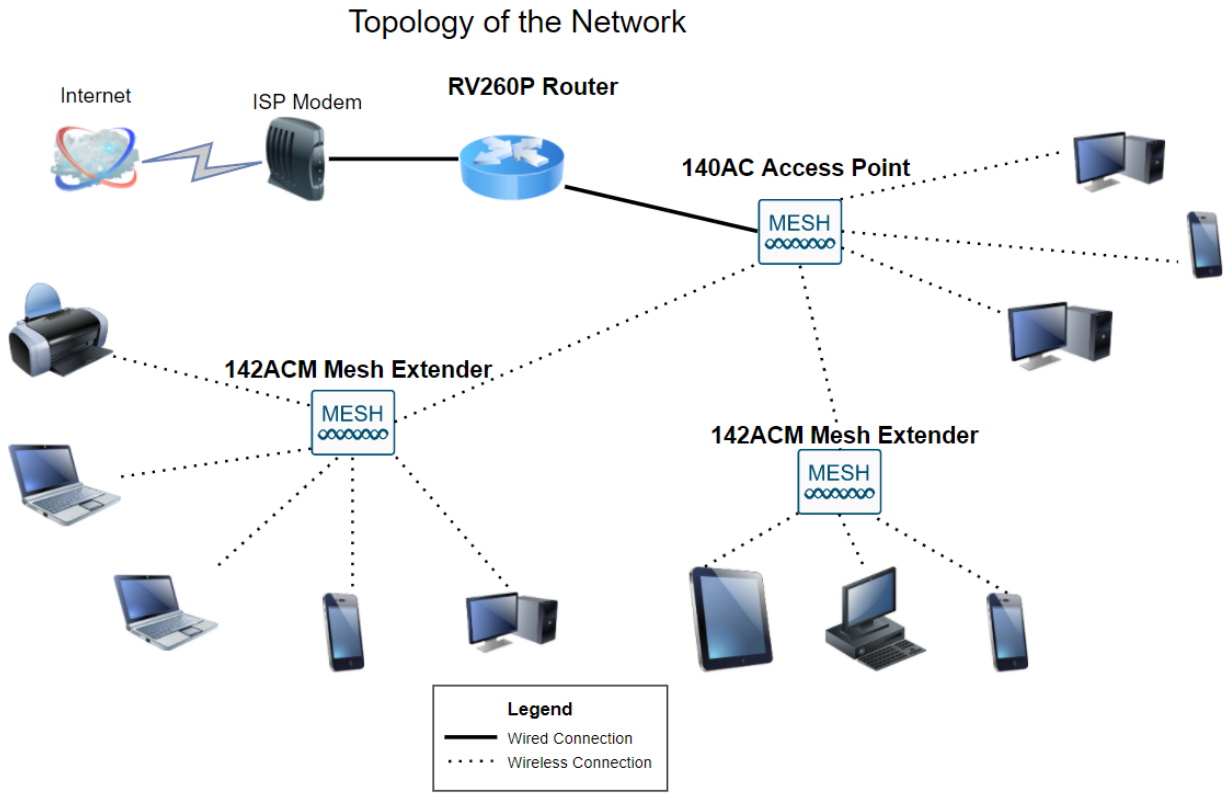
ネットワーク構成の合計：RV260PとCisco Business WirelessおよびWeb UI

目的:

このガイドでは、RV260Pルータ、CBW140ACアクセスポイント、および2つのCBW142ACMメッシュエクステンダを使用してワイヤレスメッシュネットワークを設定する方法について説明します。

この記事では、Webユーザインターフェイス(UI)を使用して、メッシュワイヤレスネットワークをセットアップします。ワイヤレスセットアップを簡単に行うために推奨されるモバイルアプリケーションを使用する場合は、クリックして、モバイルアプリケーションを使用する記事にジャンプしてください。Web UIを使用する場合は、読み続けてください！

トポロジ：



概要

これで、新しいネットワークをセットアップする準備ができました。ワクワクする1日だ！このシナリオでは、RV260Pルータを使用しています。このルータはPower over Ethernet(PoE)を備えており、CBW140ACをスイッチではなくルータに接続できます。CBW140ACおよびCBW142ACMメッシュエクステンダを使用して、ワイヤレスメッシュネットワークを作成します。

このドキュメントで使用されている用語に慣れていないか、メッシュネットワーキン

グの詳細を調べるには、次の記事を参照してください。

- シスコのビジネス:新用語一覧
- Cisco Business Wireless Mesh Networkingへようこそ
- シスコビジネスワイヤレスネットワークに関するFAQ

準備はいいか？行こう！

該当するデバイス |ソフトウェアバージョン

- RV260P |1.0.0.17
- CBW140AC |10.3.1.0
- CBW142ACM | 10.3.1.0（メッシュネットワークには少なくとも1つのメッシュエクステンダが必要）

目次

はじめに

1. セットアップ用の現在のインターネット接続があることを確認してください。
2. RV260ルータを使用する際の特別な手順については、ISPにお問い合わせください。一部のISPは、ルータが内蔵されたゲートウェイを提供しています。統合ルータを備えたゲートウェイを使用している場合は、ルータを無効にして、ワイドエリアネットワーク(WAN)のIPアドレス（インターネットプロバイダーがアカウントに割り当てる一意のインターネットプロトコルアドレス）とすべてのネットワークトラフィックを新しいルータに渡します。

3. ルータを配置する場所を決定します。可能であれば、オープンエリアが必要です。インターネットサービスプロバイダー(ISP)からブロードバンドゲートウェイ（モデム）にルータを接続する必要があるため、これは簡単ではありません。

RV260Pルータの設定

ルータはパケットをルーティングするため、ネットワークに不可欠です。コンピュータは、同じネットワークまたはサブネット上にない他のコンピュータと通信できます。ルータはルーティングテーブルにアクセスして、パケットの送信先を決定します。ルーティングテーブルには、宛先アドレスがリストされます。スタティックコンフィギュレーションとダイナミックコンフィギュレーションの両方をルーティングテーブルにリストして、特定の宛先にパケットを取得できます。

RV260Pには、多くの小規模企業に最適化されたデフォルト設定が用意されています。ただし、ネットワーク要求またはインターネットサービスプロバイダー(ISP)では、これらの設定の一部を変更する必要がある場合があります。要件についてISPに問い合わせたら、Webユーザインターフェイス(UI)を使用して変更できます。

すぐに使えるRV260P

手順 1

RV260P LAN（イーサネット）ポートの1つからコンピュータのイーサネットポートにイーサネットケーブルを接続します。コンピュータにイーサネットポートがない場合は、アダプタが必要です。初期設定を実行するには、端末がRV260Pと同じ有線サブネットワークにある必要があります。

手順 2

RV260Pに付属の電源アダプタを使用してください。別の電源アダプタを使用すると、RV260Pが損傷したり、USBドングルに障害が発生したりする可能性があります。電源スイッチはデフォルトでオンになっています。

電源アダプタをRV260Pの12VDCポートに接続しますが、電源に接続しないでください。

手順 3

モデムがオフになっていることを確認します。

手順 4

イーサネットケーブルを使用して、ケーブルまたはDSLモデムをRV260PのWANポートに接続します。

手順 5

RV260Pアダプタのもう一方の端をコンセントに差し込みます。これでRV260の電源が入ります。モデムの電源を入れ直します。電源アダプタが正しく接続され、RV260Pの起動が終了すると、前面パネルの電源ライトが緑色に点灯します。

ルータの設定

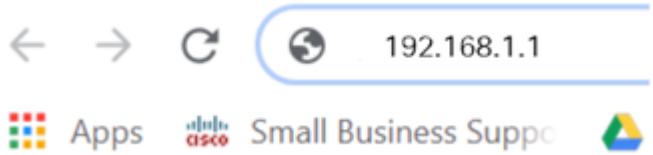
準備作業が完了しました。ここで、いくつかの設定を行います。Web UIを起動するには、次の手順を実行します。

手順 1

コンピュータがDynamic Host Configuration Protocol(DHCP)クライアントになるように設定されている場合、192.168.1.xの範囲のIPアドレスがPCに割り当てられます。DHCPは、IPアドレス、サブネットマスク、デフォルトゲートウェイ、およびその他の設定をコンピュータに割り当てるプロセスを自動化します。アドレスを取得するには、DHCPプロセスに参加するようにコンピュータを設定する必要があります。これは、コンピュータのTCP/IPのプロパティで自動的にIPアドレスを取得するようにを選択することによって行われます。

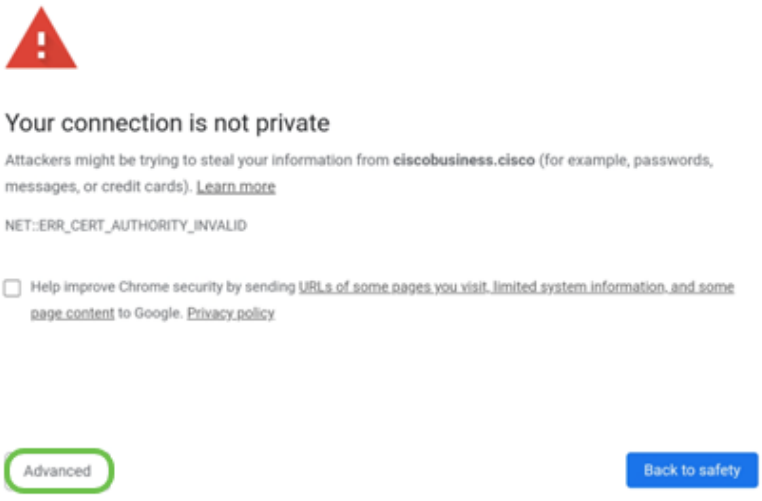
手順 2

Safari、Internet Explorer、FirefoxなどのWebブラウザを開きます。アドレスバーに、RV260PのデフォルトのIPアドレス(192.168.1.1)を入力します。



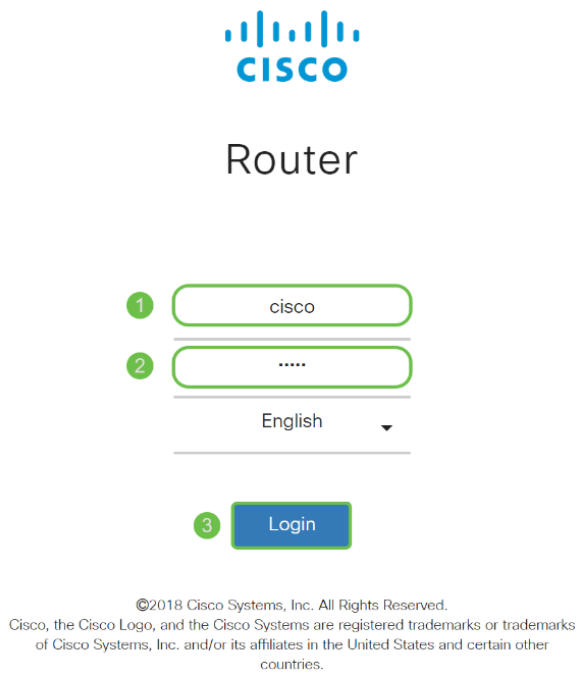
手順 3

ブラウザから、Webサイトが信頼できないという警告が表示されることがあります。Webサイトに移動します。接続していない場合は、「インターネット接続のトラブルシ[ューティング」に移動します](#)。



手順 4

サインインページが表示されたら、デフォルトのユーザ名ciscoとデフォルトのパスワードciscoを入力します。ユーザ名とパスワードの両方で大文字と小文字が区別されます。



手順 5

[Login] をクリックする。[はじめに]ページが表示されます。接続を確認し、ルータにログインしたら、この記事の「初期設定」セクションに移動します。

インターネット接続のトラブルシューティング

Dangこれを読んでいる場合、おそらくインターネットまたはWeb UIに接続できません。これらのソリューションの1つが役立ちます。

接続されているWindows OSで、コマンドプロンプトを開いてネットワーク接続をテストできます。ping 192.168.1.1（ルータのデフォルトIPアドレス）を入力します。要求がタイムアウトすると、ルータと通信できません。

接続が発生していない場合は、「RV160およびRV260ルータのトラブルシューティング」を参照してください。

その他の試し：

1. Webブラウザが[オフライン作業]に設定されていないことを確認します。
2. イーサネットアダプタのローカルエリアネットワーク接続設定を確認します。PCはDHCP経由でIPアドレスを取得する必要があります。または、デフォルトゲートウェイが192.168.1.1（RV260Pのデフォルトアドレス）に設定されている192.168.1.xの範囲にスタティックIPアドレスを設定することもできます。 接続するには、RV260Pのネットワーク設定を変更する必要がある場合があります。Windows 10を使用している場合は、Windows 10の方向を確認してネットワーク設定を変更してくださ

い。

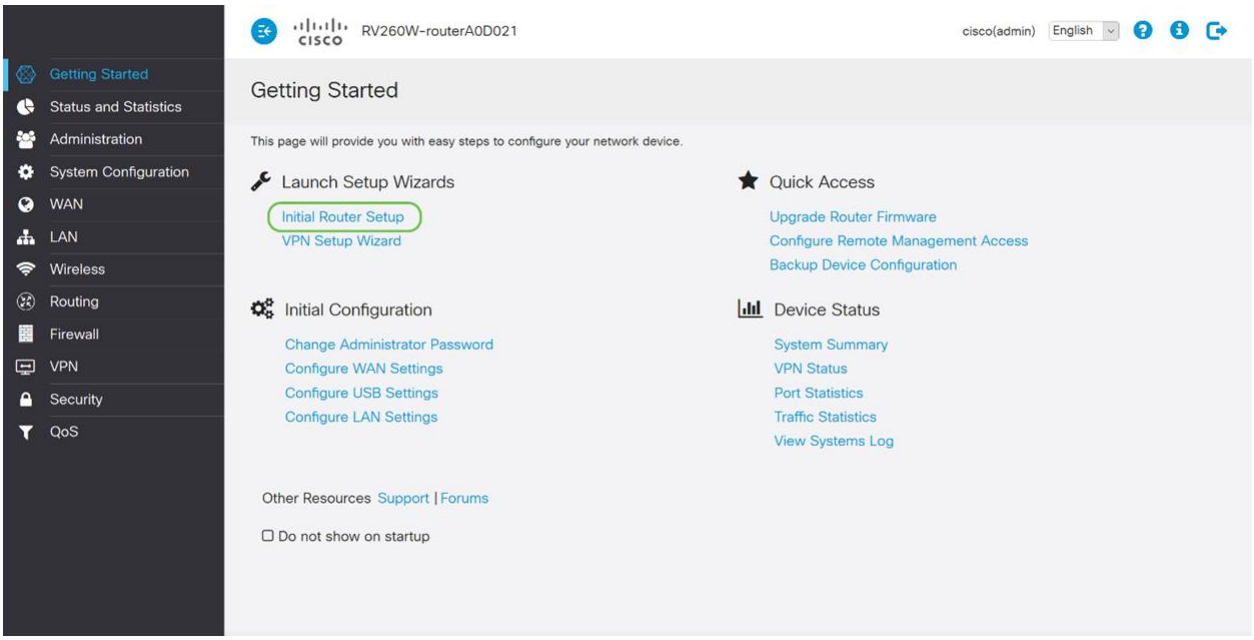
3. 192.168.1.1のIPアドレスを使用している既存の機器がある場合は、ネットワークが動作するためにこの競合を解決する必要があります。このセクションの最後に詳しく説明します。または、ここをクリックして直接説明してください。
4. 両方のデバイスの電源をオフにして、モデムとRV260Pをリセットします。次に、モデムの電源を入れ、約2分間アイドル状態にします。その後、RV260Pの電源をオンにします。これで、WAN IPアドレスが受信されます。
5. DSLモデムを使用している場合は、ISPにDSLモデムをブリッジモードにするよう依頼します。

初期設定

このセクションに記載されている初期セットアップウィザードの手順を実行することをお勧めします。これらの設定はいつでも変更できます。

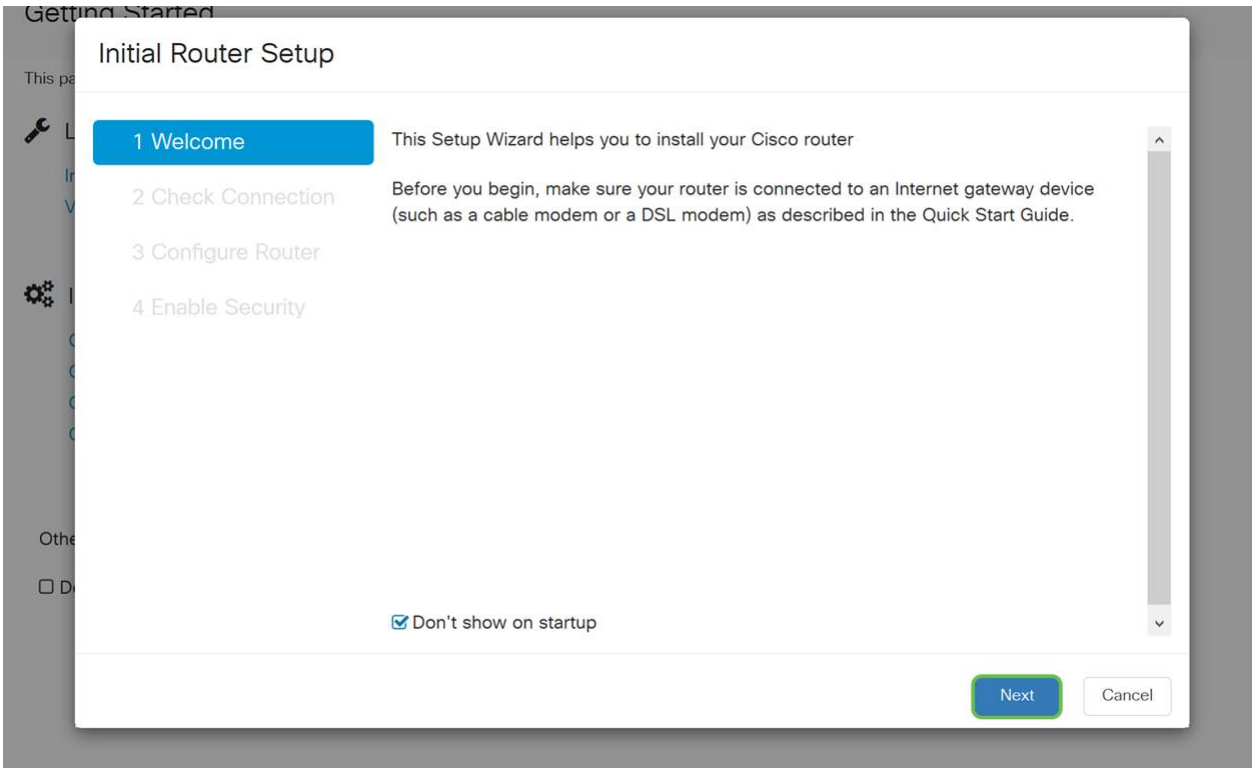
手順 1

[はじめに]ページから[初期セットアップウィザード]をクリックします。



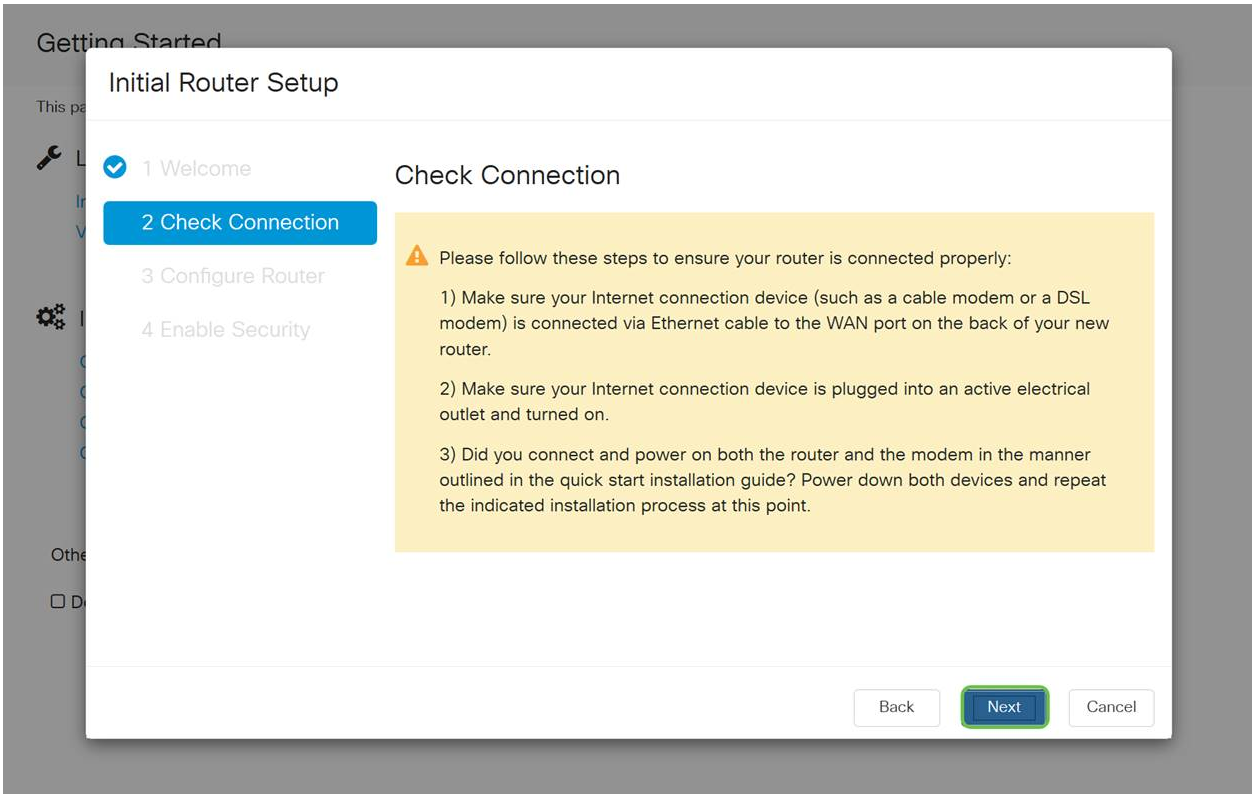
手順 2

この手順では、ケーブルが接続されていることを確認します。すでに確認したので、[次へ]をクリックします。



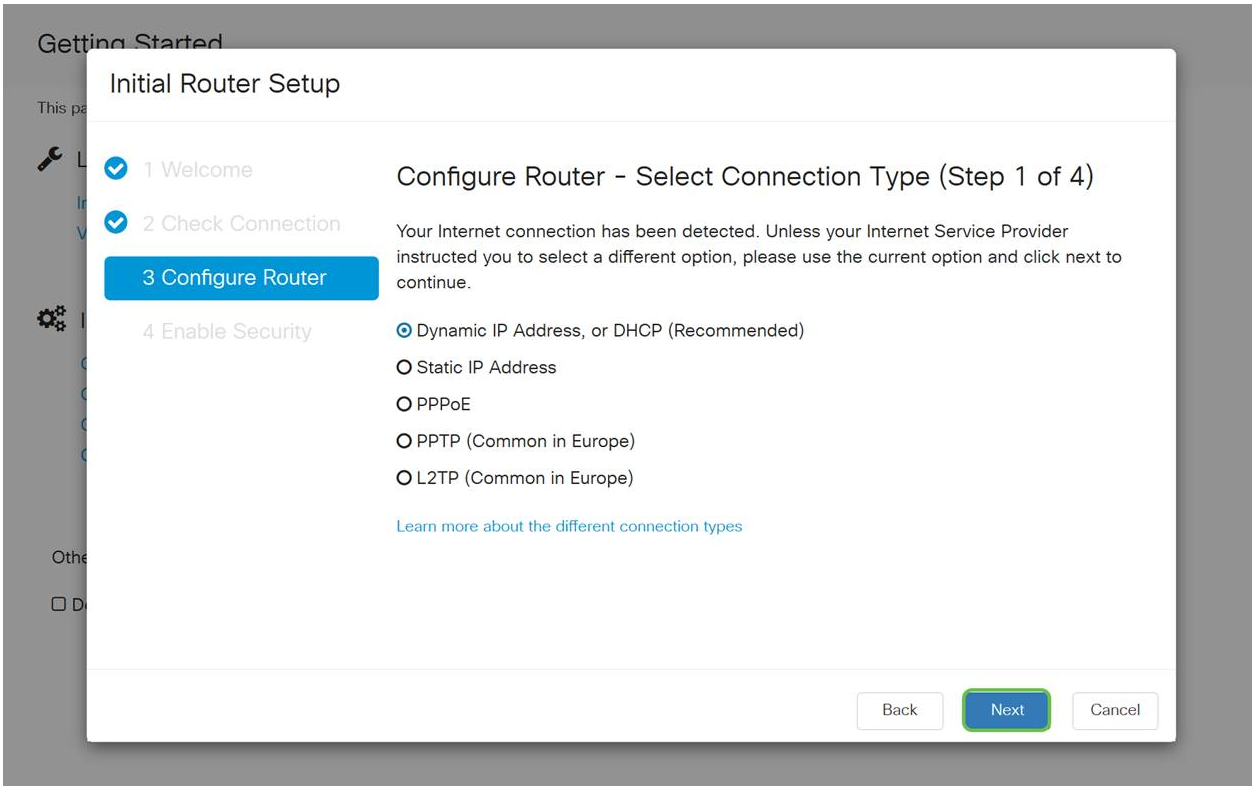
手順 3

この手順では、ルータが接続されていることを確認するための基本的な手順について説明します。これを既に確認しているため、[次へ]をクリックします。



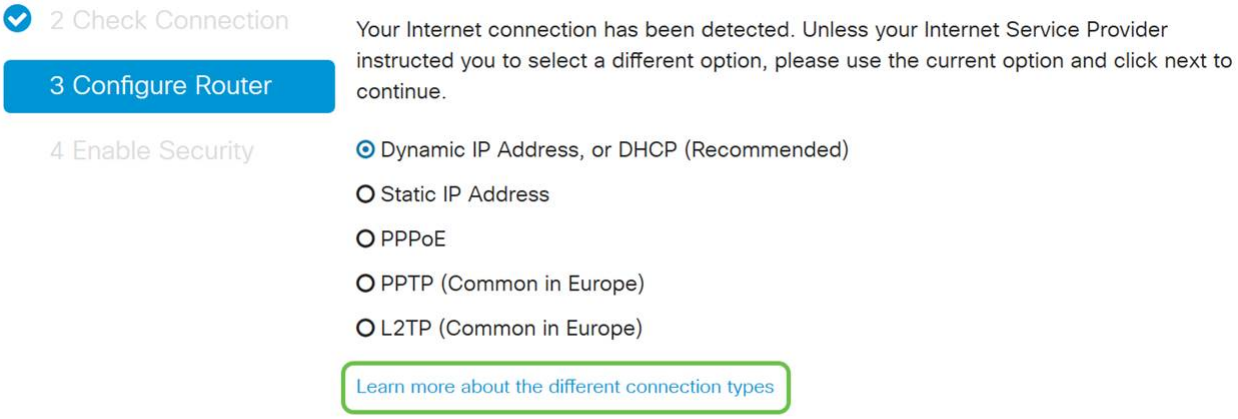
手順 4

次の画面には、ルータにIPアドレスを割り当てるオプションが表示されます。このシナリオでは、DHCPを選択する必要があります。[next] をクリックします。



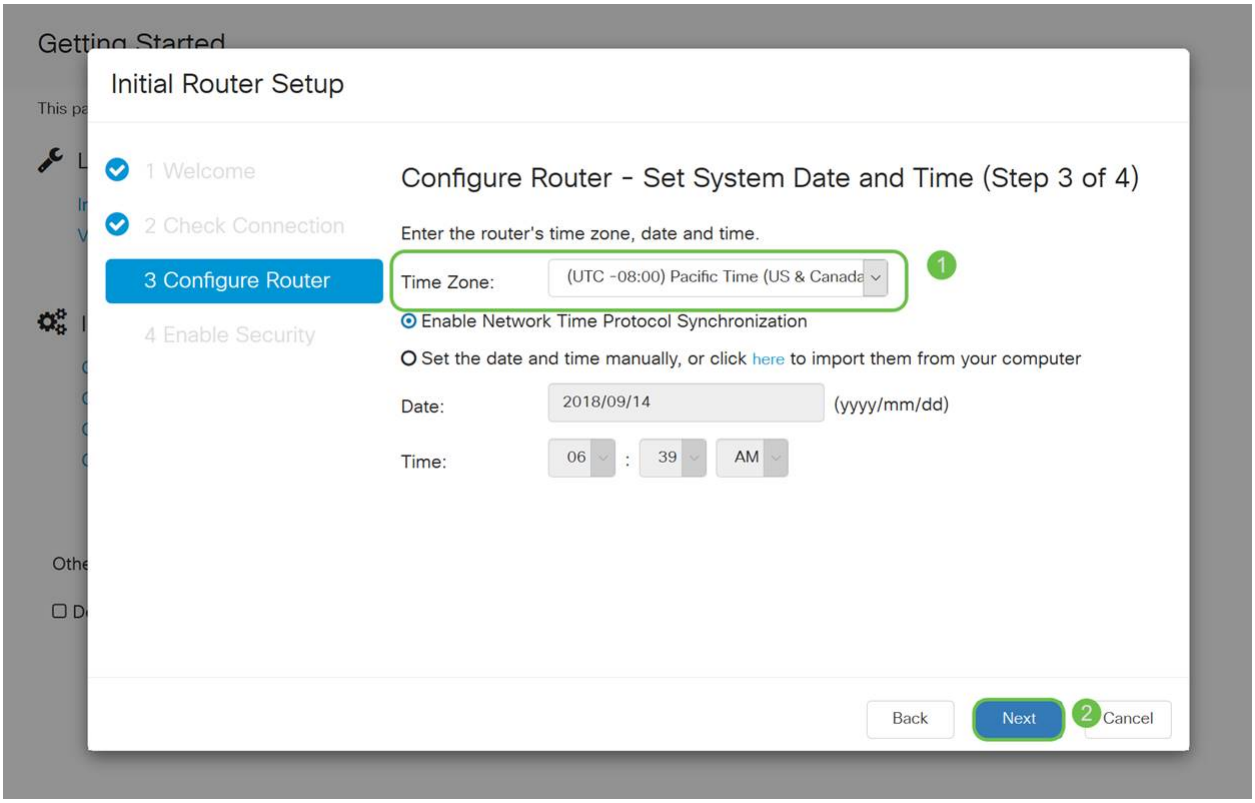
この初期設定にはDHCPを使用する必要がありますが、今後の参考として、画面下部に表示される各種の接続の種類に関する詳細を確認するように選択できます。詳細については、次の記事を参照してください。

- RV160xおよびRV260xデバイスのWAN設定
- RV160およびRV260でのスタティックルーティングの設定



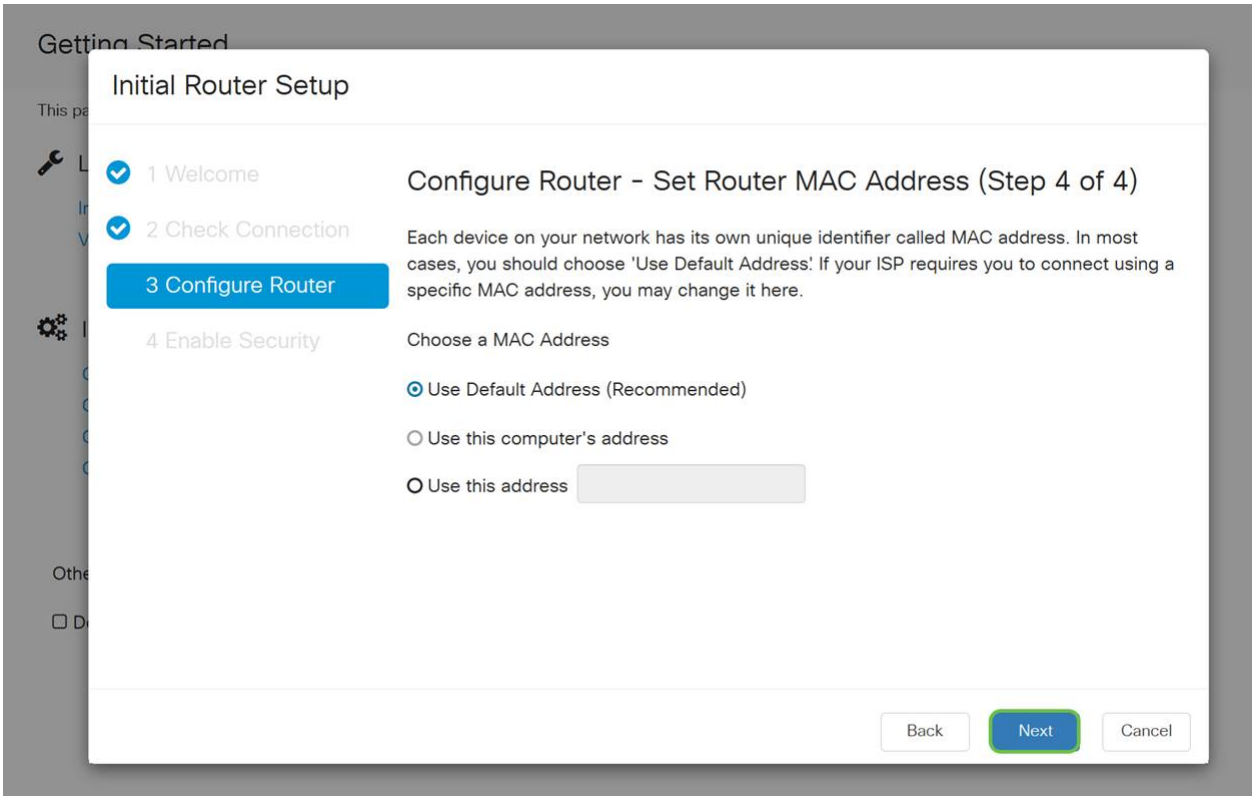
手順 5

ここでは、ルータの時刻設定を求められます。これは、ログの確認やイベントのトラブルシューティングを行う際に精度を高めることができるため、重要です。タイムゾーンを**選択し、**[次へ]をクリック**します。**



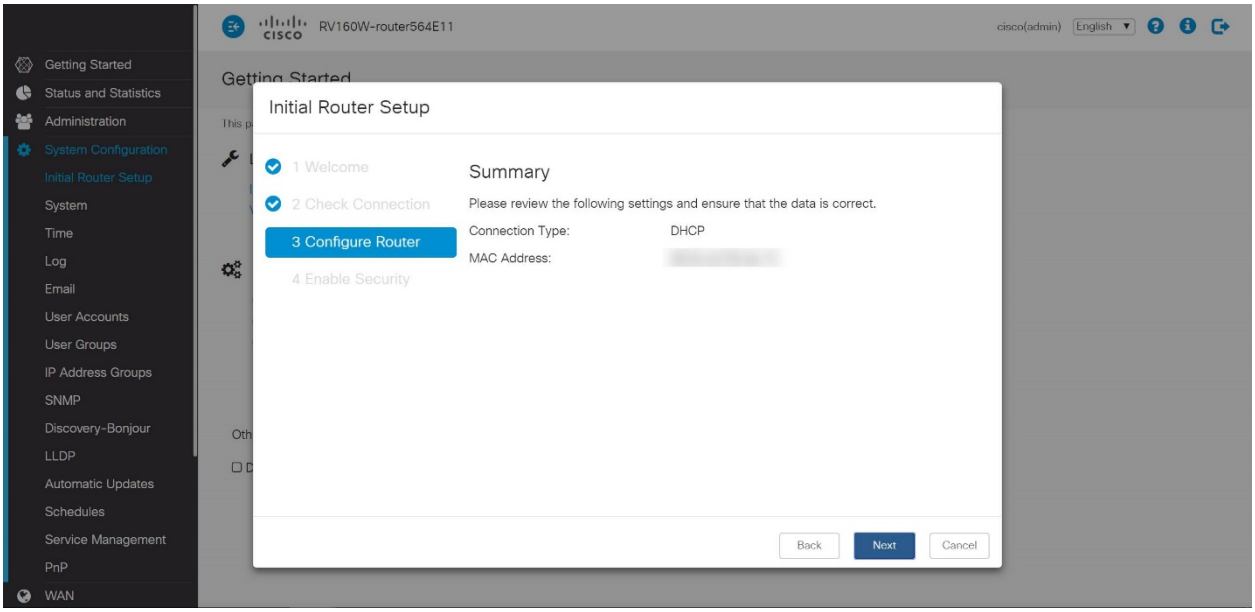
手順 6

この画面では、デバイスに割り当てるMACアドレスを選択します。ほとんどの場合、デフォルトアドレスを使用します。[next] をクリックします。



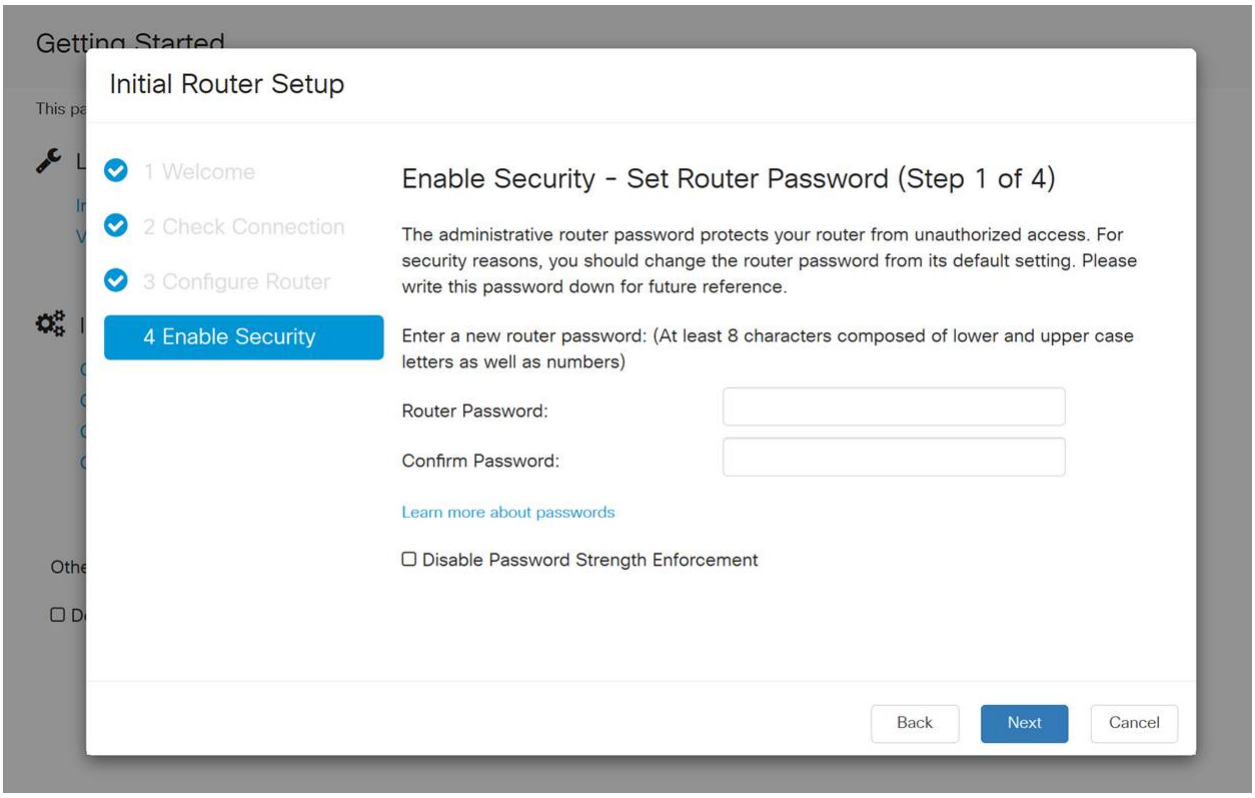
ステップ7

次のページは、選択したオプションの概要です。確認し、問題が解決した場合は**[次へ]**をクリックします。



手順 8

次の手順では、ルータにログインするときに使用するパスワードを選択します。パスワードの標準は、8文字以上（大文字と小文字の両方）と数字を含むパスワードです。強度の要件に従ってパスワードを入力してください。[next] をクリックします。今後のログインに使用するパスワードをメモします。



[パスワード強度の適用を無効にする]を選択することはお勧めしません。このオプションを使用すると、123という単純なパスワードを選択できます。このパスワードは、悪意のある攻撃者が1-2-3と同じくらい簡単に割り込むことができます。

手順 9

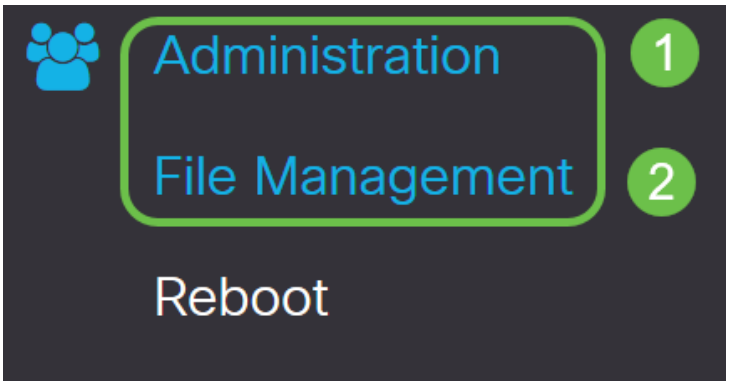
保存アイコンをクリックします。

必要に応じたファームウェアのアップグレード

これは重要なセクションです、スキップしないでください！

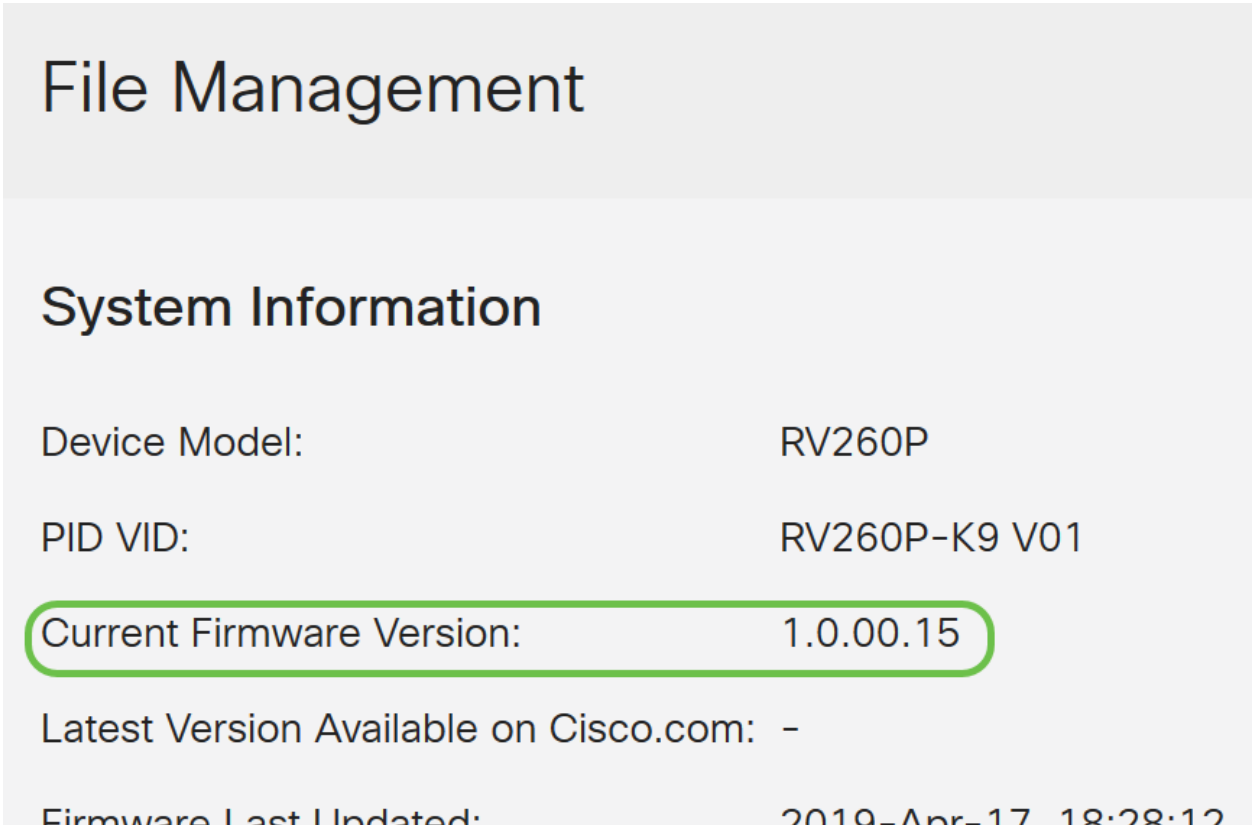
手順 1

[Administration] > [File Management]を選択します。



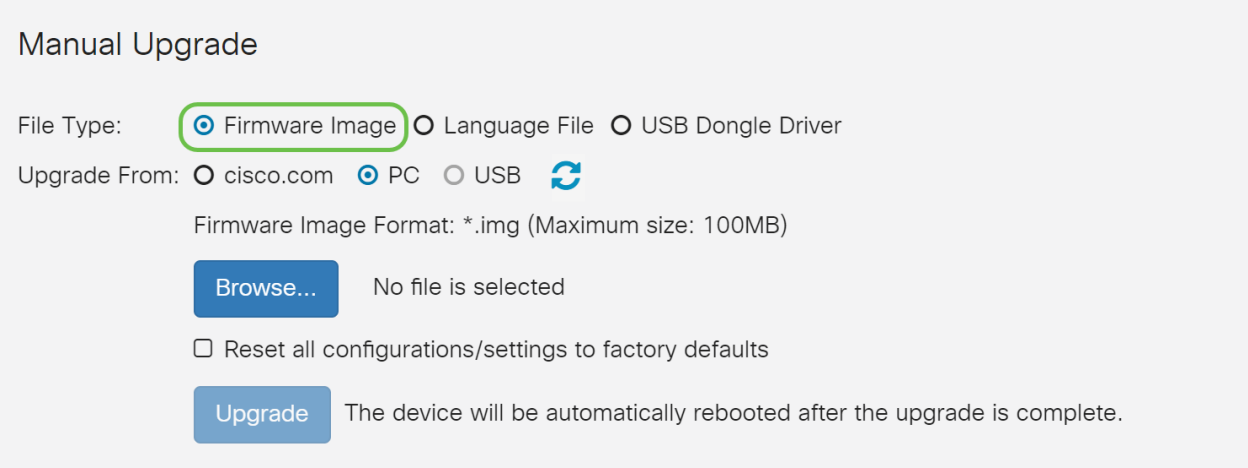
[システム情報]領域で、次のサブエリアで説明します。

- [デバイスモデル(Device Model)]：デバイスのモデルを表示します。
- PID VID：ルータの製品IDとベンダーID。
- [Current Firmware Version]：デバイスで現在実行されているファームウェア。
- Latest Version Available on Cisco.com：シスコのWebサイトで入手可能なソフトウェアの最新バージョン。
- Firmware last updated：ルータで最後にファームウェアがアップデートされた日時。



手順 2

[Manual Upgrade]セクションで、[File Type]の**[Firmware Image]ラジオボタン**をクリックします。



手順 3

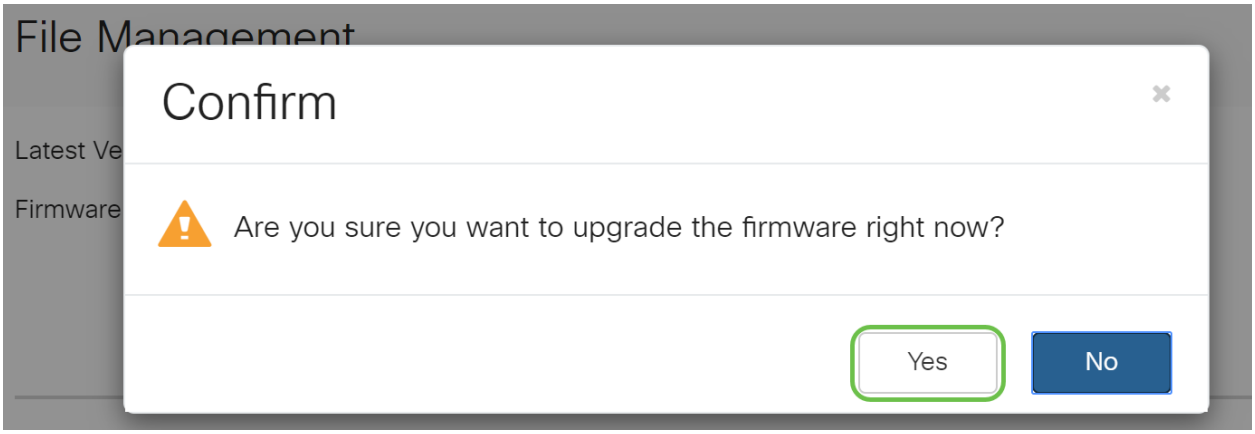
[マニュアルアップグレード]ページで、オプションボタンをクリックしてcisco.comを選択します。これには他にもいくつかのオプションがありますが、これはアップグレードを行う最も簡単な方法です。このプロセスでは、最新のアップグレードファイルをCisco Software Downloads Webページから直接インストールします。

手順 4

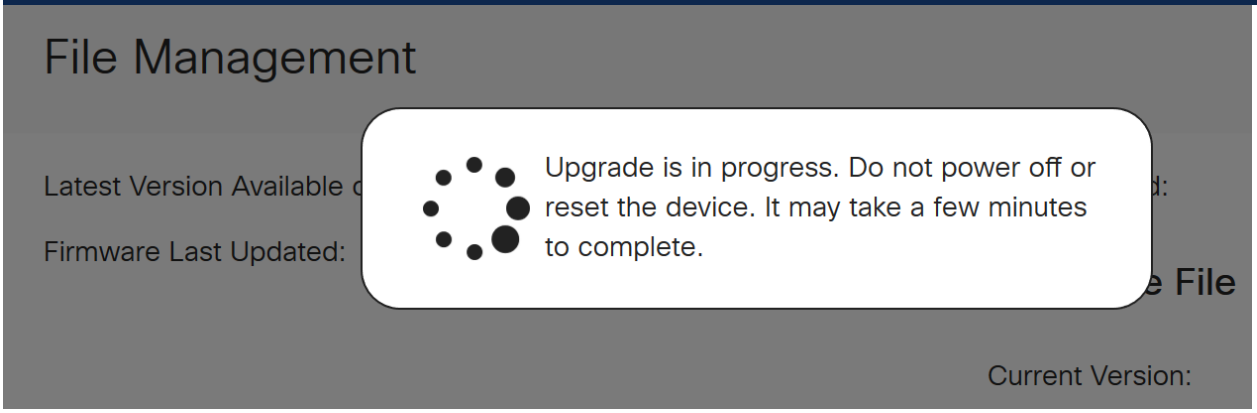
[Upgrade]をクリックします。

手順 5

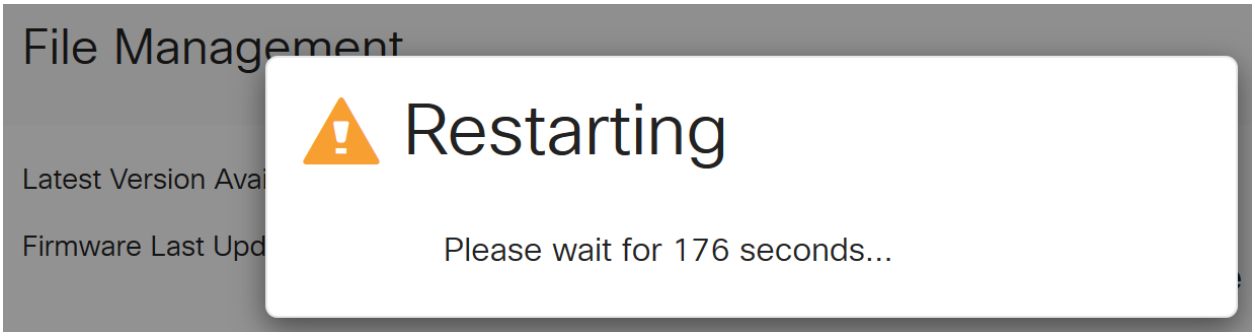
確認ウィンドウで[はい]をクリックして続行します。



アップデートプロセスは中断なく実行する必要があります。アップグレードの進行中に、次のメッセージが画面に表示されます。

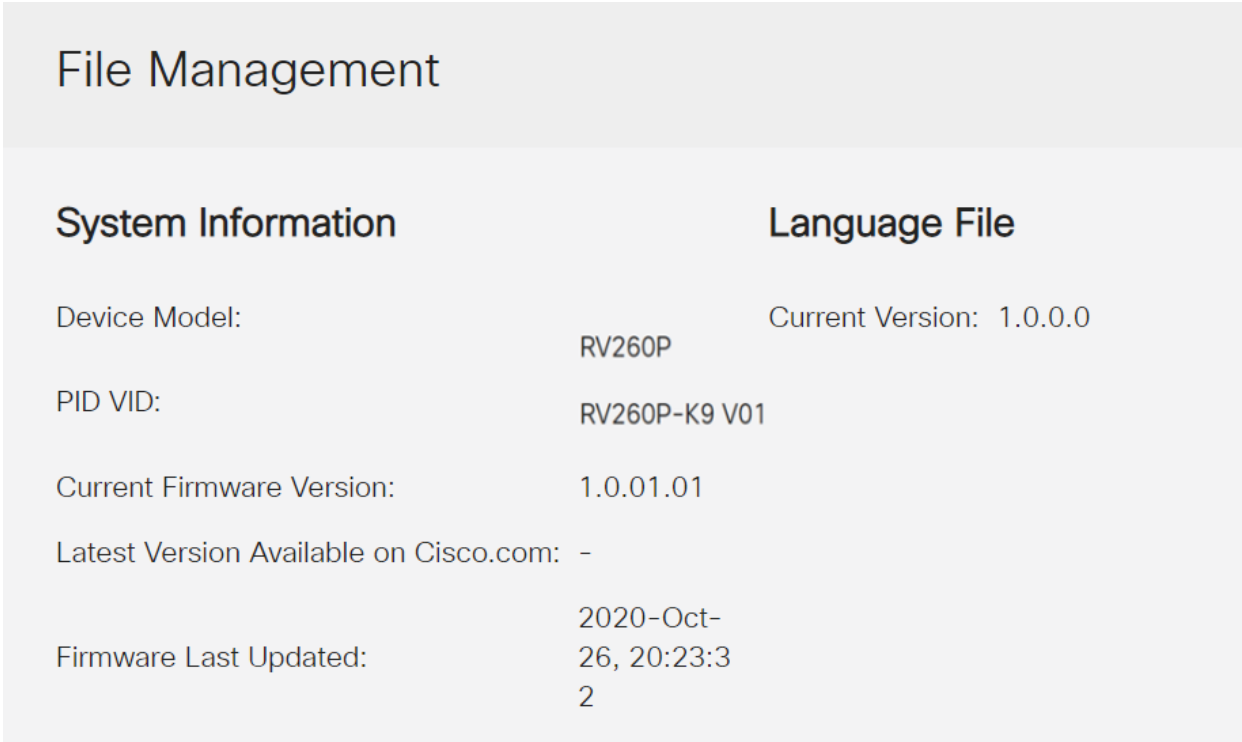


アップグレードが完了すると、通知ウィンドウがポップアップ表示され、プロセスが終了するまでの推定時間をカウントダウンしてルータが*再起動*することを通知します。その後、ログアウトされます。



手順 6

Webベースのユーティリティに再度ログインして、ルータのファームウェアがアップグレードされたことを確認し、[*System Information*]までスクロールします。これで、[Current *Firmware Version*]領域に、アップグレードされたファームウェアバージョンが表示されます。



これで、ルータの基本設定は完了です。いくつかの設定オプションを進めます。

これらのオプションについて詳しく知るために、記事をスクロールし続け、そのオプションが適用される場合は必ず説明してください。任意のハイパーリンクをクリックして、代わりにセクションにジャンプすることもできます。

- VLANの設定（オプション）
- IPアドレスの編集（オプション）
- スタティックIPアドレスの追加（オプション）
- ネットワークのメッシュワイヤレス部分を設定する準備ができました!

VLANの設定（オプション）

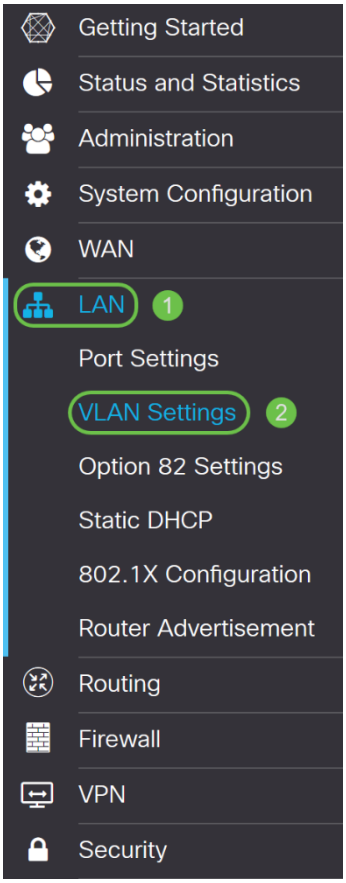
仮想ローカルエリアネットワーク(VLAN)を使用すると、ローカルエリアネットワーク(LAN)を論理的に異なるブロードキャストドメインにセグメント化できます。機密データがネットワーク上でブロードキャストされるシナリオでは、特定のVLANにブロ

ードキャストを指定することでセキュリティを強化するためにVLANを作成できます。また、VLANを使用して、ブロードキャストやマルチキャストを不要な宛先に送信する必要性を減らし、パフォーマンスを向上させることもできます。VLANは作成できますが、VLANが手動または動的に少なくとも1つのポートに接続されるまで、これは影響しません。ポートは常に1つ以上のVLANに属している必要があります。

VLANを作成しない場合は、次のセクションにスキップ**できます**。

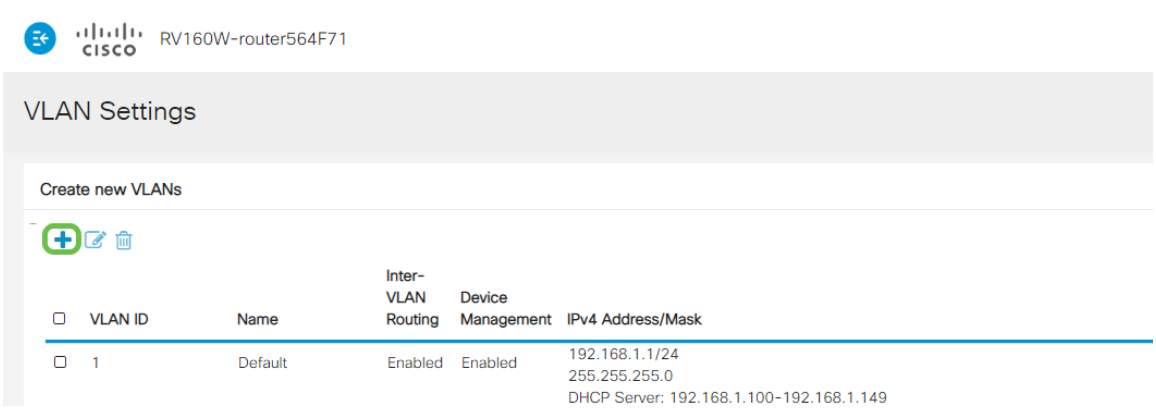
手順 1

[LAN] > [VLAN Settings]に移動します。



手順 2

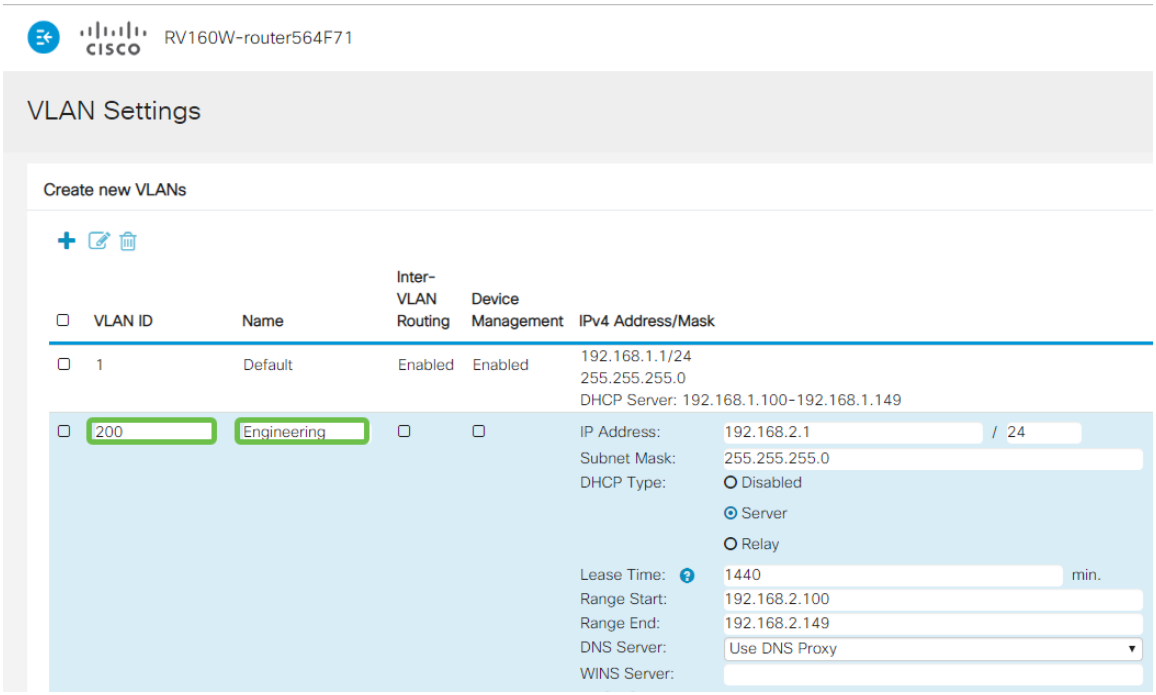
[Add]をクリックし、新しいVLANを作成します。



手順 3

作成する*VLAN ID*とその名前を入力します。VLAN IDの*範囲*は1 ~ 4093です。

VLAN IDとして**200**を入力し、*VLAN*の名前として**Engineering**を入力しました。



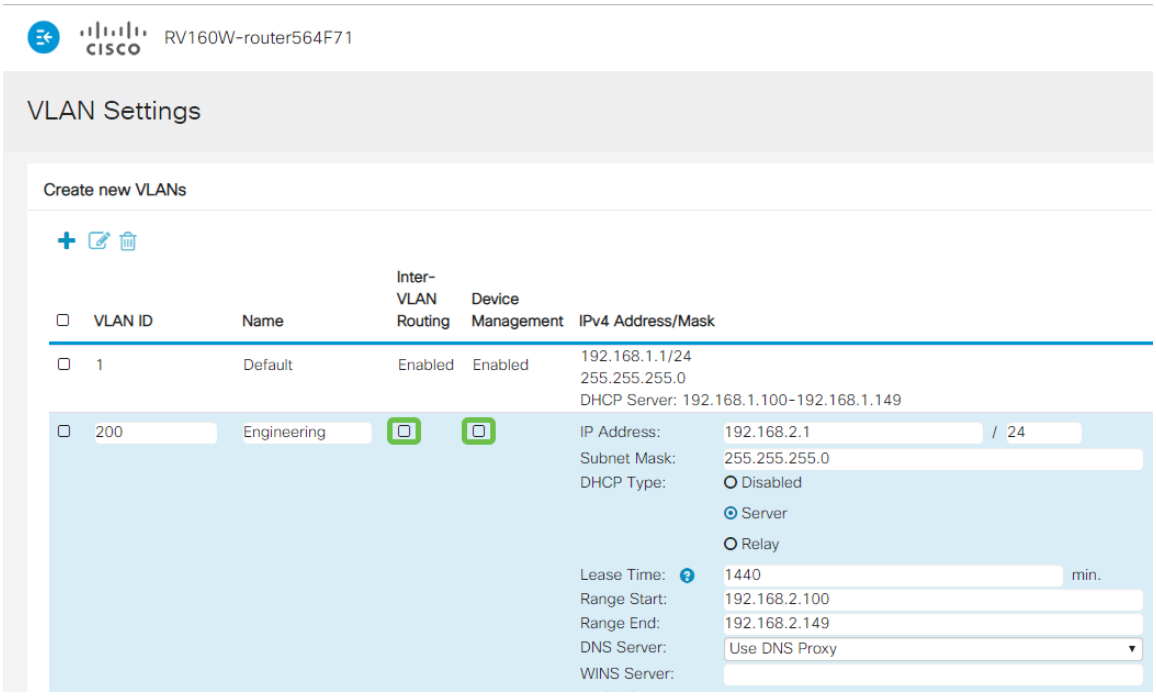
手順 4

必要に応じて、[*Inter-VLAN Routing*]と[*Device Management*]の*両方の*[*Enabled*]ボックスをオフにします。

VLAN間ルーティングは、あるVLANから別のVLANにパケットをルーティングするために使用されます。ゲストネットワークでは、VLANのセキュリティを低下させるゲストユーザを分離するため、一般に、これはゲストネットワークでは推奨されません。VLANが相互にルーティングする必要がある場合があります。このような場合は、「ターゲットACL制限のあるRV34xルータでのVLAN間ルーティング」を参照して、VLAN間で許可する特定のトラフィックを設定してください。

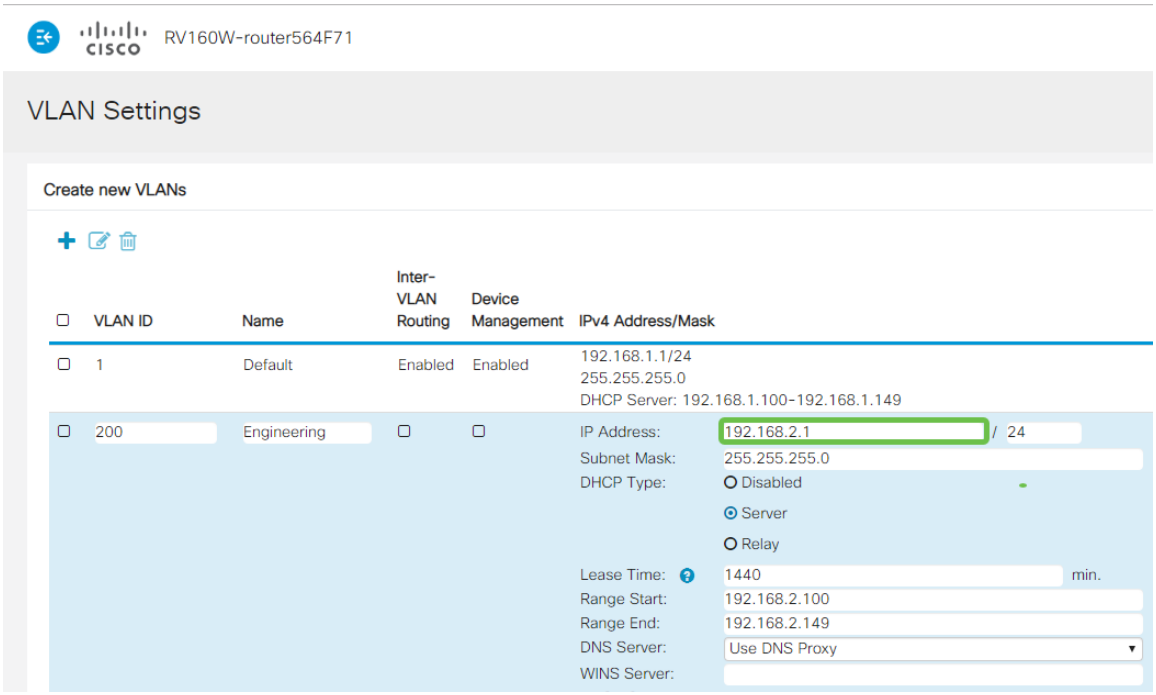
Device Managementは、ブラウザを使用してVLANからRV260PのWeb UIにログインし、RV260Pを管理できるソフトウェアです。これは、ゲストネットワークでも無効にする必要があります。

この例では、VLANをより安全に保つために*Inter-VLAN Routing*または*Device Management*を有効にしていませんでした。



手順 5

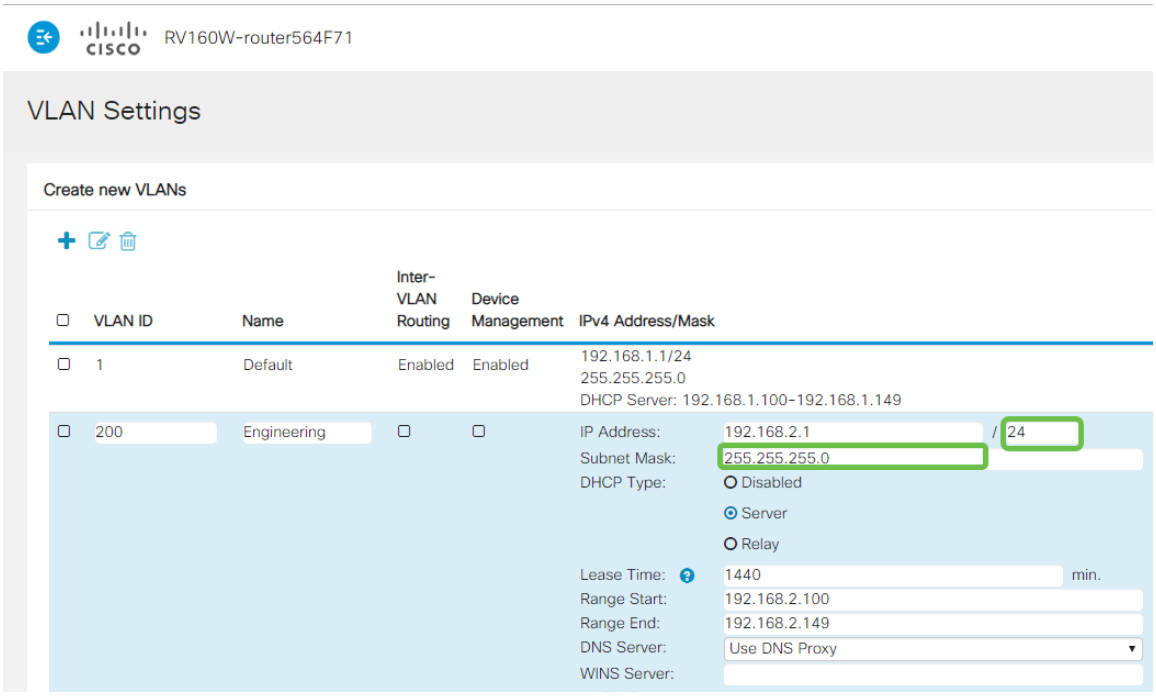
プライベートIPv4アドレスが[IPアドレス]フィールドに自*動的に入力*されます。これを調整するには、次を選択します。この例では、サブネットに192.168.2.100 ~ 192.168.2.149のIPアドレスがDHCPで使用可能です。192.168.2.1 ~ 192.168.2.99および192.168.2.150 ~ 192.168.2.254は、スタティックIPアドレスに使用できます。



手順 6

[サブネットマスク]のサブネットマスクが自動的に入力されます。変更を行うと、フィールドが自動的に調整されます。

このデモンストレーションでは、サブネットマスクを255.255.255.0または**/24のままにしています。**



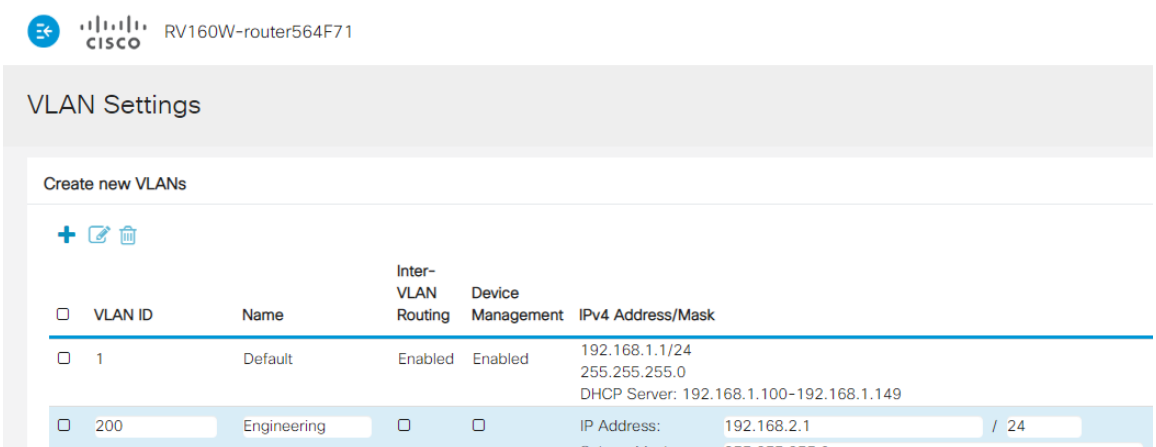
ステップ7

動的ホスト*構成プロトコル(DHCP)の種類を選択します*。次のオプションがあります。

Disabled:VLAN上のDHCP IPv4サーバを無効にします。これは、テスト環境で推奨されます。このシナリオでは、すべてのIPアドレスを手動で設定し、すべての通信を内部にする必要があります。

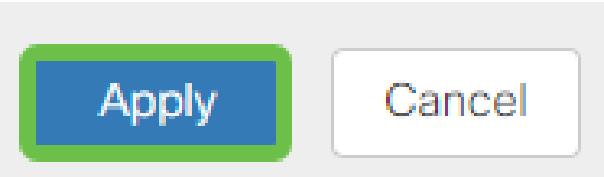
Server : これは最もよく使用されるオプションです。

- [リース時間(Lease Time)]:5 ～ 43,200分の時間値を入力します。デフォルトは1440分（24時間）です。
- Range Start and Range End：動的に割り当てることができるIPアドレスの範囲の開始と終了を入力します。
- [DNSサーバ(DNS Server)]:DNSサーバをプロキシとして使用するか、ドロップダウンリストからISPを選択します。
- WINSサーバ：WINSサーバ名を入力します。
- DHCP オプション:
    - オプション66:TFTPサーバのIPアドレスを入力します。
    - オプション150:TFTPサーバのリストのIPアドレスを入力します。
    - オプション67：設定ファイル名を入力します。
- Relay：リモートDHCPサーバのIPv4アドレスを入力して、DHCPリレーエージェントを設定します。これは、より高度な設定です。



手順 8

[Apply]をクリックし、新しいVLANを作成します。



ポートへのVLANの割り当て

RV260には16のVLANを設定でき、ワイドエリアネットワーク(WAN)用に1つのVLANを使用できます。ポート上にないVLANは除外する必要があります。これにより、ユーザが具体的に割り当てたVLAN/VLANに対して、そのポートのトラフィックが排他的に保持されます。ベストプラクティスと考えられています。

ポートは、アクセスポートまたはトランクポートに設定できます。

- アクセスポート：1つのVLANが割り当てられます。タグなしフレームが渡されます。
- トランクポート：複数のVLANを伝送できます。802.1q.トランキングにより、ネイティブVLANをタグなしにすることができます。トランクで使用しないVLANは除外する必要があります。

1つのVLANに独自のポートが割り当てられている：

- アクセスポートと見なされます。
- このポートに割り当てられているVLANは、[Untagged]というラベルが付いている必要があります。
- 他のすべてのVLANには、そのポートに対して[Excluded]というラベルを付ける必要があります。

1つのポートを共有する2つ以上のVLAN:

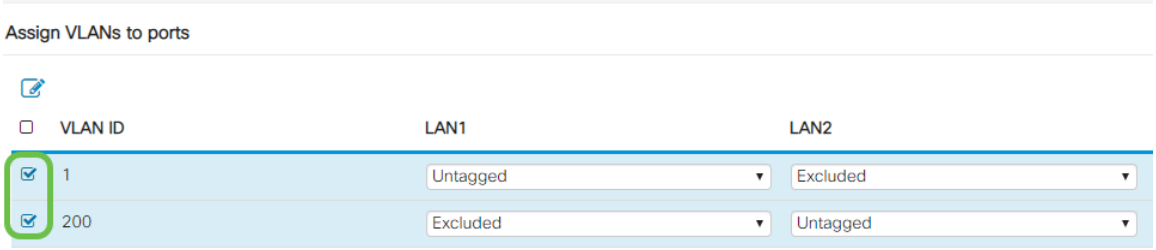
- トランクポートと見なされます。
- いずれかのVLANに[Untagged]というラベルを付けることができます。
- トランクポートの一部である残りのVLANには、[Tagged]というラベルを付ける必要があります。
- トランクポートの一部ではないVLANには、そのポートに対して[Excluded]というラベルを付ける必要があります。

注：この例では、トランクはありません。

手順 9

編集する*VLAN ID*を選択します。[Edit] をクリックします。

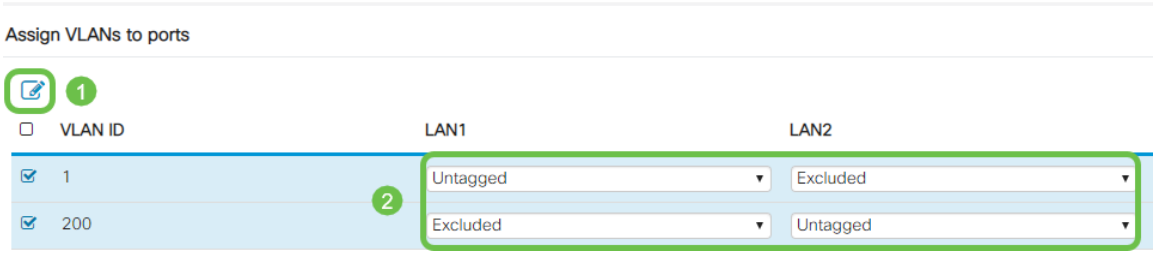
この例では、VLAN 1と*VLAN* 200を*選択*しています。



手順 10

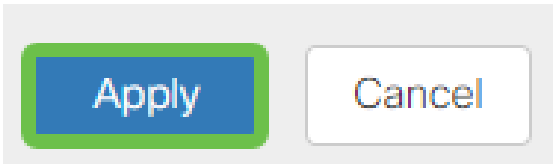
VLANをLANポートに割り当て、[Edit]をクリックし、それぞれの設定を[*Tagged*]、[*Untagged*]、または[*Excluded*]に指定します。

この例では、LAN1でVLAN 1をタグなし、VLAN 200を**除外**として割り当て**ました**。LAN2に対しては、VLAN 1を**Excluded**、VLAN 200を**Untagged**として割り当て**ました**。



手順 11

[**Apply**]をクリックして、設定を保存します。



これで、新しいVLANが正常に作成され、RV260のポートにVLANが設定されました。このプロセスを繰り返して、他のVLANを作成してください。たとえば、VLAN300はサブネット192.168.3.xのマーケティング用に作成され、VLAN400はサブネット192.168.4.xのアカウンティング用に作成されます。

これがVLANの基本です。ハイパーリンクをクリックして、シスコビジネスルータの[VLANベストプラクティスとセキュリティヒントの詳細を確認してください](#)。

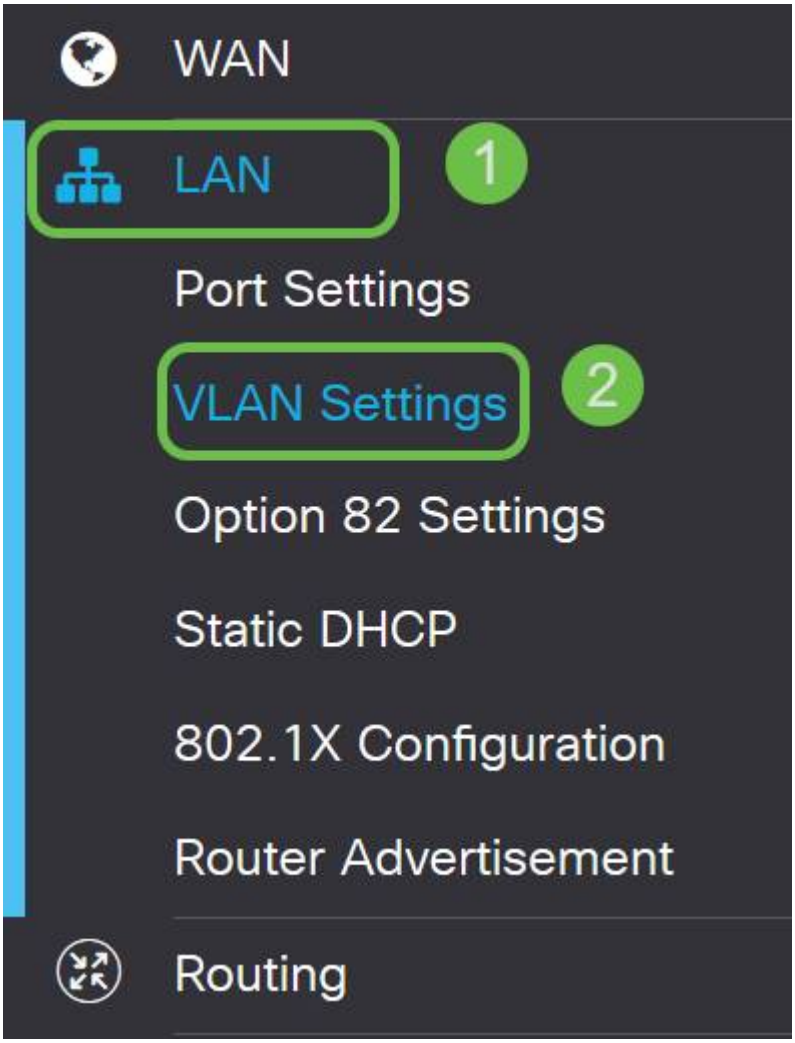
IPアドレスの編集（オプション）

*Initial Setup Wizard*を完了した後、VLAN設定を編集して、ルータにスタティックIPアドレスを設定できます。初期セットアップウィザードの再実行をスキップして、この変更を実行するには、次の手順に従います。

IPアドレスを編集する必要がない場合は、この記事の次のセクション[に移](#)動できます。

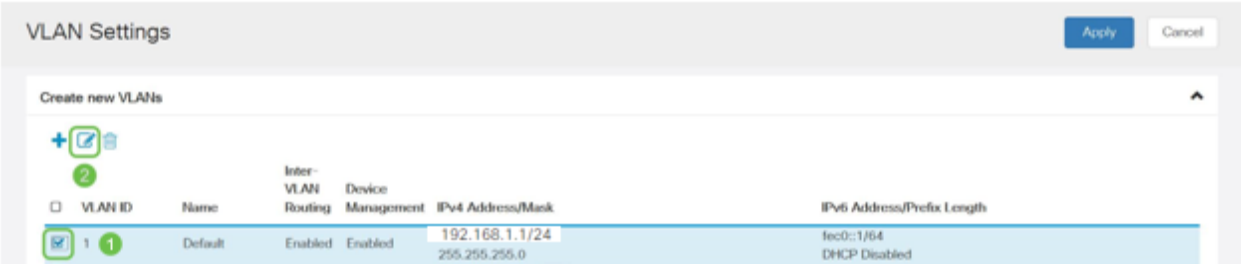
手順 1

左側のメニューバーで、[LAN] > [VLAN Settings]をクリックします。



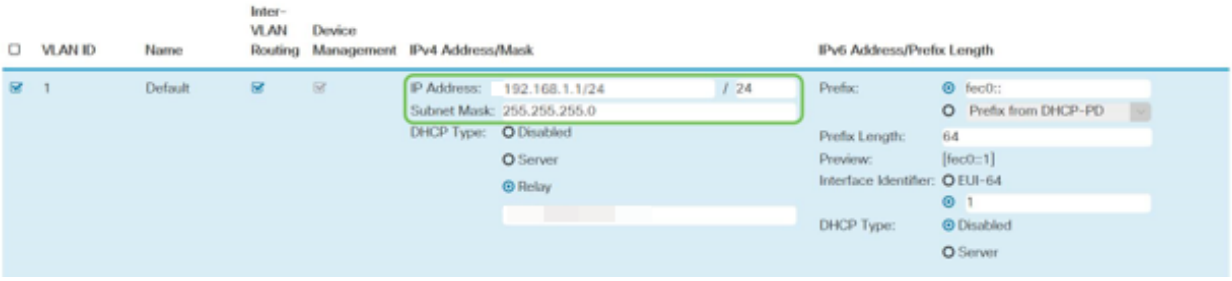
手順 2

次に、ルーティングデバイスを含むVLANを選択し、編集アイコンをクリックします。



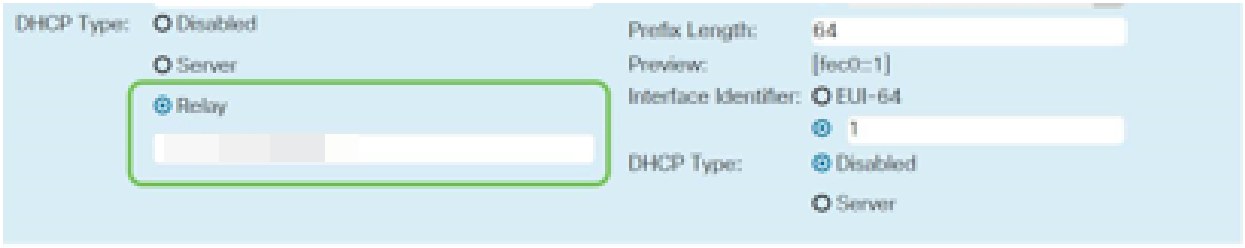
手順 3

目的の静的IPアドレスを入力し、右上隅の[Apply]をクリックします。



手順 4 (オプション)

IPアドレスを割り当てるDHCPサーバ/デバイスがルータでない場合は、DHCPリレー機能を使用してDHCP要求を特定のIPアドレスに転送できます。IPアドレスは、WAN/インターネットに接続されているルータである可能性があります。



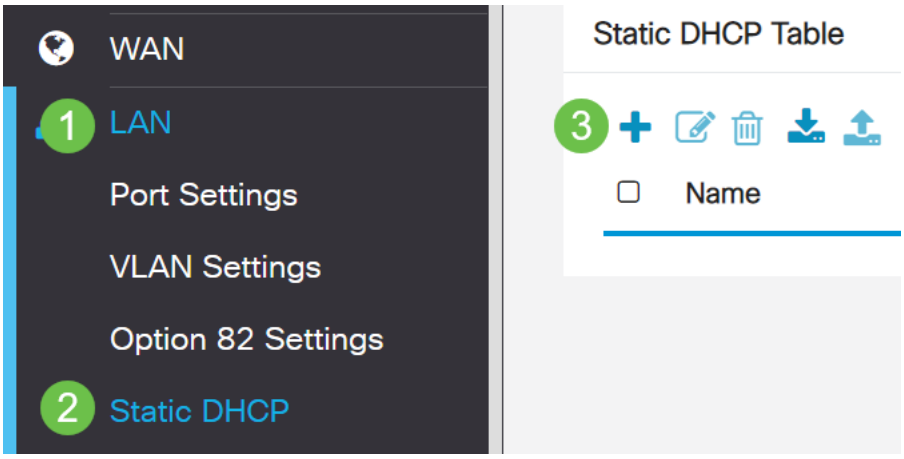
スタティックIPの追加

特定のデバイスを他のVLANに到達可能にする場合は、そのデバイスに静的なローカルIPアドレスを割り当て、アクセス可能にするアクセスルールを作成できます。これは、VLAN間ルーティングが有効になっている場合にのみ機能します。スタティックIPが役立つ場合もあります。スタティックIPアドレスの設定の詳細については、『Cisco Business Hardwareでスタティックアドレスを設定するベストプラクティス』を参照してください。

静的IPアドレスを追加する必要がない場合は、この記事の次のセクションに移ってアクセスポイントを設定できます。

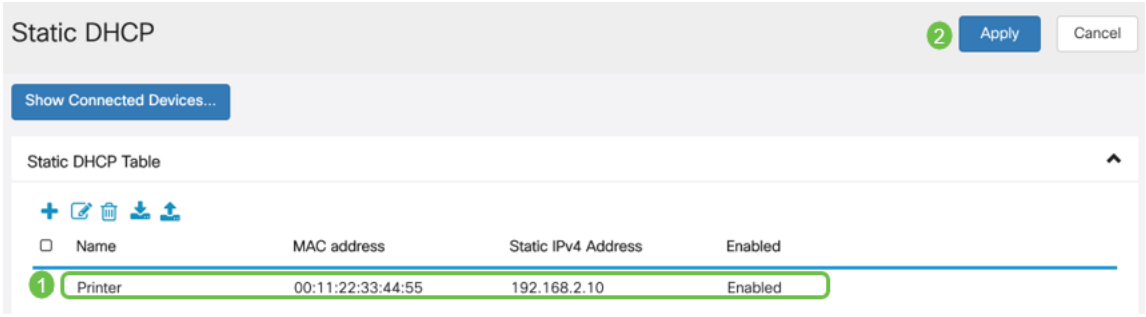
手順 1

[LAN] > [静的DHCP]に移動します。[+]アイコンを**クリックします。**



手順 2

デバイスの**静的DHCP**情報を追加します。この例では、デバイスはプリンタです。



これで、RV260Pルータの設定は完了です。次に、シスコビジネスワイヤレスデバイスを設定します。

CBW140ACの設定

CBW140ACの出荷開始

まず、CBW140ACのPoEポートからRV260PのPoEポートにイーサネットケーブルを接続します。RV260Pの最初の4つのポートはPoEを供給できるため、どれでも使用できます。

インジケータライトのステータスを確認します。アクセスポイントの起動には約10分かかります。LEDは複数のパターンで緑色に点滅し、緑、赤、オレンジが急速に交互に繰り返された後、再び緑色に変わります。LEDの色の強さと色相は、ユニットごとに小さな変化があります。LEDライトが緑色に点滅している場合は、次の手順に進みます。

プライマリAPのPoEイーサネットアップリンクポートは、LANへのアップリンクを提供するためだけに使用でき、他のプライマリ対応またはメッシュエクステンダデバイスには接続できません。

新しいアクセスポイントがない場合は、Wi-Fiオプションに表示されるように、*CiscoBusiness-Setup SSIDの工場出荷時のデフォルト設定にリセットされていることを確認*してください。この問題に関する詳細は、『RV260ルータのリブートと工場出荷時のデフォルト設定へのリセット方法』を参照してください。

Web UIでの140ACプライマリワイヤレスアクセスポイントのセットアップ

アクセスポイントは、モバイルアプリケーションまたはWeb UIを使用して設定できます。この記事では、セットアップ用にWeb UIを使用しています。これにより、設定のオプションが増えますが、もう少し複雑になります。次のセクションでモバイルアプリケーションを使用する場合は、をクリックしてモバイルアプリケーションの手順にアクセスします。

接続に問題がある場合は、この記事の「ワイヤレスのトラブルシューティングに関するヒント」セクションを参照してください。

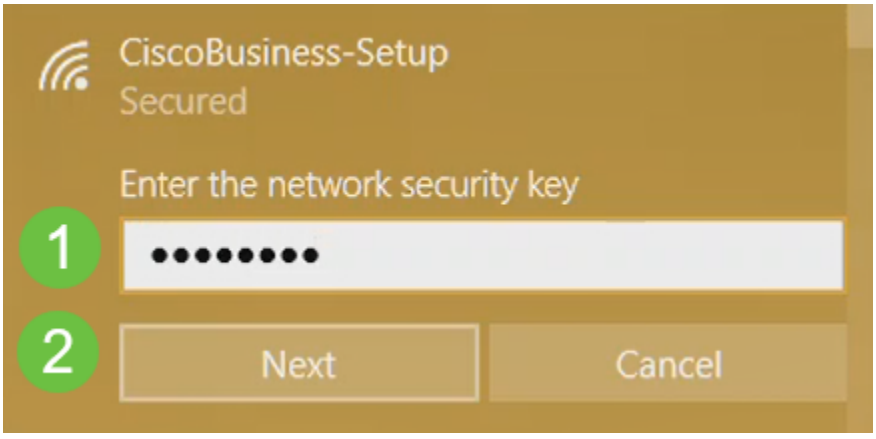
手順 1

PCで[Wi-Fi]アイコンをクリックし、**[CiscoBusiness-Setup** wireless network]*を選択*します。[Connect] をクリックします。

新しいアクセスポイントがない場合は、Wi-Fiオプションに表示されるように、*CiscoBusiness-Setup SSIDの工場出荷時のデフォルト設定にリセットされていることを確認してください。*

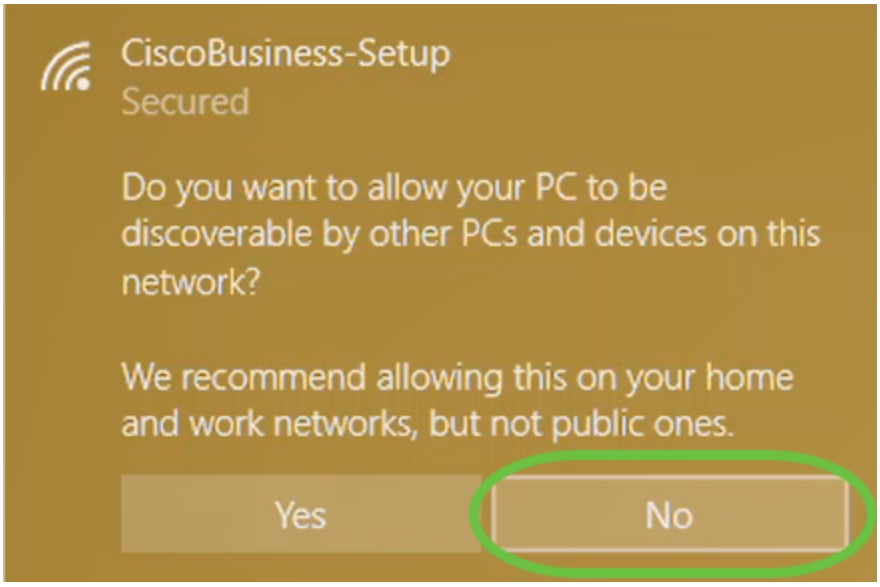
手順 2

パスフレーズ**cisco**123を入力し、[**Next**]をクリックします。



手順 3

次の画面が表示されます。一度に設定できるデバイスは1つだけなので、[いいえ]をクリックします。



CiscoBusiness-Setup SSIDに接続できるデバイスは*1つだけ*でする。2番目のデバイスが接続しようとすると、接続できません。SSIDに接続できず、パスワードを確認した場合、他のデバイスが接続している可能性があります。APを再起動し、再試行します。

手順 4

接続されると、WebブラウザがCBW APセットアップウィザードに自動的にリダイレクトされます。そうでない場合は、Internet Explorer、Firefox、Chrome、SafariなどのWebブラウザを開きます。アドレスバーに「http://ciscobusiness.cisco」と入力し、Enterキーを押します。Webページで[開始]をクリックします。

Webページが表示されない場合は、数分待つか、ページをリロードします。この初期設定の後、https://ciscobusiness.ciscoを使用してログインします。Webブラウザに *http://*が自動的に入力される場合は、アクセスを取得するために手動で *https://*を入力する必要があります。

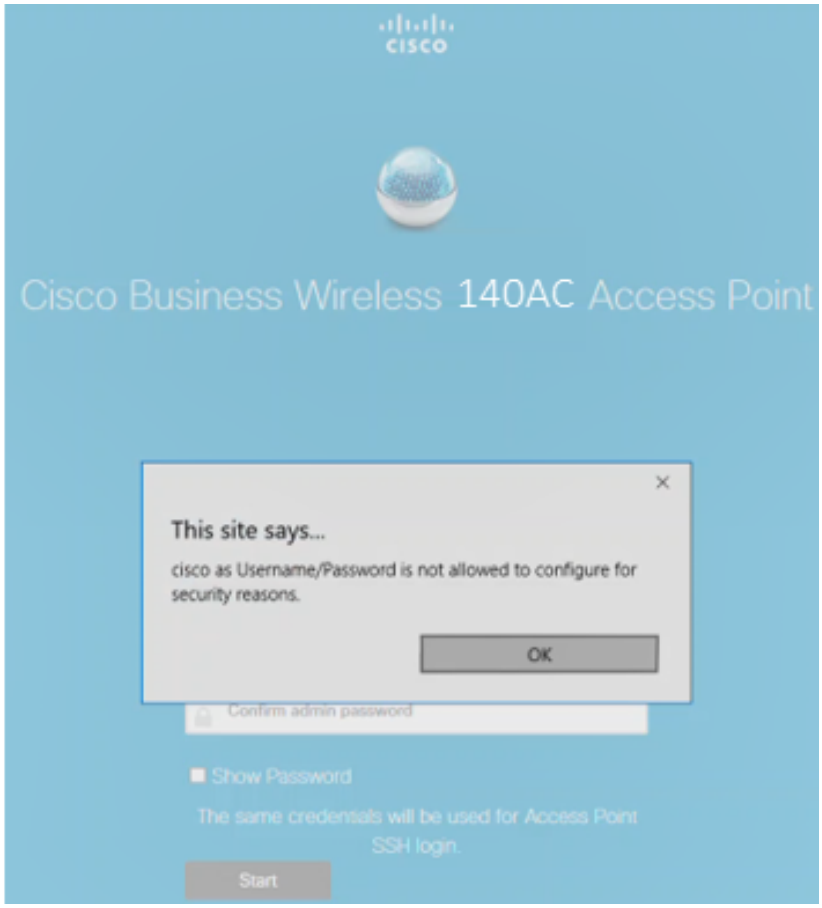
手順 5

次のように入力して*管理アカウント*を作成します。

- 管理者ユーザ名（最大24文字）
- Admin Password
- 管理者パスワードの確認

[パスワードの表示]の横のチェックボックスをオンにして、パスワードを表示することもできます。[Start（スタート）] をクリックします。

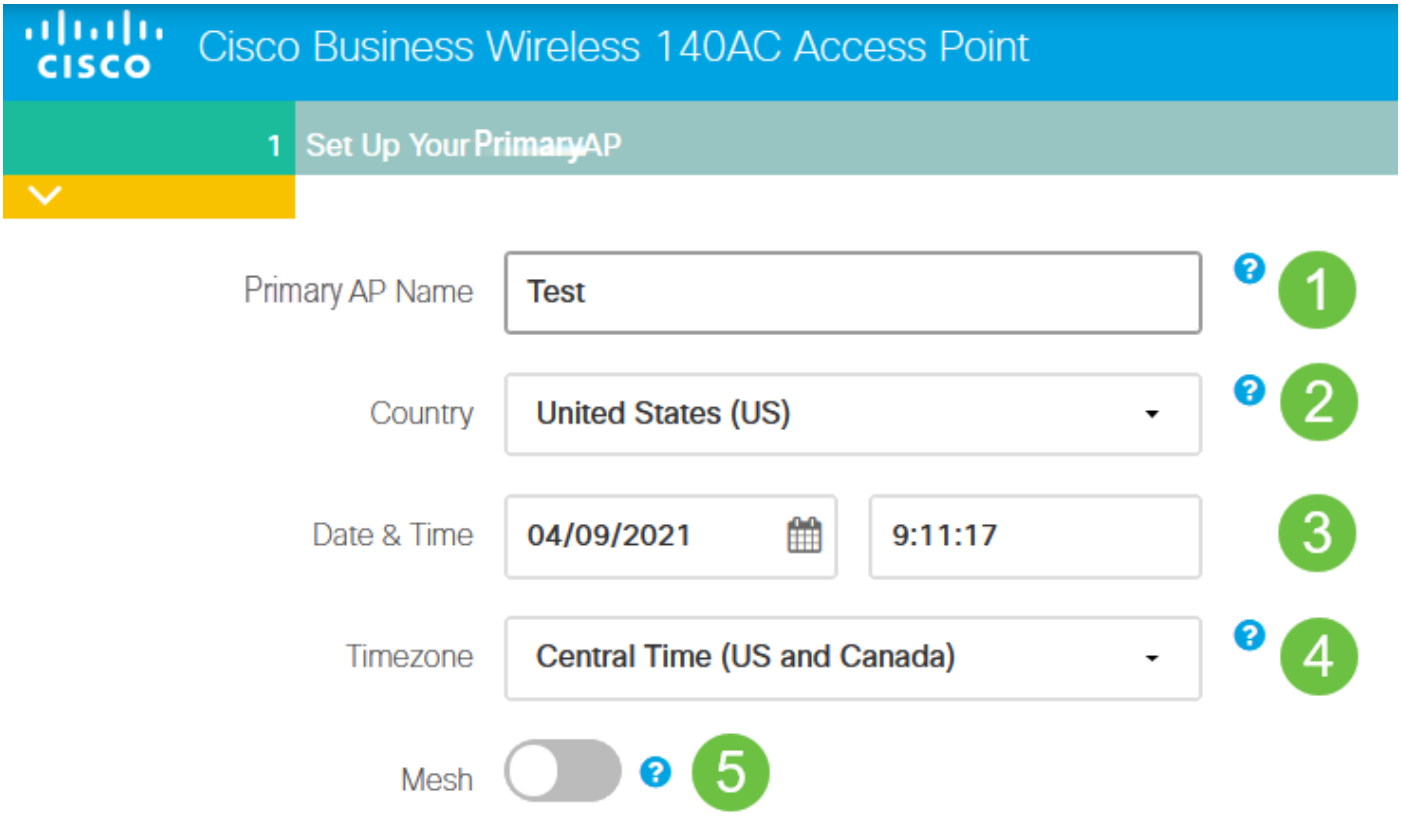
ユーザ名またはパスワード*のフィールド*に*cisco*、またはそのバリエーションを使用しないでください。これを行うと、次のようなエラーメッセージが表示されます。



手順 6

次のように入力して、プライマリAPを設定します。

- プライマリAP名
- Country
- 日時
- TimeZone
- メッシュ



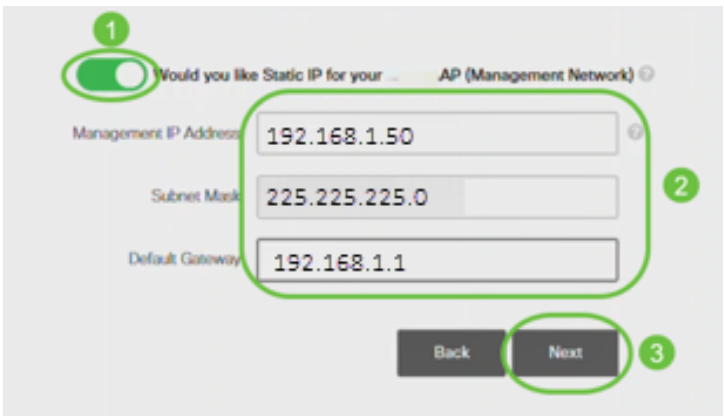
メッシュネットワークを作成する場合にのみ、メッシュを有効にする必要があります。デフォルトでは、無効になっています。

ステップ7

（オプション）管理目的で*CBW140ACの静的*IPを有効にできます。そうでない場合、インターフェイスはDHCPサーバからIPアドレスを取得します。スタティックIPを設定するには、次のように入力します。

- 管理IPアドレス
- サブネット マスク
- [Default Gateway]

[next] をクリックします。



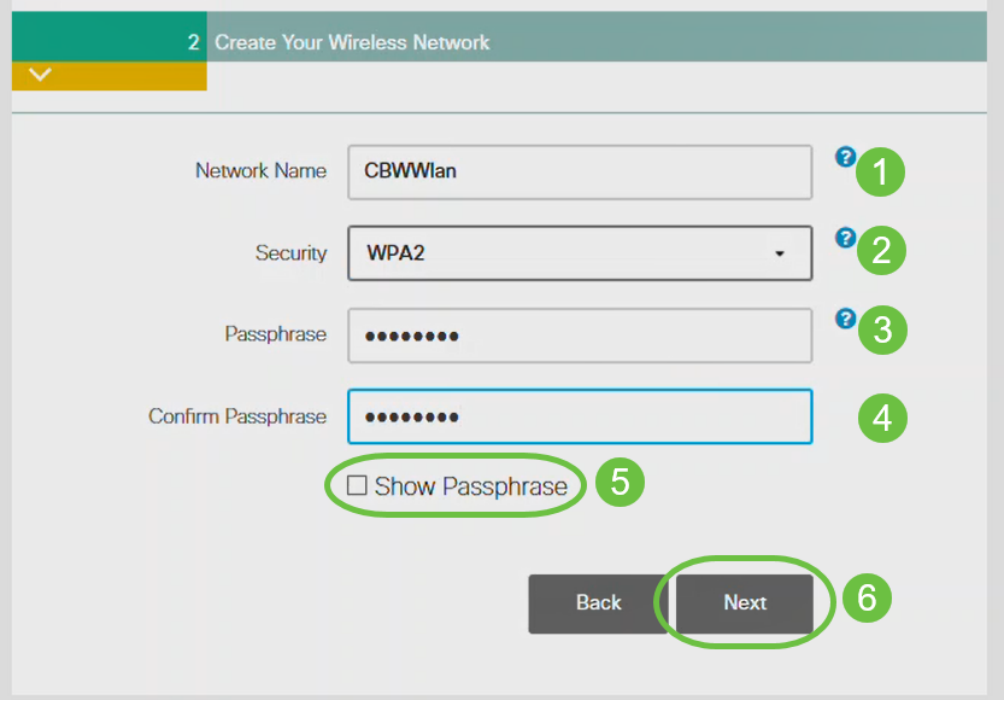
デフォルトでは、このオプションは無効になっています。

手順 8

次のコマンドを入力して、ワイヤレスネットワークを作成します。

- ネットワーク名
- セキュリティの選択
- パスフレーズ
- パスフレーズの確認
- （オプション）[Show Passphrase]チェックボックスをオンにします。

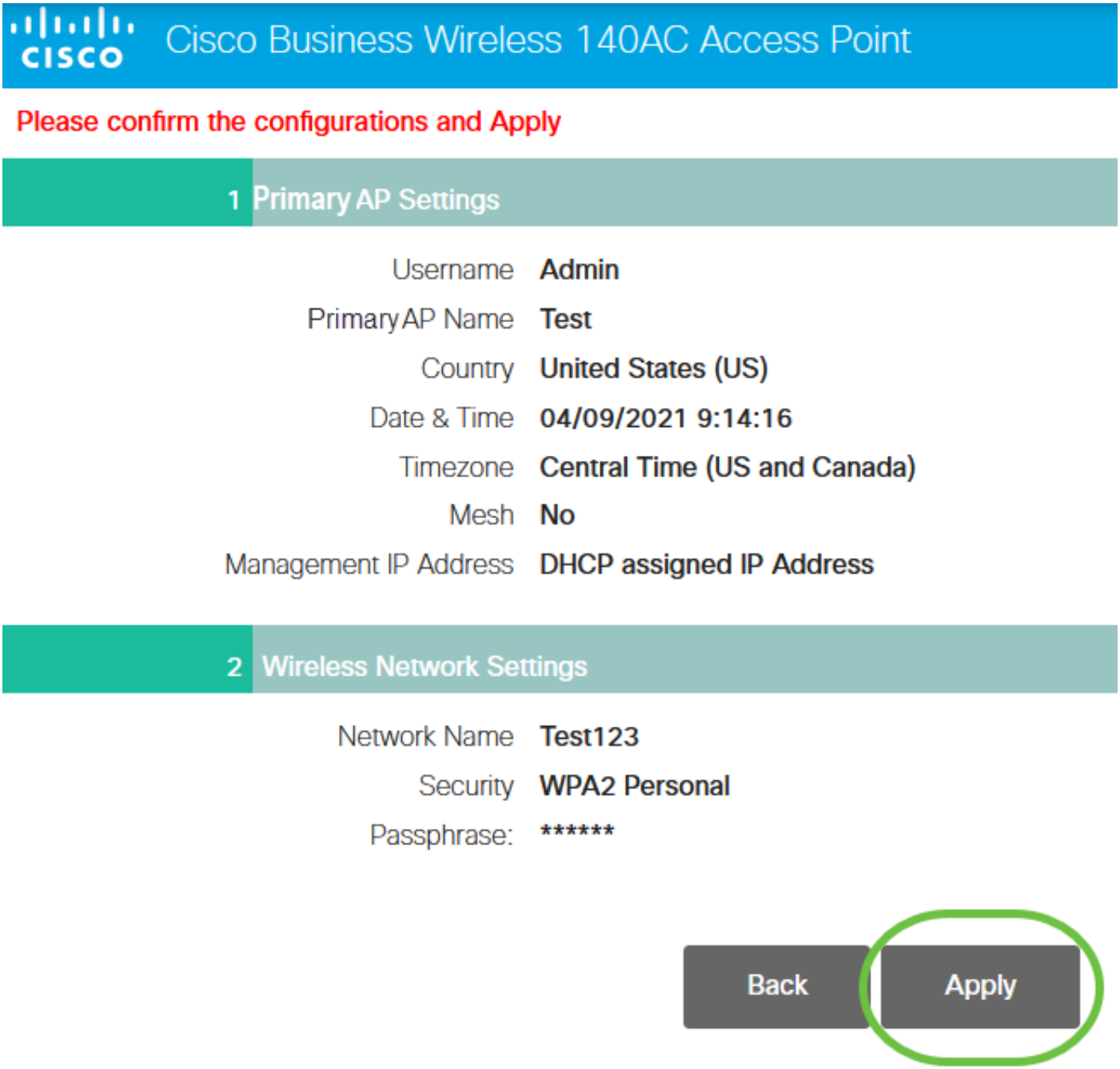
[next] をクリックします。



Wi-Fi protected Access(WPA)バージョン2(WPA2)は、Wi-Fiセキュリティの現在の標準です。

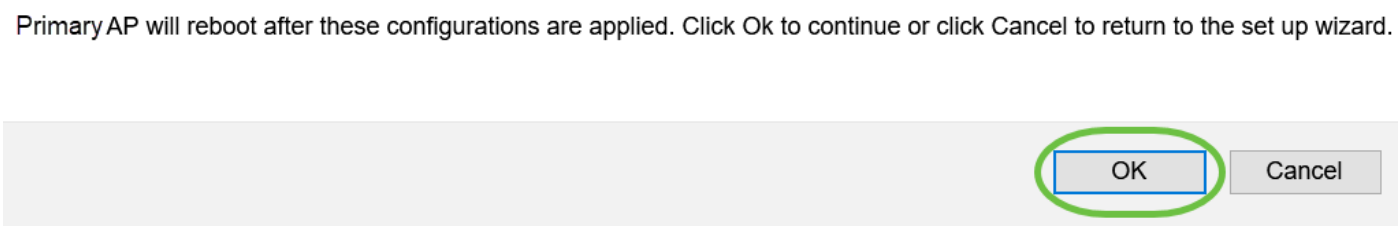
手順 9

設定を確認し、[適用]をクリックします。

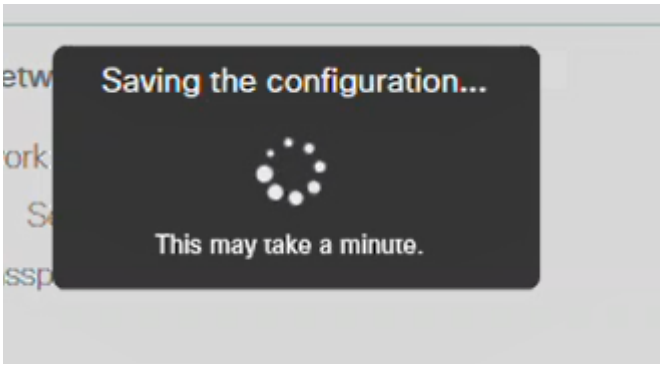


手順 10

[OK]をクリックして、設定を適用します。



次の画面が表示され、設定が保存され、システムがリブートされます。これには10分かかることがあります。

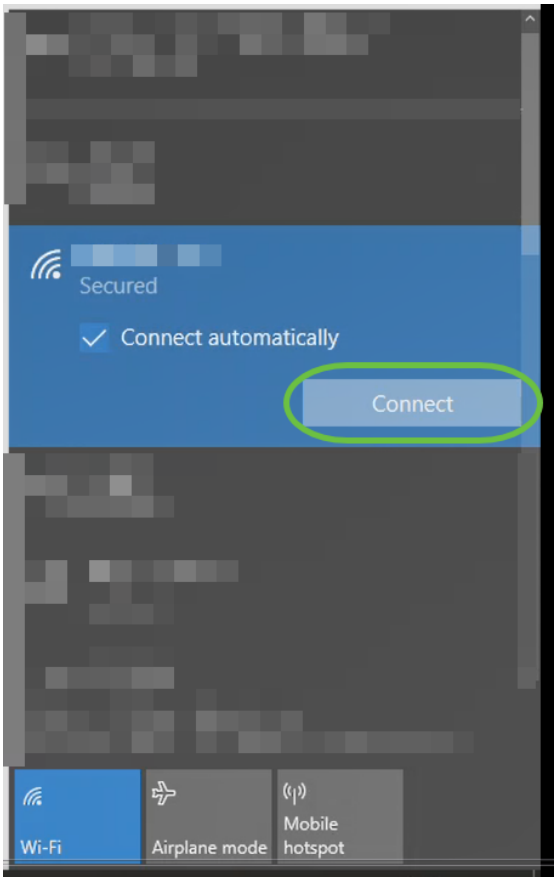


リブート中、アクセスポイントのLEDは複数のカラーパターンを通過します。LEDがグリーンに点滅している場合は、次の手順に進みます。LEDが赤い点滅パターンを超えない場合は、ネットワークにDHCPサーバがないことを示します。APがDHCPサーバを備えたスイッチまたはルータに接続されていることを確認します。

手順 11

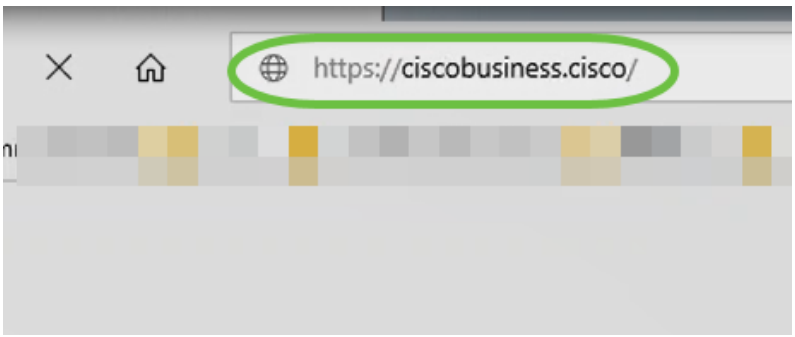
PCのワイヤレスオプションに移動し、設定したネットワークを選択します。[Connect] をクリックします。

CiscoBusiness-Setup SSIDは、リブート後に表示されなくなります。



ステップ 12

Webブラウザを開き、*https://[CBW APのIPアドレス]*を入力します。または、アドレスバーに*https://ciscobusiness.cisco*と入力し、Enterキーを押します。



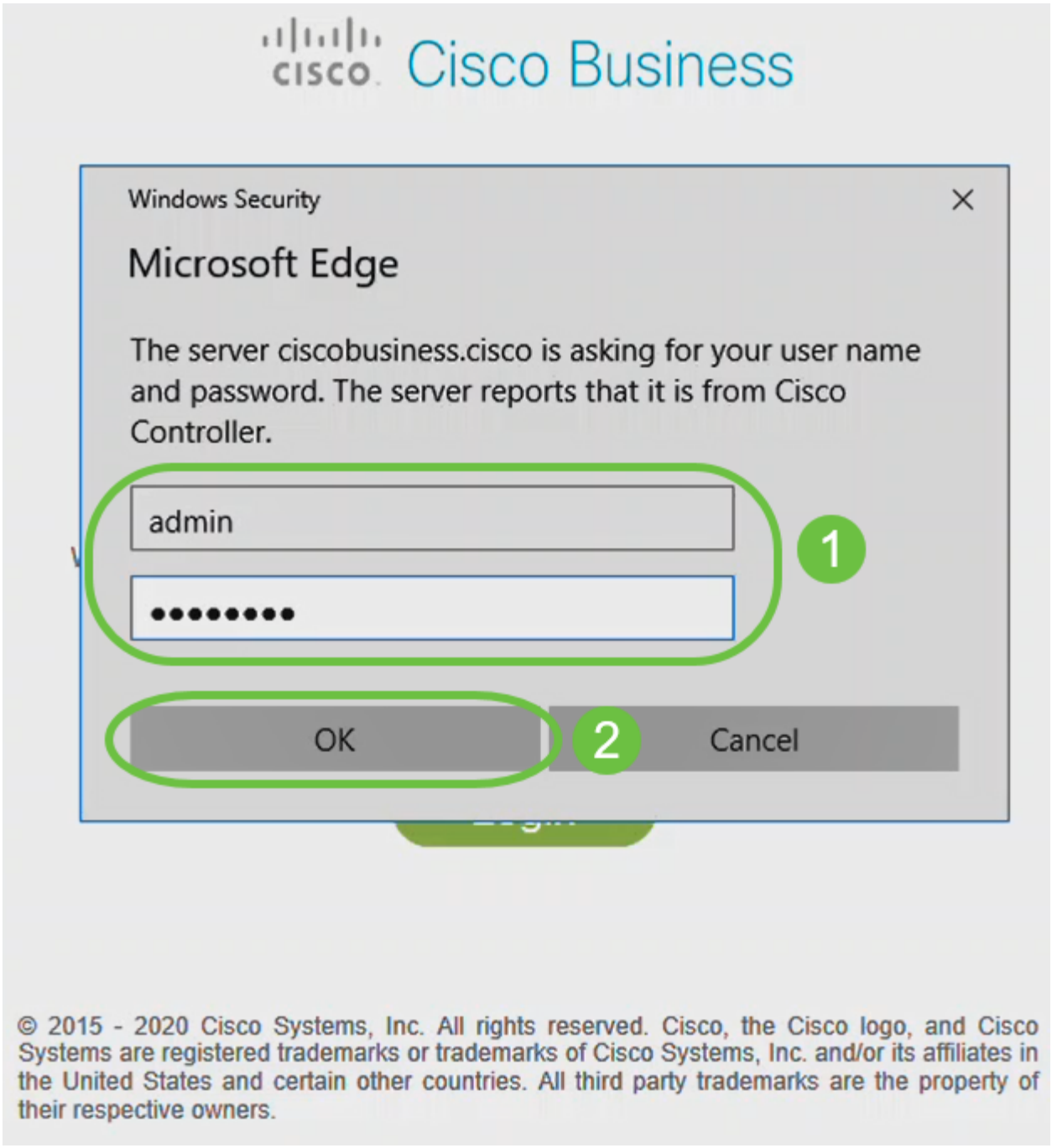
この手順では、httpではなく *https*を入力する ことを確認してください。

手順 13

[Login] をクリックする。

ステップ 14

設定したクレデンシャルを使用してログインします。[OK] をクリックします。



ステップ 15

APのWeb UIページにアクセスできます。

ワイヤレスのトラブルシューティングのヒント

問題がある場合は、次のヒントを確認してください。

- 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。
- モバイルアプリまたはラップトップの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もあります。このVPNは知らない可能性もあります。たとえば、サービスプロバイダーとしてGoogle Fiを使用するAndroid(Pixel 3)電話機には、通知なしで自動接続するVPNが内蔵されています。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。
- プライマリAPにhttps://<プライマリAPのIPアドレス>でログインします。
- 初期設定を行ったら、*ciscobusiness.cisco*にログインするか、WebブラウザにIP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、コンピュータにhttp://が自動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ファイルです。
- APの使用中にWeb UIにアクセスしたり、ブラウザの問題に関する問題を解決するには、Webブラウザ（この場合はFirefox）で[Open]メニューをクリックし、[Help] > [Troubleshooting Information]に移動して[Refresh Firefox]をクリックします。

Web UIを使用したCBW142ACMメッシュエクステンダの設定

このネットワークをセットアップするホームストレッチでは、メッシュエクステンダを追加するだけです。

手順 1

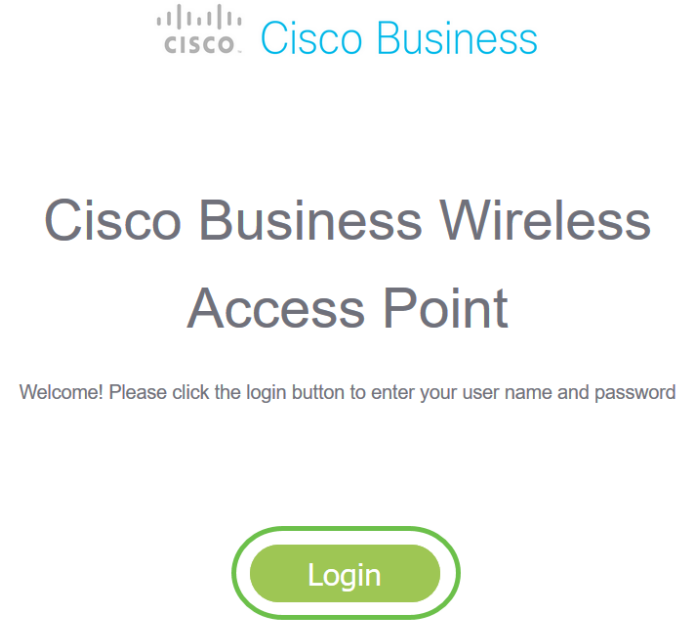
2つのメッシュエクステンダを、選択した位置の壁に差し込みます。各メッシュエクステンダのMACアドレスを書き留めます。

手順 2

メッシュエクステンダが起動するまで約10分待ちます。

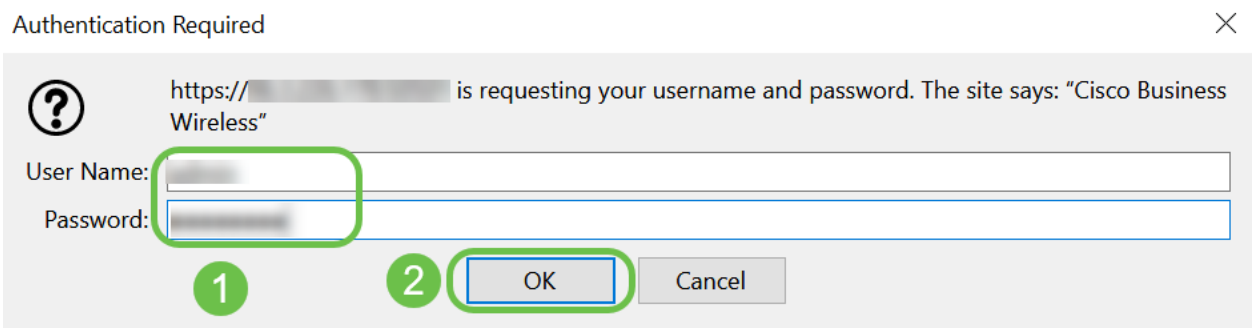
手順 3

Webブラウザでプライマリアクセスポイント(AP)のIPアドレスを入力します。[**Login**]をクリックして、プライマリAPにアクセスします。



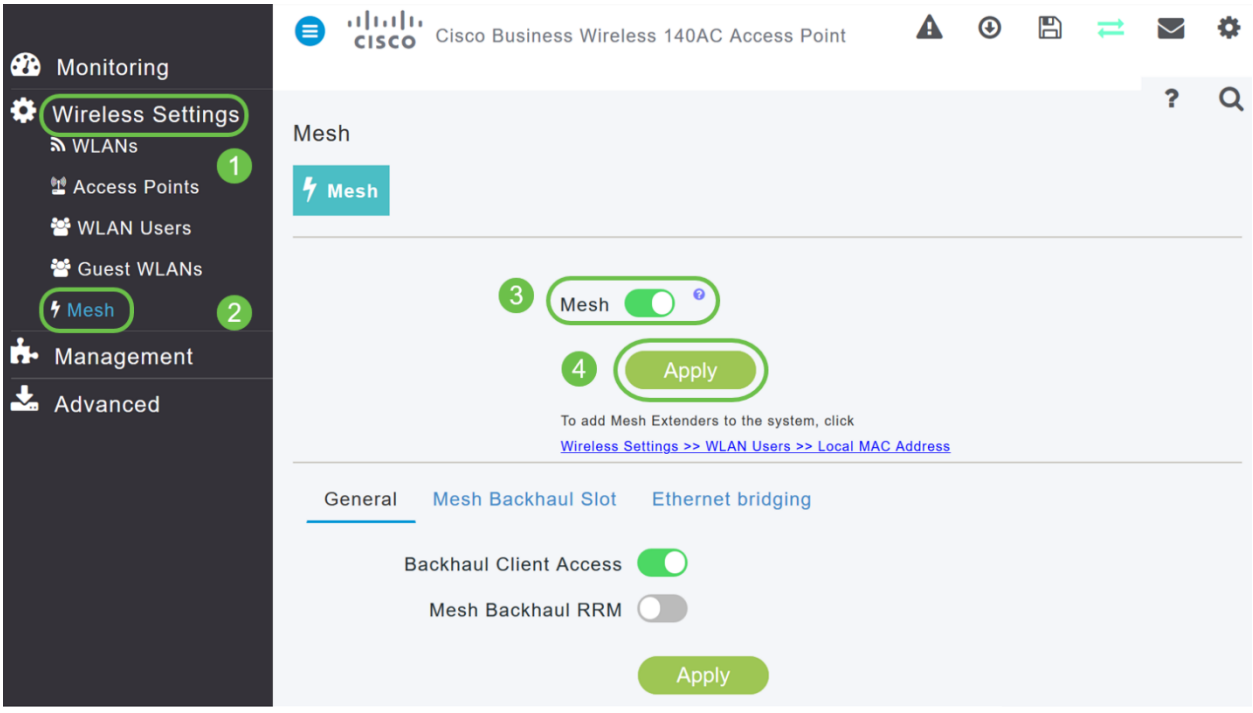
手順 4

プライマリAPにアクセスするために、ユーザ名とパスワードのクレデンシャルを入力します。[OK] をクリックします。



手順 5

[ワイヤレス設定] > **[メッシュ]に移動します**。メッシュが有効になっていることを確認してください。[Apply] をクリックします。

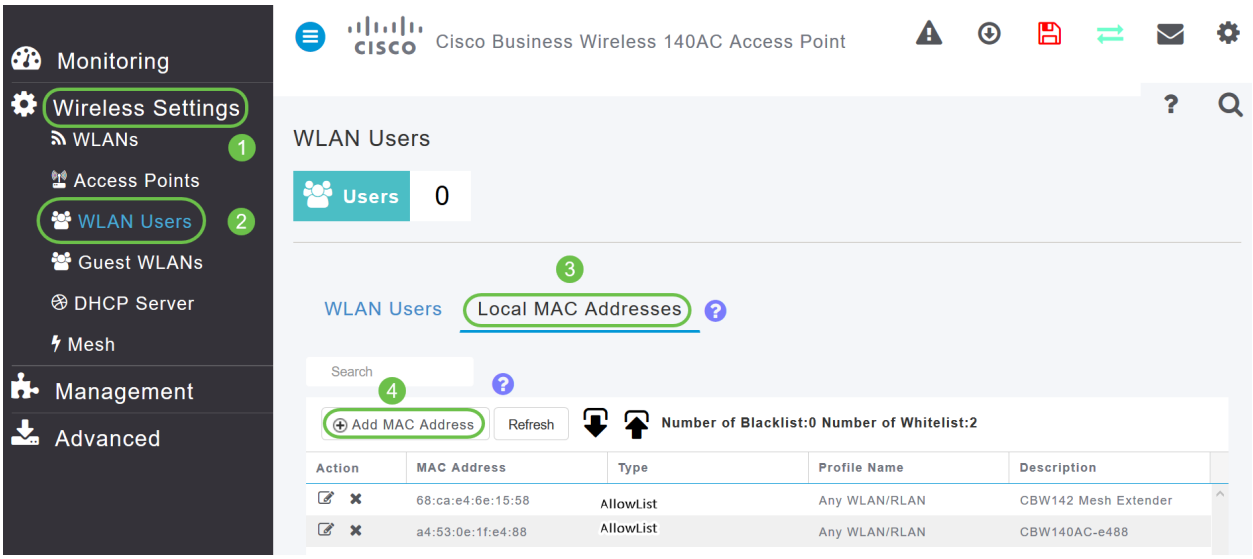


手順 6

メッシュが有効になっていない場合、WAPはリブートを実行する必要があります。ポップアップが表示され、リブートが行われます。confirm を発行した後に表示されます。これには約10分かかります。リブート中、LEDは複数のパターンで緑色に点滅し、緑、赤、オレンジの間で急速に交互に点灯してから、再び緑色に変わります。LEDの色の強さと色相は、ユニットごとに小さな変化があります。

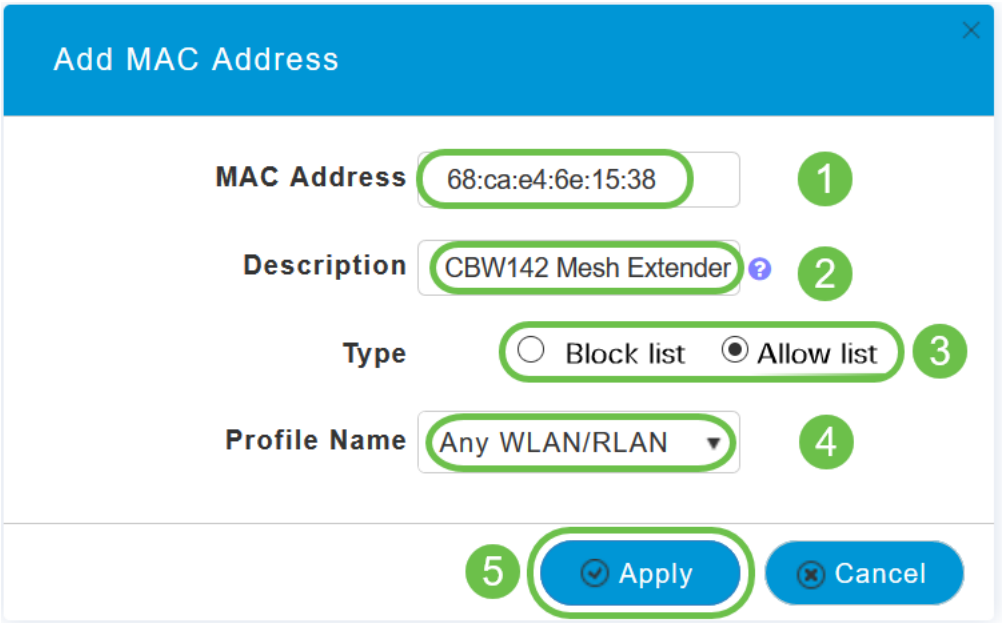
ステップ7

[Wireless Settings] > [WLAN Users] > [Local MAC Addresses]に移動します。[Add MAC Address]をクリックします。



手順 8

メッシュエクステンダのMACアドレスと説明を入力します。「タイプ」を「許可」リストとして選択します。ドロップダウンメニューから[プロファイル名]を選択します。[Apply] をクリックします。



手順 9

画面の右上のペインにある保存アイコンを押して、**すべての**設定を保存してください。

各メッシュエクステンダについて繰り返します。

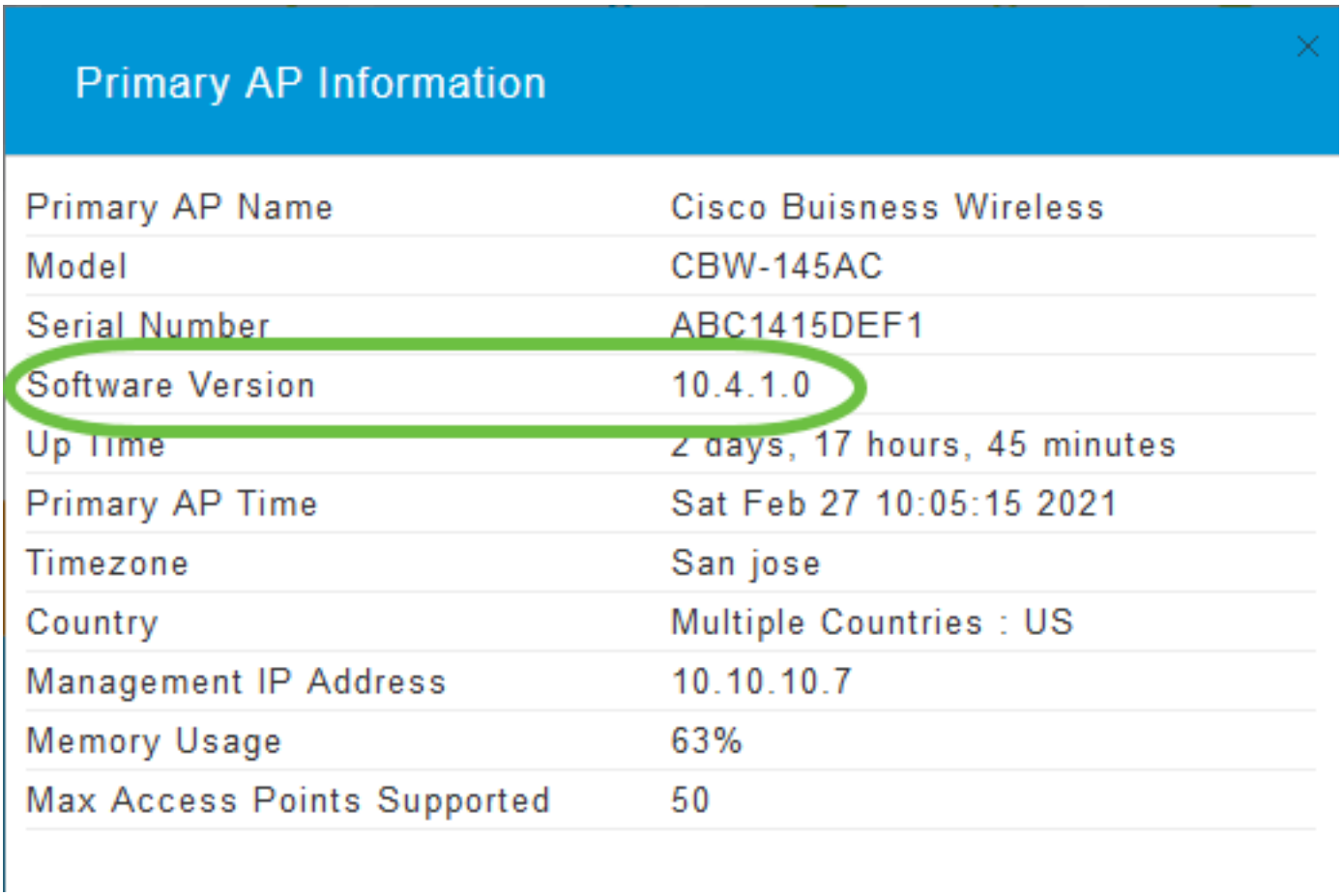
Web UIを使用したソフトウェアの確認と更新

この重要なステップを飛ばすな！ソフトウェアを更新する方法はいくつかありますが、Web UIを使用する場合に最も簡単に実行するには、次の手順を使用することをお勧めします。

プライマリAPの現在のソフトウェアバージョンを表示および更新するには、次の手順を実行します。

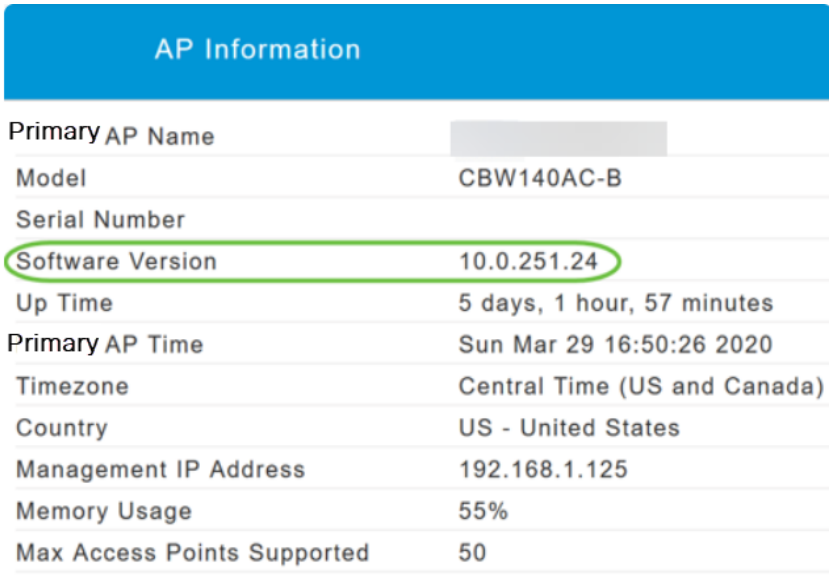
手順 1

Webインター**フェイスの**右上隅にある歯車アイコンをクリックし、[Primary AP Information]をクリ**ックします**。



手順 2

実行しているバージョンを最新のソフトウェアバージョンと比較します。ソフトウェアを更新する必要があるかどうかを確認したら、ウィンドウを閉じます。

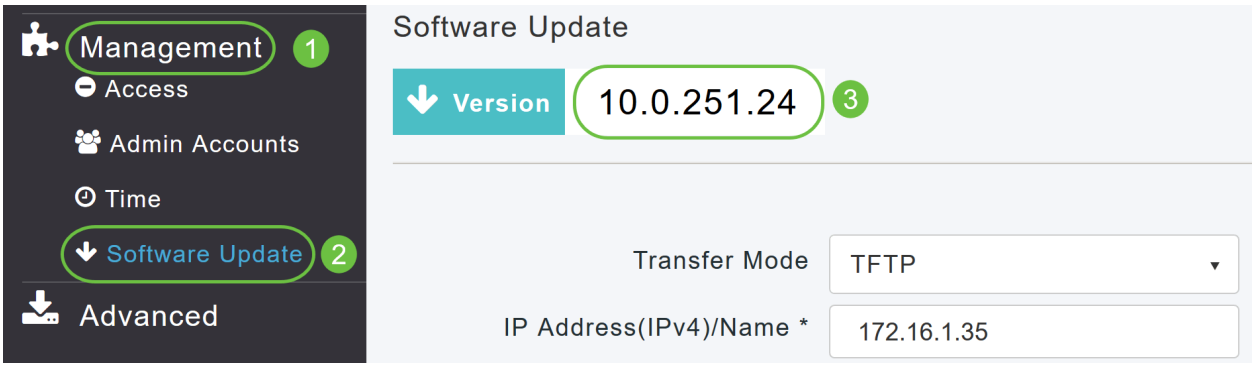


ソフトウェアの最新バージョンを実行している場合は、「WLANの作成」セクションに移動できます。

手順 3

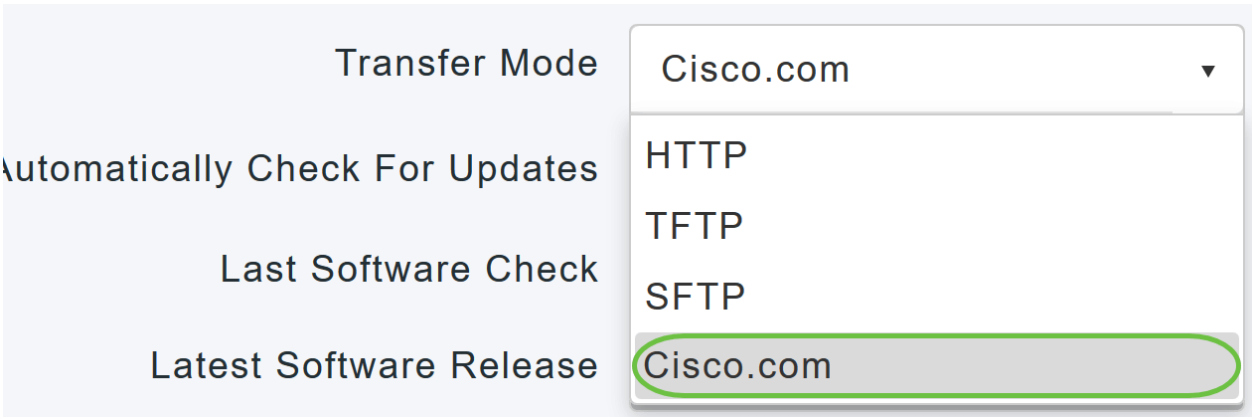
メニューから**[Management] > [Software Update]**を選択します。

[ソフトウェアの更新]ウィンドウが表示され、一番上に現在のソフトウェアバージョン番号が表示されます。



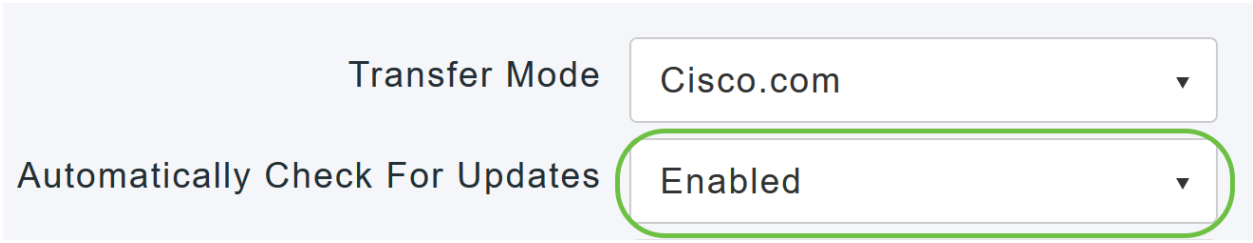
CBW APソフトウェアを更新できます。プライマリAPの現在の設定は削除されません。

[転送モード*(Transfer Mode)*]ドロップダウンリストから、**[Cisco.com]を選択します。**



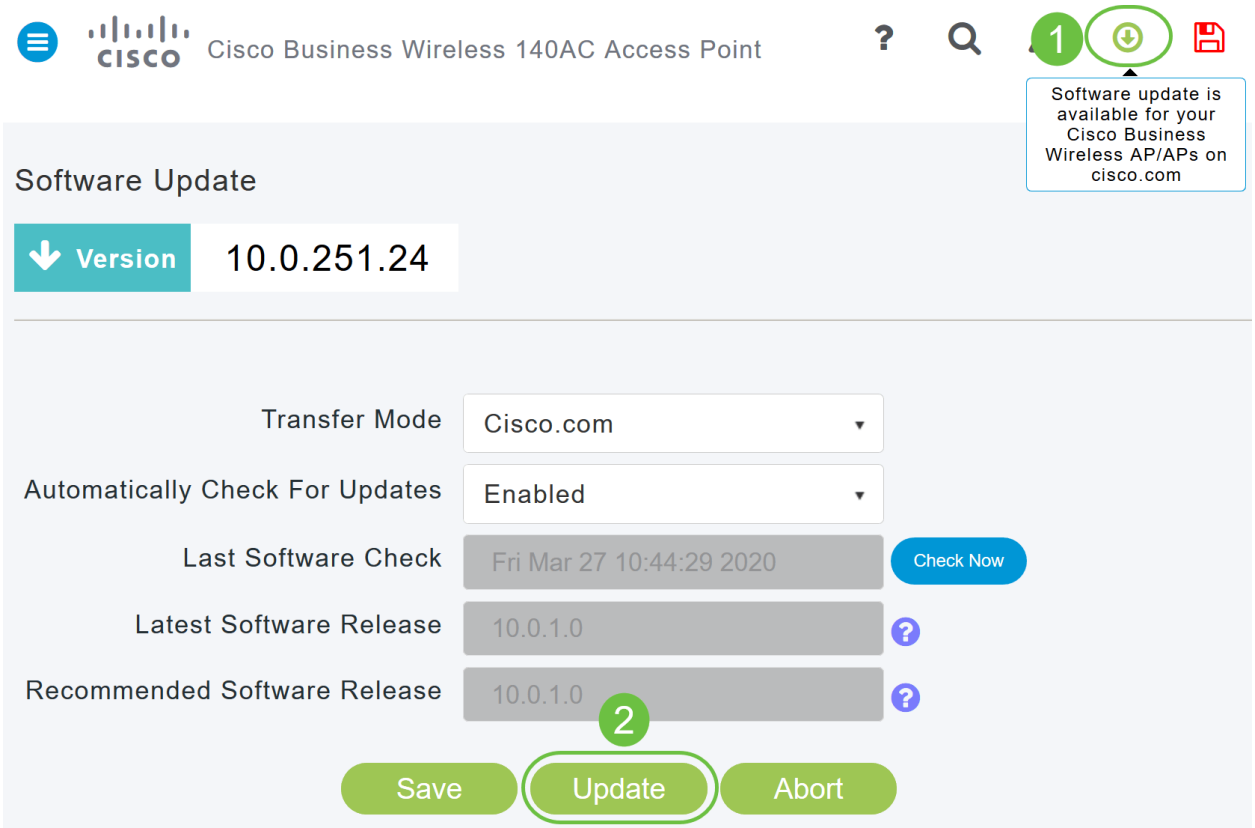
手順 4

ソフトウェアの更新を自動的に確認するようにプライマリAPを設定するには、[更新を自動的に確認(*Automatically Check for Updates)]*ドロップダウンリストで[有効(*Enabled)]*を選択します。このコマンドはデフォルトで有効になっています。



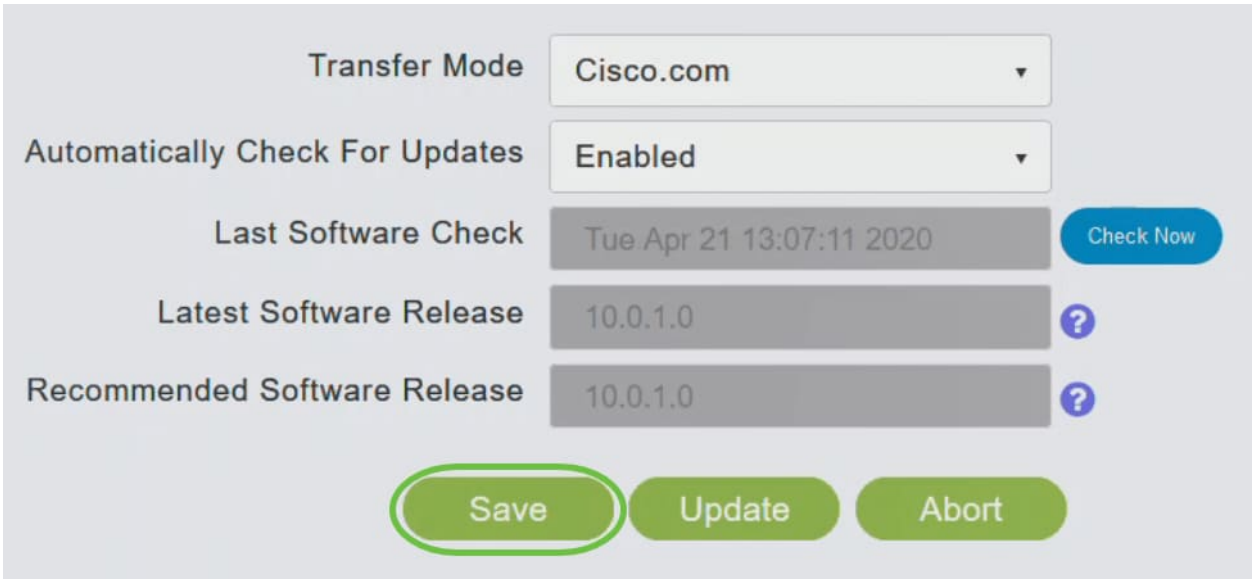
ソフトウェアチェックが完了し、Cisco.comで最新または推奨のソフトウェアアップデートが利用可能な場合は、次の手順を実行します。

- Web UIの**右上隅にある[ソフトウェア**更新アラート(Software Update Alert)]アイコンは、緑色（またはグレー）になります。 アイコンをクリックすると、[Software Update]ページが表示されます。
- [ソフトウェアの更新]ページの下部にある[*更新]*ボタンが有効になっています。

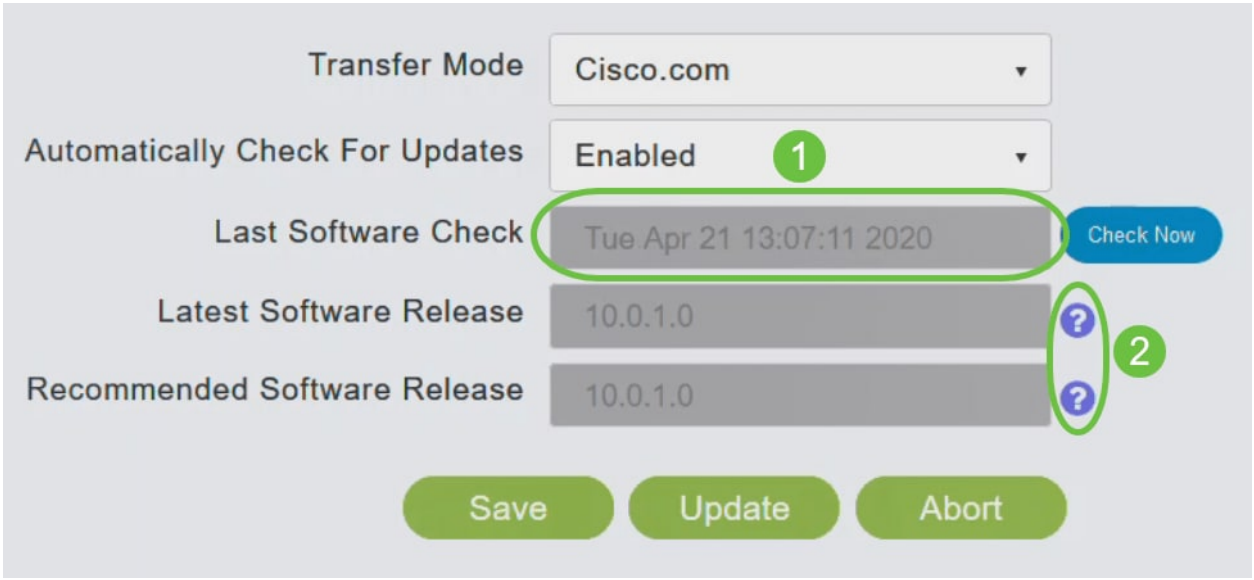


手順 5

[Save] をクリックします。これにより、転送モードと更新の自動チェックの両方で行ったエントリまたは変更が保存されます。

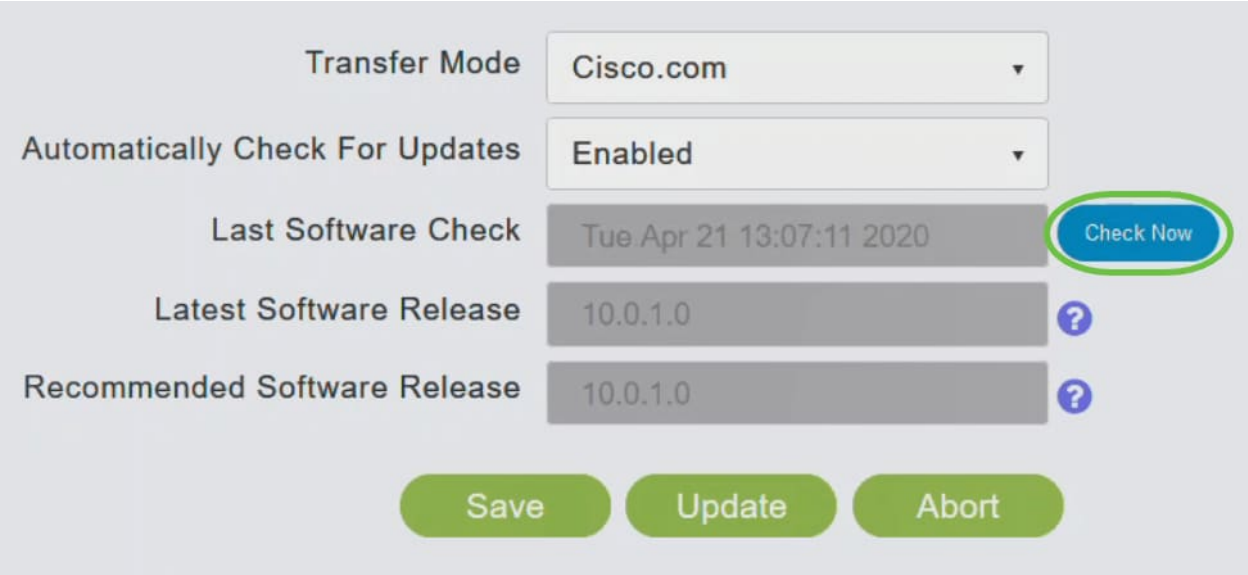


[最後のソフトウェアチェック]フィールドには、最後の自動または手動ソフトウェアチェックのタイムスタンプが表示されます。表示されたリリースの注記は、横にある疑問符アイコンをクリックすると表示できます。



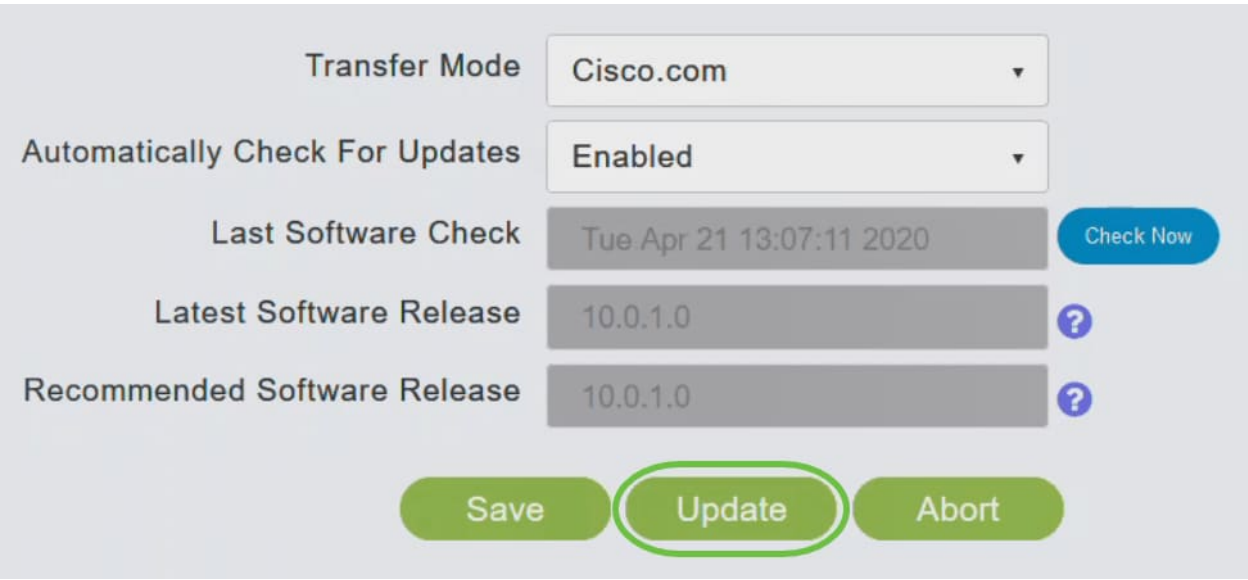
手順 6

[今すぐチェック]をクリックすると、ソフトウェアチェックをいつでも手動で実行できます。



ステップ7

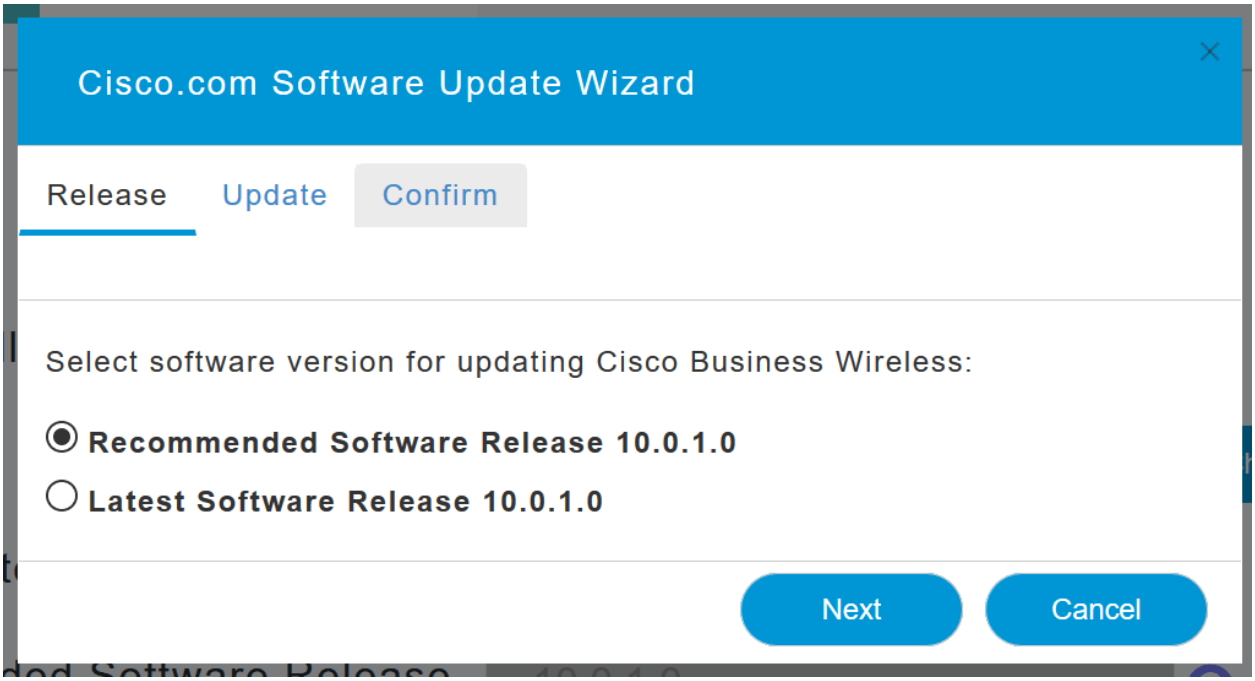
ソフトウェアの更新を続行するには、[更新]をクリックします。



[ソフトウェア*更新ウィザード*]が表示されます。このウィザードでは、次の3つのタブを順に選択できます。

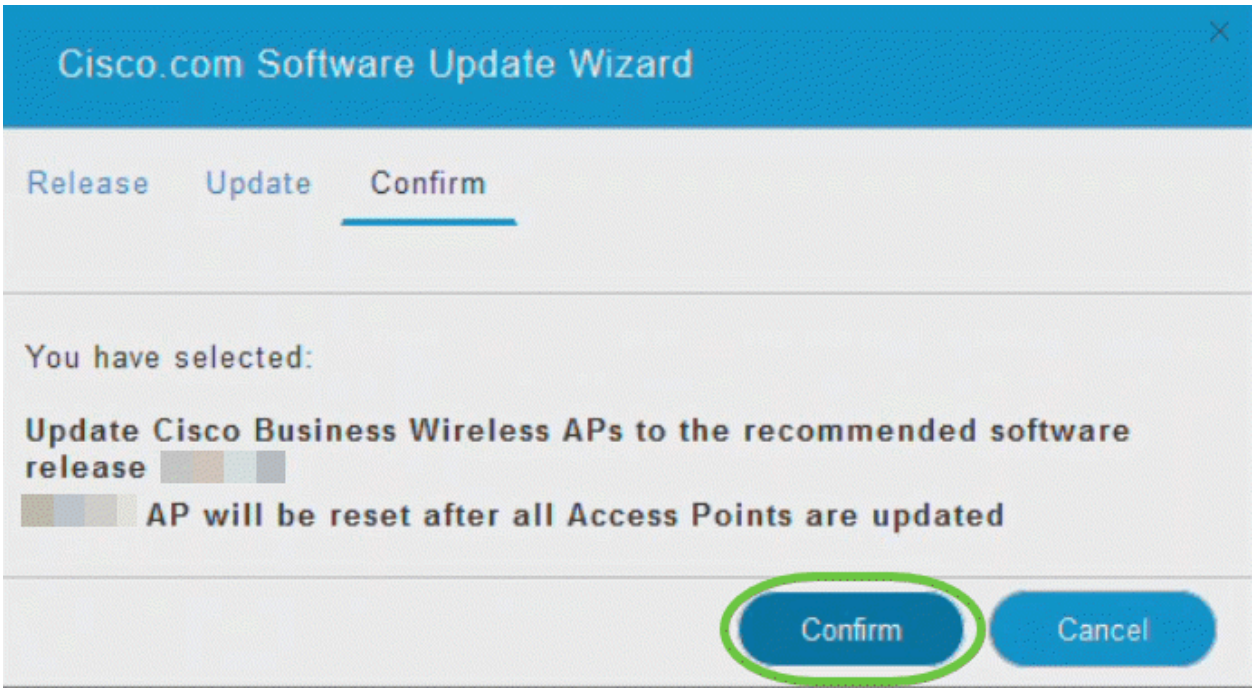
- [リリース(Release)]タブ：推奨ソフトウェアリリースまたは最新ソフトウェアリリースのどちらにアップデートするかを指定します。
- [Update]タブ：APをいつリセットするかを指定します。すぐに実行するか、後でスケジュールするかを選択できます。イメージのプレダウンロードが完了した後にプライマリAPが自動的にリブートするように設定するには、[Auto Restart]チェックボックスをオンにします。
- [Confirm]タブ：選択内容を確認します。

ウィザードの指示に従います。[確認]をクリックする前に、いつでも任意のタブに戻ることができます。



手順 8

[確認]をクリックします。

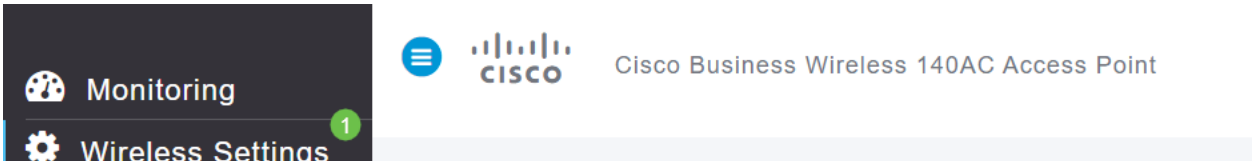


Web UIでのWLANの作成

このセクションでは、ワイヤレスローカルエリアネットワーク(WLAN)を作成できます。

手順 1

WLANを作成するには、[Wireless Settings] > [**WLANs**]に移動します。次に、[**Add new WLAN/RLAN**]を選択します。



手順 2

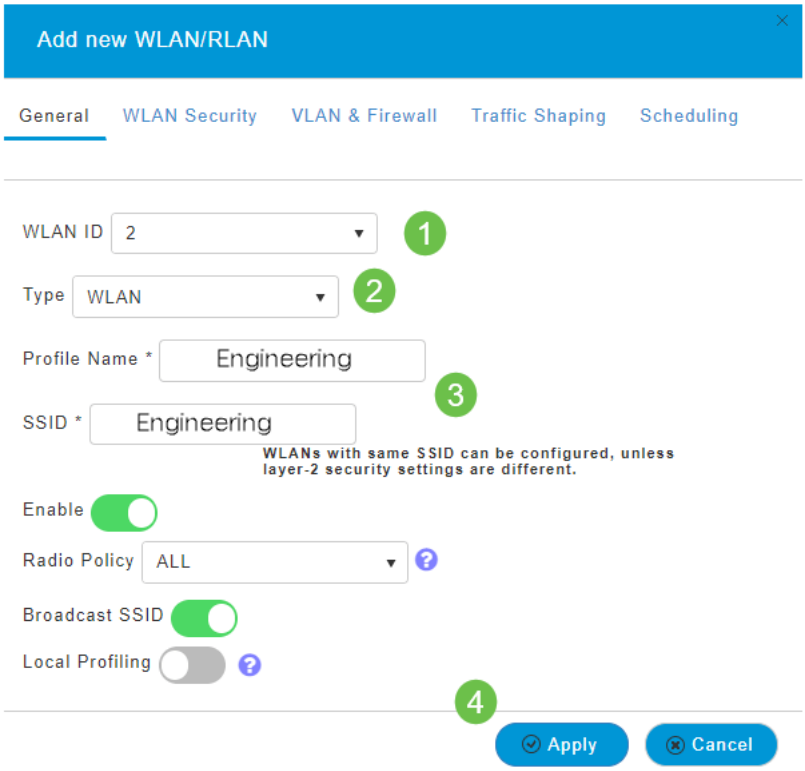
[全般]タブで、次の情報を入力します。

- [WLAN ID]:WLANの番号を選択します
- タイプ – WLANの選択
- [Profile Name]：名前を入力すると、SSIDに同じ名前が自動的に入力されます。名前は一意である必要があり、31文字を超えることはできません。

この例では、次のフィールドはデフォルトのままですが、異なる設定を行う場合に備えて説明を示します。

- SSID：プロファイル名はSSIDとしても機能します。必要に応じて変更できます。名前は一意である必要があり、31文字を超えることはできません。
- [Enable]:WLANが動作するためには、これを有効のままにしておきます。
- 無線ポリシー：通常、2.4GHzおよび5GHzクライアントがネットワークにアクセスできるように、これを**すべて**として残します。
- Broadcast SSID：通常はSSIDを検出して、これを[Enabled]のままにしておきます。
- ローカルプロファイリング：このオプションを有効にすると、クライアントで実行されているオペレーティングシステムが表示されるか、ユーザ名が表示されます。

[Apply] をクリックします。



手順 3

[*WLAN Security*]タブが表示されます。

この例では、次のオプションがデフォルトのままになっています。

- ゲストネットワーク、キャプティブネットワークアシスタント、およびMACフィルタリングは無効のままにしました。ゲストネットワークのセットアップの詳細については、次のセクションで説明します。
- WPA2 Personal - Wi-Fi Protected Access 2 with Pre-shared Key (PSK) Passphrase Format - ASCII。このオプションは、事前共有キー(PSK)を使用したWi-Fi Protected Access 2(WPA2)を表します。

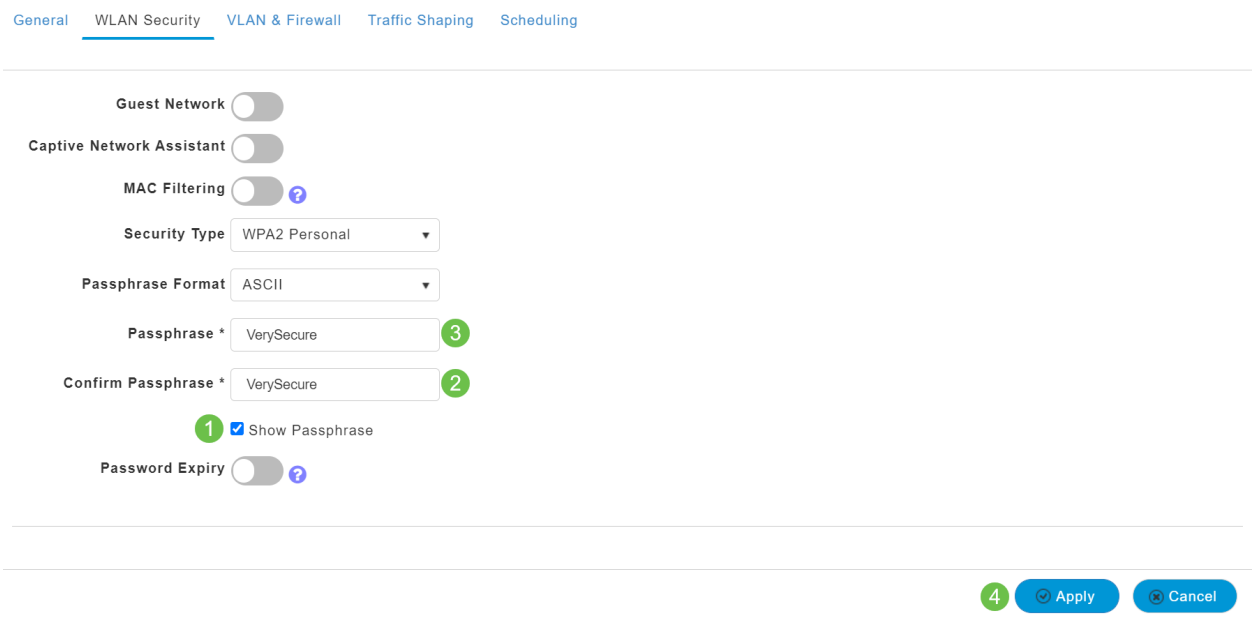
WPA2 Personalは、PSK認証を使用してネットワークを保護するために使用される方法です。PSKは、プライマリAP、WLANセキュリティポリシー、およびクライアントの両方で個別に設定されます。WPA2 Personalは、ネットワーク上の認証サーバに依存しません。

- パスフレーズ形式：**ASCIIはデフォルトのままになります。**

このシナリオでは、次のフィールドを入力しました。

- [Show Passphrase]：入力したパスフレーズを確認するには、チェックボックスをオンにします。
- [Passphrase]：パスフレーズ（パスワード）の名前を入力します。
- [Confirm Passphrase]：確認のためにパスワードをもう一度入力します。

[Apply] をクリックします。これにより、新しいWLANが自動的にアクティブになります。

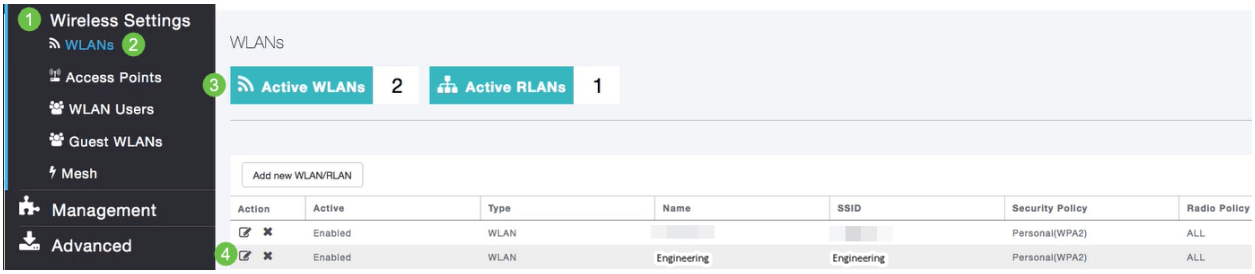


手順 4

Web UI画面の右上のパネルにある保**存アイコン**をクリックして、設定を保存してください。

手順 5

作成したWLANを表示するには、[Wireless Settings] > [**WLANs]を選択します。**アクティブなWLANの数が2に上がり、新しいWLANが表示されます。



作成する他のWLANに対してこれらの手順を繰り返します。

オプションのワイヤレス設定

これで、すべての基本設定が設定され、ロールする準備ができました。いくつかのオプションがあるので、次のセクションに進んでください。

- Web UIを使用したゲストWLANの作成（オプション）
- アプリケーション・プロファイリング（オプション）
- クライアントプロファイリング（オプション）
- まとめ、ネットワークの使用を開始する準備ができました。

Web UIを使用したゲストWLANの作成（オプション）

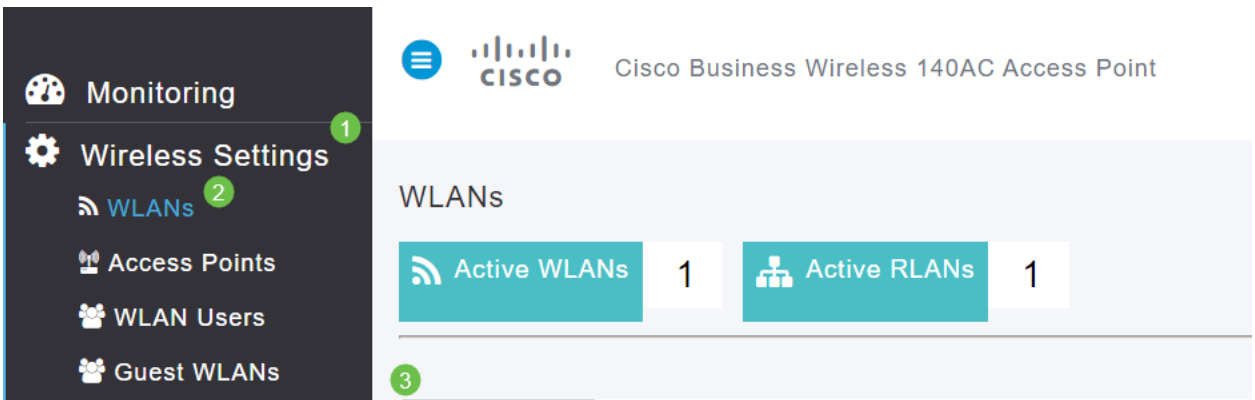
ゲストWLANは、Cisco Business Wirelessネットワークへのゲストアクセスを提供します。

手順 1

プライマリAPのWeb UIにログインします。Webブラウザを開き、www.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。プライマリAPのIPアドレスを入力してアクセスすることもできます。

手順 2

Wireless Local Area Network（WLAN；無線ローカルエリアネットワーク）を作成するには、[Wireless Settings] > [**WLANs]に移動します。**次に、[**Add new WLAN/RLAN]を選択します。**



手順 3

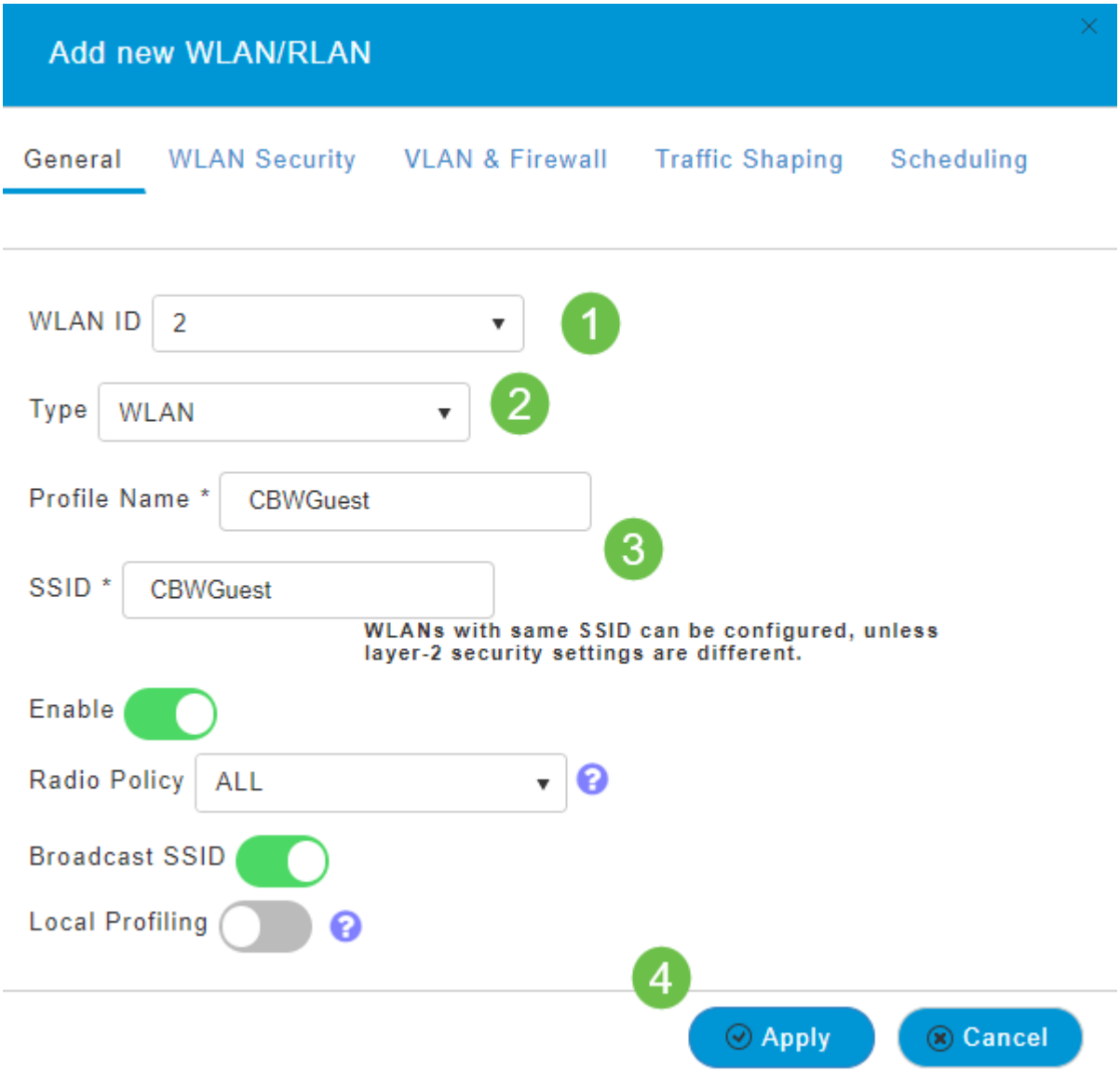
[全般]タブで、次の情報を入力します。

WLAN ID:WLANの番号を選択します
タイプ- WLANの**選択**
Profile Name : 名前を入力すると、SSIDに同じ名前が自動的に入力されます。名前は一意である必要があり、31文字を超えることはできません。

この例では、次のフィールドはデフォルトのままですが、異なる設定を行う場合に備えて説明を示します。

SSID : プロファイル名もSSIDとして機能します。必要に応じて変更できます。名前は一意である必要があり、31文字を超えることはできません。
Enable:WLANが動作するためには、これをイネーブルのままにしておきます。
無線ポリシー : 通常は、2.4GHzおよび5GHzクライアントがネットワークにアクセスできるように**All**のままにしておきます。
Broadcast SSID : 通常はSSIDを検出して、これを[Enabled]のままにしておきます。
ローカルプロファイリング : このオプションを有効にすると、クライアントで実行されているオペレーティングシステムが表示されるか、ユーザ名が表示されます。

[Apply] をクリックします。

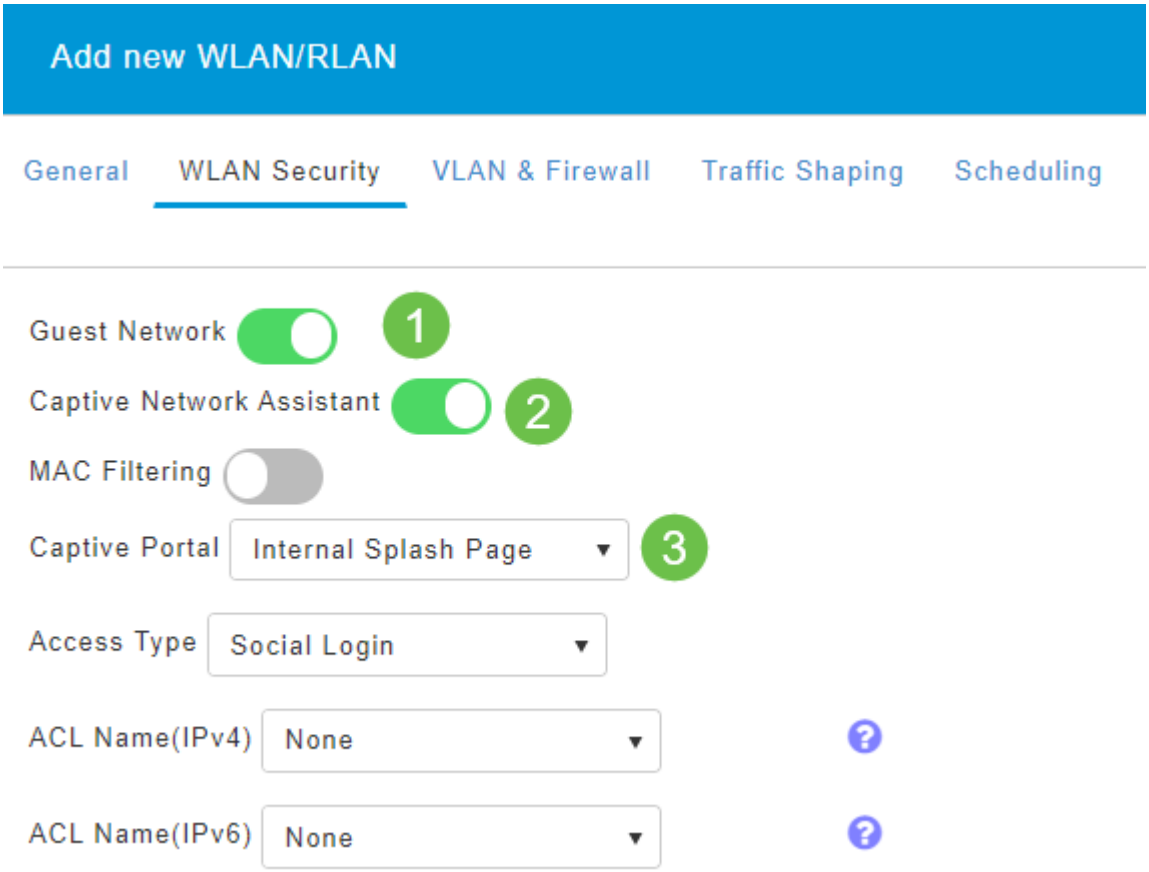


手順 4

[*WLAN Security*]タブが表示されます。この例では、次のオプションが選択されています。

- ゲストネットワーク：有効
- キャプティブネットワークアシスタント：MacまたはIOSを使用している場合は、これを有効にすることをお勧めします。この機能は、ワイヤレスネットワークへの接続時にWeb要求を送信することによって、キャプティブポータルの存在を検出します。この要求は、iPhoneモデルのUniform Resource Locator(URL)に送信され、応答を受信すると、インターネットアクセスが利用可能であると見なされ、それ以上の対話は必要ありません。応答が受信されない場合、インターネットアクセスはキャプティブポータルによってブロックされていると見なされ、AppleのCaptive Network Assistant(CNA)が疑似ブラウザを自動起動して、制御ウィンドウでポータルログインを要求します。Identity Services Engine(ISE)キャプティブポータルにリダイレクトすると、CNAが破損する可能性があります。プライマリAPは、この疑似ブラウザがポップアップするのを防止します。
- [キャプティブポータル(Captive Portal)]：このフィールドは、[ゲストネットワーク(Guest Network)]オプションが有効になっている場合にのみ表示されます。これは、認証に使用できるWebポータルのタイプを指定するために使用されます。デフォルトのCisco Webポータルベース認証を使用するには、[Internal Splash Page]を選択します。

ネットワーク外のWebサーバを使用してキャプティブポータル認証を行う場合は、[External Splash Page]を選択します。また、[Site URL]フィールドにサーバのURLを指定します。



この例では、ソーシャルログインアクセスタイプが有効になっているゲストWLANが作成されます。ユーザがこのゲストWLANに接続すると、シスコのデフォルトログインページにリダイレクトされ、GoogleとFacebookのログインボタンが表示されます。ユーザは、GoogleまたはFacebookアカウントを使用してログインし、インターネットアクセスを取得できます。

手順 5

この同じタブで、ドロップダウンメニューから*アクセスタイプ*を選択します。この例では、[Social Login]が*選択*されています。これは、ゲストがGoogleまたはFacebookのクレデンシャルを使用して認証を行い、ネットワークにアクセスできるようにするオプションです。

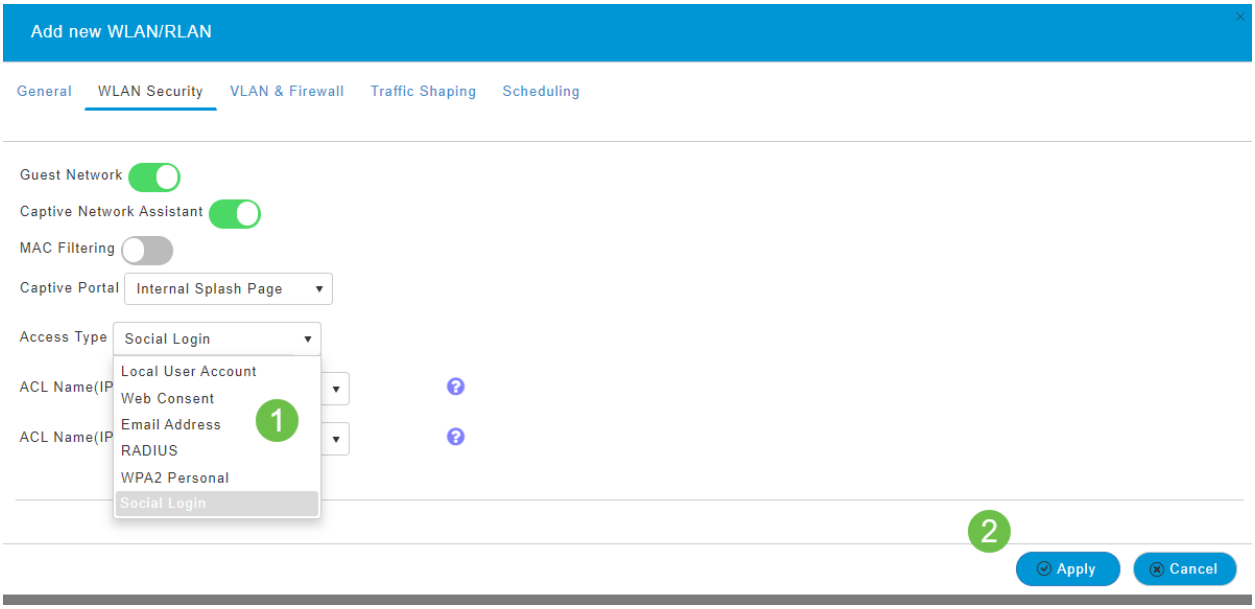
アクセスタイプのその他の*オプション*は*次*のとおりです。

ローカルユーザアカウント：デフォルトのオプション。このWLANのゲストユーザに指定できるユーザ名とパスワードを使用してゲストを認証するには、[Wireless Settings] > [WLAN Users]で、**このオプションを選択します**。これは、デフォルトの内部スプラッシュページの例です。

これをカスタマイズするには、[Wireless Settings] > [Guest WLANs]に移動します。ここから、ページの見出しとページメッセージを入力できます。[Apply] をクリックします。[プレビュー]をクリックします。

Web同意：表示された利用規約に同意すると、ゲストはWLANにアクセスできます。ゲストユーザは、ユーザ名とパスワードを入力しなくてもWLANにアクセスできます。
電子メールアドレス：ゲストユーザは、ネットワークにアクセスするために電子メールアドレスを入力する必要があります。
RADIUS：これは外部認証サーバで使用します。
WPA2 Personal - Wi-Fi Protected Access 2(WPA2)事前共有キー(PSK)

[Apply] をクリックします。



手順 6

Web UI画面の右上のパネルにある保**存アイコン**をクリックして、設定を保存してください。

これで、CBWネットワークで使用可能なゲストネットワークが作成されました。あなたのゲストは利便性に感謝します。

Web UIを使用したアプリケーションプロファイリング（オプション）

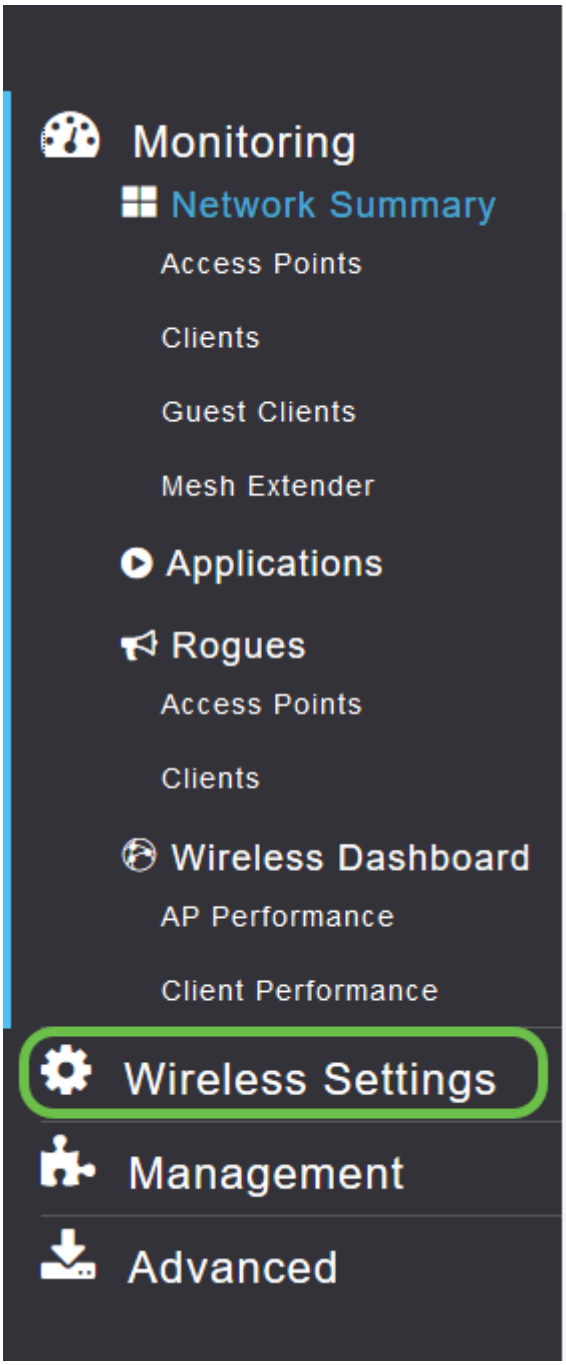
プロファイリングは、組織ポリシーを有効にする機能のサブセットです。トラフィックタイプを照合し、優先順位を付けることができます。ルールと同様に、トラフィックのランク付けやドロップの方法を決定します。Cisco Business Mesh Wirelessシステムには、クライアントとアプリケーションのプロファイリング機能があります。ユーザとしてネットワークにアクセスする行為は、まず多くの情報交換から始まります。その情報の中には、トラフィックの種類があります。ポリシーはトラフィックフローを中断し、フローチャートのようにパスを誘導します。その他のポリシー機能には、ゲストアクセス、アクセスコントロールリスト、QoSなどがあります。

手順 1

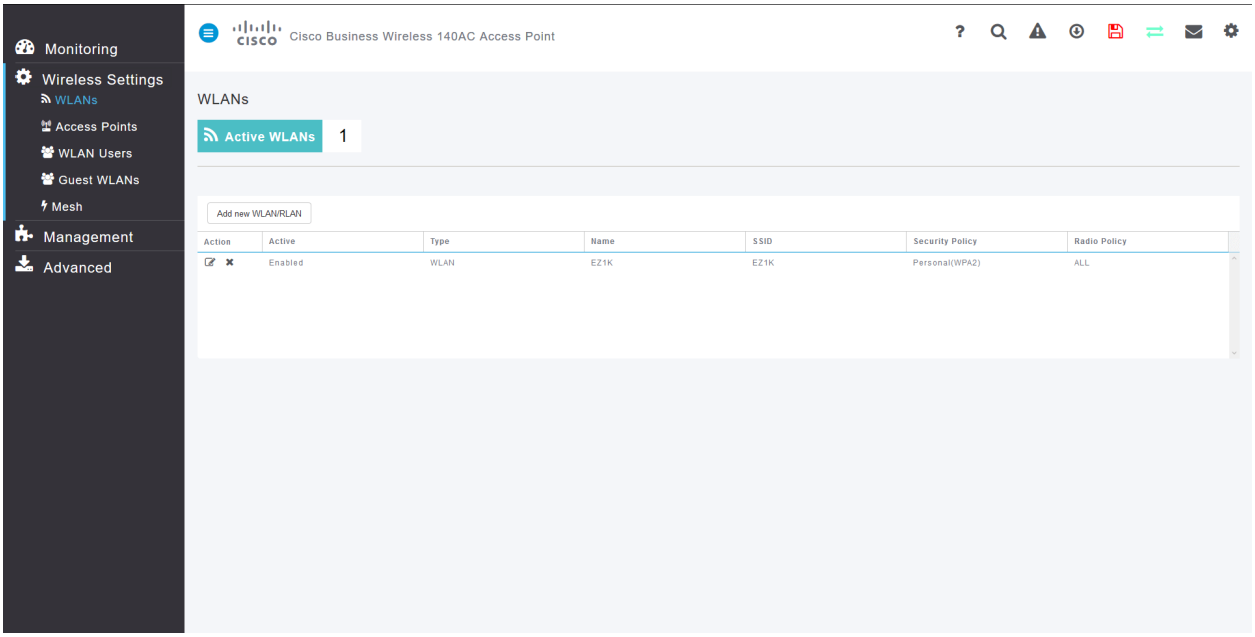
左側のメニューバーが表示されていない場合は、画面の左側にあるメニューに移動します。

手順 2

デバイスにサインインすると、[Monitoring]メニューがデフォルトでロードされます。[ワイヤレス設定]をクリック**する必要があります**。

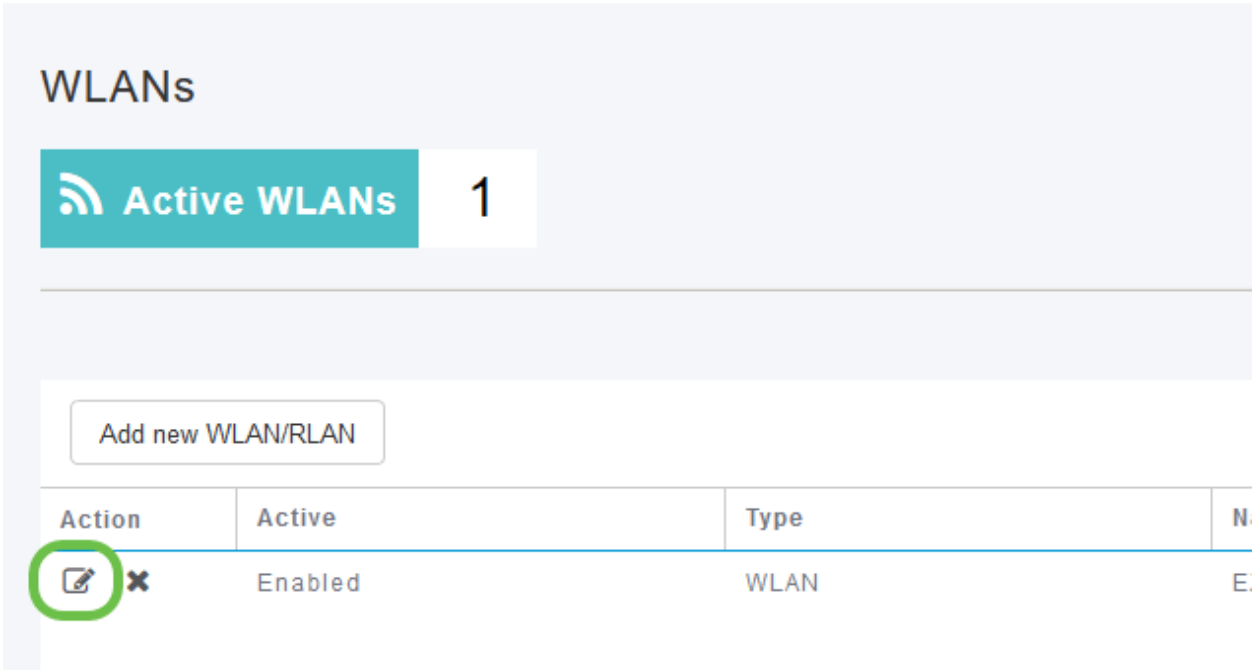


次の図は、[ワイヤレス設定(Wireless Settings)]リンクをクリックしたときに表示されるものと似ています。

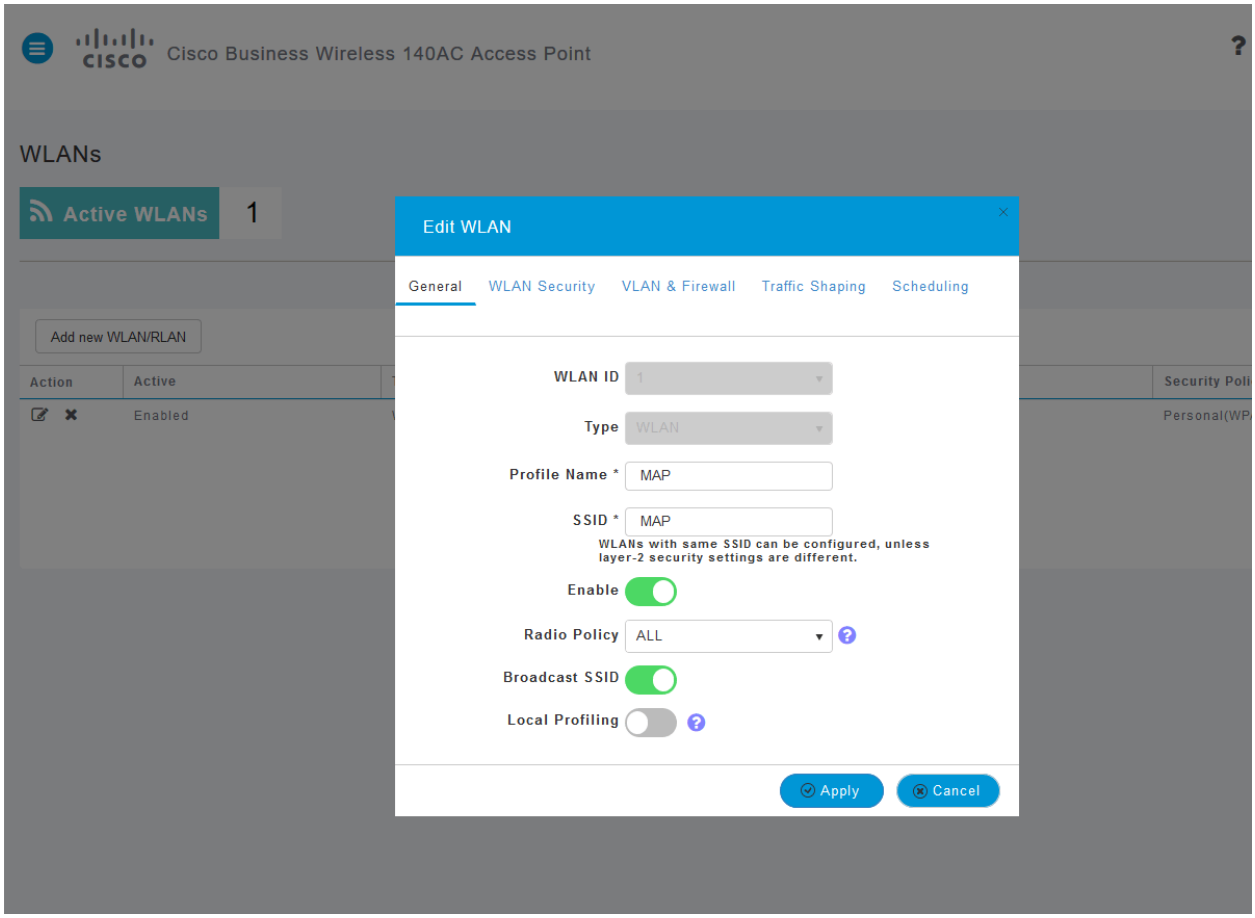


手順 3

アプリケーションを**有効にする**ワイヤレスローカルエリアネットワークの左側にある編集アイコンをクリックします。

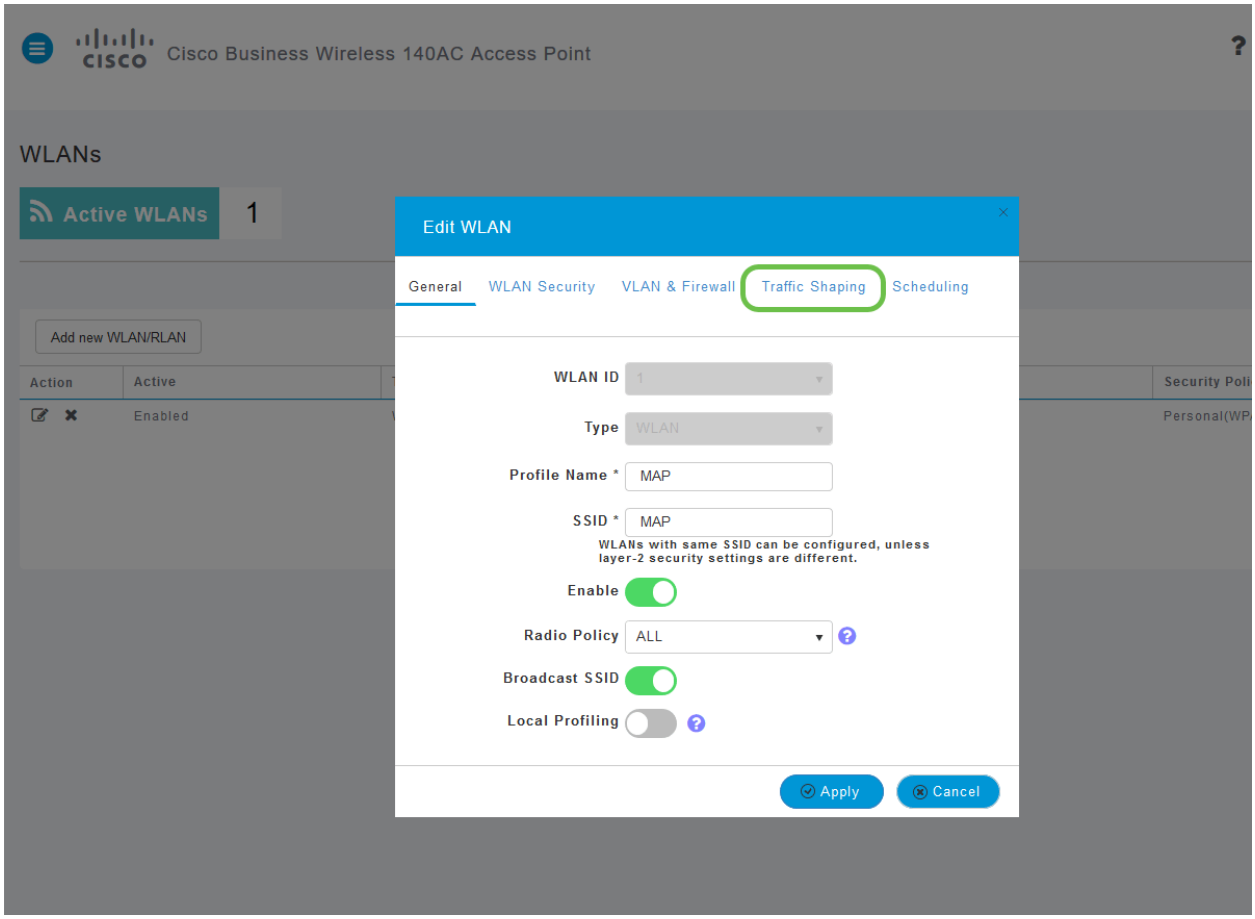


WLANを最近追加したので、[*Edit WLAN*]ページが次のように表示されます。

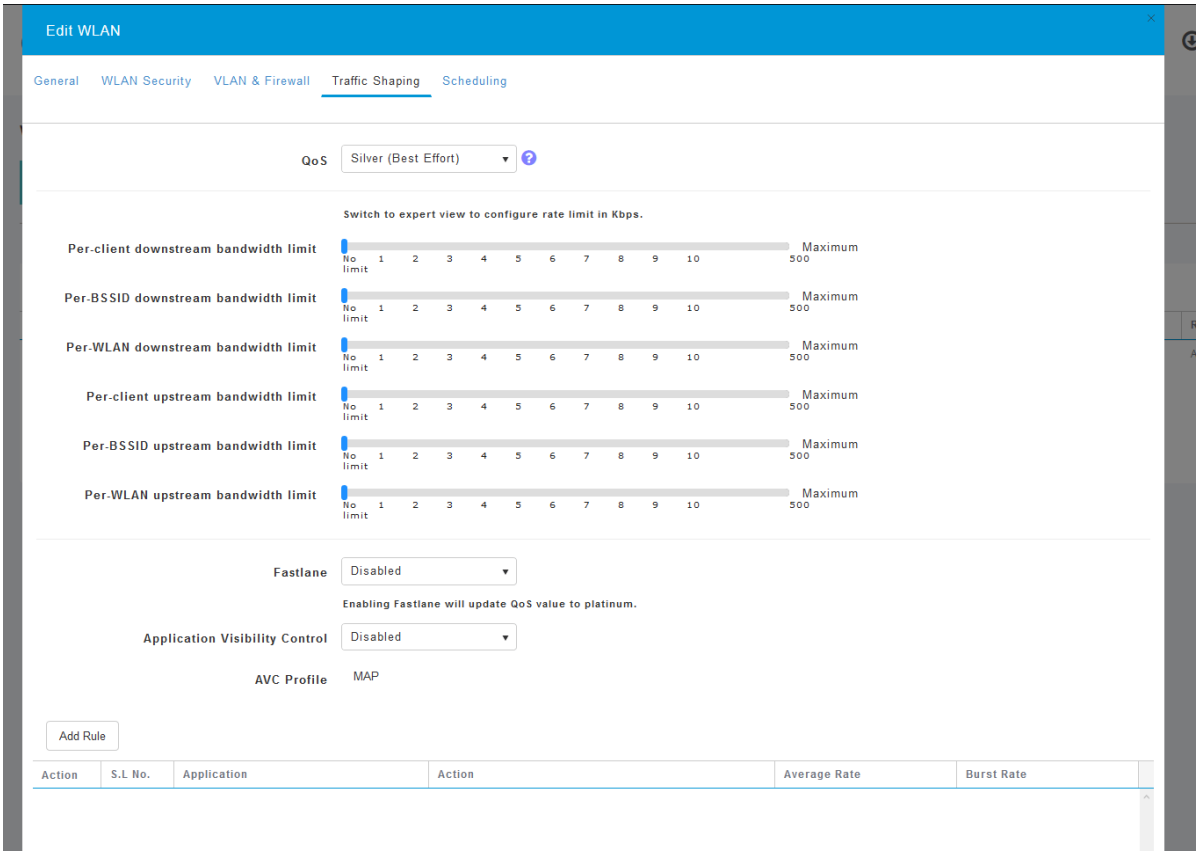


手順 4

[Traffic Shaping]タブをクリックして移動します。

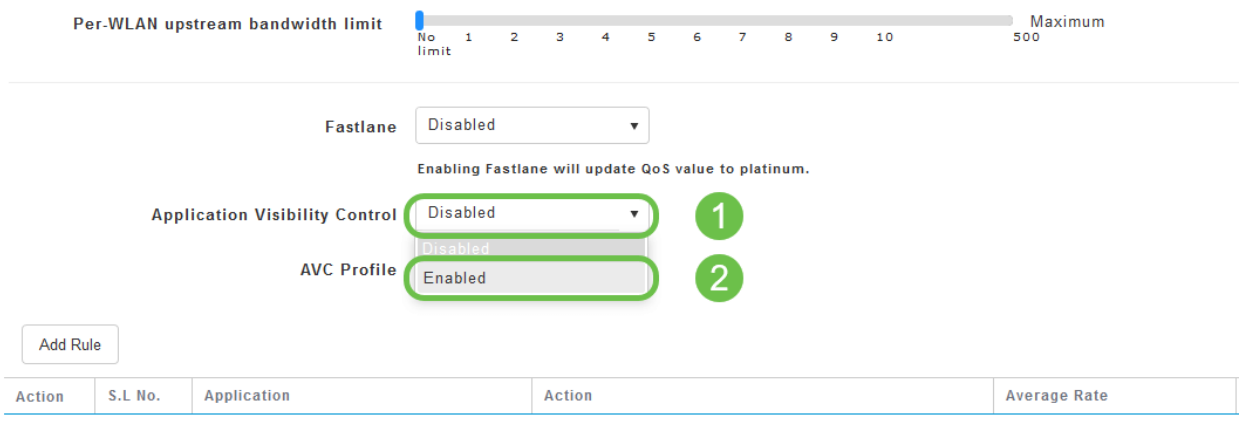


画面は次のように表示されます。



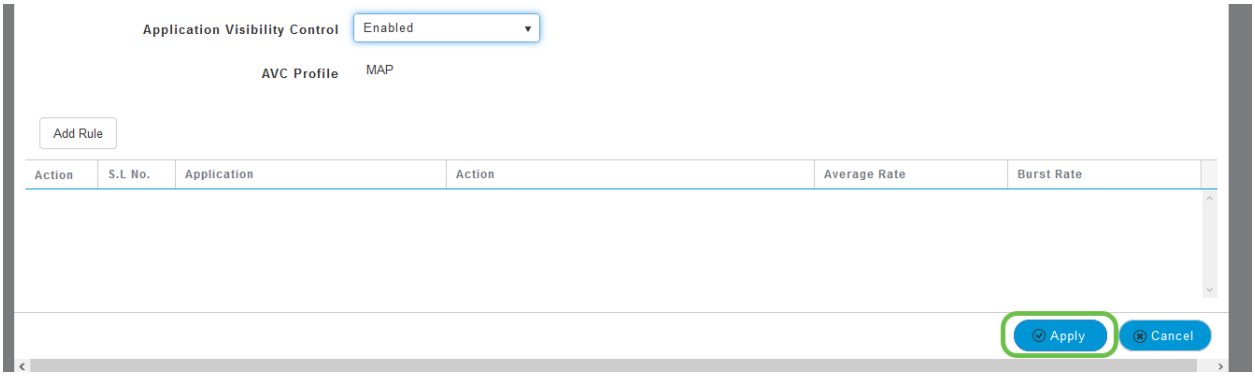
手順 5

ページの下部には、Application *Visibility* Control機能があります。これはデフォルトでは無効になっています。ドロップダウンをクリックし、[有効]を**選択します**。



手順 6

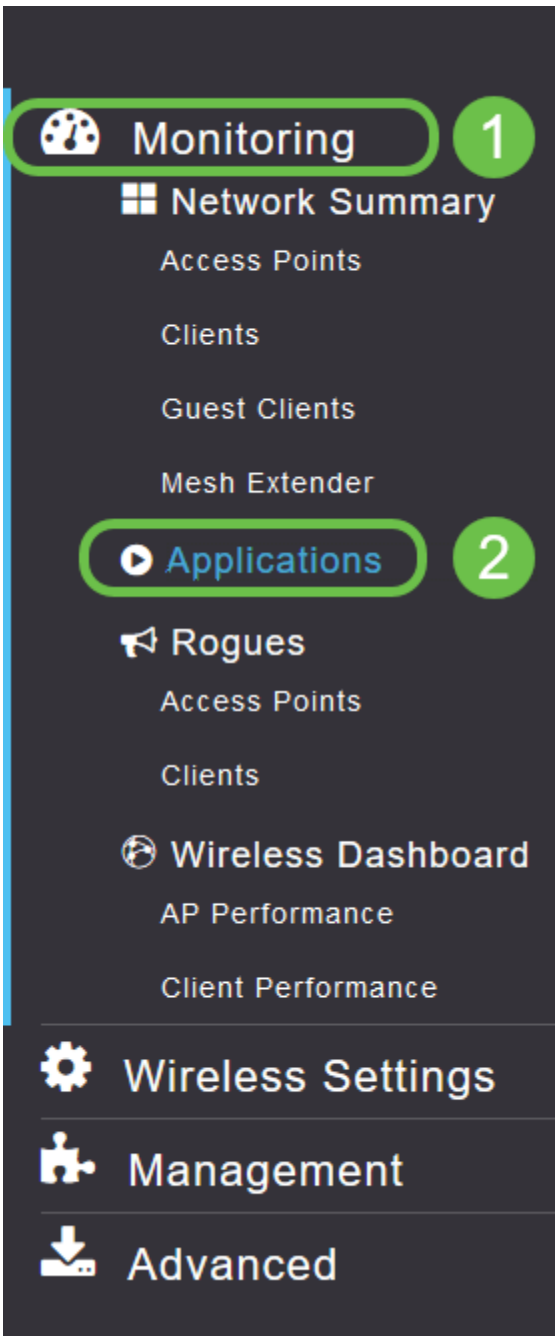
[適用]ボタンを**クリック**します。



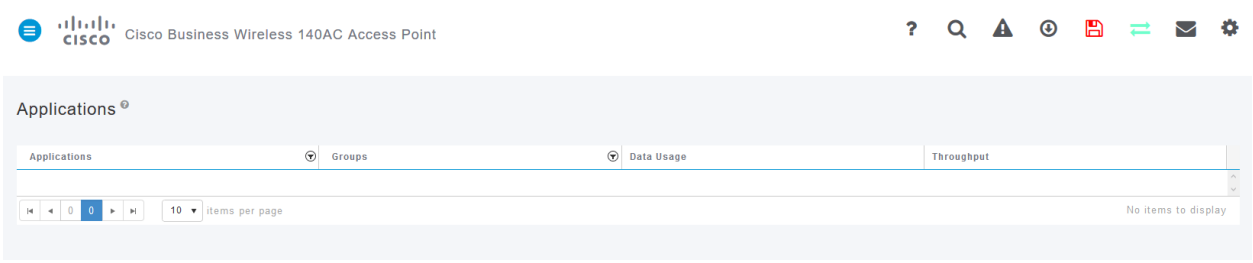
この設定を有効にする必要があります。有効にしない場合、機能は機能しません。

ステップ7

[Cancel]ボタンをクリックして、[WLAN]サブメニューを閉じます。次に、左側のメニューバーの[Monitoring]メニューをクリックします。アプリケーションのメニュー項目を**クリック**します。



送信元へのトラフィックがない場合は、次に示すようにページが空白になります。



このページには、次の情報が表示されます。

- アプリケーション：さまざまなタイプを含む
- グループ：ソートを容易にするアプリケーション· グループのタイプを示します
- データ使用量：このサービス全体で使用されるデータの量
- スループット：アプリケーションによって使用される帯域幅の量

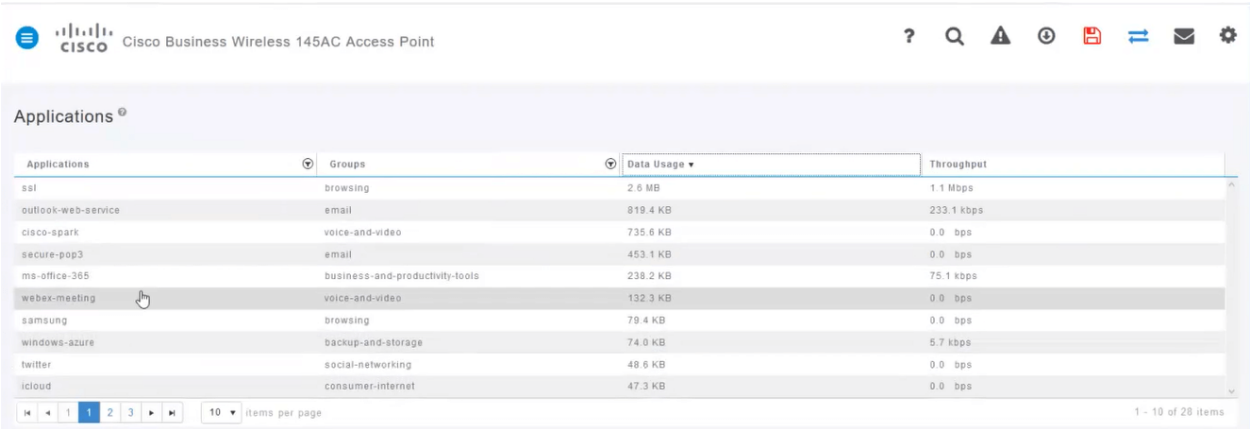
タブをクリックすると、最大から最小に並べ替えることができます。これにより、ネ

ットワークリソースの最大のコンシューマを特定できます。

この機能は、WLANリソースをきめ細かく管理するために非常に強力です。次に、より一般的なグループとアプリケーションの種類をいくつか示します。リストには、次のグループや例など、さらに多くのグループが含まれている可能性があります。

- 参照
  - 例：クライアント固有、SSL
- Email
  - 例：Outlook、Secure-pop3
- 音声およびビデオ
  - 例：WebEx、Cisco Spark、
- ビジネスおよび生産性向上ツール
  - 例：Microsoft Office 365、
- バックアップ/ストレージ
  - 例：Windows-Azure、
- コンシューマインターネット
  - iCloud、Google Drive
- ソーシャルネットワーキング
  - 例：Twitter、Facebook
- ソフトウェア アップデート
  - 例：Google-Play、IOS
- インスタントメッセージ
  - 例：ハングアウト、メッセージ

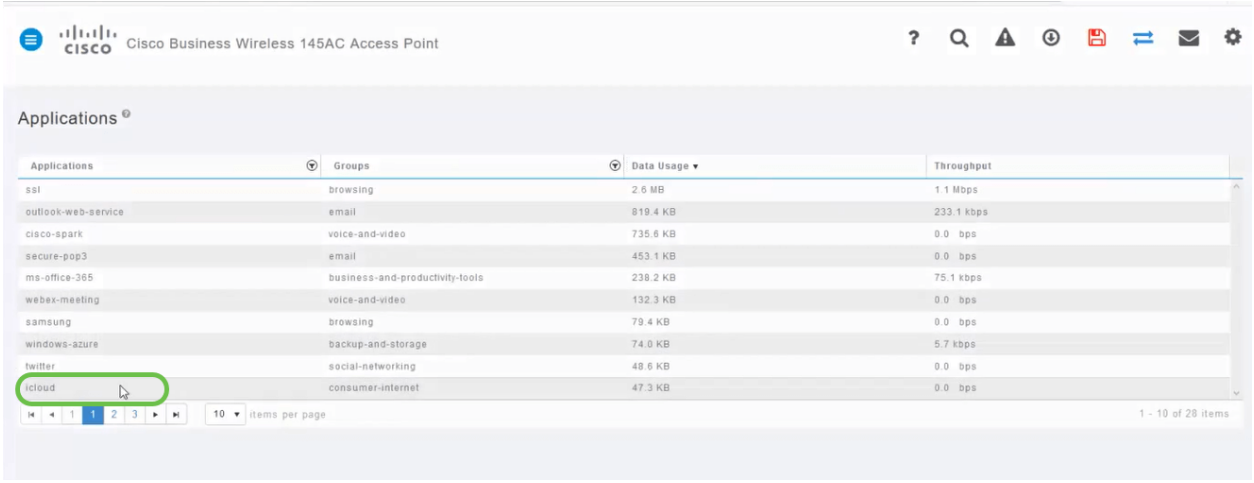
次に、ページを入力したときの表示例を示します。



各テーブルの見出しはソート用にクリック可能で、特にデータの使*用とスループット*フィールドに*便利*です。

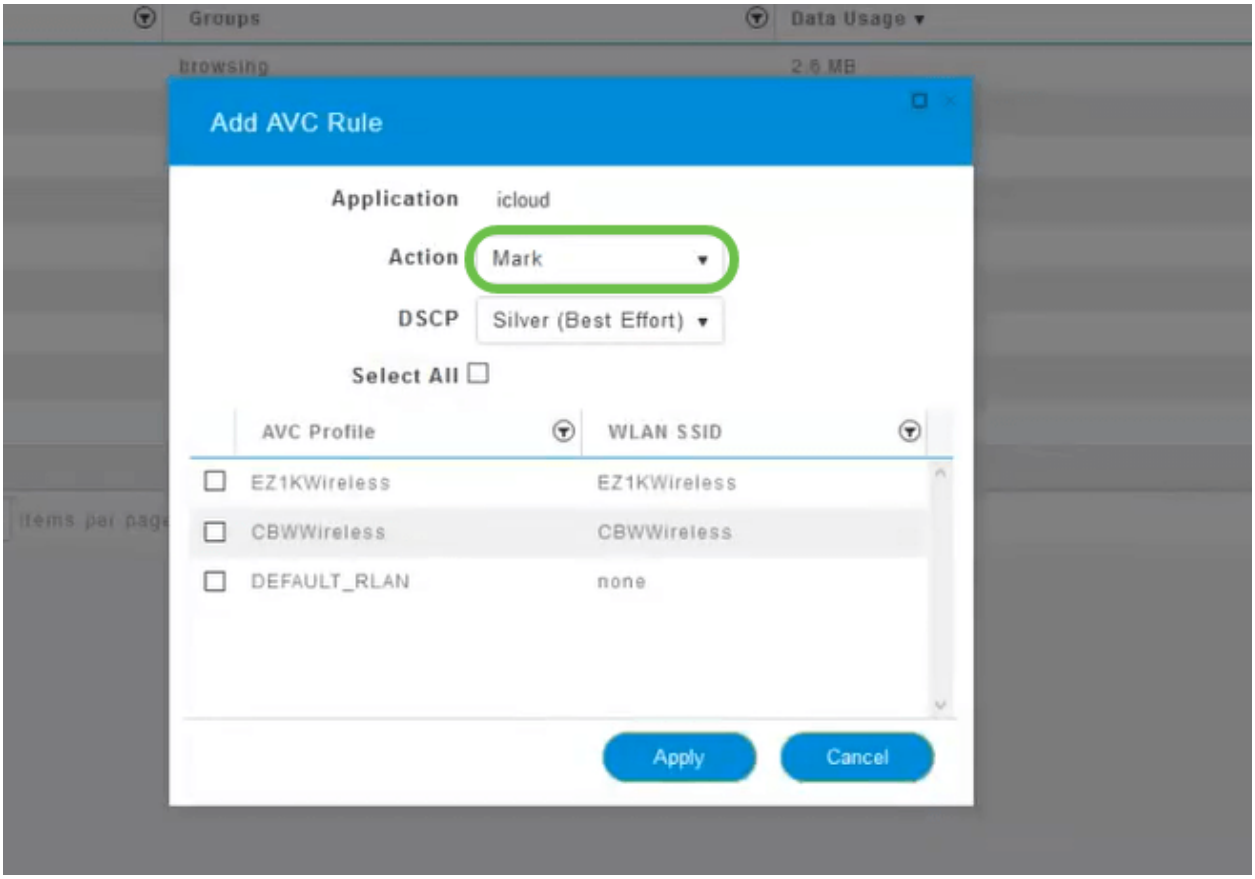
手順 8

管理するトラフィックのタイプの行をクリックします。



手順 9

[アクション(Action)]ドロップダウンボックスをクリックして、そのトラフィックタイプの処理方法を選択します。



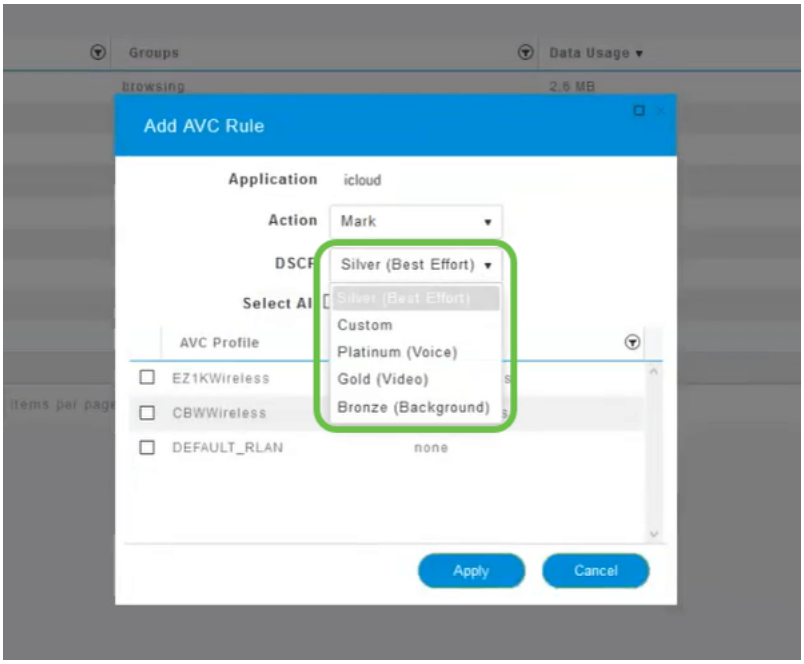
この例では、このオプションは*Mark*のままにしておきます。

トラフィックに対するアクション

- Mark：トラフィックタイプをDifferentiated Services Code Point(DSCP)3階層の1つに配置し、アプリケーションタイプで使用できるリソースの数を制御します
- ドロップ：トラフィックを廃棄する以外に何もしないでください
- レート制限：平均レート、バーストレートをKbps単位で設定できます

手順 10

[DSCP]フィールドのドロップダウンボックスをクリックして、次のオプションから選択します。



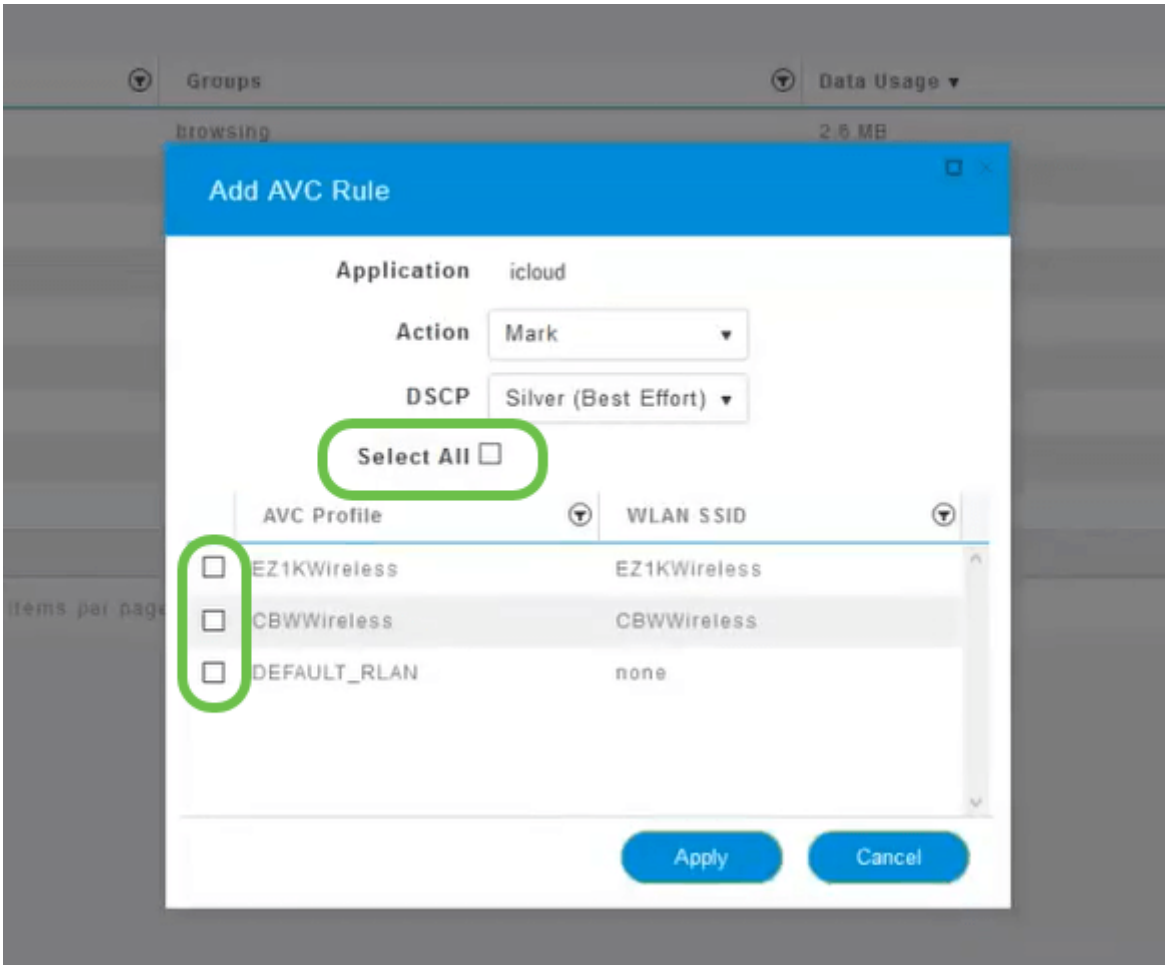
マーキングするトラフィックのDSCPオプションを次に示します。これらのオプションは、編集しているトラフィックタイプで使用できるリソース数が少なくなり、リソース数が増えます。

- ブロンズ（背景）– 低
- シルバー（ベストエフォート）
- ゴールド（ビデオ）
- Platinum（音声）その他
- カスタム – ユーザセット

Web上の慣例として、トラフィックはSSLブラウジングに移行しているため、パケットがネットワークからWANに移動する際に、パケット内の内容が表示されなくなります。そのため、Webトラフィックの大部分はSSLを使用します。SSLトラフィックを低い優先順位に設定すると、閲覧エクスペリエンスに影響を与える可能性があります。

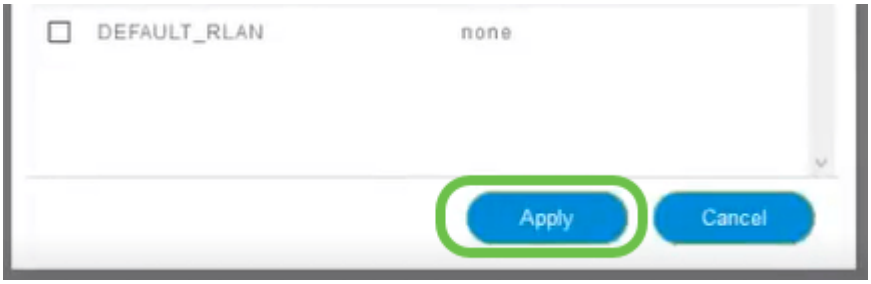
手順 11

次に、このポリシーを実行する個々のSSIDを選択するか、[すべて選択]をクリックします。



ステップ 12

次に、[Apply]をクリックし、このポリシーを開始します。



次の2つのケースが該当します。

- ゲスト/ユーザは大量のトラフィックをストリーミングするため、ミッションクリティカルなトラフィックが通過できません。音声のプライオリティを上げ、Netflixトラフィックのプライオリティを下げて改善することができます。
- 営業時間中にダウンロードする大規模なソフトウェアアップデートは、優先順位を下げるか、レートを制限することができます。

やった！アプリケーションのプロファイリングは、次のセクションで説明するように、クライアントのプロファイリングを有効にすることにより、さらに有効にできる非常に強力なツールです。

Web UIを使用したクライアントプロファイリング（オプション）

ネットワークに接続すると、デバイスはクライアントプロファイリング情報を交換します。デフォルトでは、クライアント・*プロファイリング*は無効になっています。この情報には、次のものが含まれます。

- ホスト名：またはデバイスの名前
- オペレーティングシステム – デバイスのコアソフトウェア
- OSバージョン – 該当するソフトウェアのイテレーション

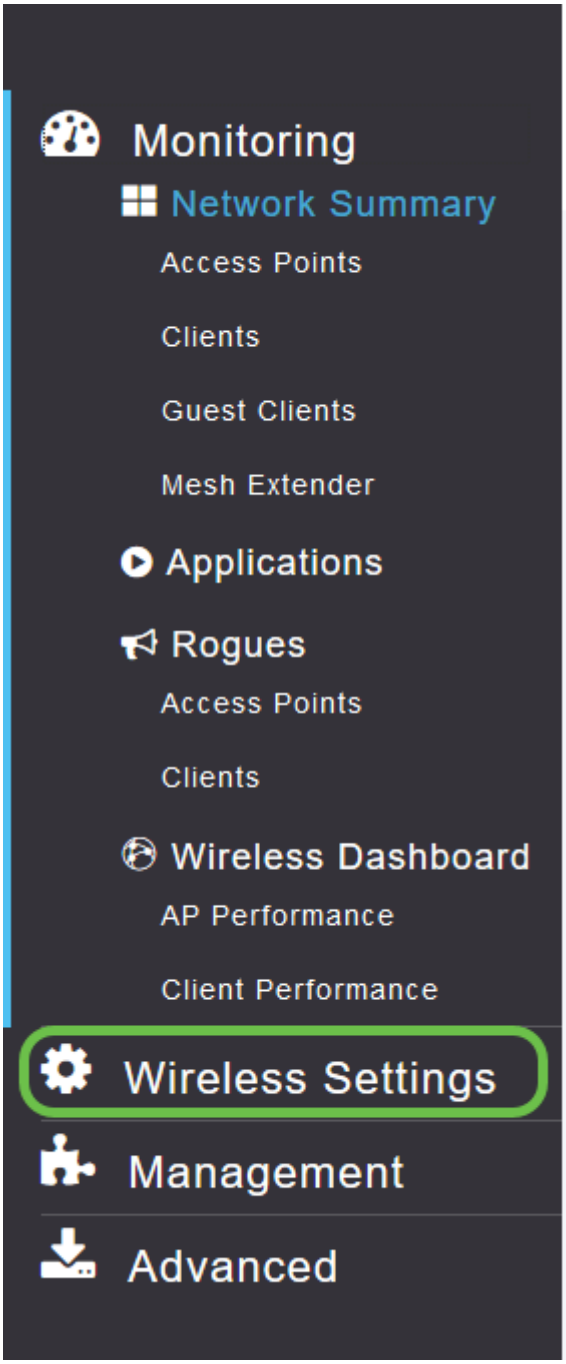
これらのクライアントに関する統計情報には、使用されるデータ量とスループットが含まれます。

クライアントプロファイルのトラッキングにより、ワイヤレスローカルエリアネットワークの制御が強化されます。または、別の機能として使用することもできます。たとえば、ミッションクリティカルなデータを伝送しないアプリケーションスロットリングデバイスタイプを使用します。

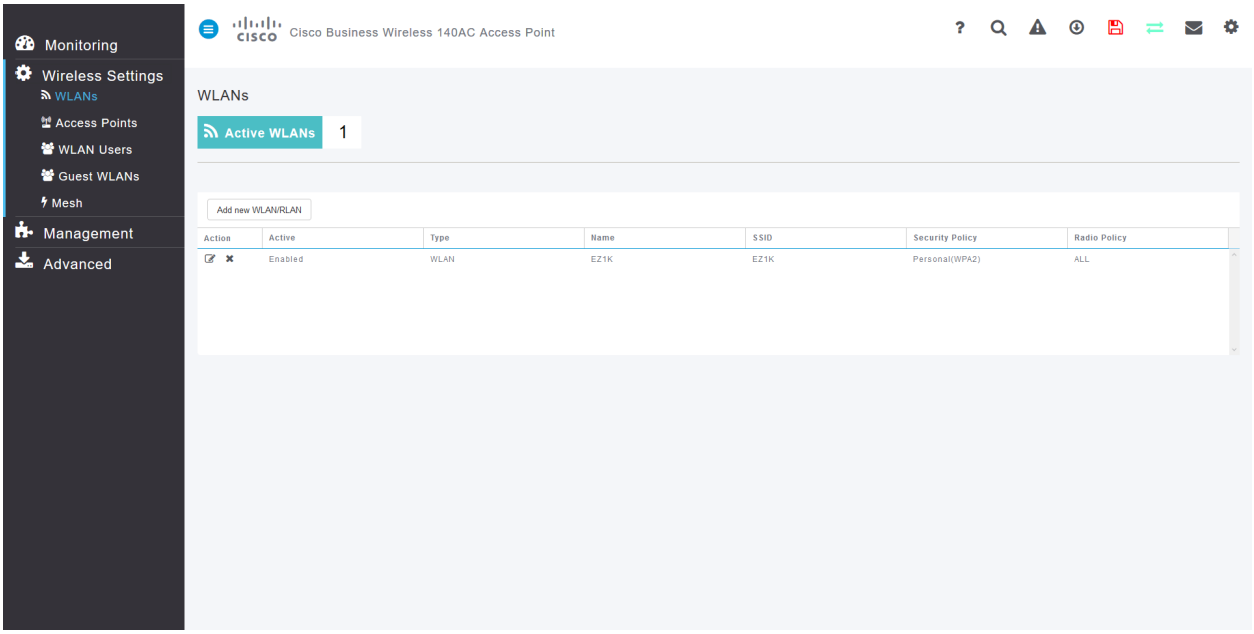
有効にすると、ネットワークのクライアントの詳細がWeb UIの[Monitoring]セクションに表示されます。

手順 1

[ワイヤレス設**定]をクリックします。**

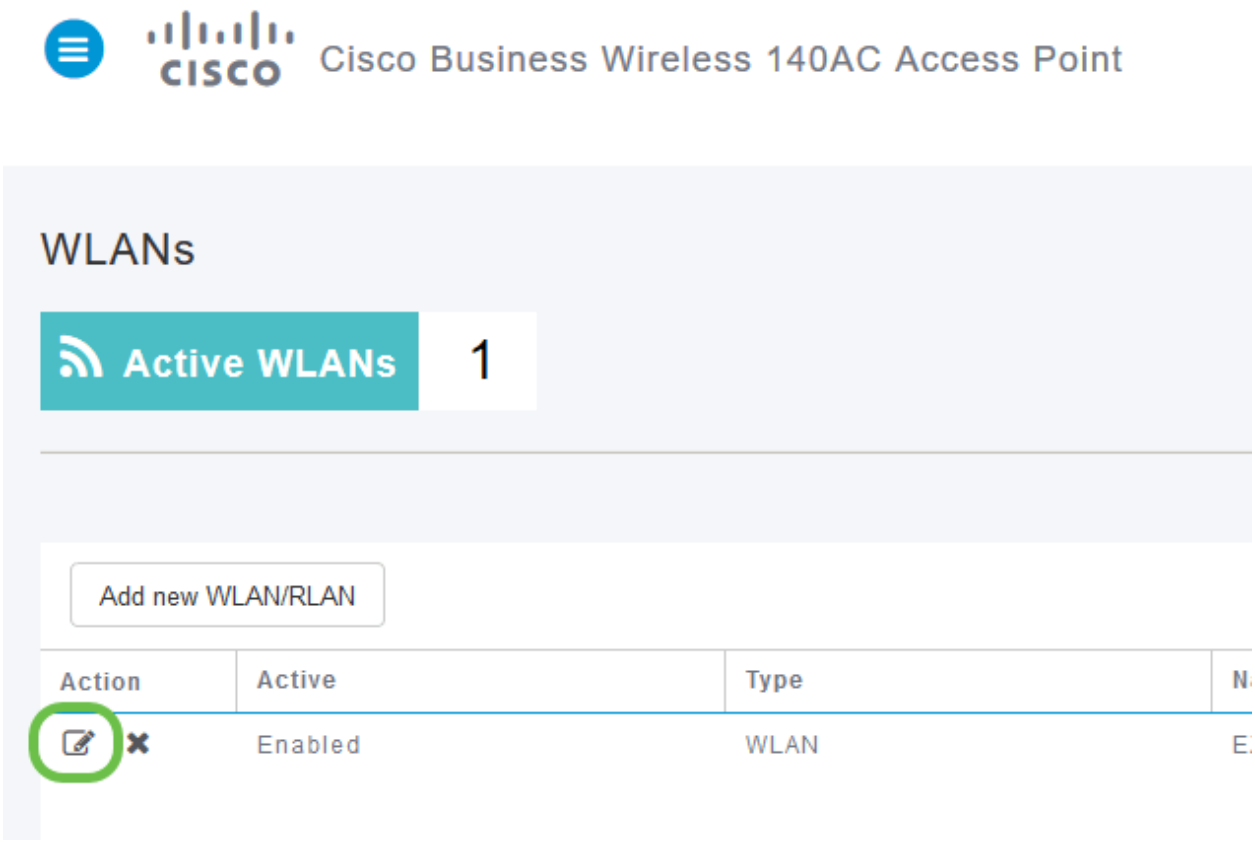


以下は、[ワイヤレス設定(Wireless Settings)]リンクをクリックしたときに表示される内容と似ています。



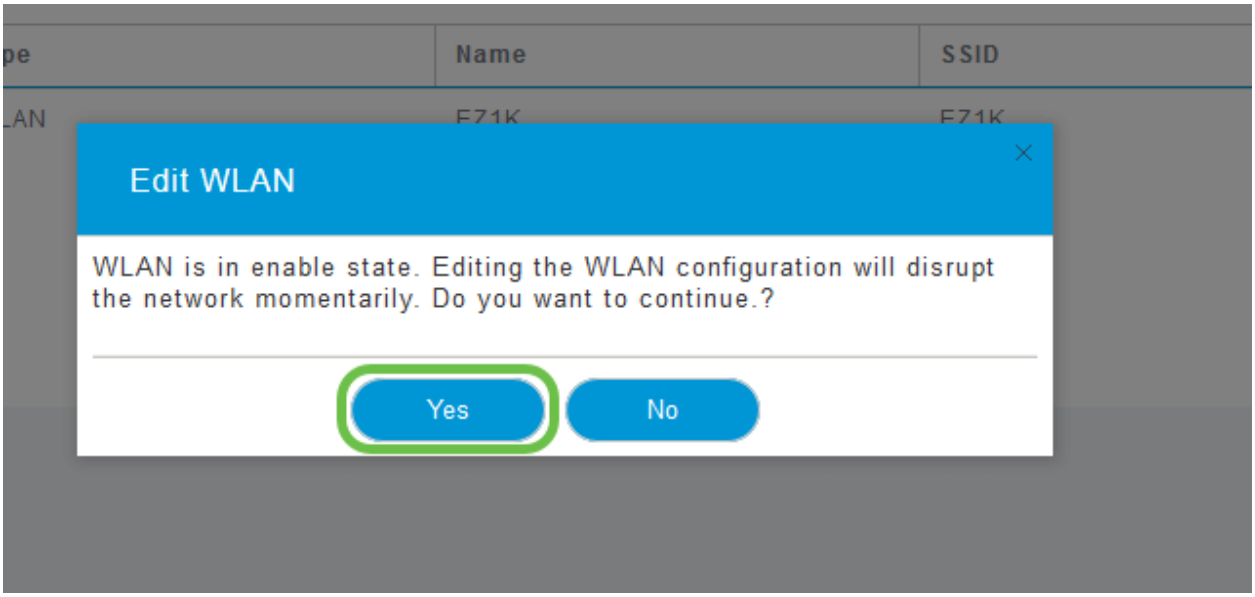
手順 2

アプリケーションに使用するWLANを決定し、その左側にある**編集アイ**コンをクリックします。



手順 3

次のようなポップアップメニューが表示されます。この重要なメッセージは、ネットワーク上のサービスに一時的に影響を与える可能性があります。[はい]をクリックして先に進みます。

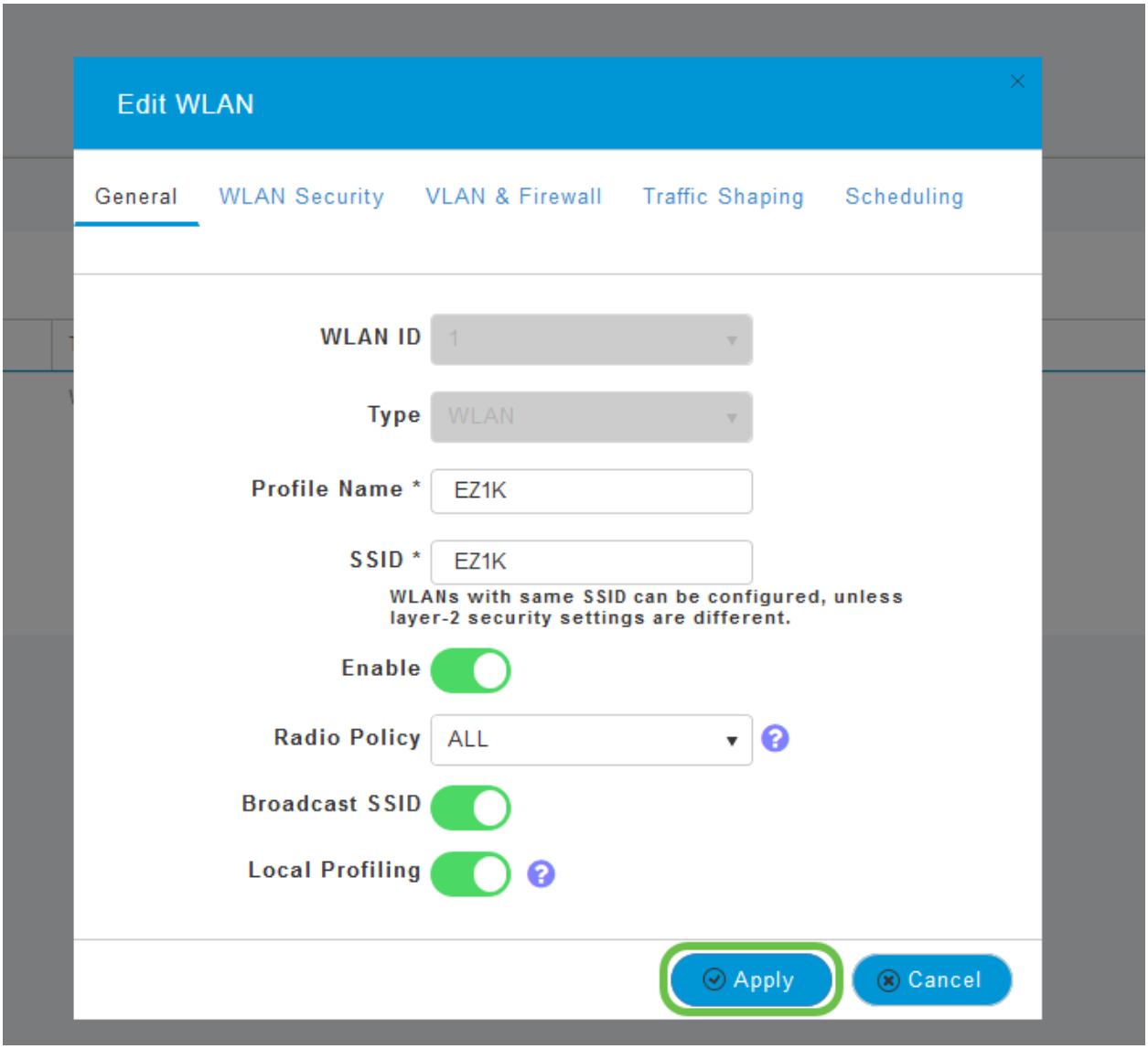


手順 4

[ローカルプロファイリング]トグルボタンをクリックして、クライ**アントのプロファイリング**を切り替えます。

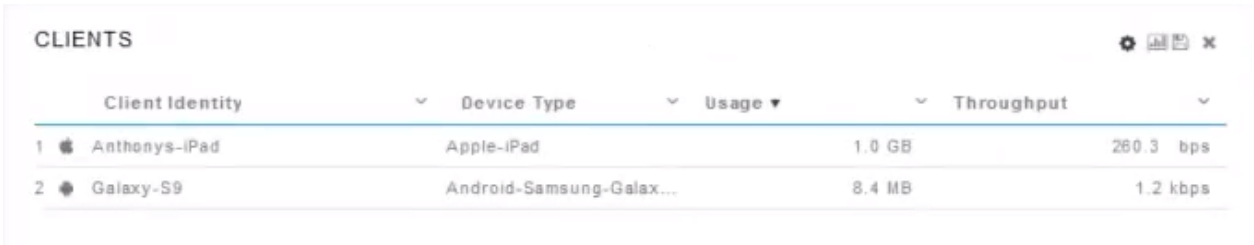
手順 5

[Apply] をクリックします。



手順 6

左側の[**Monitoring** section]メニュー項目をクリックします。[Monitoring]タブのダッシュボードにクライアントデータが表示されます。



結論

これで、セキュアネットワークのセットアップは完了です。何と素晴らしい気持ちだ、今すぐ祝って仕事に行く！

お客様に最適な内容を提供するため、このトピックに関するご意見やご提案がありましたら、シスココンテンツチームに電子メールをお送[りください](#)。

他の記事やドキュメントを読みたい場合は、ハードウェアのサポートページを確認してください。

- PoE対応Cisco RV260P VPNルータ
- Cisco Business 140ACアクセスポイント
- Cisco Business 142ACMメッシュエクステンダ