Cisco Business Wireless Network에서 비인가 클라이언트 식별

목표

이 문서의 목적은 Cisco Business Wireless(CBW) 기존 또는 메시 네트워크에서 비인가 AP(Access Point)와 비인가 무선 클라이언트를 식별하는 방법을 보여 주는 것입니다.

적용 가능한 장치 | 펌웨어 버전

- 140AC(데이터 시트) | 10.0.1.0(최신 다운로드)
- 141ACM (데이터 시트) | 10.0.1.0(최신 다운로드) - 익스텐더는 메시 네트워크에서만 사용됩니다.
- 142ACM (데이터 시트) | 10.0.1.0(최신 다운로드) - 익스텐더는 메시 네트워크에서만 사용됩니다.
- 143ACM (데이터 시트) | 10.0.1.0(최신 다운로드) - 익스텐더는 메시 네트워크에서만 사용됩니다.
- 145AC(데이터 시트) | 10.0.1.0(최신 다운로드)
- 240AC(데이터 시트) | 10.0.1.0(최신 다운로드)
- 150AX(데이터 시트) | 10.3.2.0(최신 다운로드)
- 151AXM (데이터 시트) | 10.3.2.0(최신 다운로드)

CBW 15x 시리즈 디바이스는 CBW 14x/240 시리즈 디바이스와 호환되지 않으며 동일한 LAN에서 공존할 수 없습니다.

소개

CBW AP(Access Point)는 내부 안테나가 포함된 802.11 a/b/g/n/ac(Wave 2) 기반입니다. 기존 독립형 디바이스 또는 메시 네트워크의 일부로 사용할 수 있습니다.

완벽한 세상에서는 모든 사람이 무선 네트워크를 사용할 때 공손하고 솔직하게 대할 수 있습니다. 안타깝게도, 우리는 완벽한 세상에 살고 있지 않습니다. 관리자로서 여러분의 일은 잠재적인 문제를 인식하는 것입니다.

비인가 AP는 사용자의 허가 없이 네트워크에 설치된 AP입니다. 비인가 클라이언트는 회사에 속하지 않은 다른 탐지된 장치입니다.

이러한 연결은 순전히 불법일 수 있지만, 이러한 악의적인 사용자가 네트워크를 공격하거나 중요한 정보를 훔쳐낼 위험이 항상 있습니다. 이를 따라잡기 위해 비인가 AP 및 비인가 클라이언트를 볼 수 있습니다. 일단 탐지되면 이러한 로그는 AP를 통해 차단될 수 없지만 추가 조사를 위한 정보를 제공합니다.

CBW AP는 현재 사용 중인 채널 또는 겹치는 채널의 경로만 탐지합니다.

비인가 AP 보기

이 전환된 섹션에는 초보자를 위한 팁이 강조 표시됩니다.

로그인

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

도구 설명

사용자 인터페이스의 필드에 대한 질문이 있는 경우 다음과 같은 도구 설명을 확인합니다.

Expand Main Menu(주 메뉴 확장) 아이콘을 찾는 데 문제가 있습니까?

화면 왼쪽의 메뉴로 이동한 다음 메뉴 버튼이 표시되지 않으면 이 아이콘을 클릭하여 측면 바 메뉴를 엽니다.

Cisco 비즈니스 앱

이러한 장치에는 웹 사용자 인터페이스와 일부 관리 기능을 공유하는 컴패니언 앱이 있습니다. 웹 사용자 인터페이스의 일부 기능은 앱에서 사용할 수 없습니다.

iOS 앱 다운로드 Android 앱 다운로드

자주 묻는 질문(FAQ)

아직 해결되지 않은 질문이 있는 경우, FAQ 문서를 확인하실 수 있습니다. FAQ

1단계

기본 AP의 웹 UI(사용자 인터페이스)에 로그인합니다. 이렇게 하려면 웹 브라우저를 열고 https://ciscobusiness.cisco을 *입력합니다*. 계속하기 전에 경고가 표시될 수 있습니다. 자격 증명을 입력합니다.

웹 브라우저에 https://*<ipaddress>*(기본 AP의)를 입력하여 기본 AP에 액세스할 수도 있습니다.

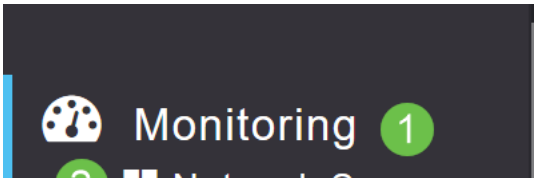
사용하는 용어에 익숙하지 않은 경우 Cisco Business: Glossary of New Terms를 확인하십시오.

2단계

이러한 컨피그레이션을 수행하려면 Expert View에 있어야 *합니다*. 웹 UI의 오른쪽 상단 메뉴에서 **화살표 아이콘**을 클릭하여 *Expert* View로 *전환합니다*.

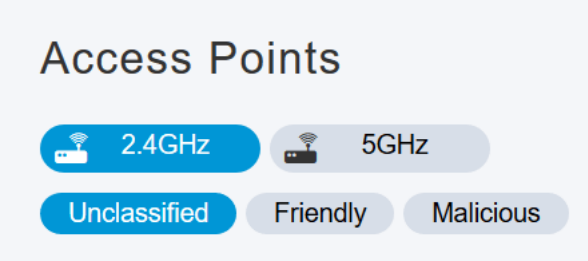
3단계

Monitoring(**모니터링**) > **Network Summary(네트워크 요약)** > **Rogues(비인가)** > **Access Points(액세스 포인트)로 이동합니다.**



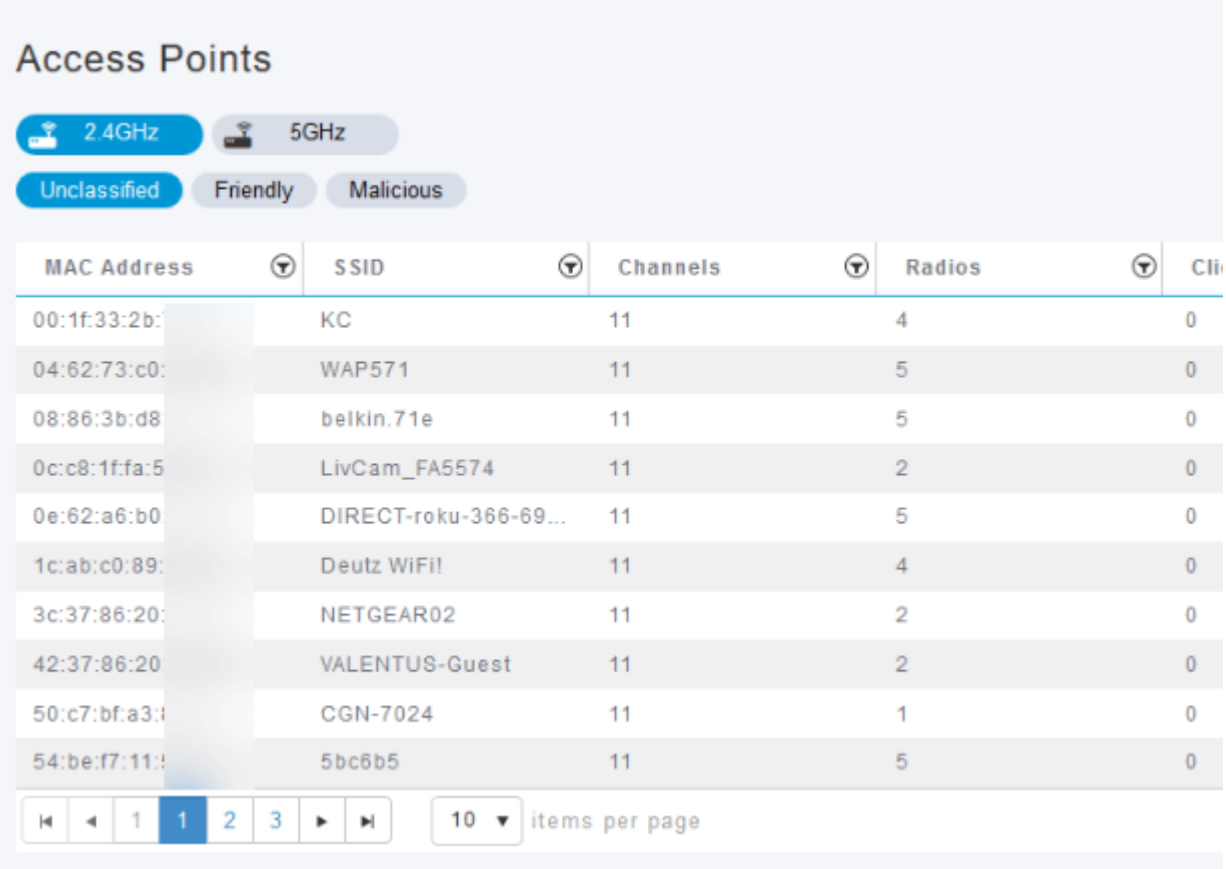
4단계

이 페이지가 열리면 탭을 클릭하여 2.4GHz 또는 5GHz를 표시하도록 선택할 수 있습니다. 기본적으로 모든 비인가 AP는 Unclassified(미분류)로 표시됩니다. AP는 비인가 AP에 대한 레이블을 변경하지 않습니다. 즉, 수동으로 변경할 수 있습니다.



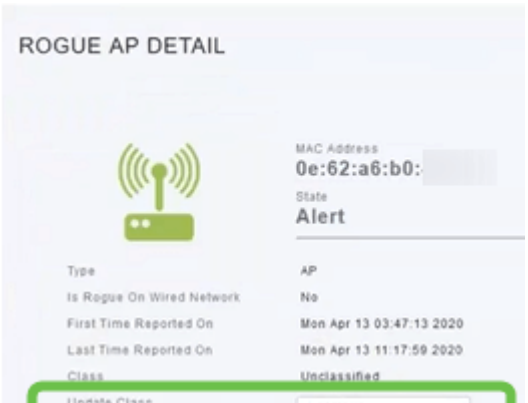
5단계

비인가 AP가 나열되면 그 중 하나를 클릭하여 자세히 조사할 수 있습니다.



6단계(선택 사항)

AP를 *Friendly* 또는 Malicious로 분류하려는 경우, Update Class(*클래스 업데이트)* 드롭다운 메뉴에서 두 옵션 중 하나를 선택할 수 *있습니다*. 향후 미분류 액세스 포인트를 살펴볼 때 전체 목록을 일일이 정렬할 필요가 없도록 해야 할 수도 있습니다. 완료되면 **Apply**(적용)를 클릭해야 합니다.



7단계(선택 사항)

AP를 *내부*(네트워크 내) 또는 *외부*(인접 회사)로 라벨링하려면 *Update Status(업데이트 상태) 섹션*에서 라벨링을 수행할 수 있습니다. 완료되면 **Apply**를 클릭합니다.

비인가 클라이언트 보기

1단계

기본 AP의 웹 UI에 로그인합니다. 이렇게 하려면 웹 브라우저를 열고 https://ciscobusiness.cisco을 *입력합니다*. 계속하기 전에 경고가 표시될 수 있습니다. 자격 증명을 입력합니다.

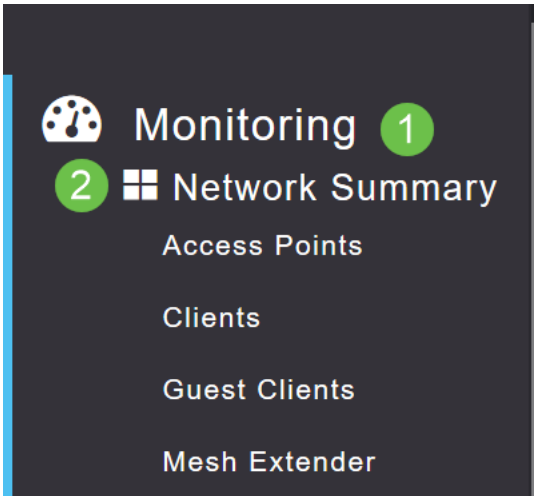
웹 브라우저에 https://*<ipaddress>*(기본 AP의)를 입력하여 기본 AP에 액세스할 수도 있습니다. Cisco Business Mobile 앱에서 몇 가지 조치를 취할 수 있습니다.

2단계

이러한 컨피그레이션을 수행하려면 Expert View에 있어야 *합니다*. 웹 UI의 오른쪽 상단 메뉴에서 **화살표 아이콘**을 클릭하여 *Expert* View로 *전환합니다*. RADIUS 서버 설정에 대한 자세한 내용은 Radius를 체크아웃

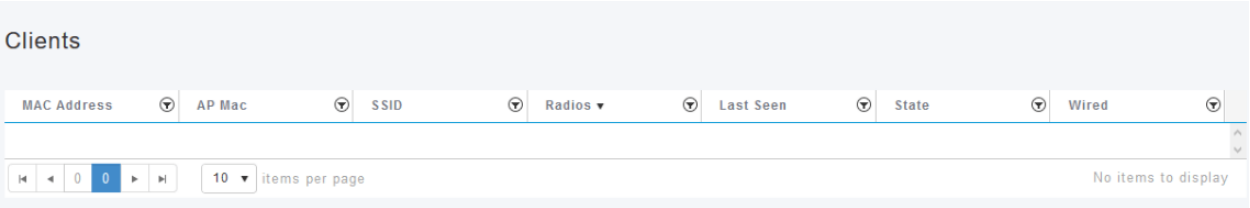
3단계

Monitoring(**모니터링**) > **Network Summary(네트워크 요약)** > **Rogues(비인가)** > **Clients(클라이언트)로 이동합니다.**



4단계

비인가 클라이언트가 있는 경우 해당 클라이언트가 나열됩니다. 이 예에서는 비인가 클라이언트가 탐지되지 않았습니다.



결론

이제 네트워크에서 비인가를 볼 수 있습니다. 사용 중인 채널에서 많은 비인가가 표시되면 채널을 변경할 수 있습니다. 염두에 두어야 할 고려 사항이 있으므로 RF 채널 변경 문서(사용 가능한 경우 링크)를 확인하십시오.

자주 묻는 질문(FAQ) RADIUS 펌웨어 업그레이드 RLAN 애플리케이션 프로파일링 클라이언트 프로파일링 기본 AP 툴 Umbrella WLAN 사용자 로깅 트래픽 셰이핑 비인가 간섭 요인 컨피그레이션 관리 포트 컨피그레이션 메시 모드 CBW 메시 네트워킹 시작 이메일 인증 및 RADIUS 계정 관리를 사용하는 게스트 네트워크 문제 해결 CBW와 함께 Draytek 라우터 사용

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.