Cisco Business Wireless Access Point에서 Simple Network Management Protocol 구성

목표

이 문서의 목적은 Cisco CBW(Business Wireless) 액세스 포인트(AP)에서 SNMP(Simple Network Management Protocol) 설정을 구성하는 방법을 보여 주는 것입니다.

적용 가능한 디바이스 | 소프트웨어 버전

- 140AC(데이터 시트) | 10.0.1.0 (최신 다운로드)
- 145AC(데이터 시트) | 10.0.1.0 (최신 다운로드)
- 240AC(데이터시트) | 10.0.1.0(최신 다운로드)

소개

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

SNMP는 네트워크에 있는 모든 디바이스에서 정보를 수집하고 이러한 디바이스를 구성 및 관리하는 데 사용되는 널리 사용되는 네트워크 관리 프로토콜입니다.마스터 AP 웹 인터페이스를 사용하여 SNMP v2c 및 SNMP v3 액세스 모드를 모두 구성할 수 있습니다.SNMPv2c는 SNMPv2에 대한 커뮤니티 문자열 기반 관리 프레임워크입니다. 커뮤니티 문자열은 일반 텍스트로 전송되는 비밀번호 유형입니다.SNMP v3 기능은 네트워크를 통해 데이터 패킷을 인증하고 암호화하여 디바이스에 대한 보안 액세스를 제공합니다.

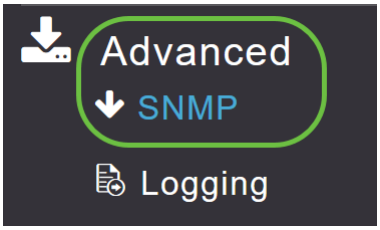
마스터 AP에 대해 다음 SNMP 액세스 모드를 구성할 수 있습니다.

- SNMP v2c 전용
- SNMP v3만
- SNMP v2c 및 SNMP v3 모두
- SNMP v2c 및 SNMP v3 모두 아님

SNMP 구성

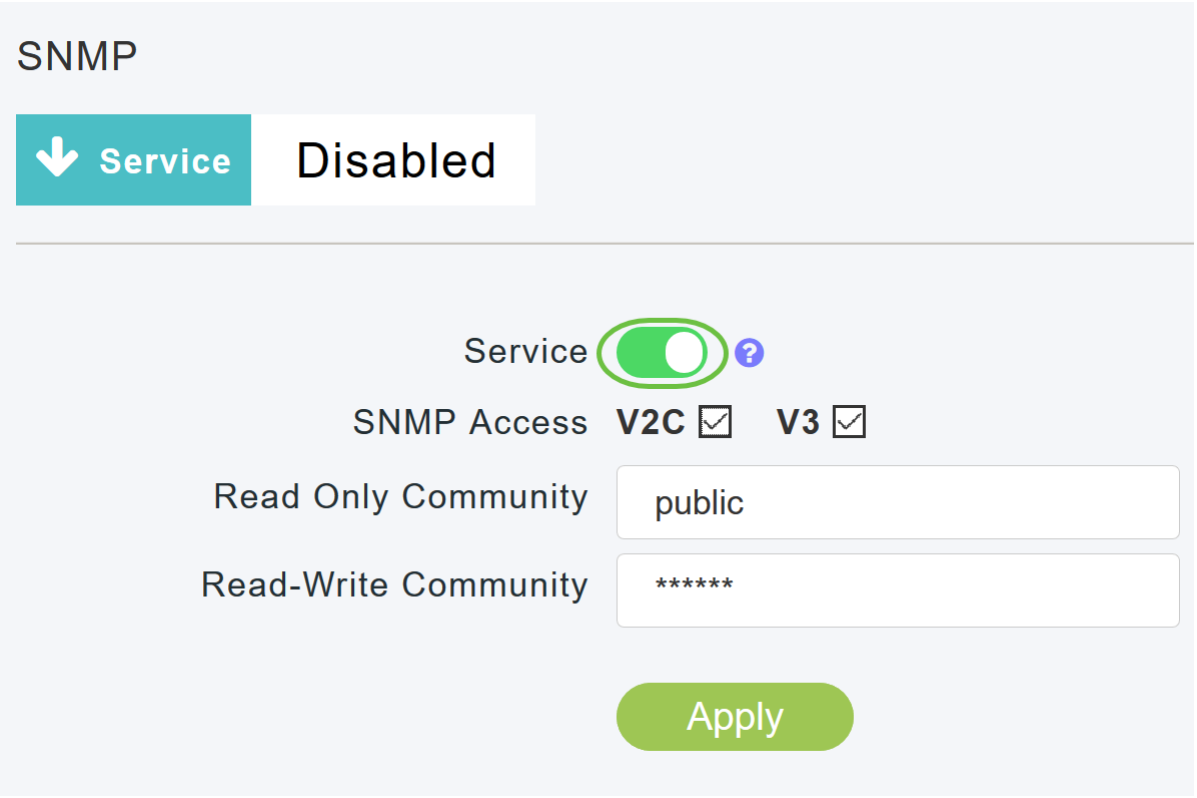
1단계

Advanced(**고급**) > **SNMP를 선택합니다**.



2단계

MIB 브라우저를 사용하여 컨피그레이션을 쿼리하기 위한 SNMP 서비스 옵션을 활성화합니다.

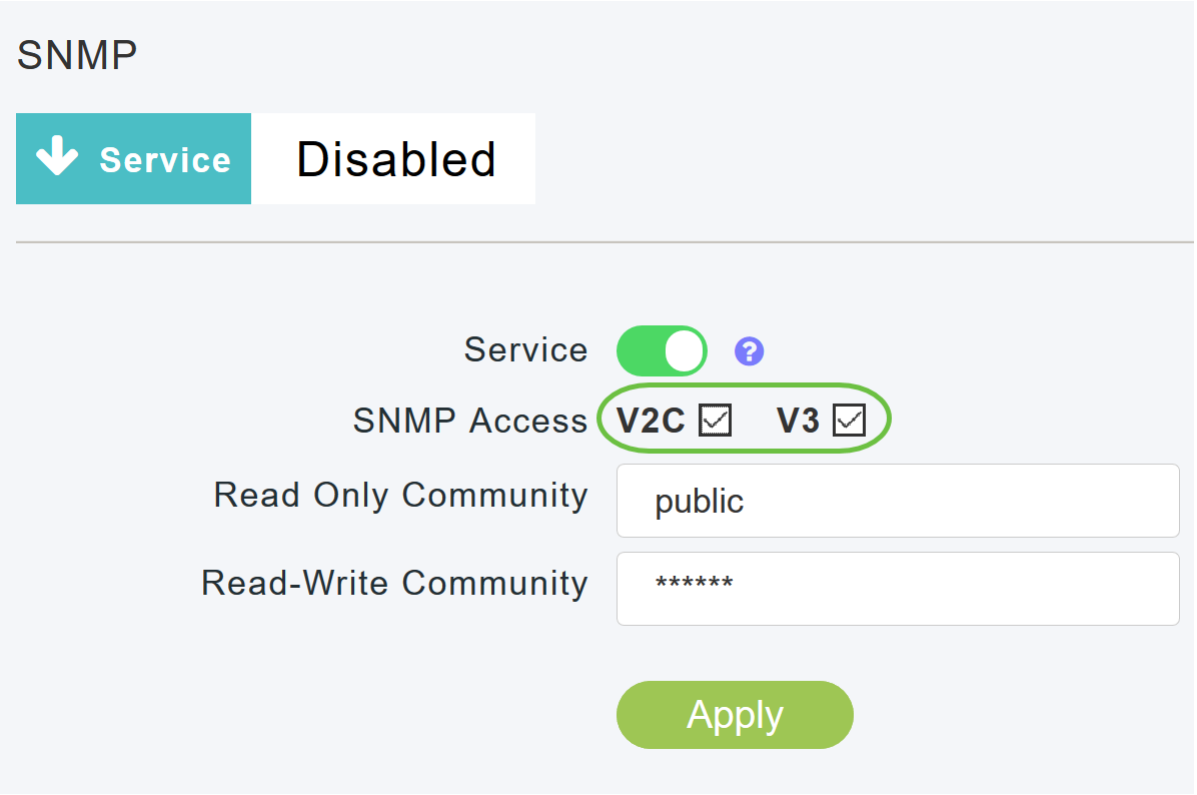


3단계

SNMP 설정 창에서 SNMP *Access* 옆에 있는 해당 확인란을 선택하여 원하는 SNMP 모드를 활성화합니다.

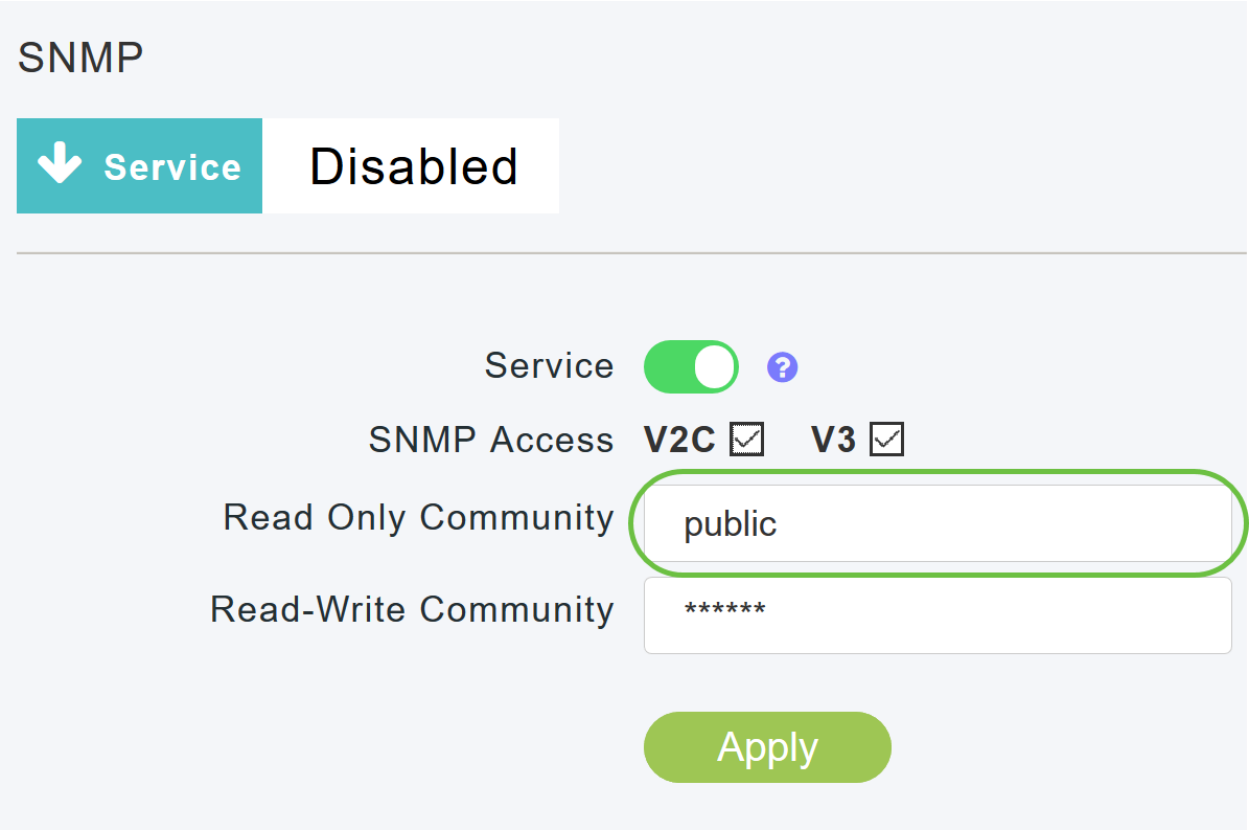
기본 모드는 v2c(또는 기본적으로 SNMP 액세스 모드 둘 다 또는 둘 다 선택되지 않음)입니다.

선택한 SNMP 액세스 모드가 활성화됩니다.



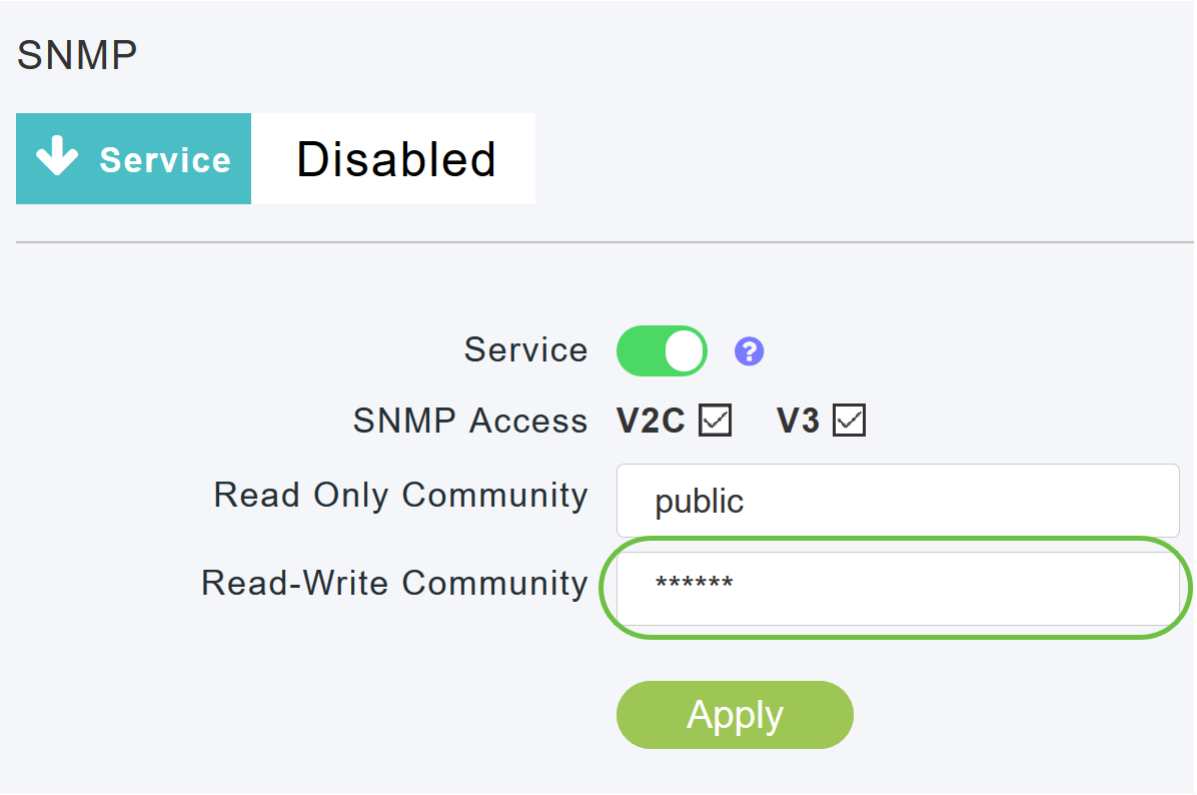
4단계

Read *Only Community* 필드에 원하는 커뮤니티 이름을 입력합니다.기본 이름은 **public**입니다.



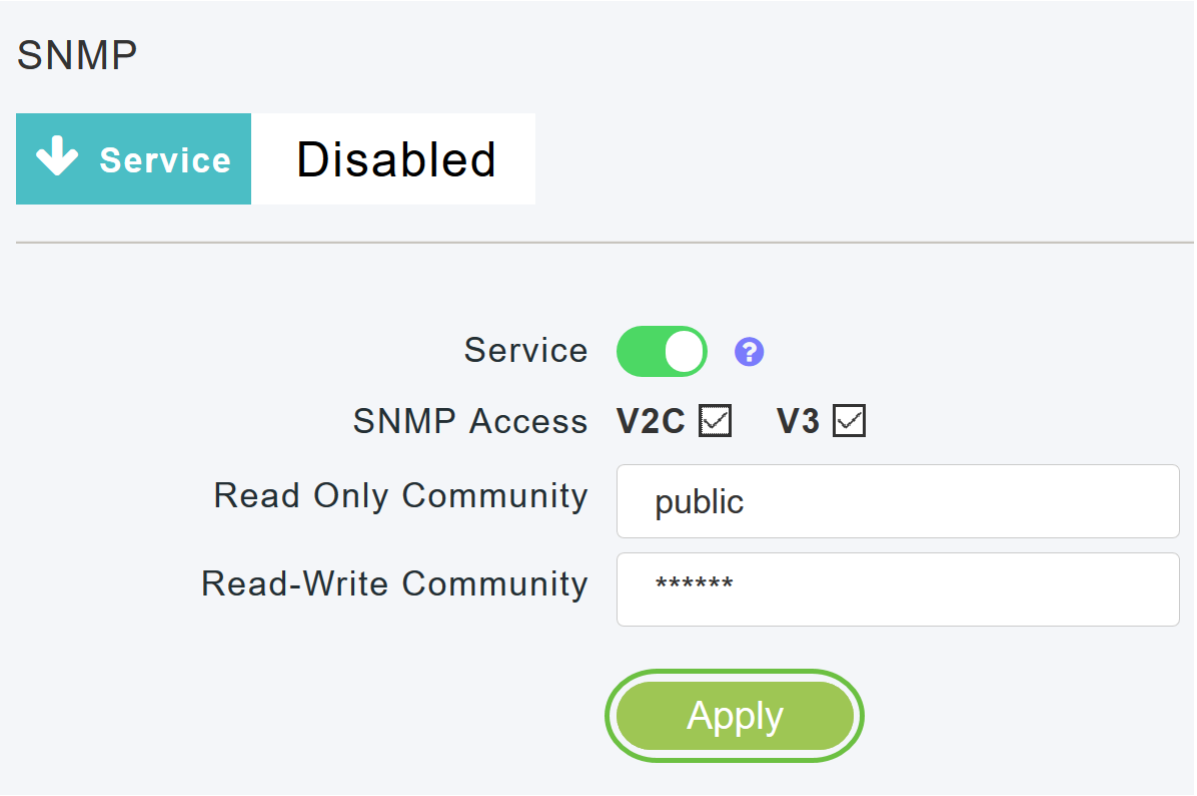
5단계

Read-*Write Community* 필드에 원하는 커뮤니티 이름을 입력합니다.기본 이름은 **private입니다**.



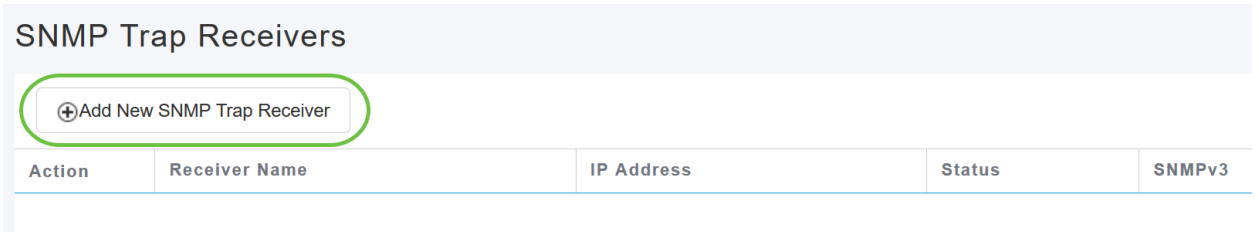
6단계

Apply를 **클릭합니다**.



7단계

SNMP Trap Receiver를 구성하려면 Add **New SNMP Trap Receiver**를 클릭합니다.이 툴은 네트워크 디바이스에서 전송된 SNMP 트랩을 수신, 로깅 및 표시합니다.기본 설정은 Disabled입니다.

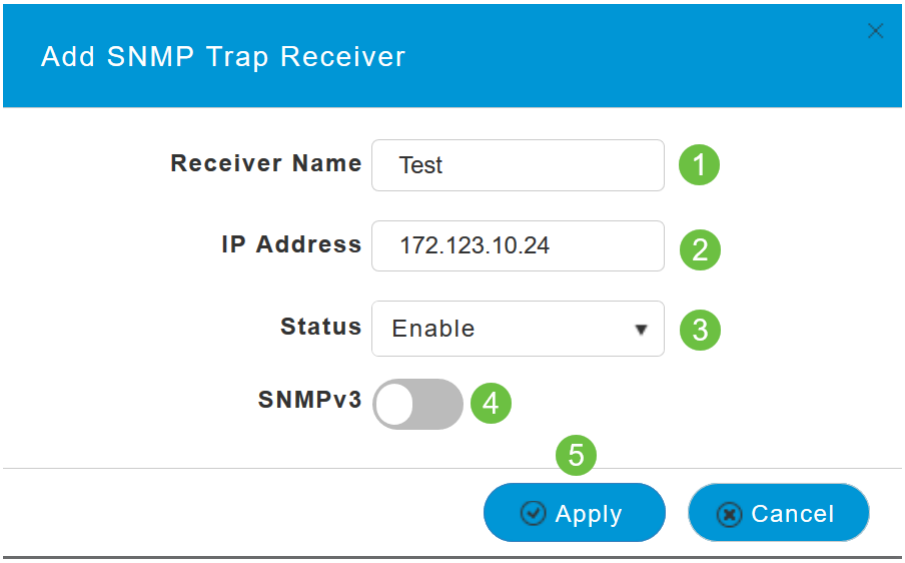


8단계

Add SNMP *Trap Receiver(SNMP 트랩 수신기 추가*) 창에서 다음을 구성합니다.

- 수신자 이름
- 연결할 서버의 IP 주소
- 상태
- SNMPv3 활성화 옵션

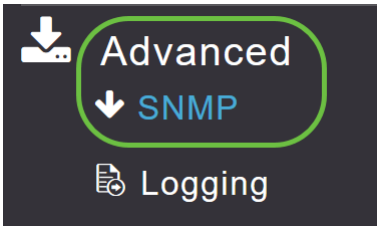
Apply를 **클릭합니다**.



SNMPv3 사용자 추가

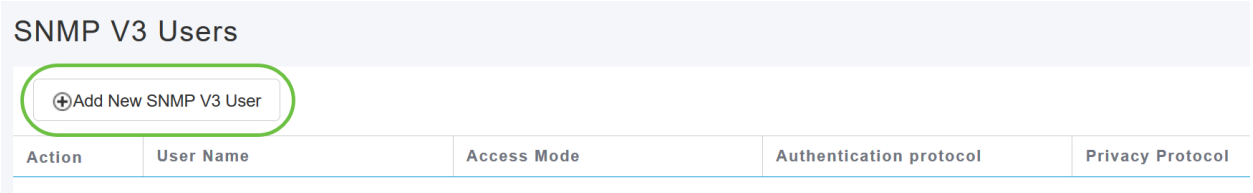
1단계

Advanced(**고급**) > **SNMP를 선택합니다**.



2단계

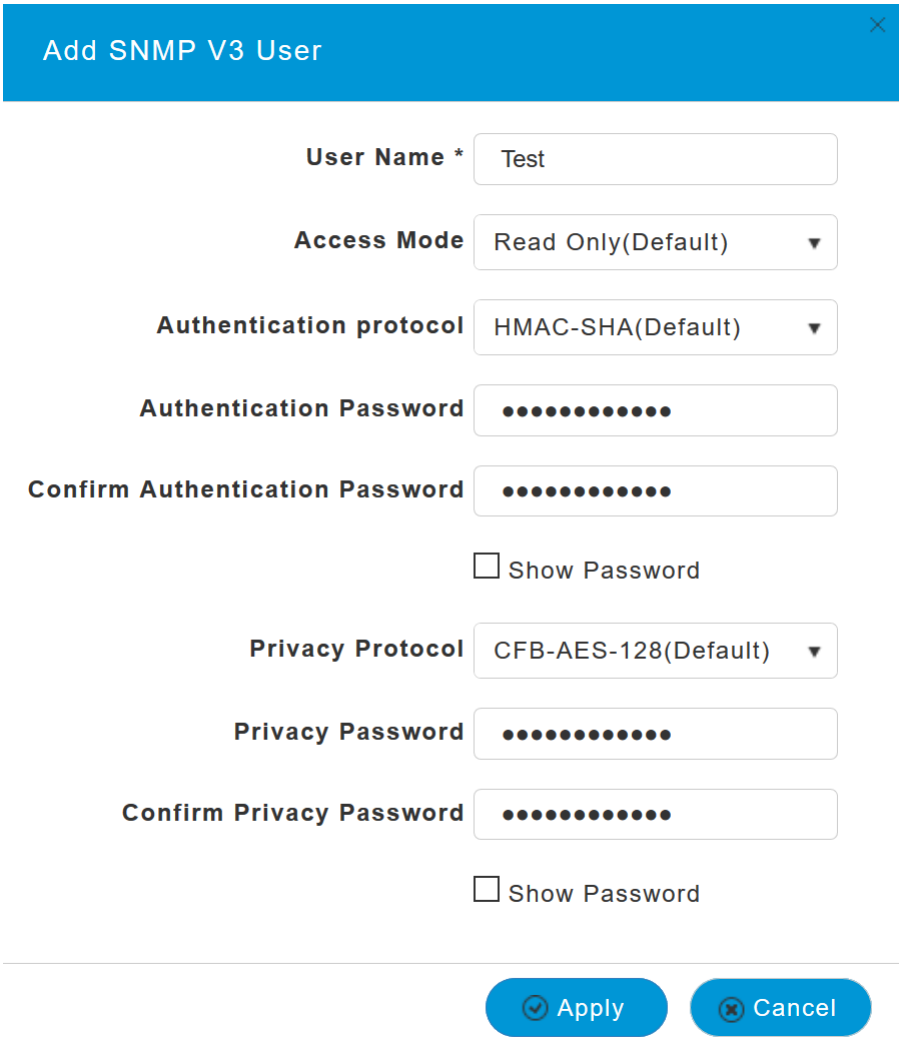
SNMP Setup(SNMP 설정) 창의 SNMPv*3 Users(SNMPv3 사용자*) 섹션에서 Add New SNMPv3 **User(새 SNMPv3 사용자 추가**) 버튼을 클릭합니다.



3단계

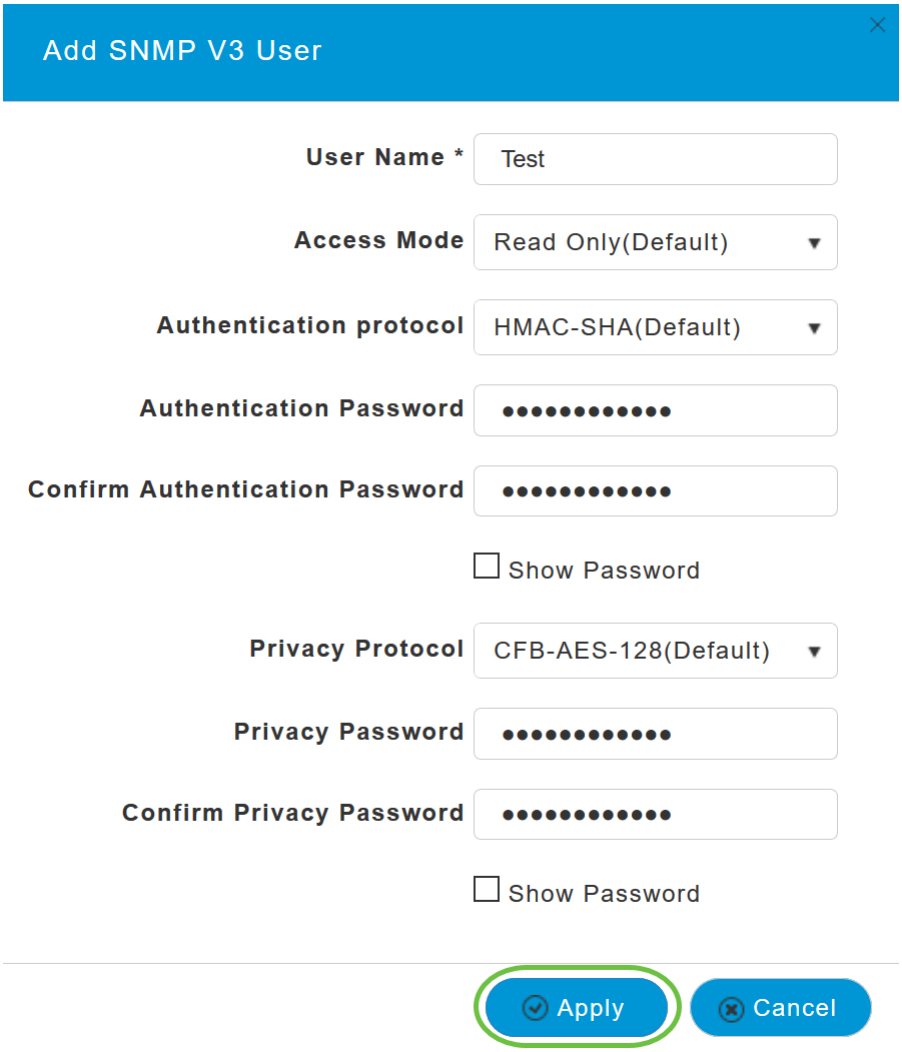
Add SNMP *v3 User(SNMP v3 사용자 추가*) 창에서 다음 세부 정보를 입력합니다.

- *User Name*(사용자 이름) - 새 SNMPv3 사용자에 대해 원하는 사용자 이름을 입력합니다.
- *액세스 모드* - 드롭다운 목록에서 원하는 모드 중 하나를 선택합니다.*읽기 전용* 또는 *읽기/쓰기.* 기본값은 **읽기 *전용입니다*.**
- *인증 프로토콜* - Authentication *Protocol* 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다 .HMAC-MD5, HMAC-SHA 또는 None입니다.기본 인증 프로토콜은 **HMAC-SHA입니다**.
- *Authentication Password(인증 비밀번호*) - 원하는 인증 비밀번호를 입력합니다.최소 비밀번호 길이는 12-31자입니다.
- *Confirm Authentication Password(인증 비밀번호 확인*) - 위에 지정된 인증 비밀번호를 확인합니다.Show Password 확인란을 선택하여 Authentication Password 및 Confirm Authentication Password 필드에 항목을 표시하고 문자가 일치하는지 확인할 수 있습니다.
- *프라이버시 프로토콜* - 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.CBC-DES, CFB-AES-128 또는 None입니다.기본 프라이버시 프로토콜은 **CFB-AES-128입니다**.
- *프라이버시 비밀번호* - 원하는 프라이버시 비밀번호를 입력합니다.최소 비밀번호 길이는 12-31자입니다.
- *Confirm Privacy Password*(프라이버시 비밀번호 확인) - 위에 지정된 프라이버시 비밀번호를 확인합니다.Show Password(비밀번호 표시) 확인란을 선택하여 Privacy Password(프라이버시 비밀번호) 및 Confirm Privacy Password(프라이버시 비밀번호 확인) 필드에 항목을 표시하고 문자가 일치하는지 확인할 수 있습니다.

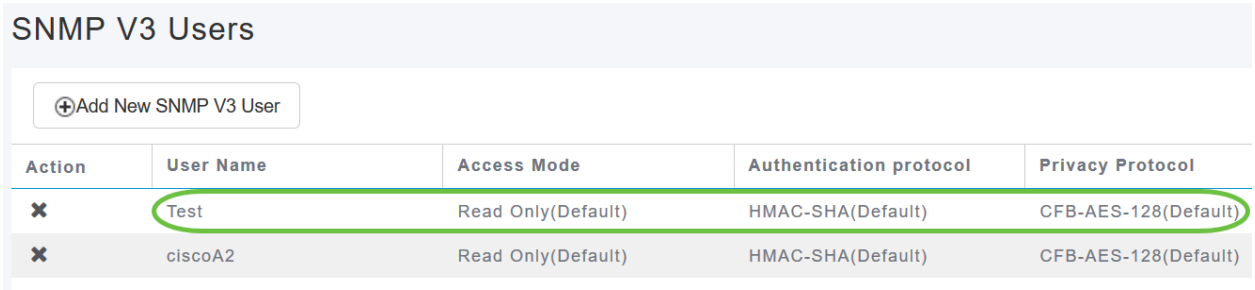


4단계

Apply(**적용**)를 클릭하여 새 SNMPv3 사용자를 생성합니다.



새로 추가된 SNMPv3 User는 SNMP Setup(SNMP 설정) 창*의 SNMP V3 Users(SNMP V3 사용자)* 테이블에 나타납니다.

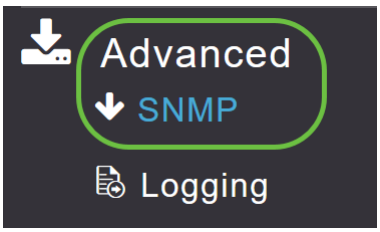


최대 7명의 SNMPv3 사용자를 추가할 수 있습니다.

SNMPv3 사용자 삭제

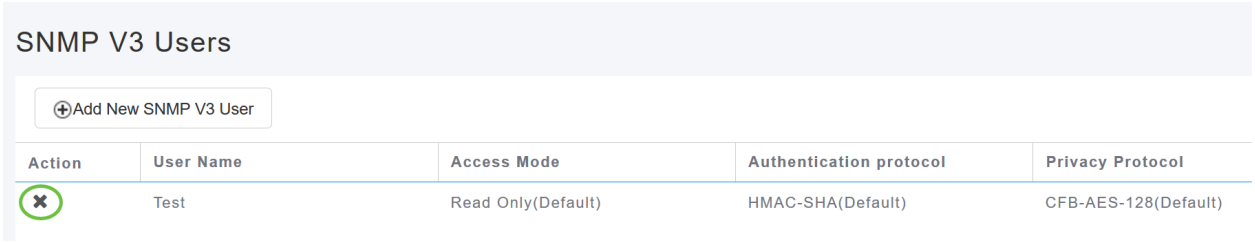
1단계

Advanced(**고급**) **> SNMP를 선택합니다**.



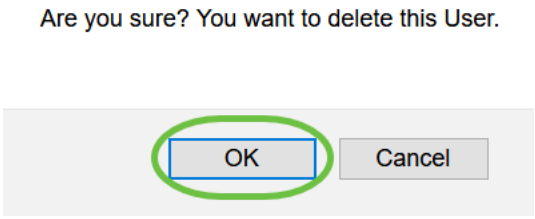
2단계

SNMP *설정*에서 삭제할 SNMPv3 사용자가 포함된 행의 **X** 아이콘을 클릭합니다.



3단계

작업을 확인하는 팝업 창이 나타납니다.**확인**을 **클릭합니다**.



SNMPv3 사용자 테이블이 새로 고쳐지고 삭제된 항목이 테이블에서 제거됩니다.

결론

모두 준비되었습니다!이제 CBW AP에서 SNMP를 성공적으로 구성했습니다.자세한 내용을 보려면 아래 기사를 읽고 손쉽게 네트워크를 관리하십시오.

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