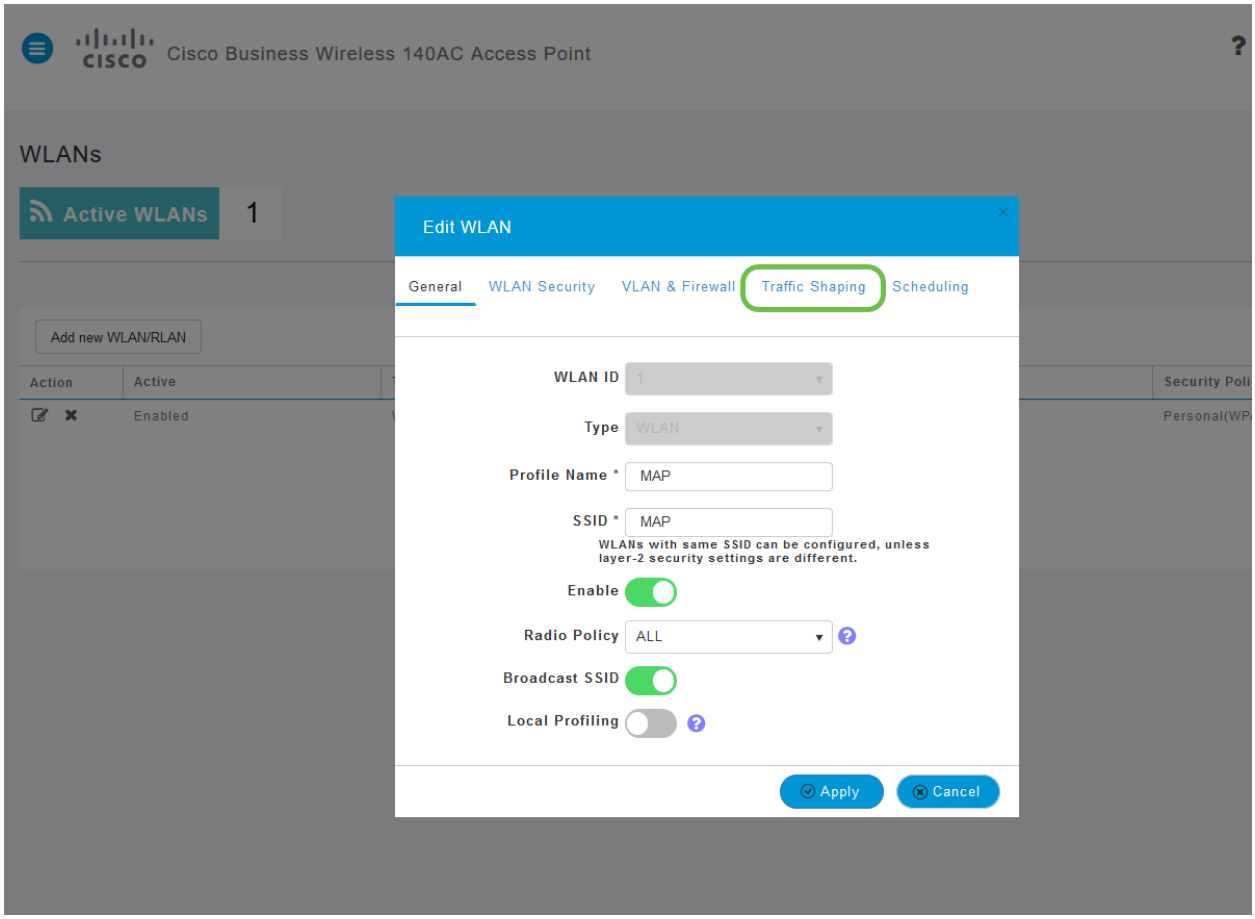


최근에 WLAN을 추가했으므로 *Edit WLAN(WLAN 편집)* 페이지가 아래와 유사하게 나타날 수 있습니다.

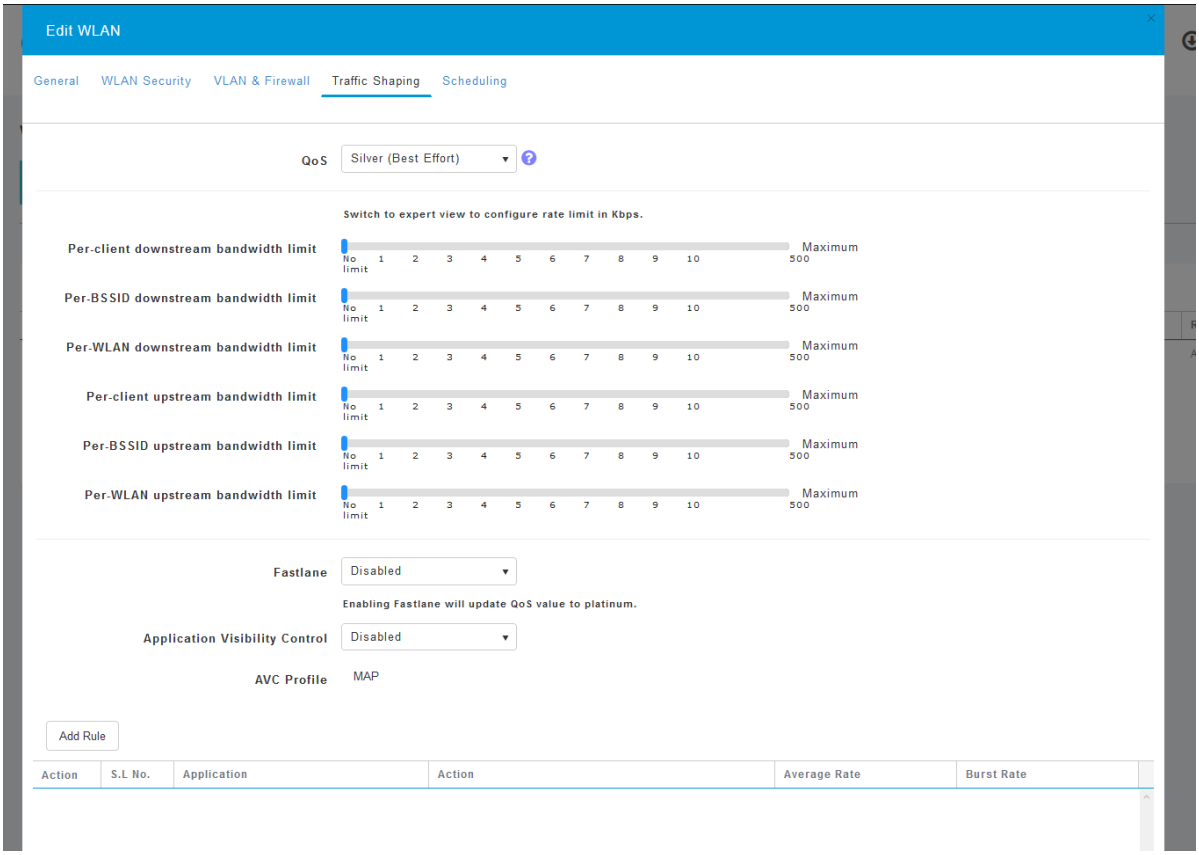


4단계

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

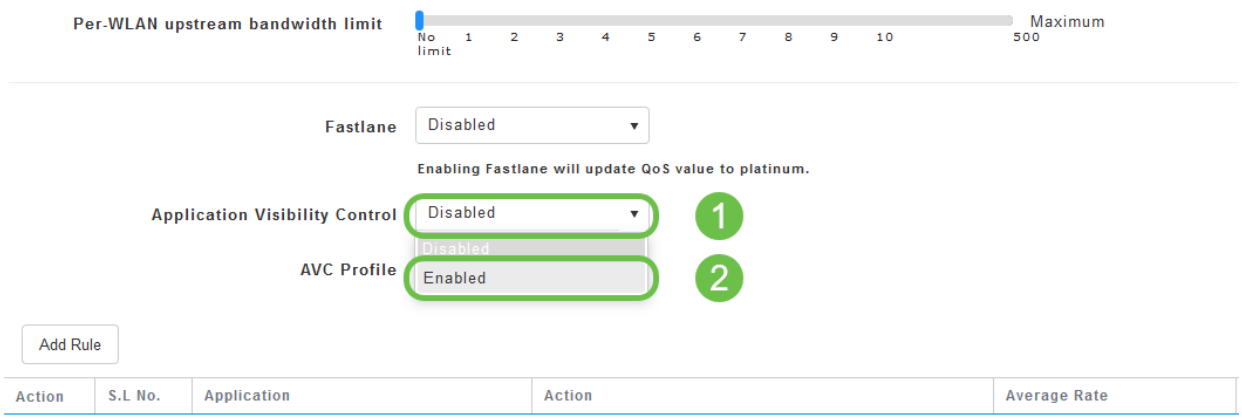


화면이 다음과 같이 표시될 수 있습니다.



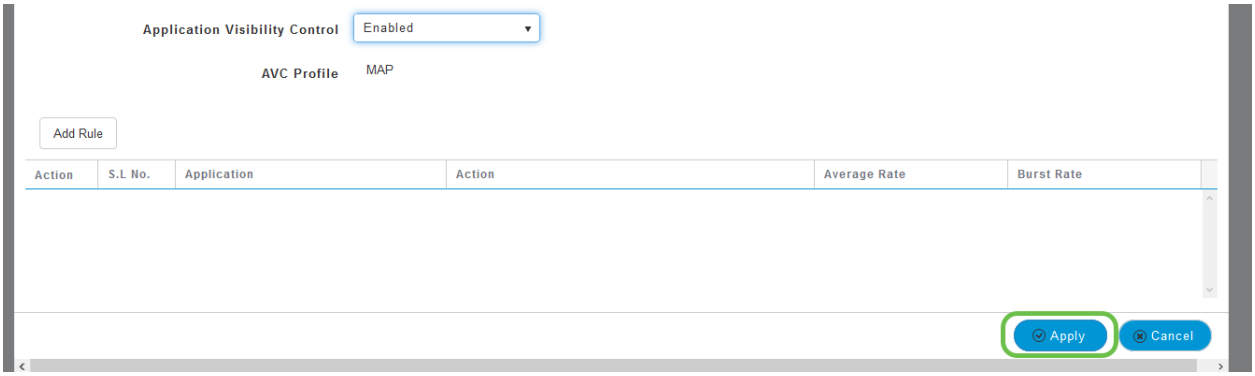
5단계

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



6단계

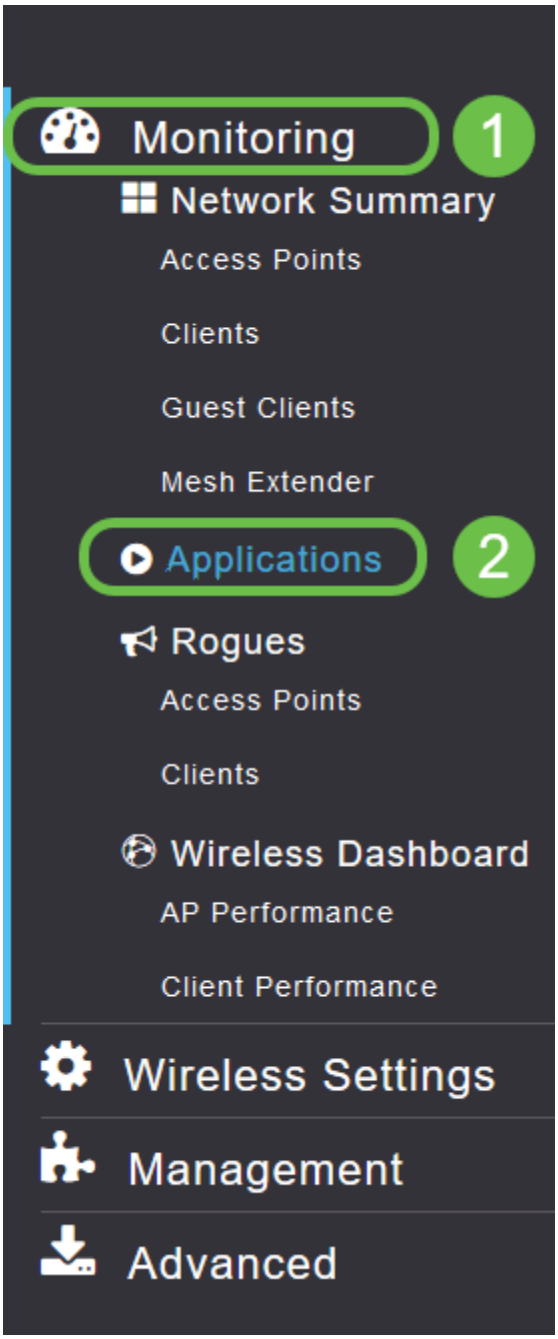
Apply(적용) 버튼을 클릭합니다.



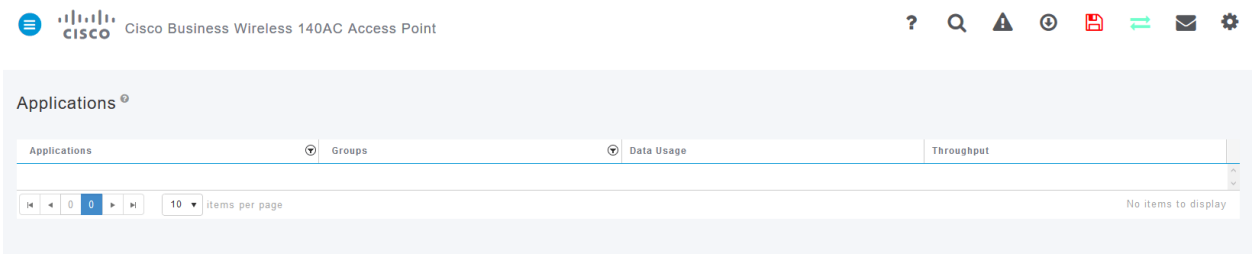
이 설정을 사용하도록 설정해야 합니다. 그렇지 않으면 기능이 작동하지 않습니다.

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.

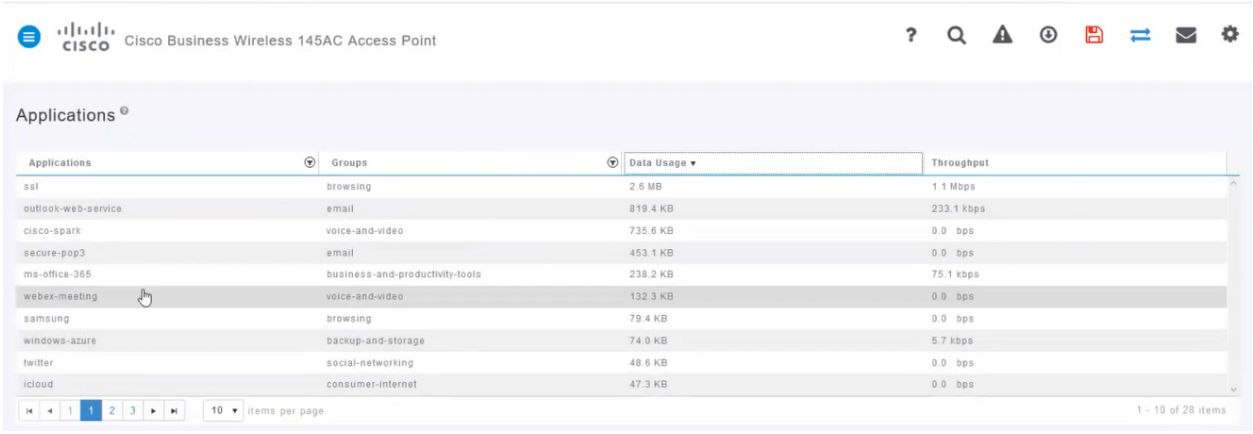
- 애플리케이션 - 다양한 유형 포함
- Groups(그룹) - 보다 쉽게 정렬할 수 있는 애플리케이션 그룹의 유형을 나타냅니다.
- 데이터 사용량 - 이 서비스에서 사용하는 전체 데이터 양
- 처리량 - 애플리케이션에서 사용하는 대역폭의 양

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

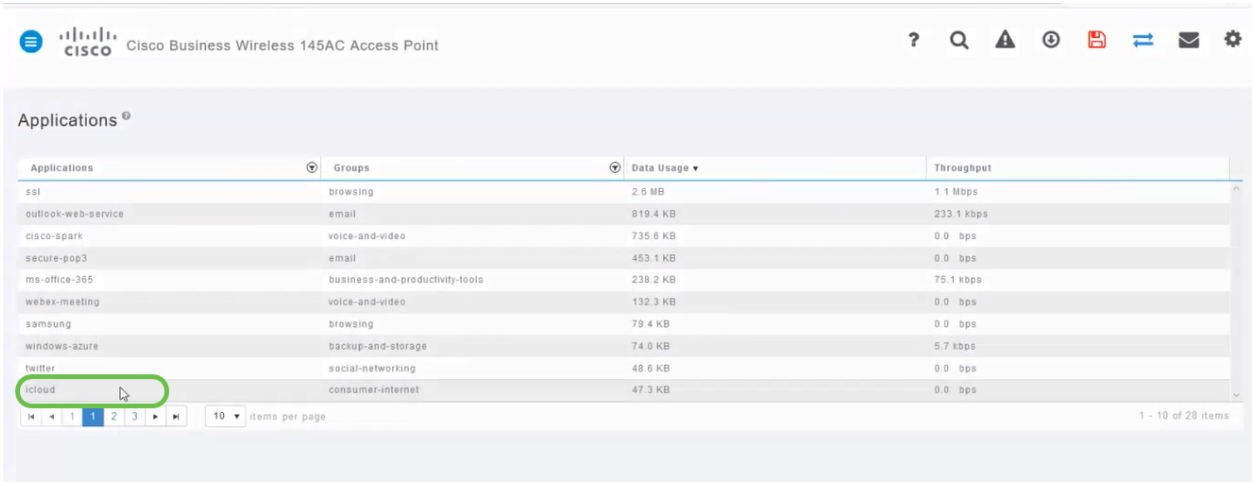
다음은 페이지를 채울 때의 모양을 보여주는 예입니다.



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

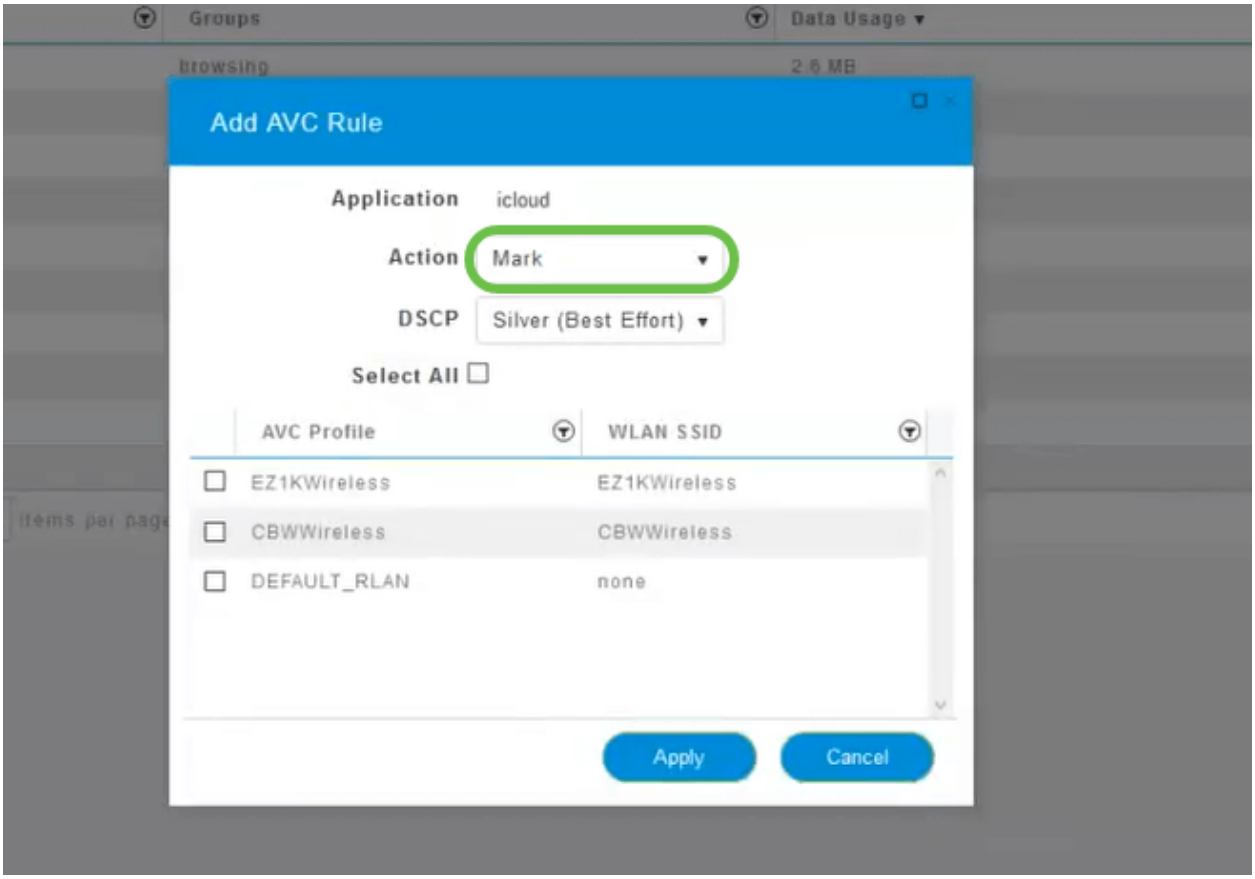
8단계

관리할 트래픽 유형의 행을 클릭합니다.



9단계

Action 드롭다운 상자를 클릭하여 해당 트래픽 유형을 처리하는 방법을 선택합니다.



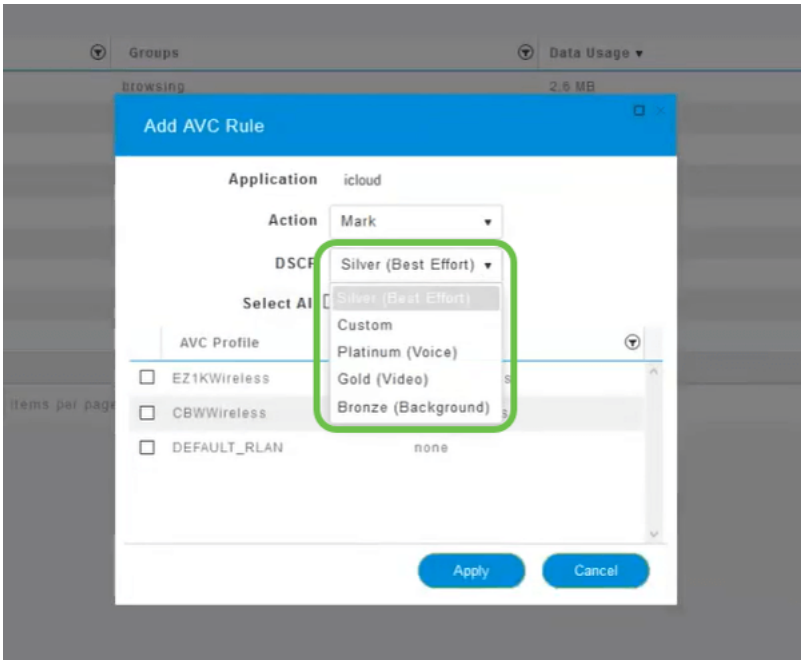
이 예제에서는 이 옵션을 *Mark*로 *둡니다*.

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.



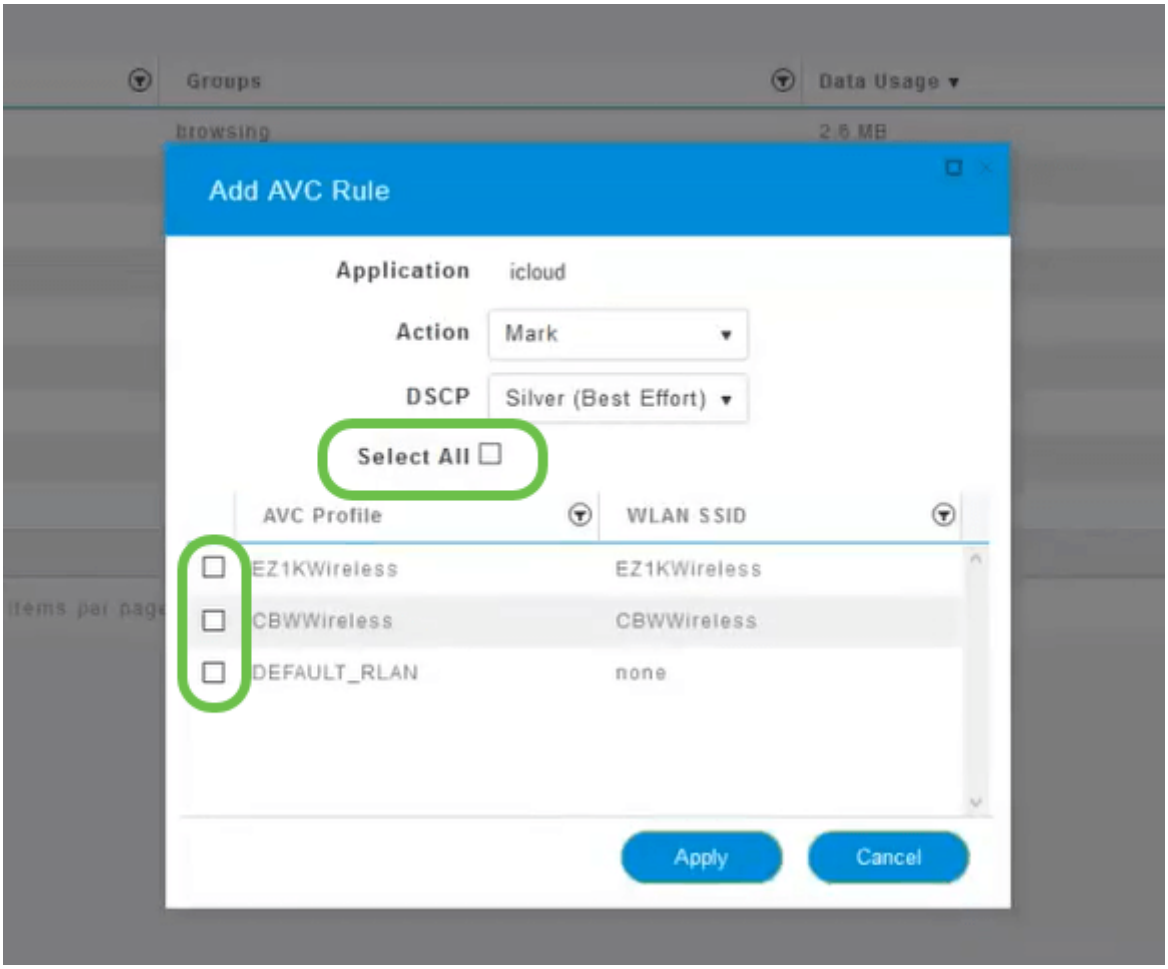
다음은 표시할 트래픽에 대한 DSCP 옵션입니다.이러한 옵션은 더 적은 리소스에서 편집 중인 트래픽 유형에 사용할 수 있는 더 많은 리소스로 진행됩니다.

- 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.

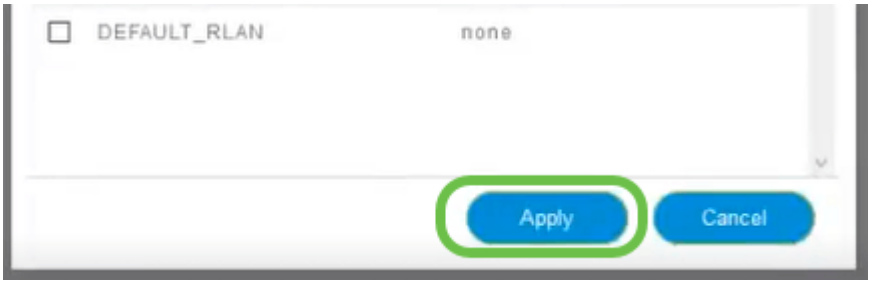
11단계

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.

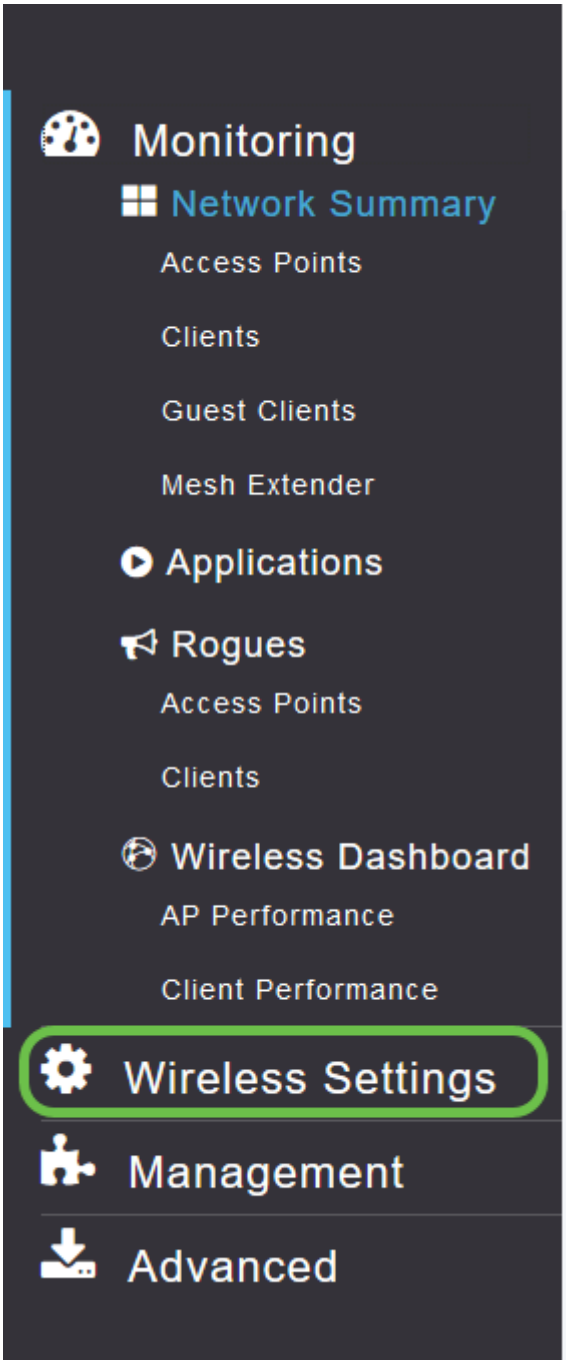
이러한 클라이언트에 대한 통계에는 사용된 데이터의 양과 처리량이 포함됩니다.

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.

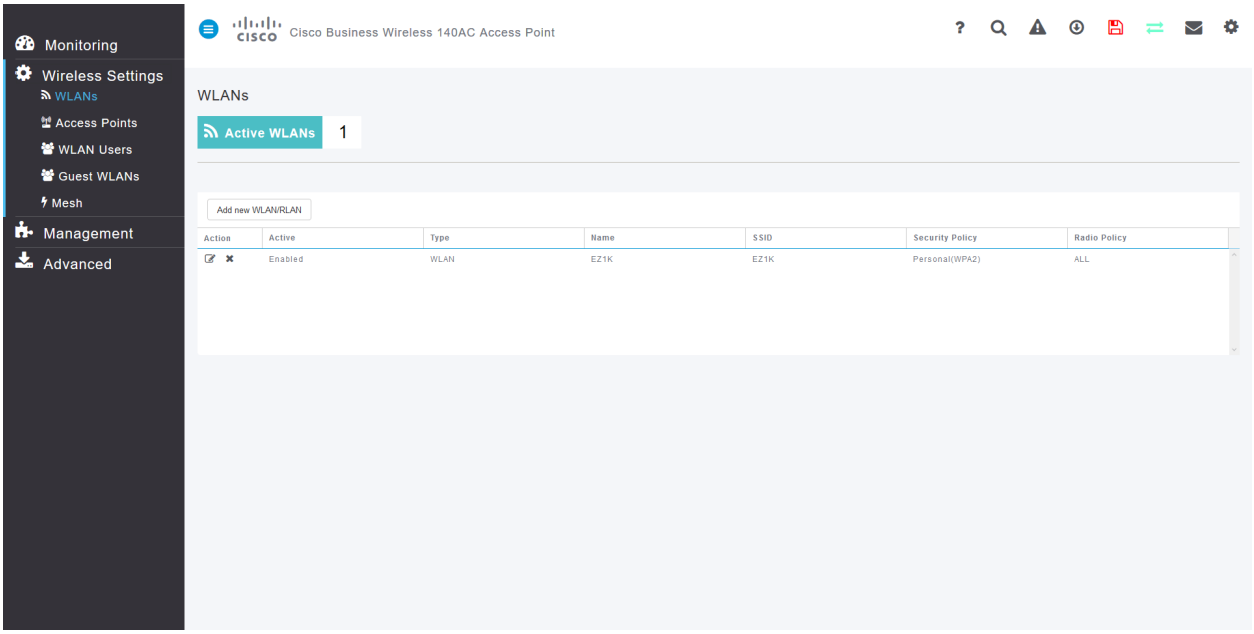
활성화되면 웹 UI의 Monitoring(모니터링) 섹션에서 네트워크에 대한 클라이언트 세부 정보를 찾을 수 있습니다.

1단계

무선 설정을 **클릭합니다**.

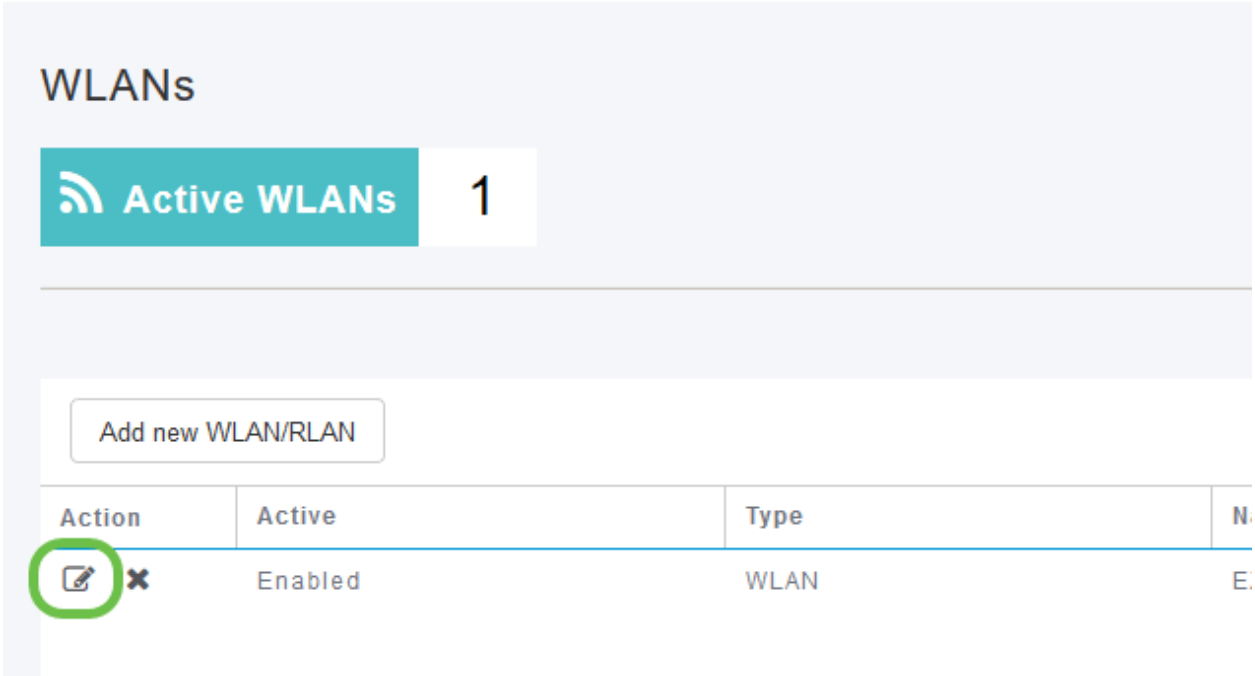


아래는 무선 설정 링크를 클릭할 때 표시되는 것과 유사합니다.



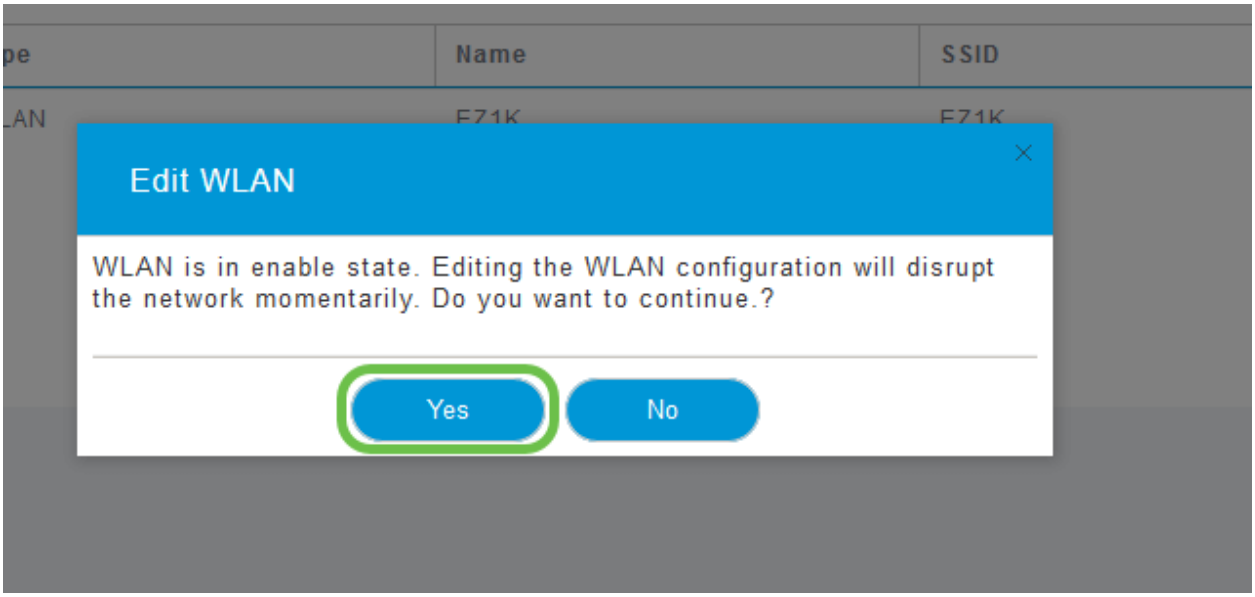
2단계

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.

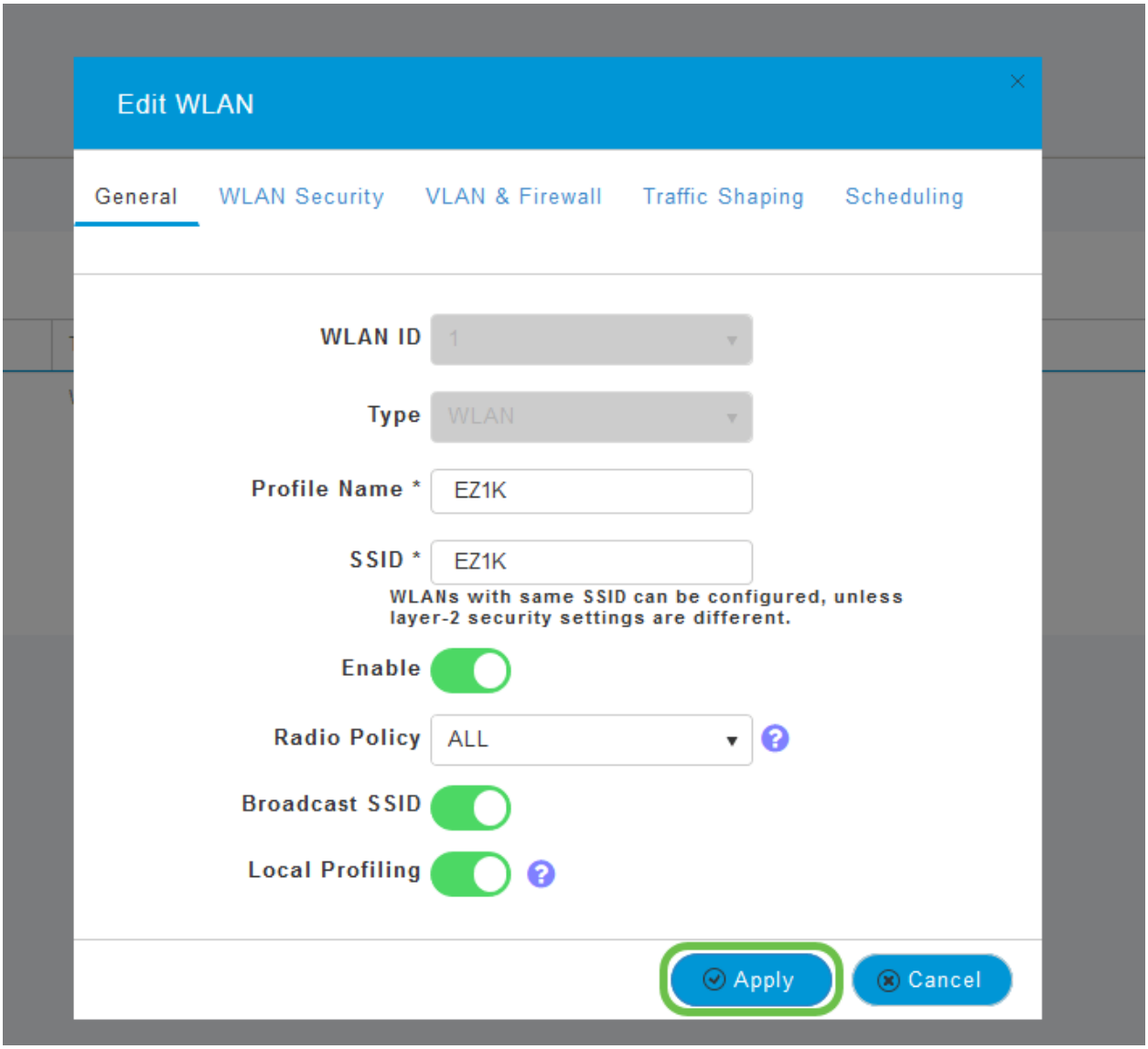


4단계

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

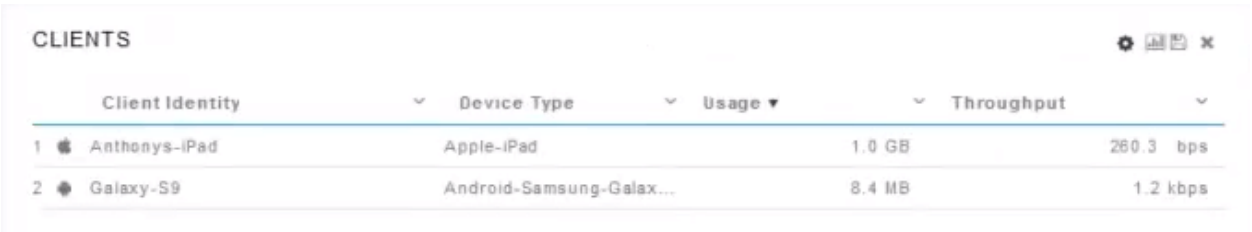
5단계

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 RV345P VPN Router with PoE
- Cisco Business 140AC Access Point
- Cisco Business 142ACM Mesh Extender