Identifizierung nicht autorisierter Clients in einem Cisco Business Wireless-Netzwerk

Ziel

In diesem Artikel wird erläutert, wie Sie in einem herkömmlichen oder Mesh-Netzwerk von Cisco Business Wireless (CBW) nicht autorisierte Access Points (APs) und nicht autorisierte Wireless-Clients identifizieren können.

Unterstützte Geräte | Firmware-Version

- 140AC (Datenblatt) | 10.0.1.0 (Aktuelle Version herunterladen)
- 141ACM (Datenblatt) | 10.0.1.0 (Neueste Version herunterladen) - Extender werden nur in einem Mesh-Netzwerk verwendet
- 142ACM (Datenblatt) | 10.0.1.0 (Neueste Version herunterladen) - Extender werden nur in einem Mesh-Netzwerk verwendet
- 143ACM (Datenblatt) | 10.0.1.0 (Neueste Version herunterladen) - Extender werden nur in einem Mesh-Netzwerk verwendet
- 145AC (Datenblatt) | 10.0.1.0 (Aktuelle Version herunterladen)
- 240AC (Datenblatt) | 10.0.1.0 (Aktuelle Version herunterladen)
- 150AX (Datenblatt) | 10.3.2.0 (Aktuelle Version herunterladen)
- 151AXM (Datenblatt) | 10.3.2.0 (Aktuelle Version herunterladen)

Geräte der Serie CBW 15x sind nicht mit Geräten der Serie CBW 14x/240 kompatibel, und die gleichzeitige Verwendung im gleichen LAN wird nicht unterstützt.

Einleitung

CBW Access Points (APs) basieren auf 802.11 a/b/g/n/ac (Wave 2) und verfügen über interne Antennen. Sie können als herkömmliche Einzelgeräte oder als Teil eines Mesh-Netzwerks verwendet werden.

In einer perfekten Welt wäre jeder respektvoll und ehrlich, wenn er Ihr Wireless-Netzwerk nutzen würde. Leider leben wir nicht in einer perfekten Welt. Als Administrator ist es Ihre Aufgabe, mögliche Probleme zu erkennen.

Nicht autorisierte APs sind APs, die ohne Ihre Erlaubnis in einem Netzwerk installiert wurden. Als nicht autorisierte Clients werden alle anderen erkannten Geräte bezeichnet, die nicht zu Ihrem Unternehmen gehören.

Diese Verbindungen können völlig unschuldig sein, aber es besteht immer das Risiko, dass diese Schurken versuchen, Ihr Netzwerk anzugreifen oder vertrauliche Informationen zu stehlen. Sie können die nicht autorisierten APs und Clients anzeigen, um den Überblick zu behalten. Sobald diese unberechtigten Geräte erkannt wurden, können sie nicht mehr über den Access Point blockiert werden. Sie erhalten jedoch Informationen, die Sie weiter untersuchen können.

Die CBW APs erkennen nur unberechtigte Teilnehmer auf Kanälen, die Sie derzeit verwenden, oder Kanäle, die sich überschneiden.

Nicht autorisierte APs anzeigen

Diese umschaltbare Sektion zeigt Tipps für Anfänger.

Anmeldung

Melden Sie sich bei der Webbenutzeroberfläche (UI) des primären Access Points an. Öffnen Sie dazu einen Webbrowser, und geben Sie https://ciscobusiness.cisco ein. Möglicherweise erhalten Sie eine Warnung, bevor Sie fortfahren. Geben Sie Ihre Anmeldeinformationen ein.Sie können auch auf den primären Access Point zugreifen, indem Sie https://[ipaddress] (des primären Access Points) in einen Webbrowser eingeben.

Quick-Info

Wenn Sie Fragen zu einem Feld in der Benutzeroberfläche haben, überprüfen Sie, ob der Tooltipp wie folgt aussieht: 

Probleme beim Auffinden des Symbols "Hauptmenü erweitern"?

Navigieren Sie zum Menü auf der linken Seite des Bildschirms. Wenn die Menüschaltfläche nicht angezeigt wird, klicken Sie auf dieses Symbol, um das Menü in der Seitenleiste zu öffnen. 

Cisco Business-Anwendung

Diese Geräte verfügen über Begleitanwendungen, die einige Verwaltungsfunktionen mit der Web-Benutzeroberfläche teilen. Nicht alle Funktionen der Web-Benutzeroberfläche sind in der App verfügbar.

iOS-App herunterladen Android-App herunterladen

Häufig gestellte Fragen

Wenn Sie noch Fragen haben, können Sie unser Dokument mit häufig gestellten Fragen lesen. Häufig gestellte Fragen

Schritt 1

Melden Sie sich bei der Webbenutzeroberfläche (UI) des primären Access Points an. Öffnen Sie dazu einen Webbrowser, und geben Sie *https://ciscobusiness.cisco ein*. Möglicherweise erhalten Sie eine Warnung, bevor Sie fortfahren. Geben Sie Ihre Anmeldeinformationen ein.

Sie können auch auf den primären Access Point zugreifen, indem Sie *https://<ipaddress>* (des primären Access Points) in einen Webbrowser eingeben.

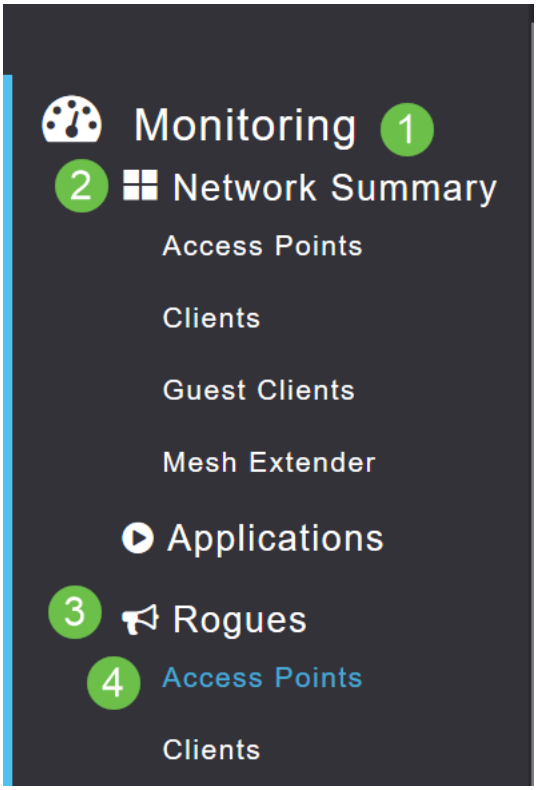
Wenn Sie mit den verwendeten Begriffen nicht vertraut sind, lesen Sie Cisco Business: Glossar der neuen Begriffe.

Schritt 2

Um diese Konfigurationen vorzunehmen, benötigen Sie eine *Expertenansicht*. Klicken Sie auf das **Pfeilsymbol** oben rechts in der Webbenutzeroberfläche, um zur *Expertenansicht* zu wechseln.

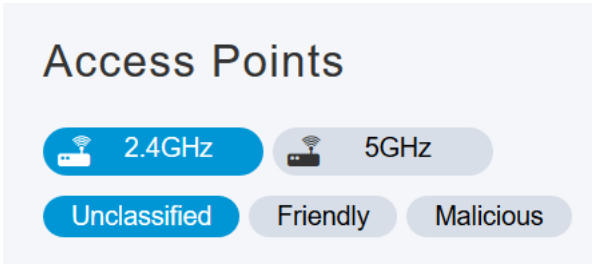
Schritt 3

Navigieren Sie zu **Monitoring > Network Summary > Rogues > Access Points.**



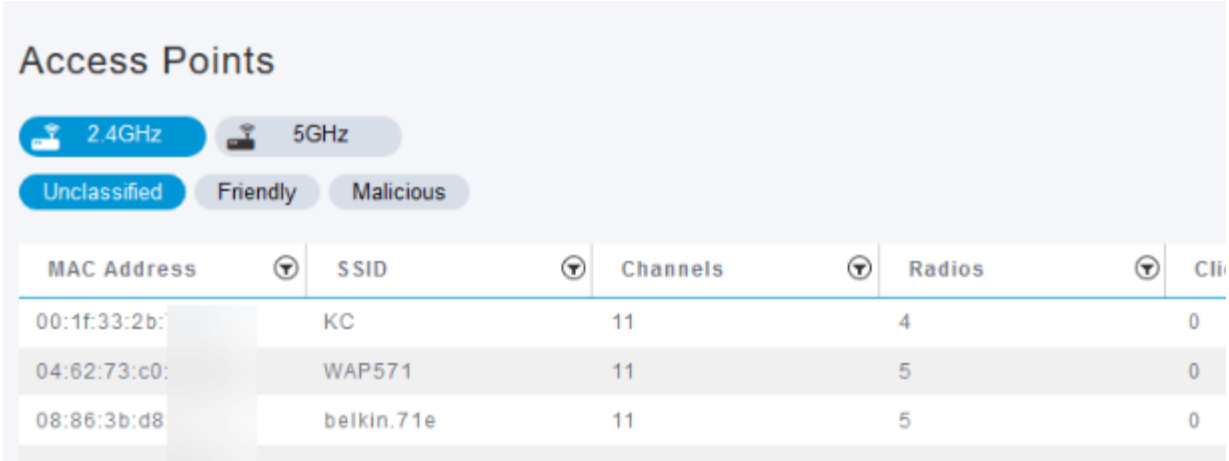
Schritt 4

Wenn diese Seite geöffnet wird, können Sie durch Klicken auf die Registerkarte auswählen, dass 2,4 GHz oder 5 GHz angezeigt wird. Standardmäßig sind alle nicht autorisierten Access Points als nicht klassifiziert gekennzeichnet. Der Access Point ändert die Beschriftungen für die nicht autorisierten Access Points nicht. Dies müssen Sie manuell vornehmen.



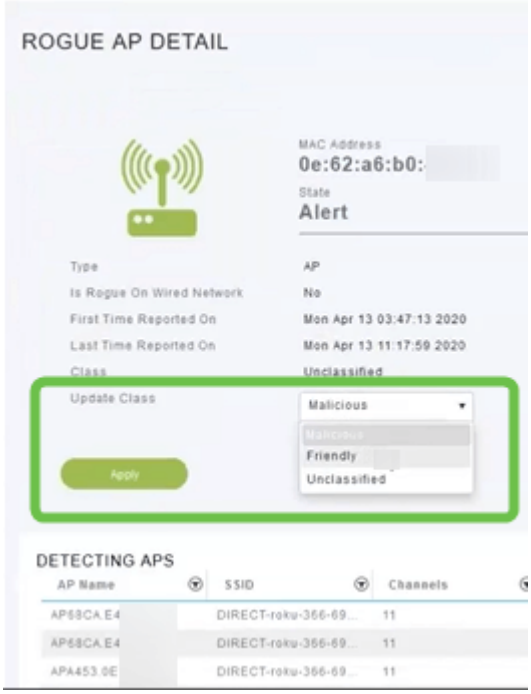
Schritt 5

Die nicht autorisierten APs werden aufgelistet. Sie können auf einen dieser APs klicken, um eine weitere Untersuchung durchzuführen.



Schritt 6 (optional)

Wenn Sie einen der APs als *freundlich* oder *bösartig* klassifizieren möchten, können Sie eine der Optionen im Dropdown-Menü unter *Update Class (Klasse aktualisieren)* auswählen. Dies könnte sinnvoll sein, damit Sie bei einem zukünftigen Blick auf nicht klassifizierte Access Points nicht eine ganze Liste durchsuchen müssen. Klicken Sie abschließend auf **Apply** (Anwenden).



Schritt 7 (optional)

Wenn Sie einen Access Point als *Intern (*im Netzwerk) oder *Extern (*möglicherweise ein benachbartes Unternehmen) bezeichnen möchten, können Sie dies im Abschnitt *Update Status (Status aktualisieren)* tun. Klicken Sie abschließend auf **Apply**.

Nicht autorisierte Clients anzeigen

Schritt 1

Melden Sie sich bei der Webbenutzeroberfläche des primären Access Points an. Öffnen Sie dazu einen Webbrowser, und geben Sie *https://ciscobusiness.cisco ein*. Möglicherweise erhalten Sie eine Warnung, bevor Sie fortfahren. Geben Sie Ihre Anmeldeinformationen ein.

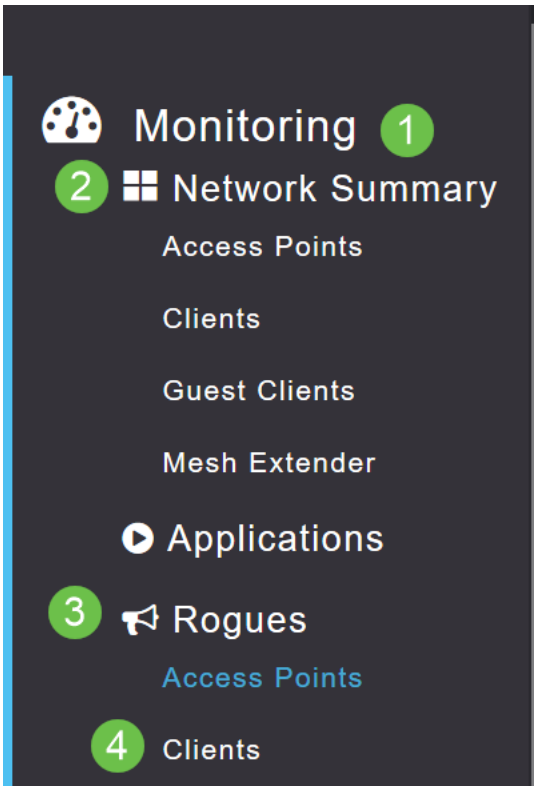
Sie können auch auf den primären Access Point zugreifen, indem Sie *https://<ipaddress>* (des primären Access Points) in einen Webbrowser eingeben. Für einige Aktionen können Sie die Cisco Business Mobile-App verwenden.

Schritt 2

Um diese Konfigurationen vorzunehmen, benötigen Sie eine *Expertenansicht*. Klicken Sie auf das **Pfeilsymbol** oben rechts in der Webbenutzeroberfläche, um zur *Expertenansicht* zu wechseln. Weitere Informationen zum Einrichten eines RADIUS-Servers finden Sie unter Radius.

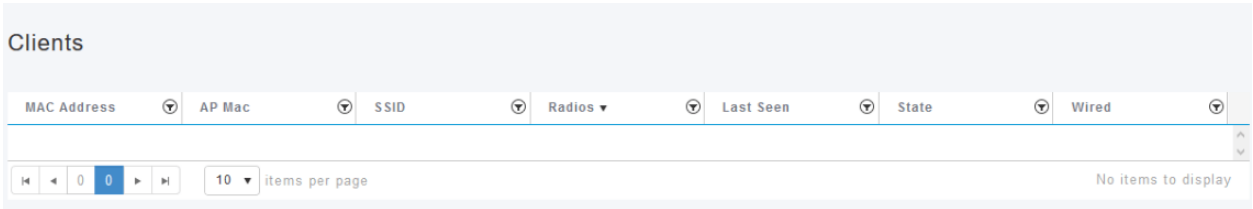
Schritt 3

Navigieren Sie zu **Monitoring > Network Summary > Rogues > Clients.**



Schritt 4

Wenn es unberechtigte Clients gibt, werden diese aufgelistet. In diesem Beispiel wurden keine nicht autorisierten Clients erkannt.



Schlussfolgerung

Jetzt haben Sie die Möglichkeit, unberechtigte Benutzer in Ihrem Netzwerk zu erkennen. Wenn Sie viele unberechtigte Benutzer auf einem von Ihnen verwendeten Kanal sehen, können Sie den

Kanal ändern. Es gibt einige Überlegungen, die Sie beachten sollten. Sehen Sie sich daher den Artikel zur Änderung des Funkkanals an (Link, wenn verfügbar).

Häufig gestellte Fragen RADIUS Firmware-Upgrade RLANs Erstellung von Anwendungsprofilen Client-Profilerstellung Primäre AP-Tools Umbrella WLAN-Benutzer Protokollieren Traffic Shaping Schurken Störfaktoren Konfigurationsverwaltung Netzmodus für Portkonfiguration Willkommen bei CBW Mesh Networking Gastnetzwerk mit E-Mail-Authentifizierung und RADIUS-Accounting Fehlerbehebung Verwenden eines Draytek-Routers mit CBW

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.