Cisco Business Wireless Networkにおける不正なクライアントの特定

目的

この記事の目的は、Cisco Business Wireless(CBW)の従来のネットワークまたはメッシュネットワークで、不正なアクセスポイント(AP)と不正なワイヤレスクライアントを特定する方法を示すことです。

該当するデバイス |ファームウェアバージョン

- 140AC(データシート) | 10.0.1.0(最新版をダウンロード)
- 141ACM(データシート) | 10.0.1.0(最新版をダウンロード) : エクステンダはメッシュネットワークでのみ使用されます。
- 142ACM(データシート) | 10.0.1.0(最新版をダウンロード) : エクステンダはメッシュネットワークでのみ使用されます。
- 143ACM(データシート) | 10.0.1.0(最新版をダウンロード) : エクステンダはメッシュネットワークでのみ使用されます。
- 145AC(データシート) | 10.0.1.0(最新版をダウンロード)
- 240AC(データシート) | 10.0.1.0(最新版をダウンロード)
- 150AX(データシート) | 10.3.2.0(最新版をダウンロード)
- 151AXM(データシート) | 10.3.2.0(最新版をダウンロード)

CBW 15xシリーズデバイスはCBW 14x/240シリーズデバイスと互換性がなく、同じLAN上での共存はサポートされていません。

概要

CBWアクセスポイント(AP)は802.11 a/b/g/n/ac(Wave 2)ベースで、内部アンテナを備えています。これらは、従来のスタンドアロンデバイスとして、またはメッシュネットワークの一部として使用できます。

完璧な世界では、誰もがワイヤレスネットワークを使用する際に敬意と正直になります。残念ながら、私たちは完璧な世界に住んでいません。管理者としての仕事は、潜在的な問題を認識することです。

不正APとは、ユーザの許可なくネットワークにインストールされたAPです。不正クライアントとは、検出されたその他のデバイスで、会社に属していないものです。

これらの接続は完全に無実である可能性がありますが、これらの不正がネットワークを攻撃したり、機密情報を盗んだりしようとするリスクが常にあります。この点を把握するために、不正なAPと不正なクライアントを表示できます。検出された不正はAPを介してブロックできませんが、詳細な調査のための情報は提供されます。

CBW APは、現在使用しているチャネルまたはオーバーラップしているチャネルの不正だけを検出します。

不正APの表示

この切り替えられたセクションでは、初心者向けのヒントを紹介します。

ログイン

プライマリAPのWebユーザインターフェイス(UI)にログインします。これを行うには、Webブラウザを開き、https://ciscobusiness.ciscoと入力します。続行する前に警告が表示されることがあります。クレデンシャルを入力します。Webブラウザに（プライマリAPの）https://[ipaddress]と入力して、プライマリAPにアクセスすることもできます。

ツールヒント

ユーザインターフェイスのフィールドに関する質問がある場合は、次のようなツールヒントを確認してください。

[メインメニューの展開]アイコンが見つからない

画面左側のメニューに移動します。メニューボタンが表示されていない場合は、このアイコンをクリックしてサイドバーメニューを開きます。

Ciscoビジネスアプリケーション

これらのデバイスには、一部の管理機能をWebユーザインターフェイスと共有するコンパニオンアプリケーションがあります。Webユーザインターフェイスのすべての機能がアプリケーションで使用できるとは限りません。

iOSアプリのダウンロード Androidアプリのダウンロード

よく寄せられる質問（FAQ）

まだ未回答の質問がある場合は、よくある質問のドキュメントを確認できます。FAQ

手順 1

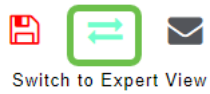
プライマリAPのWebユーザインターフェイス(UI)にログインします。これを行うには、Webブラウザを開き、*https://ciscobusiness.cisco*と入力します。続行する前に警告が表示されることがあります。認証情報を入力してください。

Webブラウザに（プライマリAPの）*https://<ipaddress>*と入力して、プライマリAPにアクセスすることもできます。

使用される用語に慣れていない場合は、『シスコビジネス：新しい用語の用語集』を参照してください。

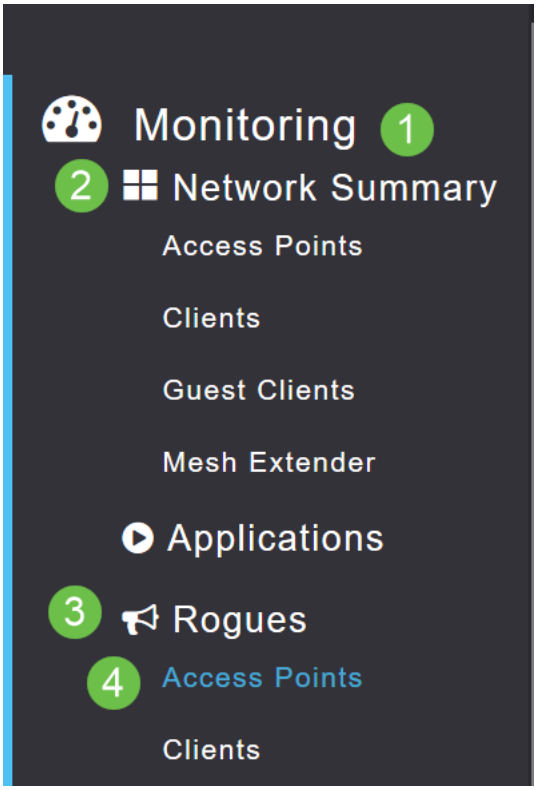
手順 2

これらの設定を行うには、*Expert View*に入っている必要があります。Web UIの右上のメニューにある**矢印アイコン**をクリックして、*Expert View*に切り替えます。



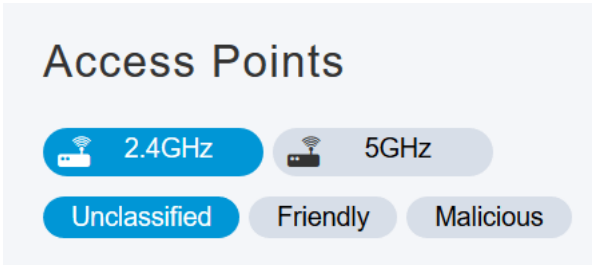
手順 3

[Monitoring] > [Network Summary] > [Rogues] > [Access Points] に移動します。



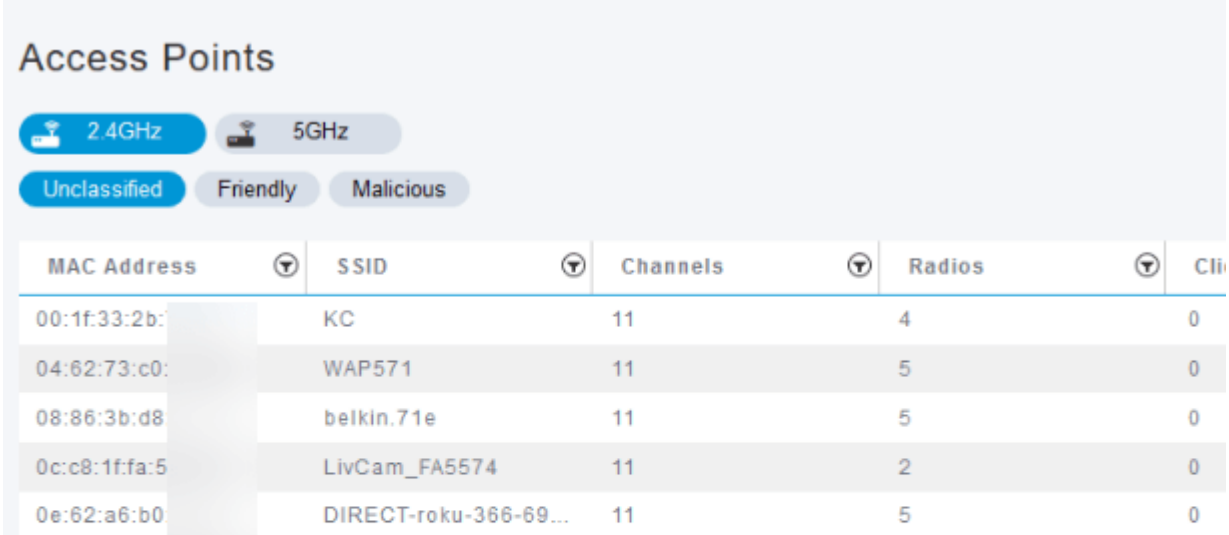
手順 4

このページが開いたら、タブをクリックして2.4 GHzまたは5 GHzを表示するように選択できます。デフォルトでは、すべての不正APに[Unclassified]というラベルが付けられます。APは不正APのラベルを変更しません。これは手動で行います。



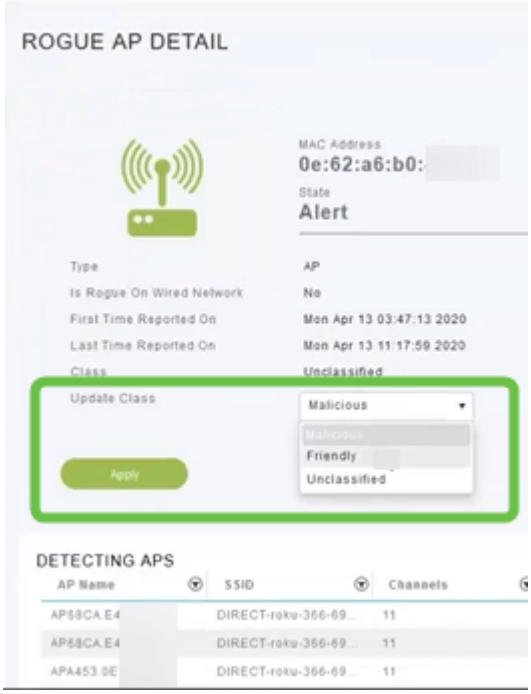
手順 5

不正なAPがリスト表示されます。任意のAPをクリックしてさらに詳しく調査できます。



ステップ 6 (オプション)

APのいずれかを*Friendly*または*Malicious*として分類する場合は、[Update Class] の下のドロップダウンメニューからいずれかのオプションを選択できます。今後、未分類のアクセスポイントを表示するときに、リスト全体を並べ替える必要がなくなるように設定できます。完了したら、必ず[Apply] をクリックしてください。



ステップ 7 (オプション)

APに*Internal* (ネットワーク内) または*External* (隣接する会社の可能性あり) のラベルを付ける場合は、[Update Status] セクションで行うことができます。完了したら、[Apply] をクリックします。

不正クライアントの表示

手順 1

プライマリAPのWeb UIにログインします。これを行うには、Webブラウザを開き、*https://ciscobusiness.cisco*と入力します。続行する前に警告が表示されることがあります。認証情報を入力してください。

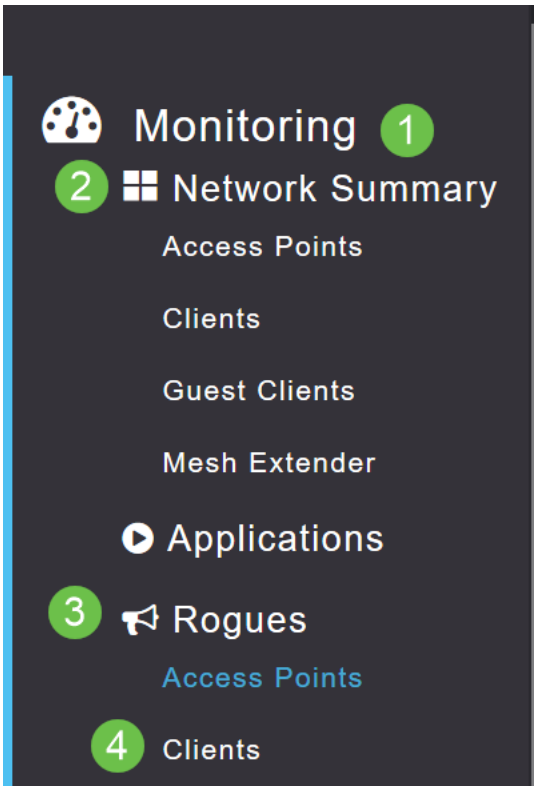
Webブラウザに（プライマリAPの）*https://<ipaddress>*と入力して、プライマリAPにアクセスすることもできます。一部のアクションについては、Cisco Business Mobileアプリをご利用ください。

手順 2

これらの設定を行うには、*Expert View*に入っている必要があります。Web UIの右上のメニューにある**矢印アイコン**をクリックして、*Expert View*に切り替えます。RADIUSサーバの設定の詳細については、Radius

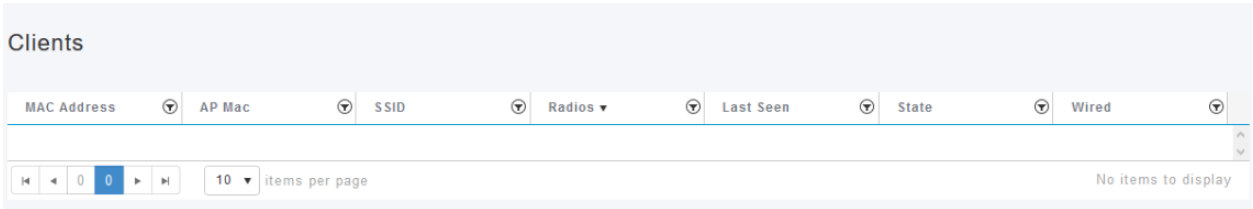
手順 3

[Monitoring] > [Network Summary] > [Rogues] > [Clients] に移動します。



手順 4

不正なクライアントがある場合は、そのクライアントがリストされます。この例では、不正クライアントは検出されていません。



結論

これで、ネットワーク内の不正を確認できるようになりました。使用しているチャンネルに多くの不正が見られる場合は、チャンネルを変更できます。RFチャネルの変更に関する記事（利用可

能な場合はリンク）を参照してください。

よく寄せられる質問（FAQ） Radius Firmware Upgrade RLAN アプリケーションプロファイリング クライアントプロファイリング プライマリAPツール Umbrella WLANユーザ Logging トラフィック シェーピング Rogues 干渉源 構成管理 ポート設定メッシュモード CBWメッシュネットワーキングへようこそ 電子メール認証とRADIUSアカウンティングを使用するゲストネットワーク トラブルシューティング CBWでのDraytekルータの使用

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。