シスコのビジネスワイヤレスメッシュネットワークのトラブルシューティング

目的

このドキュメントでは、Cisco Business Wireless(CBW)メッシュネットワークのトラブルシューティングを行う際に分析するいくつかの領域について説明します。

従来のワイヤレスネットワークを使用している場合は、『従来のCiscoビジネスワイヤレスネットワークのトラブルシューティング』を参照してください。

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) | 10.1.1.0(最新版をダウンロード)
- 141ACM(データシート) | 10.1.1.0(最新版をダウンロード)
- 142ACM(データシート) | 10.1.1.0(最新版をダウンロード)
- 143ACM(データシート) | 10.1.1.0(最新版をダウンロード)
- 145AC(データシート) | 10.1.1.0(最新版をダウンロード)
- 240AC(データシート) | 10.1.1.0(最新版をダウンロード)

目次

概要

メッシュワイヤレスネットワークは素晴らしいですが、それに直面しましょう、物事は起こります！他のワイヤレスネットワークと同様に、多くの問題が発生する可能性があります。簡単な修正もあれば、より複雑な修正もあります。

このドキュメントの用語に慣れていない場合は、Cisco Business:新規用語一覧.

最適なパフォーマンスと信頼性を得るためには、次の点に留意してください。

1. 予想される数のクライアントとそのアプリケーションに対して、その工リアが完全にカバーされていることを確認します。ワイヤレスインフラストラクチャ全体のパフォーマンスを向上させるには、ワイヤレスアクセスポイントを追加する必要があります。
2. 使用しているアプリケーションのタイプ（または管理者として使用できるアプリケーションのタイプ）に注意してください。
3. ビデオストリーミングアプリケーションを実行しているクライアントは、オーディオのみのプログラムをストリーミングするクライアントよりも多くの帯域幅を消費します。ビデオアプリケーションは、適切なエクスペリエンスを提供するためにバッファリングに依存します。
4. 音声関連のアプリケーションを実行しているクライアントは、帯域幅を大量に消費することなく、遅延のない迅速なサービスを必要とします。音声コールではバッファリングが行われないため、パケットがドロップされないことが非常に重要です。

トラブルシューティングの準備はできていますか。掘り返そう！

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.com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。

シスコ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わけではありません。

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、FAQドキュメントを確認できます。FAQ

トラブルシューティングの際に、基本から始めてみませんか。

物理的条件と環境条件の確認

これは最も簡単なトラブルシューティング方法ですが、見過ごされることがよくあります。当たり前のように思えるかもしれませんが、基本から始めるのが良いでしょう。

1. すべての機器の電源が入っていますか。
2. 全てに力が？
3. リンクライトは常に点灯していますか。緑色のライトは良い兆候です！
4. ケーブルは正しく接続されていますか。
5. ケーブル不良でしょうか。
6. 装置が過熱していますか。
7. 場所などの環境要因が考えられますか。
8. APとワイヤレスデバイスの間に金属製または厚手の壁がありますか。
9. クライアントが完全に接続できない場合、クライアントは範囲外ですか。

その他の考慮事項

1. APの再起動
2. スイッチに接続しているAPの場合は、スイッチの設定をチェックし、スイッチが正常に動作していることを確認します。CPU使用率、温度、およびメモリ使用率は、指定されたしきい値レベルを下回る必要があります。
3. Web UIの[Monitoring] で、[Wireless Dashboard] をオンにして、パフォーマンスやその他の問題に関する情報を収集します。
4. ルータで*Bonjour*および*Link Layer Discovery Protocol(LLDP)*が使用可能な場合はこれを有効にします。
5. ゲームおよびストリーミングアプリケーションで使用可能な場合は、*ワイヤレスマルチキャスト転送*を有効にします。
6. すべてのプライマリ対応APが同じVLANにあることを確認します。
7. ワイヤレス経由でプライマリAPにログインし、VLANなどの特定の設定を編集すると、接続が切断される場合があります。有線でプライマリAPに接続すると、接続の安定性が高まります。

SSID の数

すべてのSSIDは100ミリ秒(ms)ごとにビーコンフレームを送信する必要があり、これによりチャネル使用率が大幅に低下する可能性があります。

メッシュネットワークでサポートできるSSIDの物理的な制限は無線あたり16個ですが、AP上のSSIDの総数は、無線あたり、またはAPあたり1 ~ 2個に制限するのが最適です。

プライマリAPへのログインに問題がありますか。

おそらく、*ciscobusiness.cisco*にログインしようとして、問題が発生している可能性があります。次の簡単な提案を確認してください。

- Day Zero設定を完了した場合は、アプリを閉じてから再起動してください。
- 正しいService Set Identifier(SSID)が選択されていることを確認します。これは、ワイヤレスネットワーク用に作成した名前です。
- *https://<IP address of the Primary AP>*を使用してプライマリAPにログインします。プライマリAPアドレスは、初期セットアップ手順で使用した割り当て済みのIPアドレスです。その時点で手動アドレスの割り当てを中止した場合は、ルータの[Primary AP management]ページに指定されているDHCP IPアドレスを確認します。管理アドレスは、MACアドレス00:00:5e:00:01:01に割り当てられます。
- 初期設定を行ったら、*ciscobusiness.cisco*にログインしているか、WebブラウザにIP管理アドレスを入力して、*https://*が使用されていることを確認します。設定によっては、ブラウザに*http://*が自動的に入力されている場合があります。これは、初めてログインしたときに使用したものです。
- Webブラウザに問題がある可能性があります。たとえば、Firefoxでは、画面の右上にあるメニューをクリックします。[Help] > [Troubleshooting Information] を選択し、[Refresh Firefox] をクリックします。
- モバイルアプリまたはラップトップのバーチャルプライベートネットワーク(VPN)を切断します。モバイルサービスプロバイダーが使用しているVPNに接続している可能性があり、そのVPNを知らないこともあります。たとえば、サービスプロバイダーとしてGoogle Fiを使用しているAndroid（ピクセル3）電話には、通知なしで自動接続する組み込みVPNがあります。プライマリAPを見つけるには、これを無効にする必要があります。
- Androidフォンを使用している場合は、プライベートドメインネームサーバ(DNS)を使用している可能性があり、接続のためにこの機能を無効にする必要があります。これを確認するには、通常、[Settings] > [Network and Internet] > [Advanced] > [Private DNS]の下にあります。

APで最新バージョンを実行していますか。

重要な理由

ファームウェアはソフトウェアとも呼ばれ、アクセスポイントに組み込まれています。ファームウェアをアップグレードすると、APのパフォーマンスと安定性が向上します。アップグレードには新機能が含まれたり、以前のバージョンのソフトウェアで発生した脆弱性が修正されたりします。そんなに重要なのか？絶対に！アップグレード用のすべてのリンクは、この記事の「ファームウェアバージョン」セクションで追加することが非常に重要です。これは、ネットワークに問題がある場合に試す簡単な解決策です。最初のMesh Extenderをネットワークに追加する際にファームウェアバージョンの不一致が発生すると問題が発生する可能性があるため、すぐにアップデートしてください。

プライマリ対応APを更新する前に、すべてのメッシュエクステンダを更新することが非常に重要です。

ファームウェアはさまざまな方法でアップグレードできますが、アップグレードには*Cisco.com*

を使用することをお勧めします。ファームウェアのアップグレードに関するサポートが必要な場合は、Cisco Business Wirelessアクセスポイントのソフトウェアのアップデートを参照してください。

アップグレードのトラブルシューティング

アップグレードがスムーズに行われない場合があります。次のような簡単な操作を試すことができます。

1. Webブラウザを更新または閉じます。
2. ブラウザのキャッシュをクリアし、プライマリAPに再度ログインします。このプロセスは、使用するWebブラウザによって異なります。
3. プライマリAPのWebユーザインターフェイス(UI)で別のページまたはタブをクリックし、[Software Update]ページに戻ってファームウェアイメージのダウンロードを再試行します。
4. 新しいWebブラウザを試します。たとえば、Chromeを使用していて動作しない場合は、Firefoxを試してみてください。
5. 管理ページがファームウェアのアップグレードを開始できなかったり、応答しない（アップグレードの開始後にステータスが変化しない）場合は、まれに、ネットワーク上のすべてのアクセスポイントとメッシュエクステンダの電源をオフ/オンにして、ファームウェアのアップグレードを再試行する必要があります。

次の状況のどれが該当しますか。

- CBW240のダウンストリームイーサネットポートを使用している場合は、別のポートに切り替えます。
- キャプティブポータルを使用している場合は、Microsoft EdgeなどのChromeベースのブラウザを使用しないでください。ネットワークに参加できない場合があります。ブラウザと同じようにFirefoxを使用するくらい簡単かもしれません。
- クライアントがスプリットトンネリング/スプリットDNSなしでVPN接続を使用している場合、CBW管理ページにアクセスできず、モバイルアプリが機能しない可能性があります。CBW管理機能にアクセスするために、クライアントでVPNを一時的に無効にしてみてください。
- クライアントでプライベートDNSが有効な場合、DNSクエリは暗号化され、CBWはDNSクエリを代行受信できません。これにより、Cisco Businessモバイルアプリが動作しなくなり、ciscobusiness.ciscoが解決できなくなります。プライベートDNSを使用せずにネットワークに参加しているクライアントからCBWを管理するか、管理IPアドレス経由でWeb UIを使用してCBWを管理することを推奨します。
- CBWデバイスがCiscoワイヤレスLANコントローラと同じVLANに設定されていないことを確認します。

接続の問題である可能性がありますか。

Webユーザインターフェイス(UI)からの接続テストの実行

APが有効になるには、他のデバイスと通信できる必要があります。これを確認する簡単な方法は、pingを実行することです。

特定のアクセスポイントに接続（関連付け）されている少なくとも2つのクライアントからAPにpingを実行します。

ルータからアクセスポイントのIPアドレスにpingを実行し、エンドツーエンド接続が使用可能かどうかを確認します。ルータからAPに関連付けられたワイヤレスクライアントにpingを実行し、メインネットワークから到達できるかどうかを確認します。

DHCPの潜在的な問題

プライマリAPにスタティックIPアドレスを割り当てた場合でも、このAPはDHCPサーバにアクセスする必要があります。このDHCPサーバは動作していて、APのLANイーサネットポートから到達可能である必要があります。これは、プライマリAPがネットワークに参加するすべてのAPとクライアントにIPアドレスを提供するために必要です。リブート後にプライマリで赤色のライトが点滅している場合は、問題の可能性があります。

スタティックIPアドレスはCBW管理に選択できますが、適用されるのは管理IPアドレスだけです。メッシュエクステンダを含むすべてのアクセスポイントは、アクセスポイント機能のために個別のIPアドレスを必要とします。管理MACアドレスは00:00:5e:00:01:01です。

すべてのCBWアドレスがスタティックとして設定されている場合でも、新しいAPまたはメッシュエクステンダを追加する際には、新しいデバイスの初期インストールにDHCPサーバが必要です。これは、後でスタティックIPアドレスに変更する予定の場合でも同様です。

IPアドレスを必要とするクライアントの数が、DHCPプールで使用可能な数よりも多い可能性があります。詳細については、「*DHCPのIPアドレスプールを表示または変更する方法*」セクション(『Ciscoビジネスハードウェアでの静的IPアドレスの設定に関するベストプラクティス』を参照してください。

キャッシュされるDHCPアドレスの数が多すぎると、クライアントがIPアドレスを取得できなくなることがあります。詳細については、「DHCP IPアドレッシングでARPテーブルを使用できるようにするヒント」を参照してください。この方が便利な場合は、ルータをリブートすることもできます。

Windowsサポート

Windowsを使用している場合は、[Network Connections]パネルからワイヤレス接続を選択し、そのステータスが[Enabled] であることを確認します。

ワイヤレスネットワーク接続のトラブルシューティングに関する詳細なガイダンスについては、Microsoftサポートフォーラムの次のリンクをクリックしてください。WindowsのWi-Fi接続の問題を修正します。

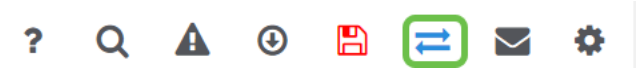
おそらくCBW設定を調整する必要があります

一部の古いデバイスで接続の問題を引き起こす可能性のあるデフォルト設定がいくつかあります。次の設定を変更してみてください。

RF最適化

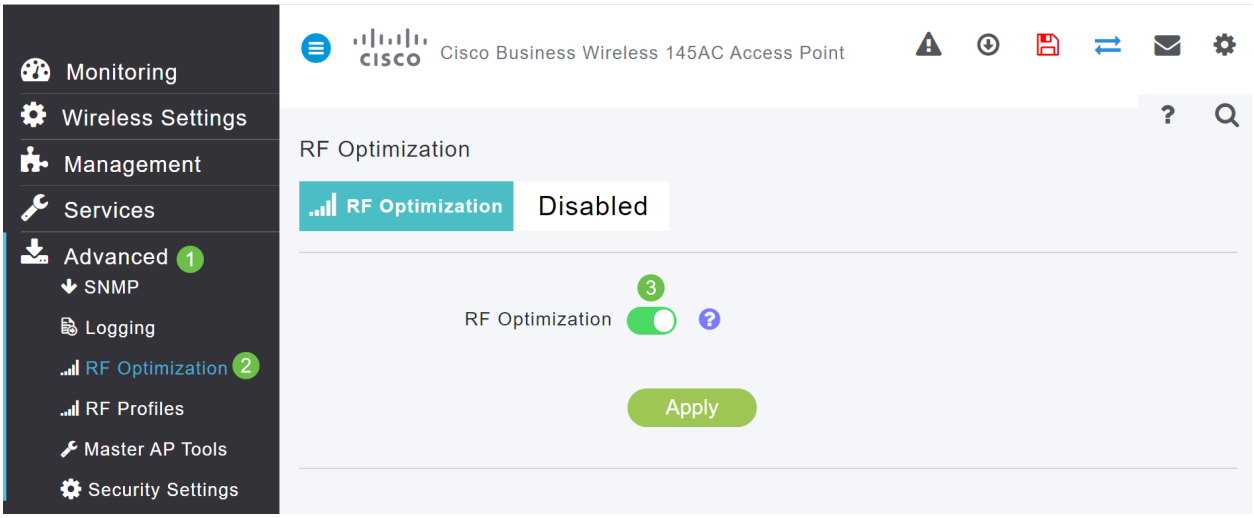
手順 1

これらの設定が*エキスパートビュー*にあることを確認します。



手順 2

[Advanced] > [RF Optimization] に移動します。[RF Optimization] をオンにします。

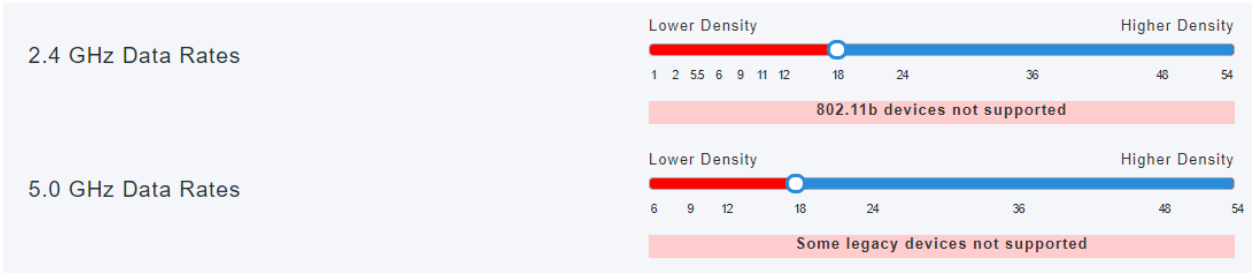


手順 3

画面の一番下までスクロールします。各無線データレート内で、802.11bクライアントなどの古いレガシーワイヤレスモードクライアントを削除するために、低い制御レートのサポートを削除します。

手順 4

古いデバイスがサポートされていないという通知が表示されます。スライドを右に移動するほど、接続できる距離が短くなります。



ブリッジグループ名

工場出荷時のデフォルトですべてのAPを使用してネットワークを設定する場合

メッシュネットワークのゼロデイ設定を行うと、BGNが自動的に作成されました。これは、最初に入力したService Set Identifier(SSID)と同じで、最初の10文字までです。このBGNは、APを関連付け、APが適切に接続されていることを確認するためにAP内で使用されます。プライマリAPを設定し、下位APを結合すると、BGNは自動的に一致し、それ以上の設定は必要ありません。

プライマリAPをリセットした場合、または設定したAPを新しいネットワークに移動した場合

プライマリAPで工場出荷時のデフォルトへのリセットを実行するか、APを設定されたネットワークから別のネットワークに移動すると、BGNの不一致が発生する可能性があります。

BGNが使用可能なネットワークのいずれとも一致しないシナリオでAPがネットワークへの加入を試みると、下位APは引き続き最も強い信号を使用して一時的にネットワークへの加入を試みます。APは、Allow Listedで承認されている場合、ネットワークに参加できます。

APがネットワークに加入すると、BGNが一致しないため、下位APは引き続き10 ~ 15分ごとに一致するBGNを探します。これにより、接続がドロップされ、一致するBGNが見つからない場合は再度接続されます。これは、特に別の無線ネットワークから強い無線信号が来る可能性がある場合、無線ネットワークの接続に多くの問題を引き起こす可能性があります。

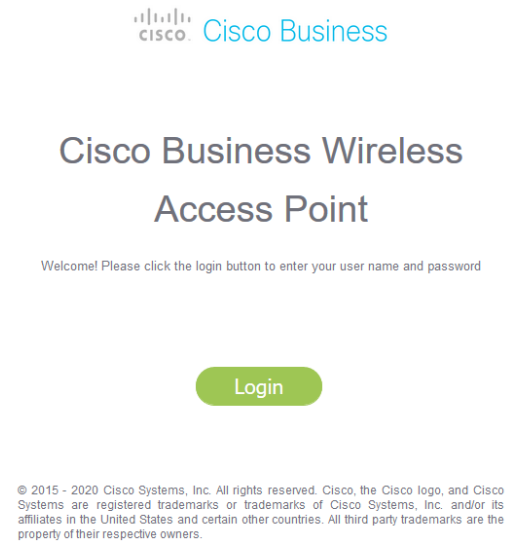
簡単な解決策として、すべてのAPを連携させるには、すべてのAPのBGNが正確に一致していることを確認する必要があります。他のAPのBGNをクリアするには、工場出荷時の状態にリセットするか、各APを手動で変更します。

APでブリッジグループ名(BGN)を表示または変更する場合

BGNは、最も多くのホップを最初に設定し、最も少ないホップ数まで動作するメッシュエクステンダに割り当てることをお勧めします。その後、プライマリ対応APのBGNを割り当てる必要があります。プライマリAP BGNは最後に設定する必要があります。次の手順を実行して、一度に1つずつ表示および変更できます。

手順 1

APにログインし、クレデンシャルを入力します。

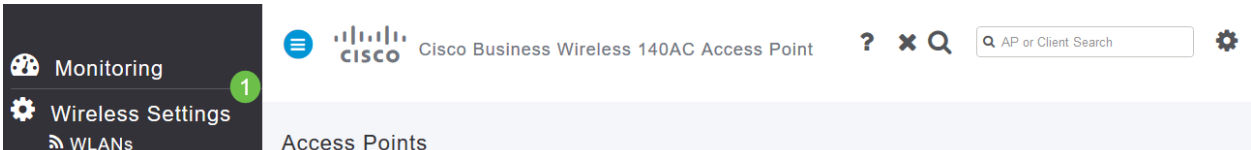


手順 2

矢印アイコンをクリックして、*エキスパートビュー*に切り替えます。

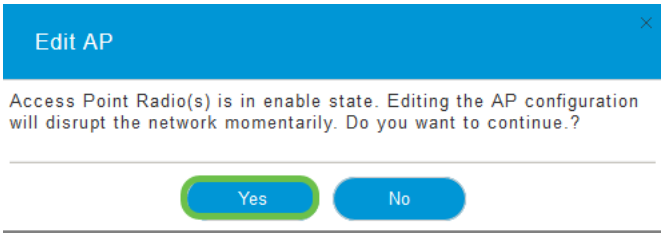
手順 3

[Wireless Settings] > [Access Points] に移動します。編集または表示するAPの[Edit] アイコンをクリックします。



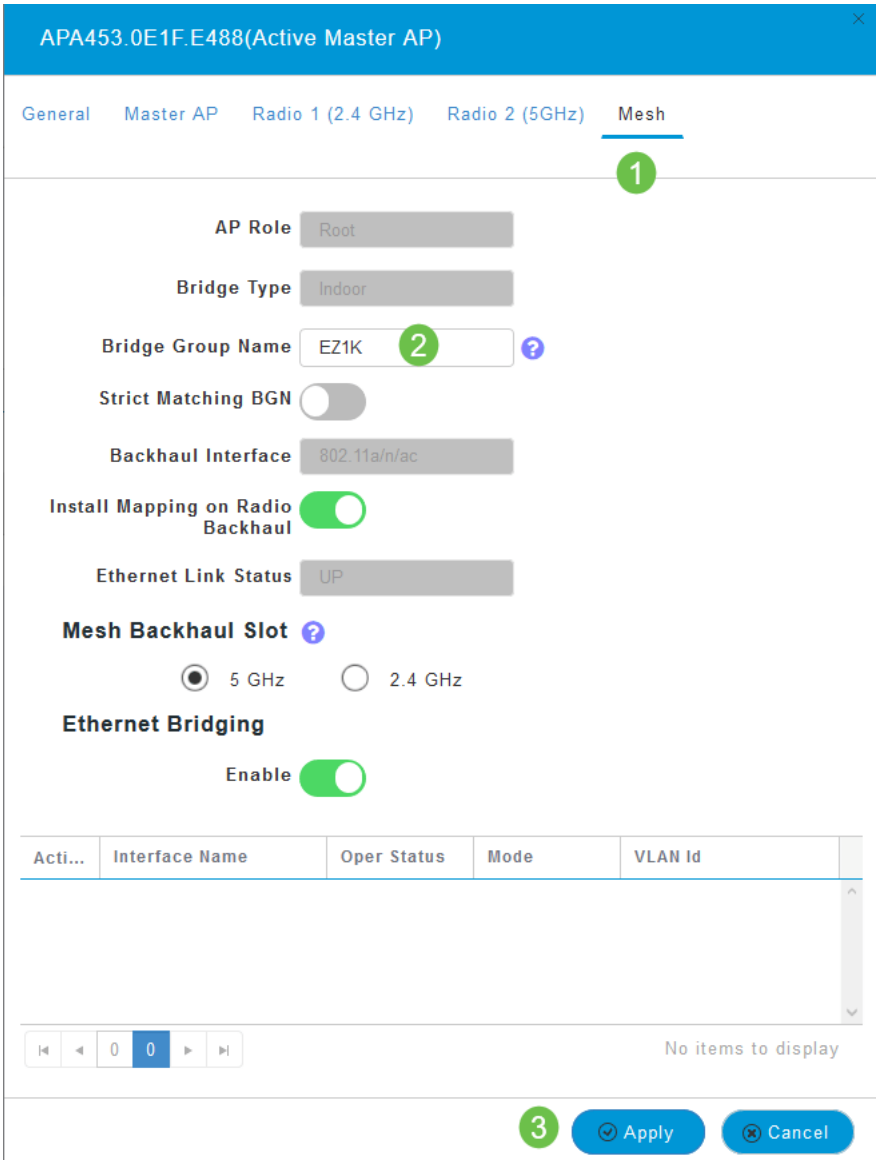
手順 4

AP設定を編集するかどうかを確認するポップアップが表示されます。[Yes] を選択します。



手順 5

[Mesh] タブをクリックします。ここでは、*ブリッジグループ名*を表示および変更できます。変更を行う場合は、必ず**Apply**をクリックしてください。



手順 6

確認するネットワーク内の各APに対して、この手順を繰り返します。変更を永続的に保存するには、**save**アイコンをクリックします。ブリッジグループ名が割り当てられると、デバイスがリブートを実行することに注意してください。リブートによってWi-Fiが中断されるため、営業時間中は再起動しないことをお勧めします。

許可リスト

他のプライマリ対応APとメッシュエクステンダを接続するには、すべてのAPのMedia Access Control(MAC)アドレスを含む許可リストをプライマリAP上に作成する必要があります。

さらに、下位APは、プライマリAPが他のAPにアクセスしてアップグレードできるように、[Allow Listed]にする必要があります。これは、ネットワークの稼働を維持するために不可欠です。

この許可リストは、同じブリッジグループ名(BGN)を持つすべてのAPとともに、APが効率的かつ一貫して接続するのに役立ちます。Media Access Control（MAC；メディアアクセスコントロール）アドレスを追加し、Allow Listとしてラベル付けするには、次の手順に従います。

手順 1

APのMACアドレスを知る必要があります。APのMACアドレスがわかっている場合は、ステップ4に進んでください。

MACアドレスには、コロンで区切られた数字と文字のペアが含まれます。

手順 2

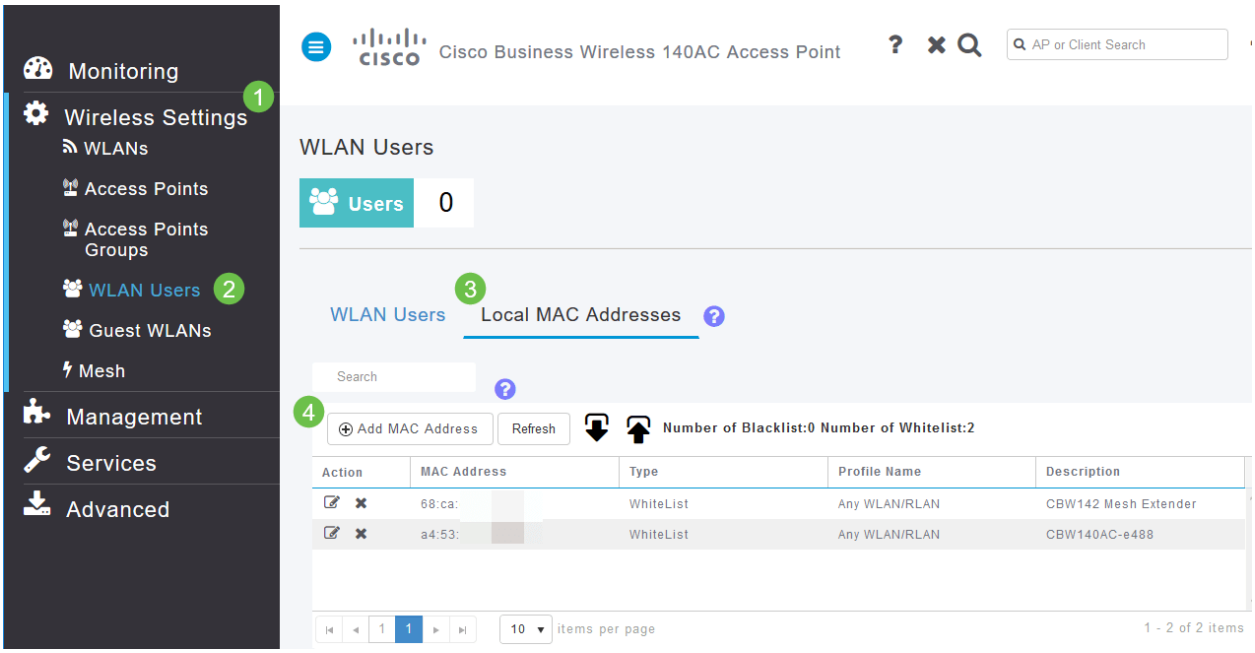
ほとんどのAPでは、MACアドレスは実際のAPの外部にあります。142ACMと143ACMでは、MACアドレスを表示するために電源装置をスライドさせる必要があります。これを行うには、矢印が示す場所でAPを軽く押します。電源コンポーネントをスライドさせて持ち上げます。

手順 3

142ACMおよび143ACMでは、次に示す場所にMACアドレスが表示されます。

手順 4

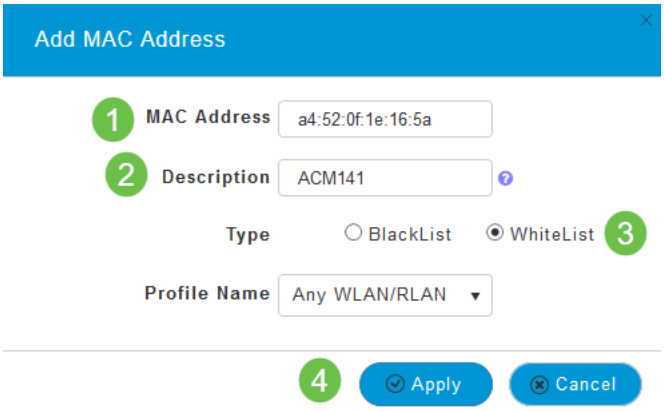
1. [Wireless Settings] を選択します
2. **WLANユーザの選択**
3. **ローカルMACアドレス**の選択
4. [Add MAC Address] を選択します



手順 5

次の情報を入力します。

1. *MAC アドレス*
2. *説明* (最大32文字)
3. [Allow List] オプションボタンを選択します
4. Apply をクリックします。



干渉と間隔の考慮事項

不正、干渉源、RFチャネル...おやおや！

干渉はワイヤレスネットワークに問題を引き起こす可能性があり、かつてないほど多くのソースから発生する可能性があります。電子レンジ、防犯カメラ、スマートウォッチ、動作検知器、または蛍光灯でさえ、干渉を引き起こす可能性があります。

ネットワークに及ぼす影響は、オブジェクトが常にオンになっている場合や断続的な場合に発生する電力量など、さまざまな要因によって異なります。信号が強いほど、あるいは発生頻度が高いほど、発生する可能性のある問題が多くなります。

同じチャネルに多数の不正APと不正クライアントが存在すると、問題が発生する可能性があります。

干渉はワイヤレスパフォーマンスの主要な阻害要因となり、セキュリティの脆弱性とワイヤレスネットワークの不安定性を生み出します。

現在使用しているチャネル**を監視するためのツールがあります**。チャネルを変更することもできます。詳細については、次の記事を参照してください。

- 不正クライアントの特定
- 干渉源の特定
- RFチャネルの変更

間隔と配置の推奨事項

1. プライマリ対応APのサイトのラインにメッシュエクステンダを配置します。
2. 親メッシュエクステンダのサイト内のダウンストリームメッシュエクステンダ。
3. ダウンストリームメッシュエクステンダでは、アップストリームのプライマリ対応APからのバックホールSSID信号強度が良好/良好であることが必要です。
4. メッシュエクステンダのSignal to Noise Ratio（SNR；信号対雑音比）の最小値は30です。
5. 他のメッシュエクステンダや他のプライマリ対応APに近すぎるメッシュエクステンダを配置しないでください。

次の表に、オープンスペースで想定されるカバレッジエリアを示します。開いていないエリアにネットワークを展開する場合は、これらの値を20 ~ 30 %減らします。

Model	Recommended Distance (Meters)	Recommended Distance (Feet)
CBW240AC	18 - 21	60 - 70
CBW140AC	15 - 18	50 - 60
CBW145AC	15 - 18	50 - 60
CBW141ACM	15 - 18	50 - 60
CBW142ACM	10 - 13	32 - 42
CBW143ACM	10 - 13	32 - 42

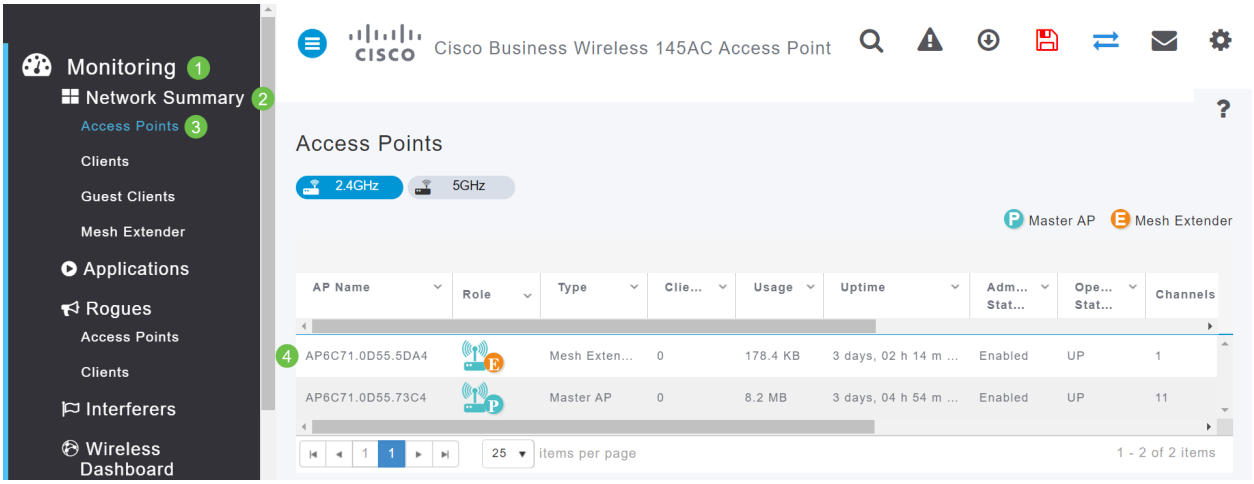
「ホップ」間の信号対雑音比

すべてのネットワークで、クライアントとAP間の強い信号に取り組む必要があります。メッシュネットワークでは、さまざまなAP間で相互に強い信号が発生していることを確認する必要もあります。「ホップ」の1つに大きな信号がなく、信号対雑音比が高い場合は、それをトラブルシューティングする必要があります。干渉の原因を確認するには、位置を調整するか、確認する必要があります。

手順 1

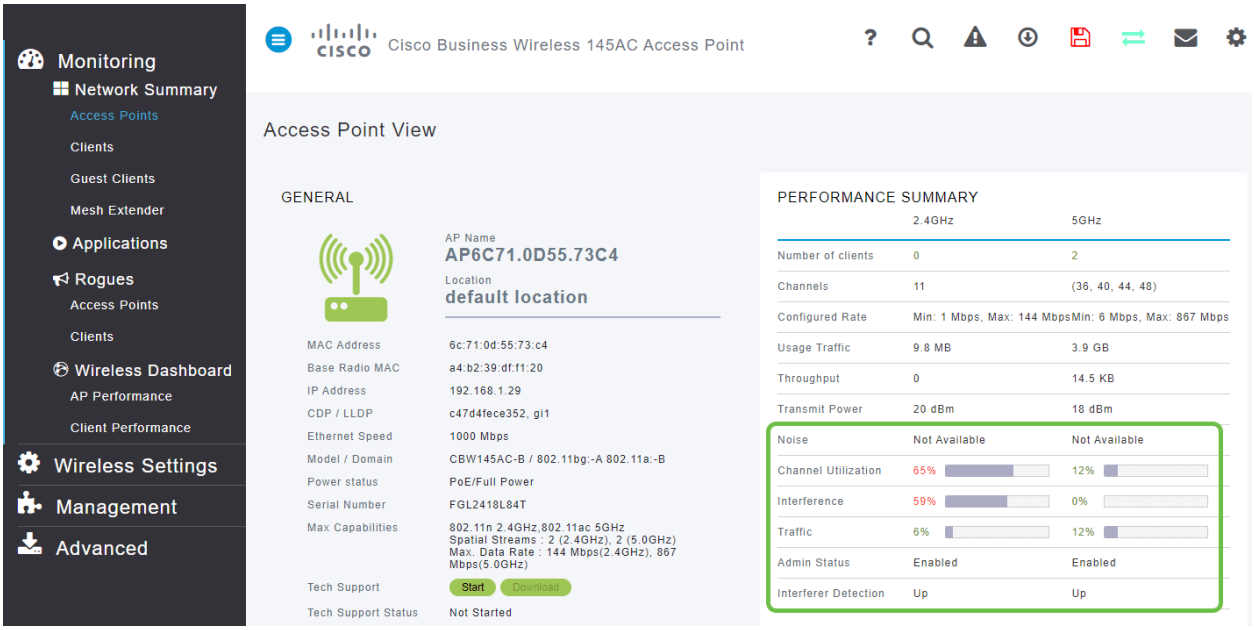
[Monitoring] > [Network Summary] > [Access Points] に移動し、テーブル内の任意のアクセスポイ

ントをクリックして、関連付けられているクライアントの信号強度を確認します。



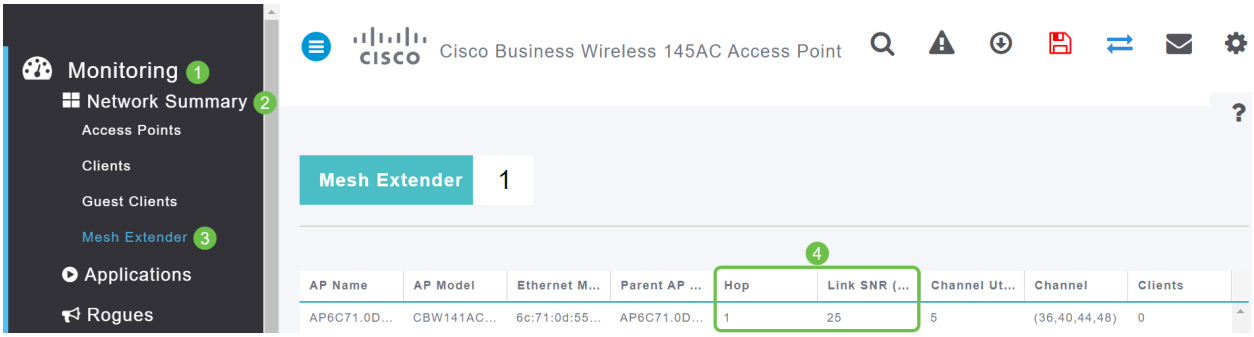
手順 2

[Access Point View] が開いたら、[Performance Summary] の下の情報に目を通します。



手順 3

また、すべてのメッシュエクステンダのホップ数と*信号対雑音比*に関する情報を収集することもできます。[Monitoring] > [Network Summary] > [Mesh Extender] に移動します。



カーテンの後ろを見る

Syslog

イベントを認識することで、ネットワークを円滑に運用し、障害を防止できます。syslogは、ネットワークのトラブルシューティング、パケットフローのデバッグ、およびイベントの監視に役立ちます。

これらのログは、プライマリAPのWebユーザインターフェイス(UI)で表示できます。設定されている場合は、リモートログサーバで表示できます。イベントは通常、リモートサーバに保存されていない場合は、リブート時にシステムから消去されます。

詳細については、『CBWネットワークでのシステムメッセージログ(Syslog)の設定』を参照してください。

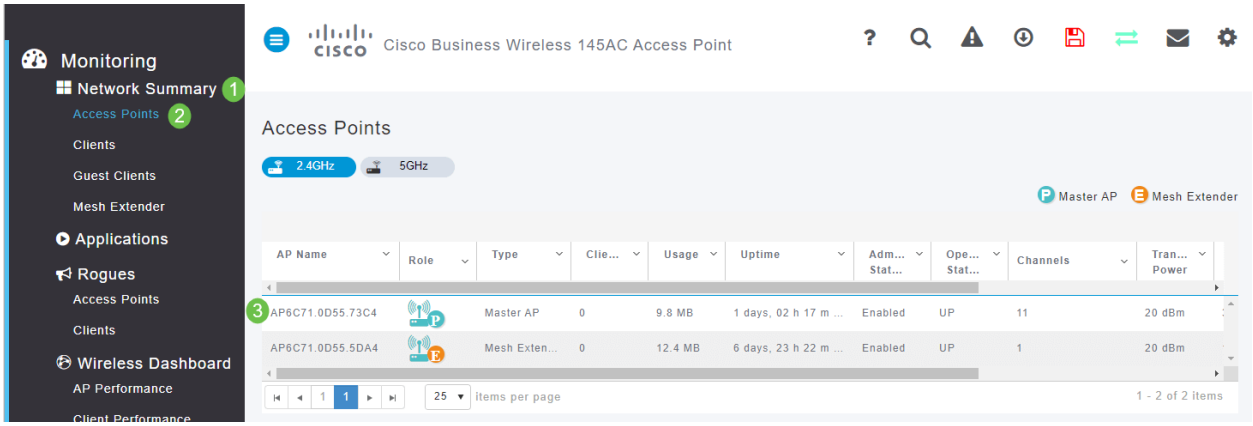
サポートバンドル

このCBW機器で使用できる機能の1つは、サポートバンドルをダウンロードすることです。サポートバンドルは、トラブルシューティングに役立つツールです。APのブートアップログを提供し、適用される設定を指定します。全体像を把握するには、すべてのAPでこの作業を行う必要があります。

プライマリAPでサポートバンドルをダウンロードする前に、ファームウェアの最新リリースを実行していることを確認してください。ファームウェアをアップデートするには、[Applicable Devices] で正しいリンクを選択します。|ファームウェアバージョン。ファームウェアのアップグレードに関するサポートが必要な場合は、Cisco Business Wirelessアクセスポイントのソフトウェアのアップデートを参照してください。

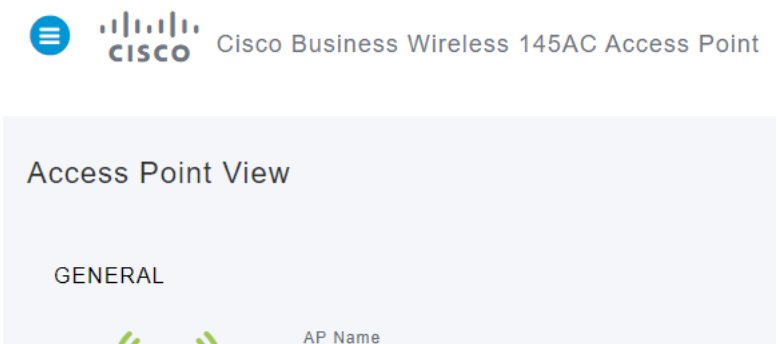
手順 1

アクセスポイント機能に固有のテクニカルサポートバンドルをダウンロードするには、[Monitoring] > [Access Points] を選択します。アクセスするAPを選択します。



手順 2

[Tech Support] セクションで、[Start] を選択します。

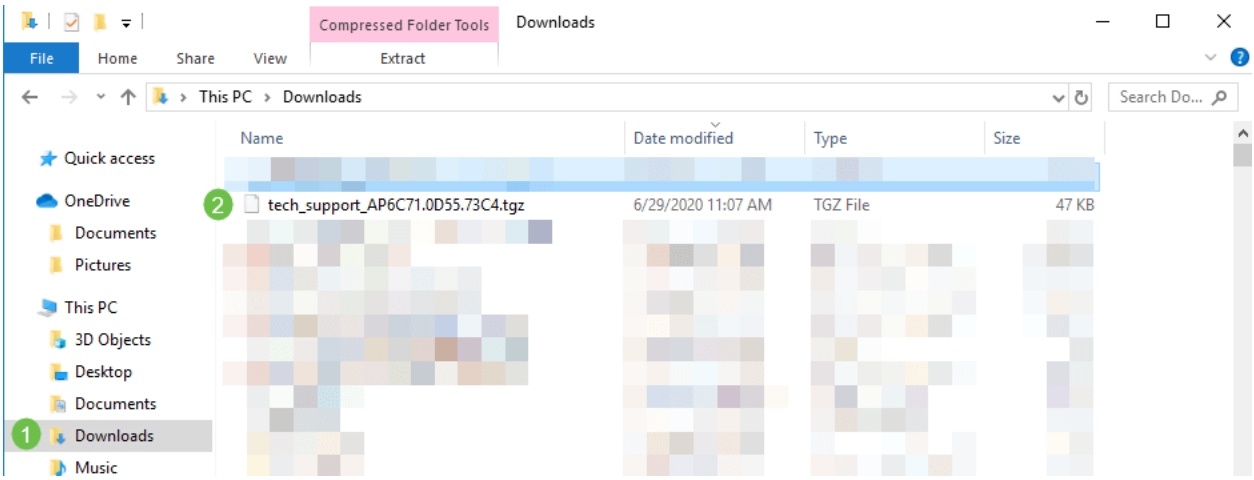


手順 3

ダウンロードが完了すると、[Tech Support Status] が[Completed] と表示されます。**Download**ボタンを選択して、ファイルをダウンロードします。この時点で、ダウンロードが失敗しても、APのメモリから削除されます。これは、ポップアップを許可しない場合に発生します。

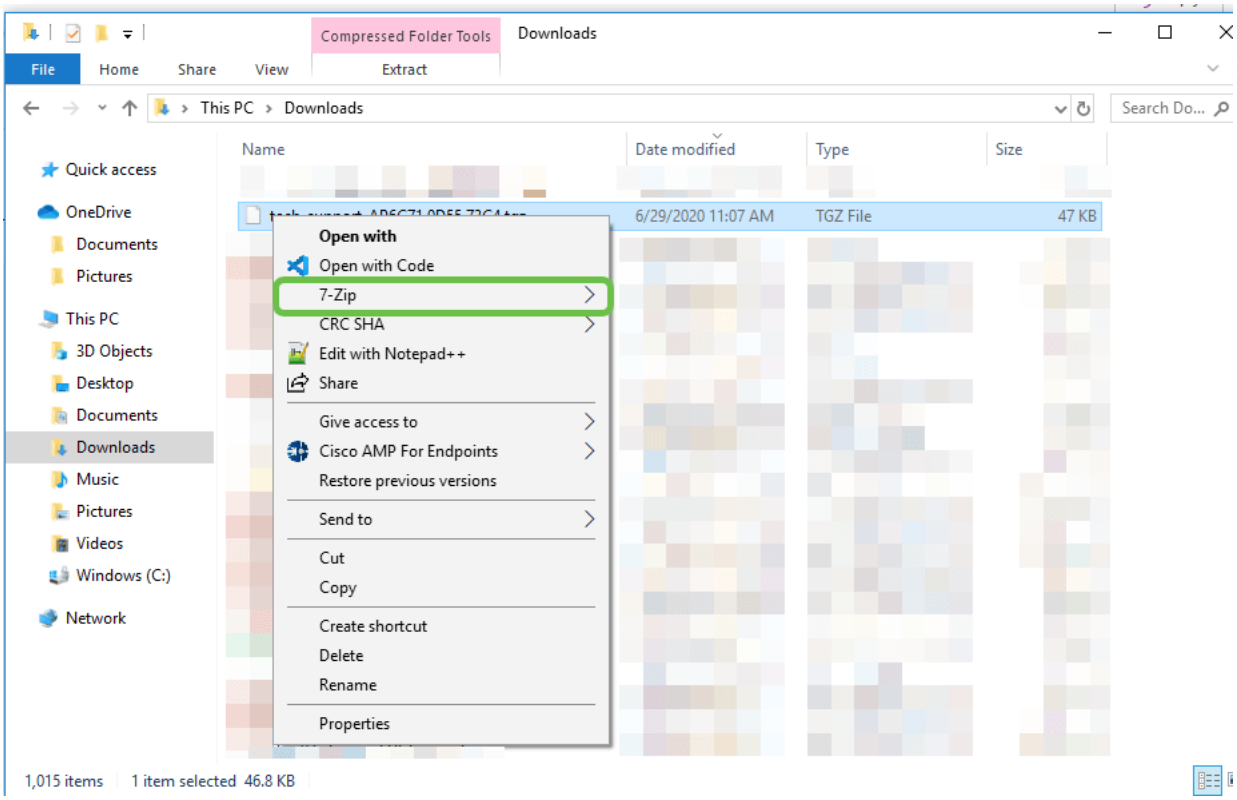
手順 4

コンピュータファイルの*Download*フォルダに、テクニカルサポートの*.tgz*ファイルが表示されます。このフォルダ内のファイルを抽出する必要があります。

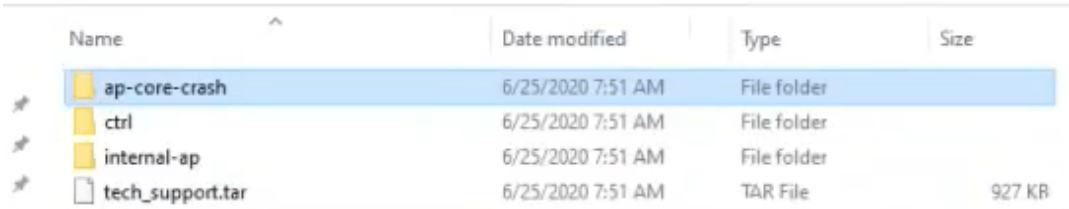


手順 5

右クリックして、使用する解凍アプリケーションを選択します。この例では、*7-Zipを使用*しています。選択すると、選択した場所にファイルが抽出されます。デフォルトでは、ファイルは*Downloads*フォルダに送信されます。

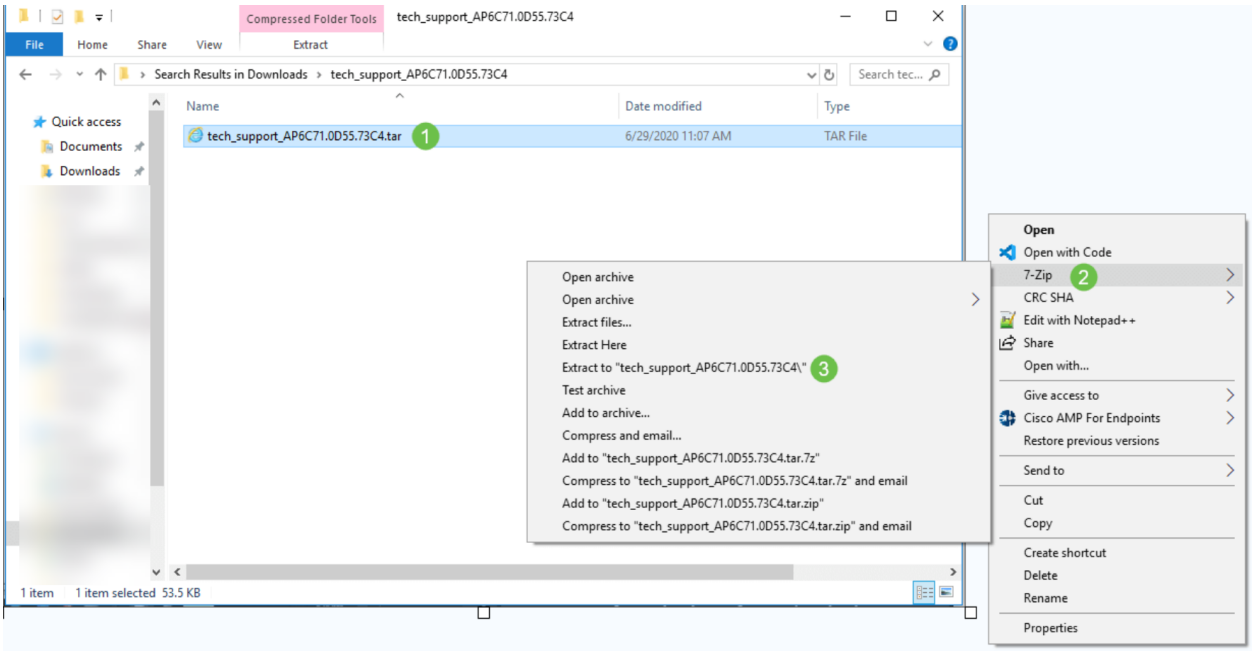


（代替ビュー）コアクラッシュが発生した場合、代わりにこれらのフォルダが表示される場合があります。



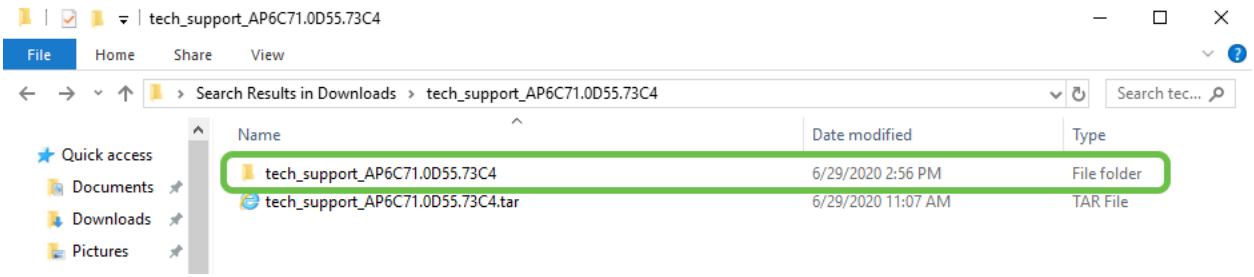
手順 6

*.tgz*ファイルからファイルを抽出すると、ファイルは*.tar*ファイルになります。このファイルを再度抽出する必要があります。



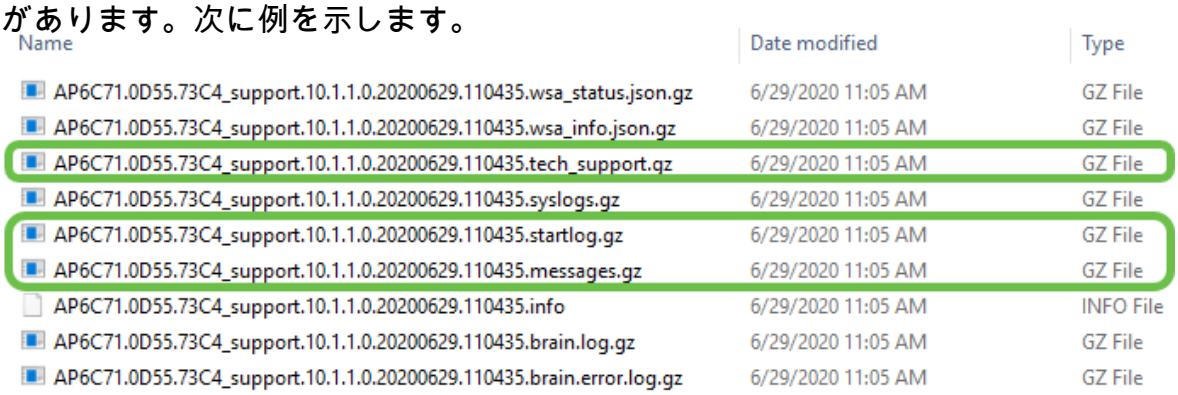
ステップ7

*tech_support*フォルダが表示されます。フォルダをダブルクリックしてファイルを開きます。



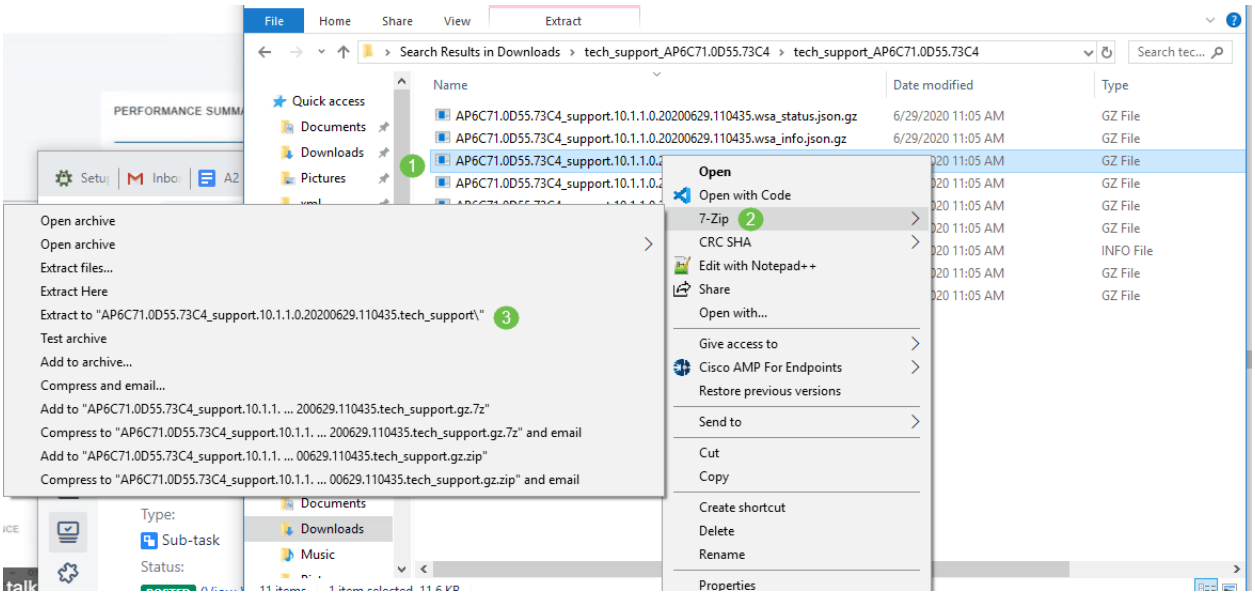
手順 8

サポートバンドル内では、*cli_file*（コンフィギュレーションファイル）、*msg/syslogs*（イベントログ）、および*startlog*が最も関連性の高い情報を提供します。表示されるファイルは異なる場合があります。次に例を示します。



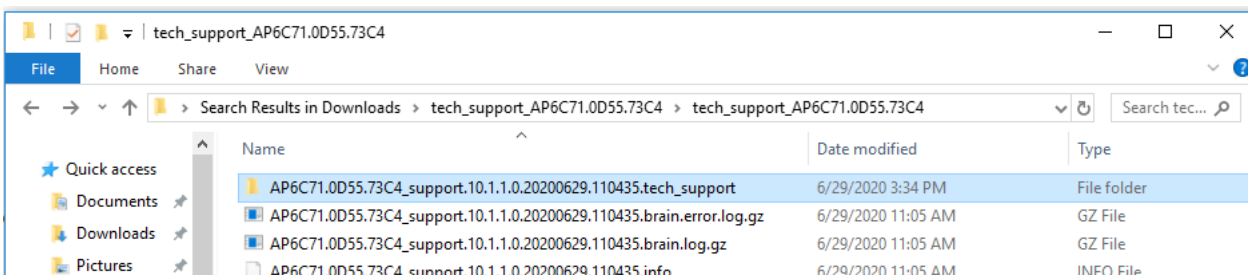
手順 9

解凍したいファイルを右クリックします。この例では、ファイルは*tech_support*のフォルダに解凍されます。



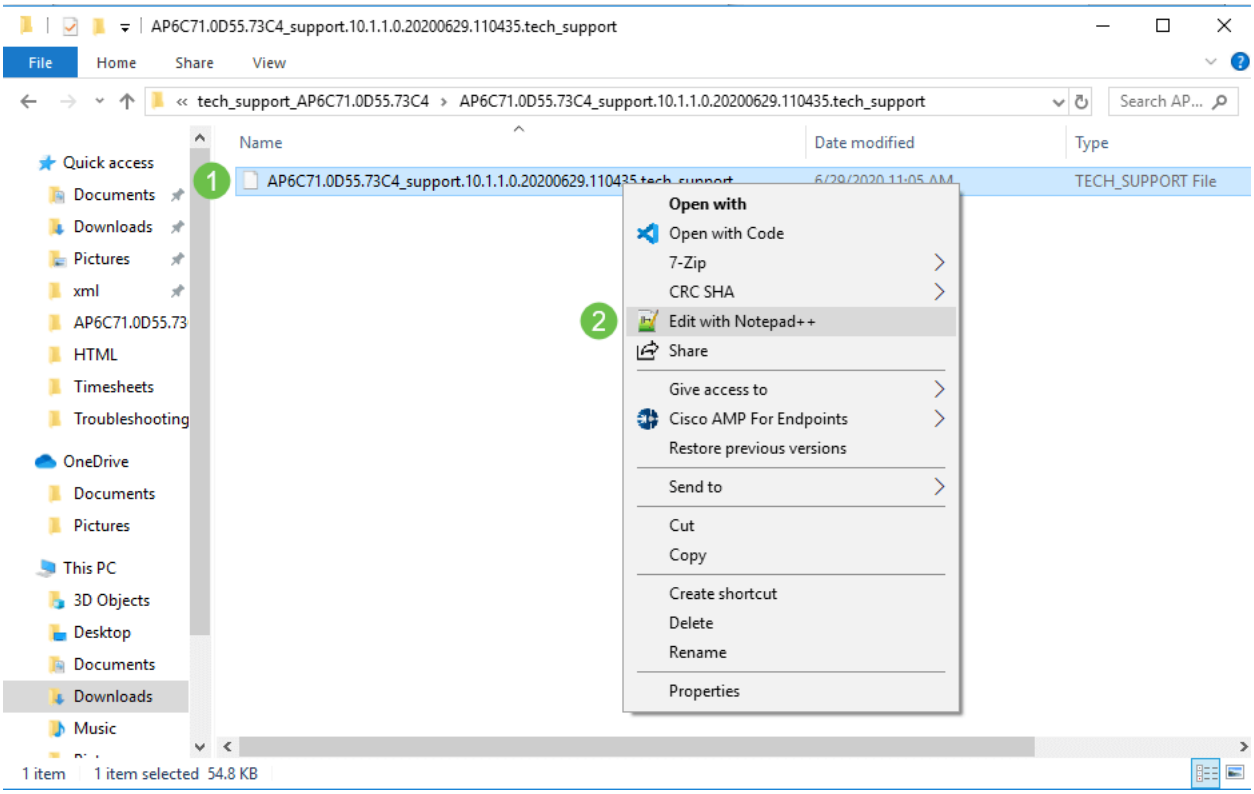
手順 10

*tech_support*フォルダが表示されます。ダブルクリックしてフォルダを開きます。



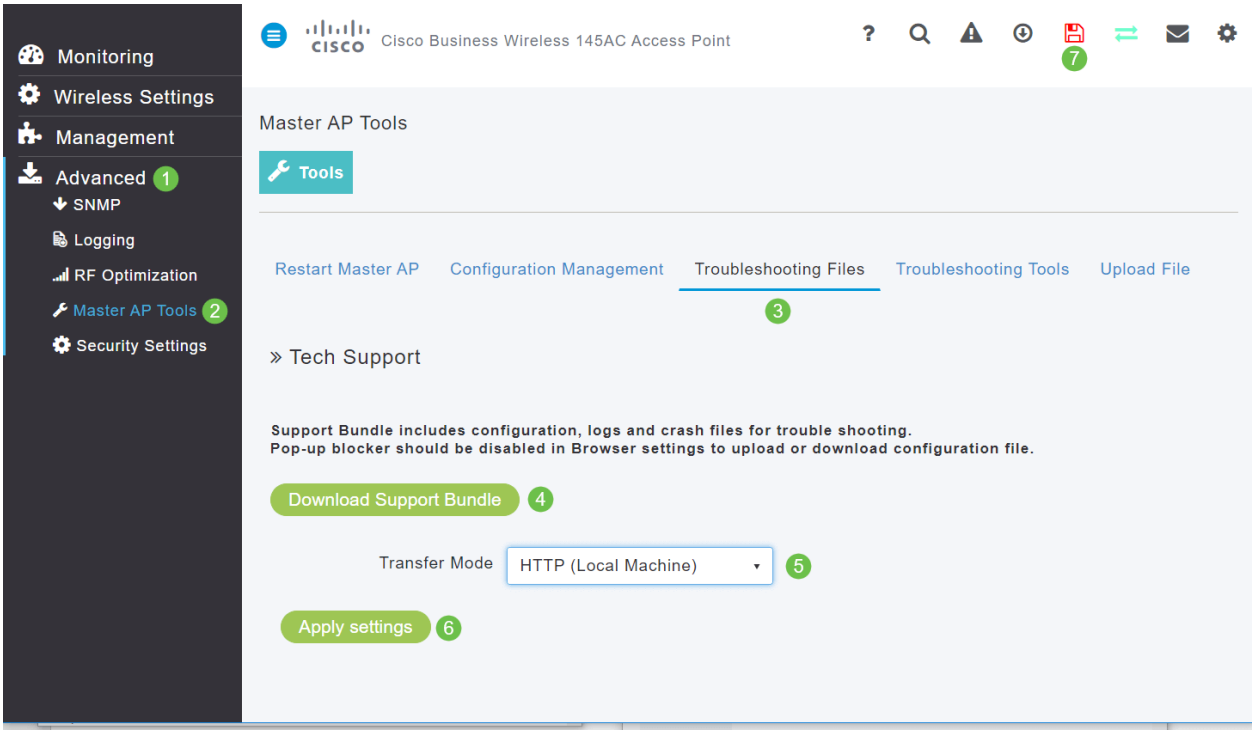
手順 11

ファイルを右クリックし、テキストファイルリーダーを選択します。この例では、**Edit with Notepad++**を使用しています。



プライマリAPテクニカルサポートバンドルへのアクセス

プライマリAPテクニカルサポートバンドルが診断の主要なソースです。プライマリAPまたは仮想コントローラバンドルに組み込まれているテクニカルサポートバンドルをダウンロードするには、[Advanced] > [Primary AP Tools] に移動します。[Troubleshooting Files] タブを選択します。[Download Support Bundle] を選択します。[Transfer Mode] で、[HTTP] または[FTP] を選択します。[Apply settings] をクリックします。**Save**アイコンをクリックします。

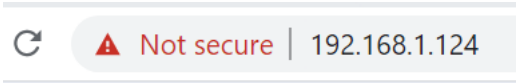


CBW携帯電話設定の1つを調整します

CBWネットワークの802.11r設定の変更

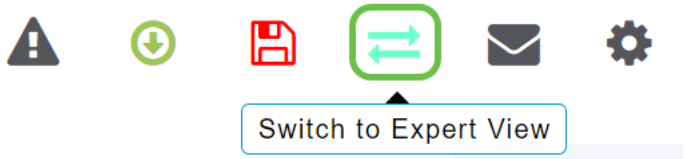
手順 1

Webブラウザにプライマリアクセスポイントの IP アドレスを入力して、Webユーザインターフェイス(UI)にアクセスします。Virtual Private Network (VPN ; バーチャルプライベートネットワーク) に接続していないことを確認してください。接続されていないと動作しません。セキュリティ警告が表示されたら、プロンプトを選択して続行します。



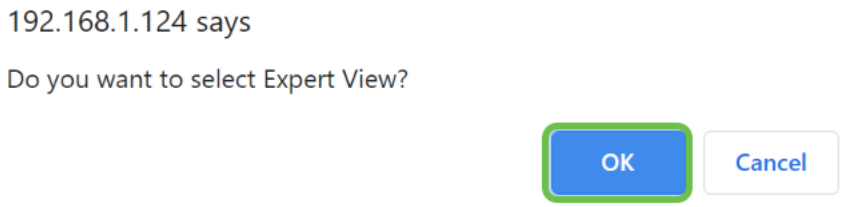
手順 2

Web UIの右上で、反対側の矢印をクリックしてエキスパートビューに切り替えます。



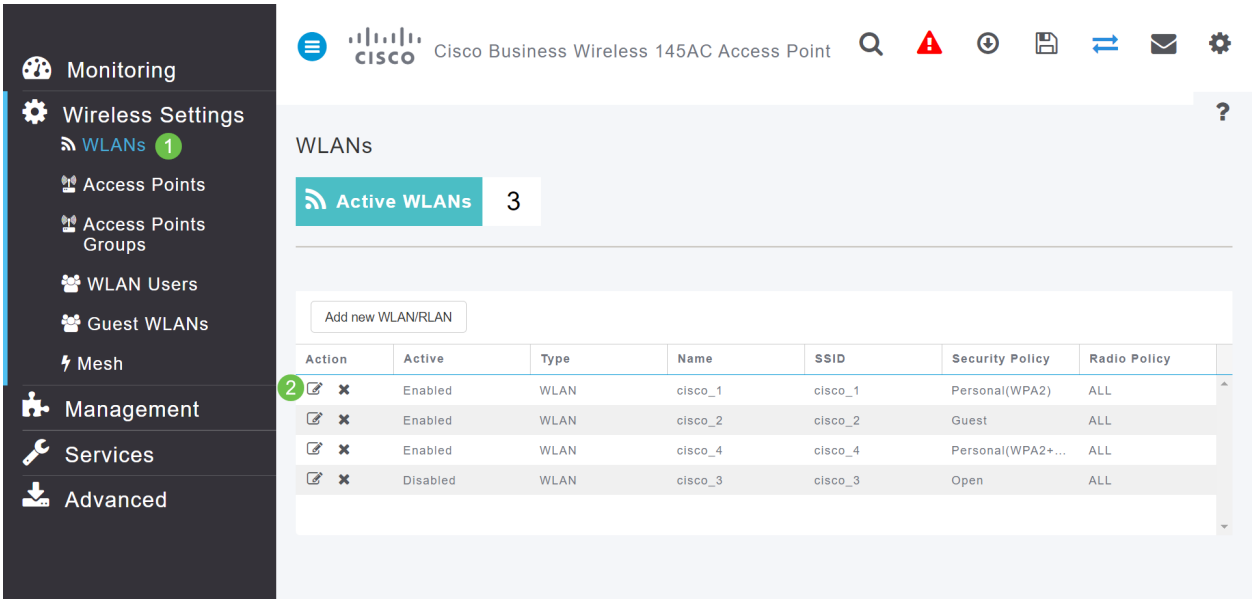
手順 3

ポップアップウィンドウが表示され、エキスパートビューを選択するかどうかを尋ねられます。[OK] をクリックします。



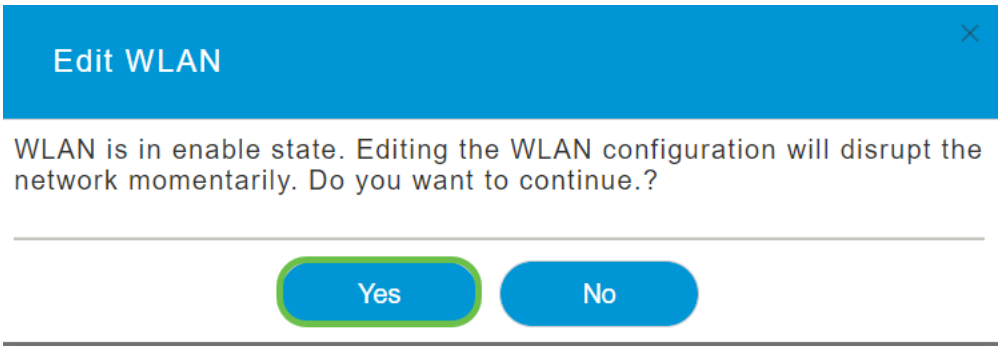
手順 4

WLANsを選択し、編集するWLANの**edit icon**を選択します。



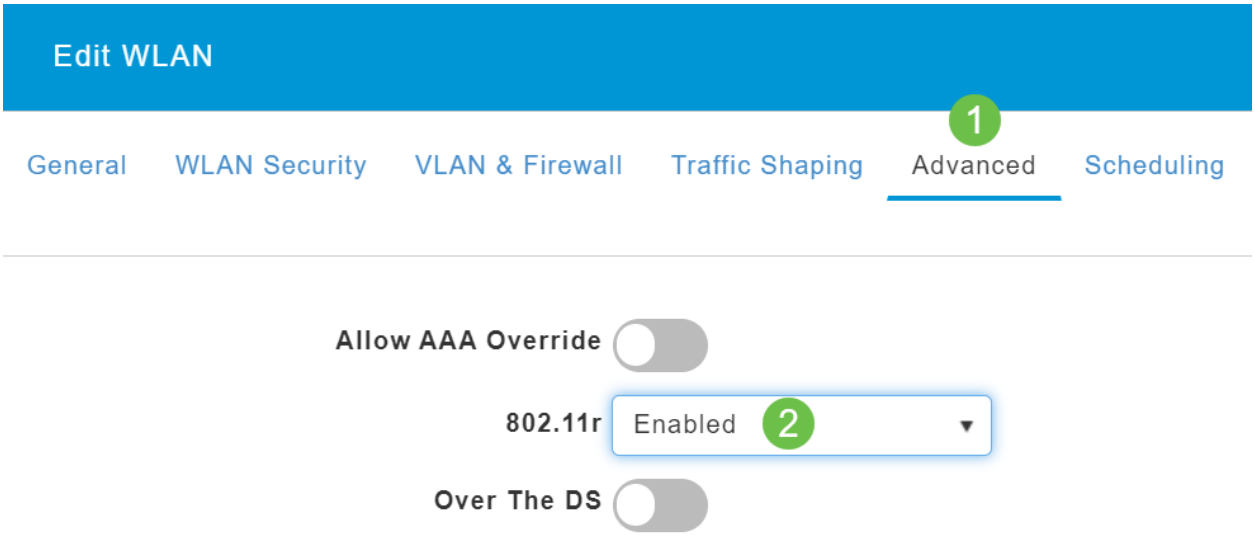
手順 5

ポップアップウィンドウが表示され、続行するかどうかを尋ねられます。[Yes] をクリックします。



手順 6

[詳細] タブをクリックします。802.11rのドロップダウンメニューをクリックし、**Enabled**を選択します。



ステップ7

[Apply] をクリックします。

手順 8

これらの設定を永続的に保存するには、画面の右上にある[save] アイコンをクリックします。

他のすべてに失敗した場合は、工場出荷時のデフォルト設定にリセットします

管理ポータルにアクセスできなくなるなどの最も深刻な問題を解決するためだけに行う必要があるラストリゾートオプションは、ルータでハードウェアリセットを実行することです。

工場出荷時のデフォルト設定にリセットすると、すべての設定が失われます。接続の詳細を確認するため、ルータを最初から再設定する必要があります。

新しいCBW APでのプロセスは、他のAPでの経験とは少し異なります。リセットの詳細については、「CBW APを工場出荷時のデフォルト設定にリセットする」を参照してください。

結論

メッシュネットワークのトラブルシューティングに関する複数のオプションを提供することを目的としています。任務完了！これで接続が確立され、1日の作業を進めることができます。

この記事に関連するビデオを見る...

シスコのその他の技術に関する講演を表示するには、ここをクリックしてください。

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。