

CBW 액세스 포인트의 개인 사전 공유 키 기능

목표

이 문서에서는 Cisco CBW(Business Wireless) AP(Access Point) 펌웨어 버전 10.6.1.0의 개인 사전 공유 키(PSK) 기능에 대해 설명합니다.

적용 가능한 디바이스 | 소프트웨어 버전

- Cisco Business Wireless 140AC Access Point | 10.6.1.0([최신 다운로드](#))
- Cisco Business Wireless 145AC Access Point | 10.6.1.0([최신 다운로드](#))
- Cisco Business Wireless 240AC Access Point | 10.6.1.0([최신 다운로드](#))

소개

네트워크에 CBW 기어가 있는 경우 이제 펌웨어 버전 10.6.1.0에서 개인 PSK 기능을 사용할 수 있습니다!

개인 PSK(iPSK)라고도 하는 개인 PSK는 관리자가 동일한 WPA2(Wi-Fi Protected Access II) 개인 WLAN(Wireless Local Area Network)에 대해 개별 장치에 대해 고유한 사전 공유 키를 발급할 수 있는 기능입니다. 고유한 PSK는 디바이스의 MAC 주소에 연결되어 있습니다. WPA3 정책이 활성화된 WLAN에서는 지원되지 않습니다.

이 기능은 RADIUS 서버를 사용하여 클라이언트를 인증합니다. 일반적으로 IoT 디바이스와 회사에서 지급한 랩톱과 모바일 디바이스에서 사용합니다.

목차

- [사전 요구 사항](#)
- [CBW RADIUS 설정 구성](#)
- [WLAN 설정 구성](#)
- [다음 단계](#)

사전 요구 사항

- CBW AP 펌웨어를 10.6.1.0으로 업그레이드했는지 확인하십시오. [펌웨어 업데이트 수행에 대한 단계별 지침을 보려면 클릭하십시오.](#)
- 개인 PSK 및 디바이스의 MAC 주소를 구성해야 하는 RADIUS 서버가 필요합니다.
- 이 CBW 기능은 FreeRADIUS, Microsoft의 NPS 및 Cisco의 ISE의 세 가지 다른 RADIUS 서버에서 지원됩니다. 구성은 사용된 RADIUS 서버에 따라 달라집니다.

CBW RADIUS 설정 구성

CBW AP에서 RADIUS 설정을 구성하려면 다음 단계를 수행합니다.

1단계

CBW AP의 UI(웹 사용자 인터페이스)에 로그인합니다.



Cisco Business Wireless Access Point

Welcome! Please click the login button to enter your user name and password



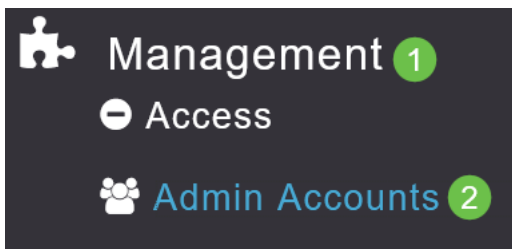
2단계

양방향 화살표 기호를 클릭하여 전문가 보기로 전환합니다.



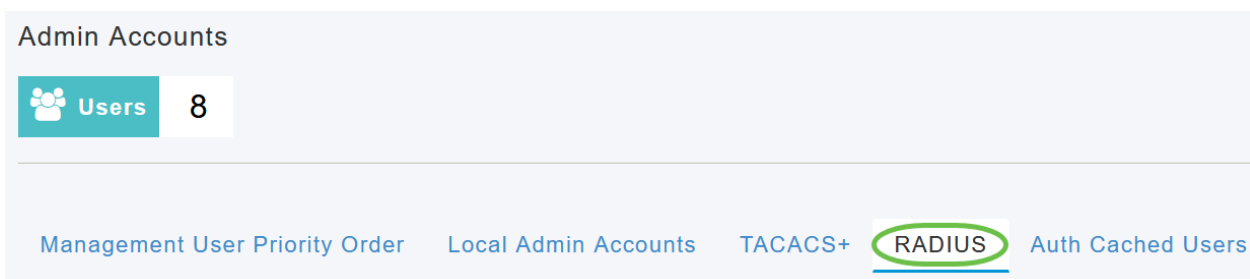
3단계

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



4단계

RADIUS 탭을 선택합니다.



5단계

Add RADIUS Authentication Server를 클릭합니다.

Action	Server Index	Network User
x	1	<input checked="" type="checkbox"/>

6단계

다음을 구성합니다.

- 서버 인덱스 - 1부터 6까지 선택
- 네트워크 사용자 - 상태를 활성화합니다. 기본적으로 이 옵션은 Enabled입니다.
- 관리 - 상태를 활성화합니다. 기본적으로 이 옵션은 Enabled입니다.
- 상태 - 상태를 활성화합니다. 기본적으로 이 옵션은 Enabled입니다.
- CoA - CoA(Charge of Authority)가 활성화되어 있는지 확인합니다.
- 서버 IP 주소 - RADIUS 서버의 IPv4 주소를 입력합니다.
- 공유 암호 - 공유 암호 키를 입력합니다.
- Port Number(포트 번호) - RADIUS 서버와 통신하는 데 사용할 포트 번호를 입력합니다.
- Server Timeout(서버 시간 제한) - 서버 시간 제한을 입력합니다.

Apply를 클릭합니다.

Add/Edit RADIUS Authentication Server. x

Server Index

Network User

Management

State

CoA

Server IP Address

Shared Secret

Confirm Shared Secret

Show Password

Port Number

Server Timeout Seconds

2
Apply
Cancel

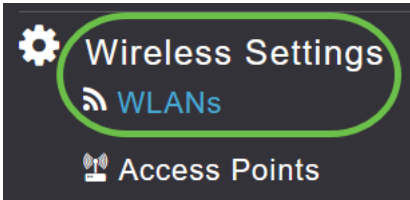
WLAN 설정 구성

표준 WPA2 개인 보안 WLAN으로 WLAN을 생성합니다.

사전 공유 키는 개인 PSK 장치에 사용되지 않습니다. 이는 RADIUS 서버에서 인증되지 않은 디바이스에만 사용됩니다. 이 WLAN에 연결할 장치의 MAC 주소를 이 장치의 허용 목록에 추가해야 합니다.

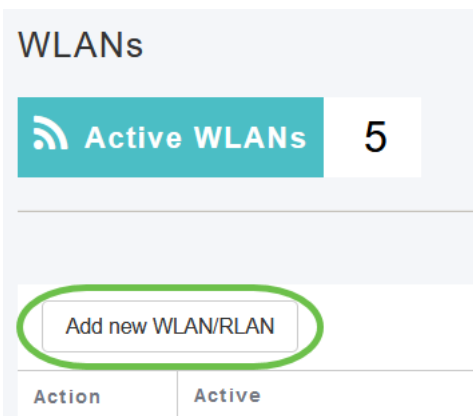
1단계

Wireless Settings(무선 설정) > WLANs(WLAN)로 이동합니다.



2단계

Add new WLAN/RLAN(새 WLAN/RLAN 추가)를 클릭합니다.



3단계

General(일반) 탭에서 WLAN의 Profile Name(프로파일 이름)을 입력합니다.

Add new WLAN

1

General **WLAN Security** VLAN & Firewall Traffic Shaping Advanced Scheduling

WLAN ID 4

Type WLAN

Profile Name * Personal

SSID * Personal

WLANs with same SSID can be configured, unless layer-2 security settings are different.

Enable

Radio Policy ALL ?

Broadcast SSID

Local Profiling ?

Apply

Cancel

4단계

WLAN Security(WLAN 보안) 탭으로 이동하고 토글을 슬라이딩하여 MAC 필터링을 활성화합니다.

1

General **WLAN Security** VLAN & Firewall Traffic Shaping

Guest Network

Captive Network Assistant

MAC Filtering ? 2

Security Type WPA2/WPA3 Personal

WPA2 WPA3

Passphrase Format ASCII

Passphrase * *****

Confirm Passphrase * *****

Show Passphrase

Password Expiry ?

5단계

Add RADIUS Authentication Server(RADIUS 인증 서버 추가)를 클릭하여 이전 섹션에서 구성한 RADIUS 서버를 추가하여 이 WLAN에 대한 인증을 제공합니다.

Authentication Caching

Add RADIUS Authentication Server

6단계

팝업 창이 나타납니다. Server IP Address, State 및 Port Number를 입력합니다. Apply를 클릭합니다.

Add RADIUS Authentication Server ✕

Radius Server can be configured from 'Admin Accounts > RADIUS'(Expert view).

Server IP Address

State

Port Number

2 Apply
Cancel

7단계

(선택 사항)

인증 캐싱을 활성화합니다. 이 옵션을 활성화하면 다음 필드가 표시됩니다.

- *User Cache Timeout* - 캐시에서 인증된 자격 증명이 만료되는 기간을 지정합니다.
- *사용자 캐시 재사용* - 캐시 시간 초과 전에 자격 증명 캐시 정보를 사용합니다. 기본적으로
을(를) 사용할 수 없습니다.

Authentication Caching

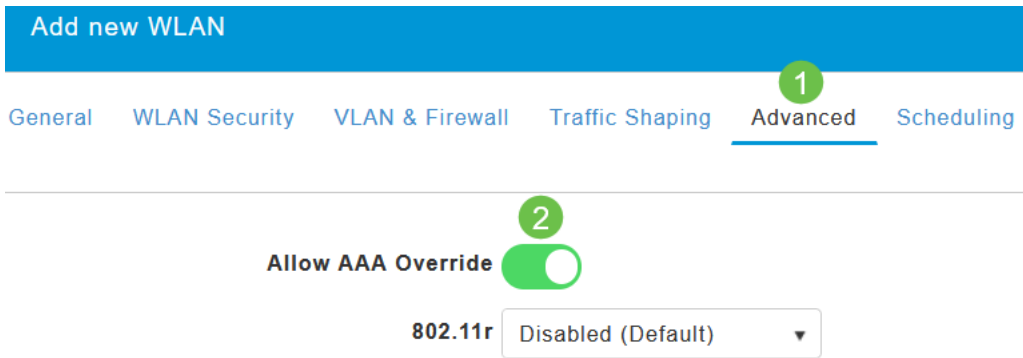
User Cache Timeout minutes

User Cache Reuse

이 기능이 활성화된 경우, 이 서버에 이미 인증된 클라이언트는 향후 24시간 내에 이 WLAN에 다시 연결할 때 RADIUS 서버에 데이터를 전달할 필요가 없습니다.

8단계

Advanced(고급) 탭으로 이동합니다. 토글을 슬라이딩하여 Allow AAA Override를 활성화합니다.

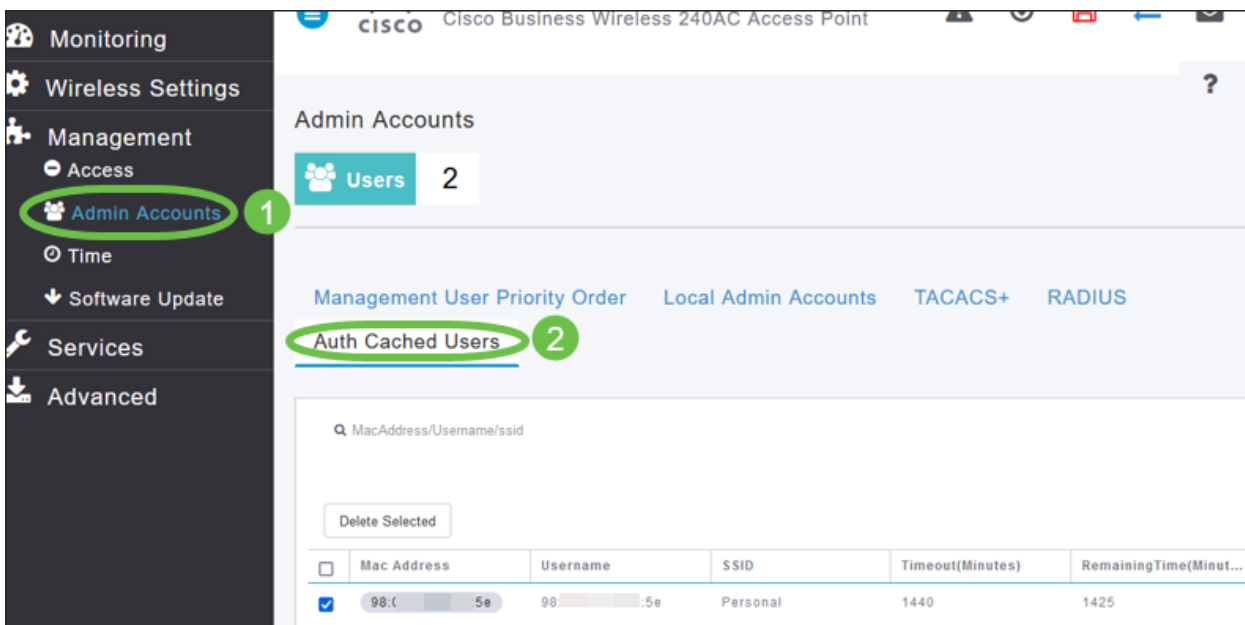


고급 탭은 전문가 보기에 있는 경우에만 표시됩니다.

다음 단계

CBW AP에서 설정을 구성하고 RADIUS 서버를 설정했으면 장치를 연결할 수 있어야 합니다. 해당 MAC 주소에 대해 구성된 맞춤형 PSK를 입력하면 네트워크에 연결됩니다.

인증 캐싱을 구성한 경우 Admin Accounts(관리 계정) 아래의 Auth Cached Users(인증 캐시된 사용자) 탭으로 이동하여 WLAN에 가입한 디바이스를 볼 수 있습니다. 필요한 경우 삭제할 수 있습니다.



결론

자, 간다! 이제 CBW AP에서 개인 PSK 기능의 혜택을 누릴 수 있습니다.