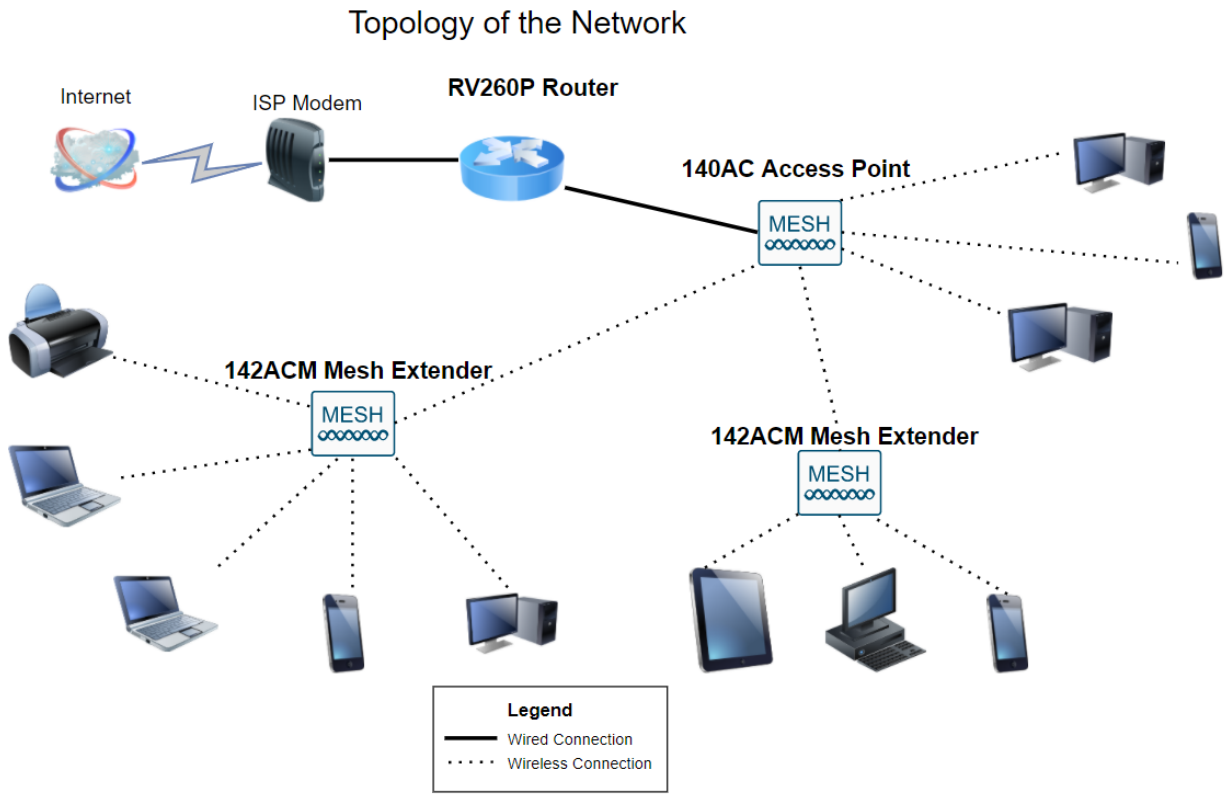
ネットワーク構成の合計：RV260PとCBWおよびCisco Business Mobile App

目的:

このガイドでは、RV260Pルータ、CBW140ACアクセスポイント、2つのCBW142ACMメッシュエクステンダ、およびCisco Business Wirelessアプリケーション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。

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、Cisco Business Wireless(CBW)140ACをスイッチではなくルータに接続できます。CBW140ACアクセスポイントと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。

- 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

CBWで基本設定を行う最も簡単な方法としてモバイルアプリケーションを推奨します

が、アプリケーションですべての機能を設定できるわけではありません。Cisco Business Wirelessアプリを初めて使用する場合は、次の記事をご覧ください。

- Cisco Business CB-Wireless-Meshアプリケーションについて
- Cisco Business Wireless:CBWアプリケーションとWeb UI機能

メッシュワイヤレスネットワークの設定時にWeb UIを使用する場合は、をクリックしてWeb UIのみを使用するバージョンを表示します。

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

モデムも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。

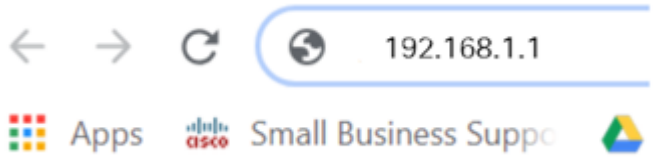
手順 1

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、コンピュータ上の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。

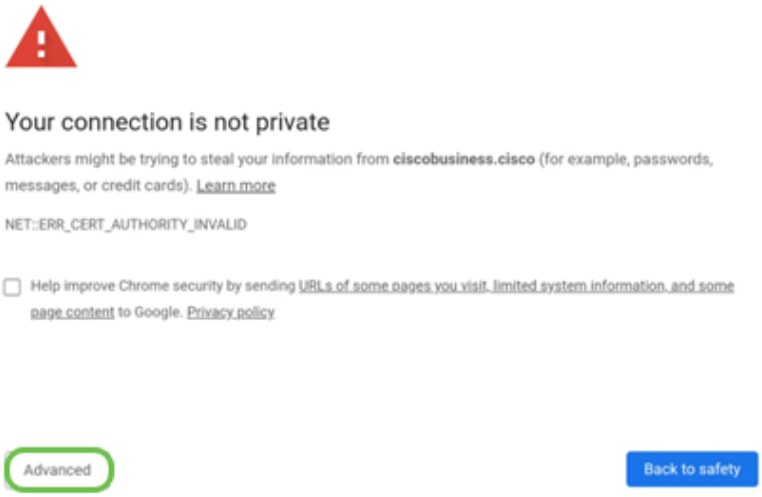
手順 2

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、192.168.1.1のデフォルトIPアドレスを入力します。



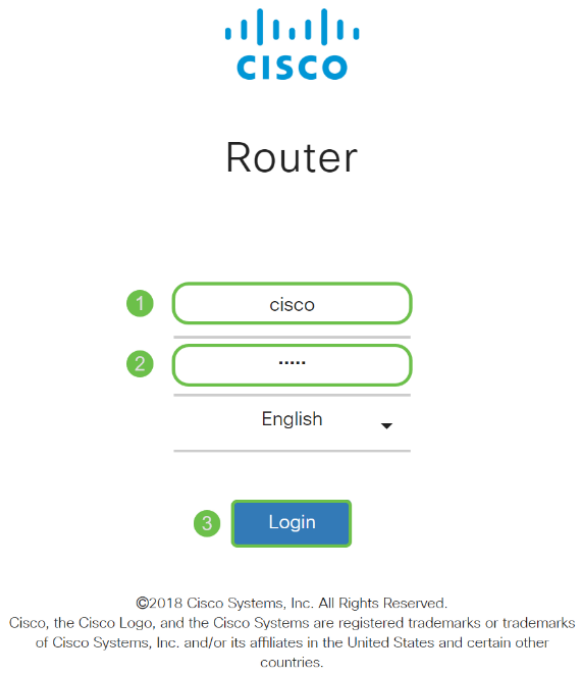
手順 3

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。応答を受け取った場合は、接続が確立され、この記事の「初期構成」セクションに進むことができます。

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の指示を参照してRV260Pの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。

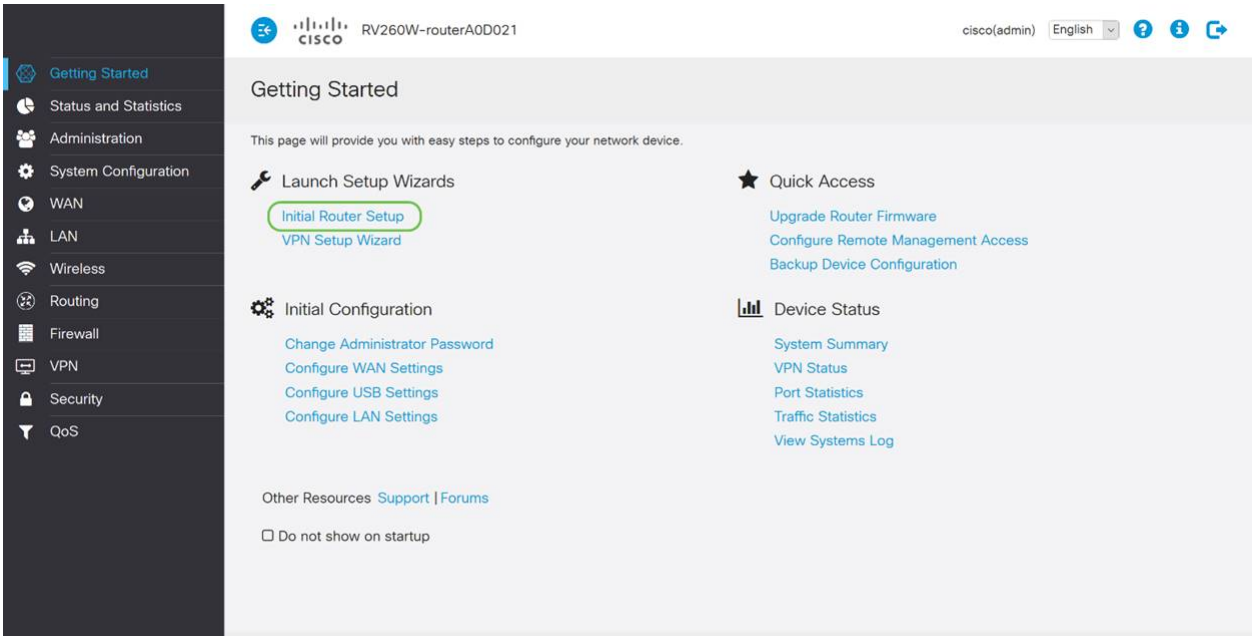
5. DSLモデムを使用している場合は、ISPにDSLモデムをブリッジモードにするよう依頼します。

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。特定の設定の記事がある場合は、手順の最後にリストされます。

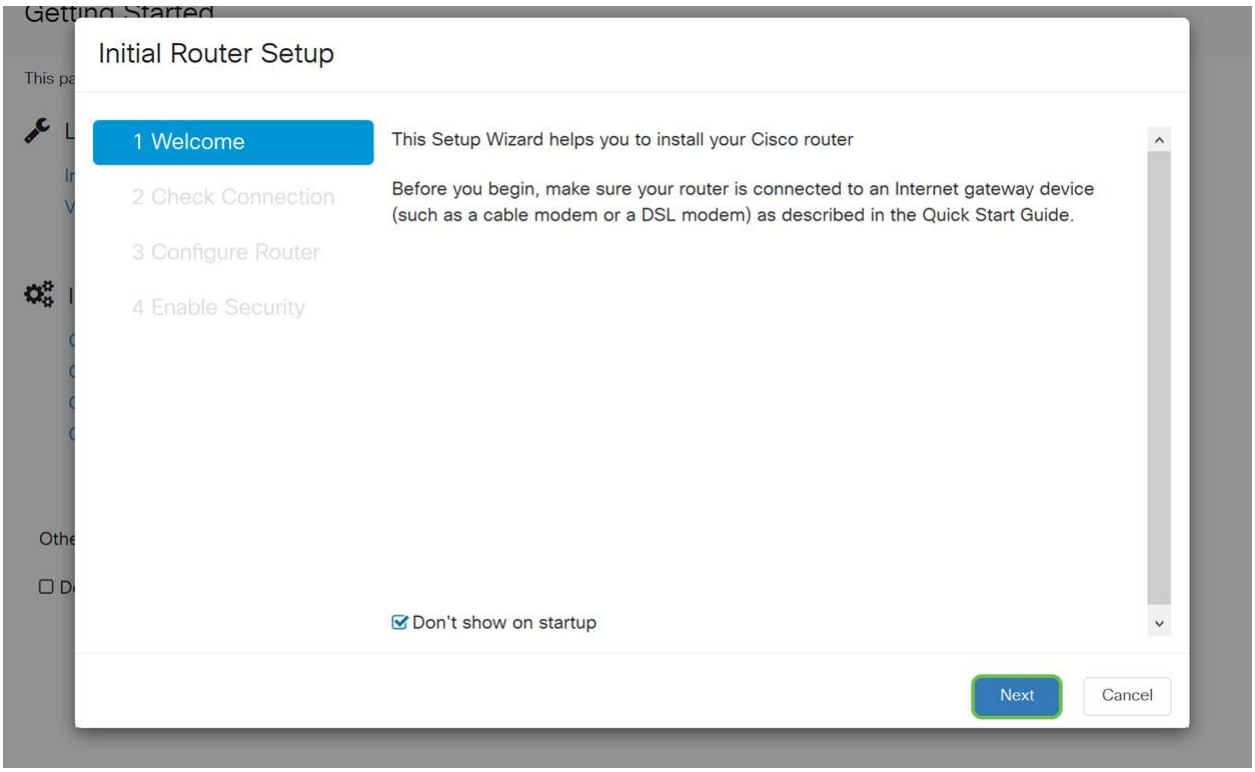
手順 1

[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。



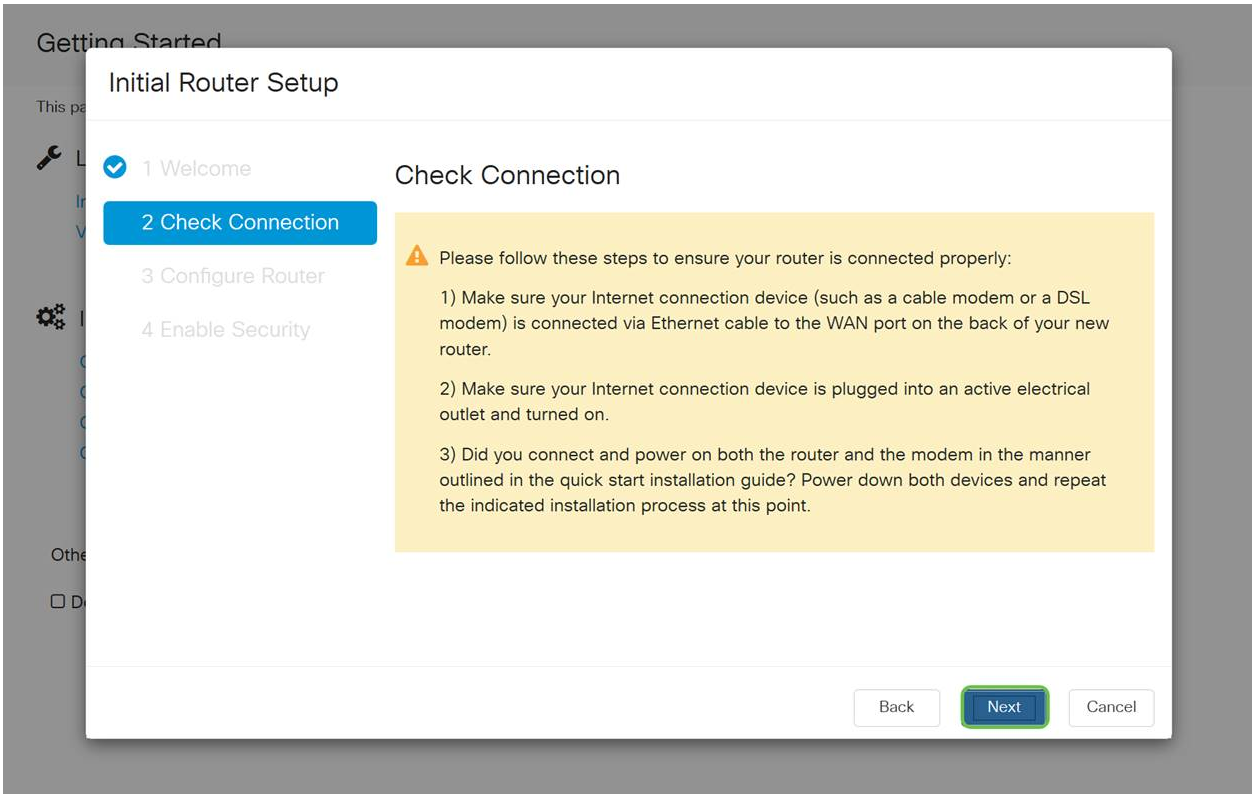
手順 2

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。



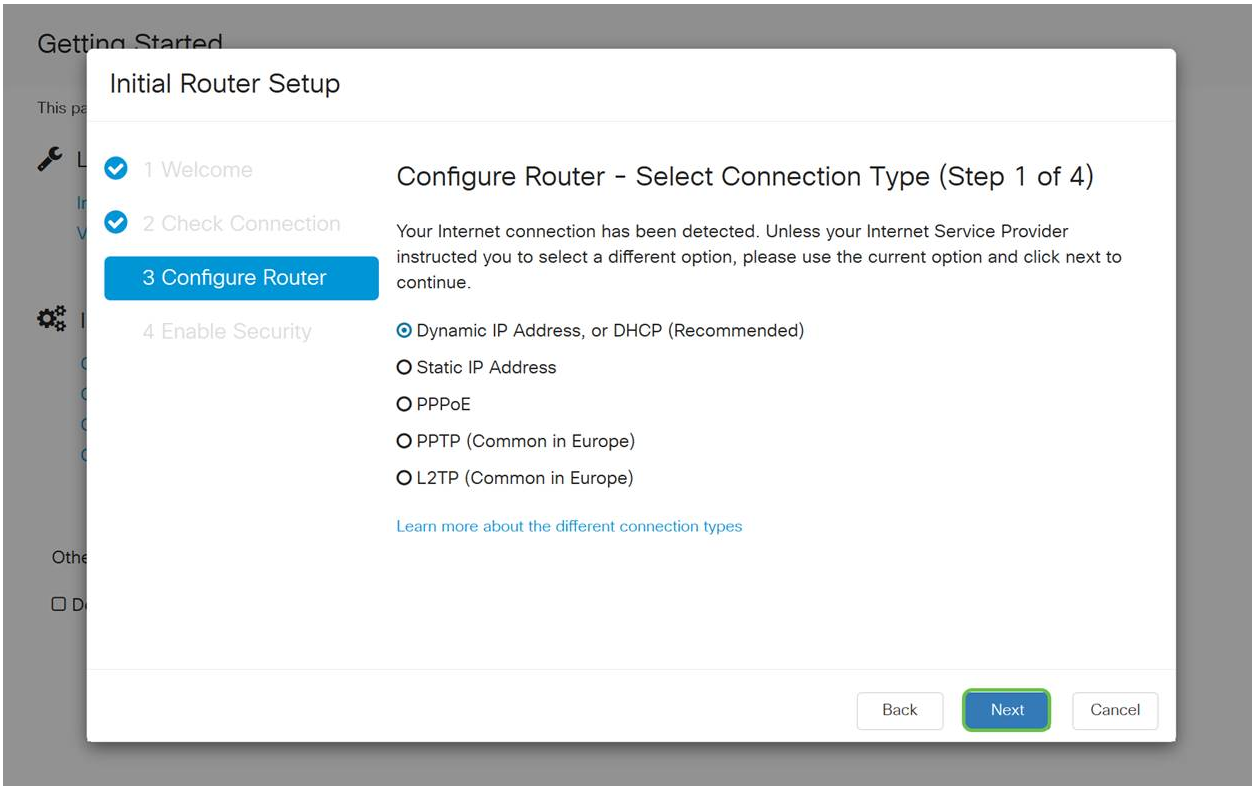
手順 3

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。



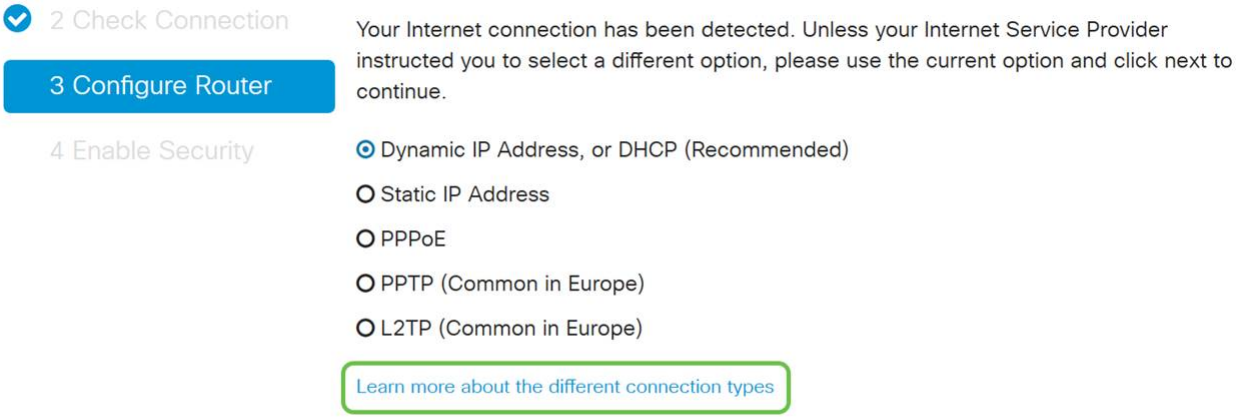
手順 4

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。



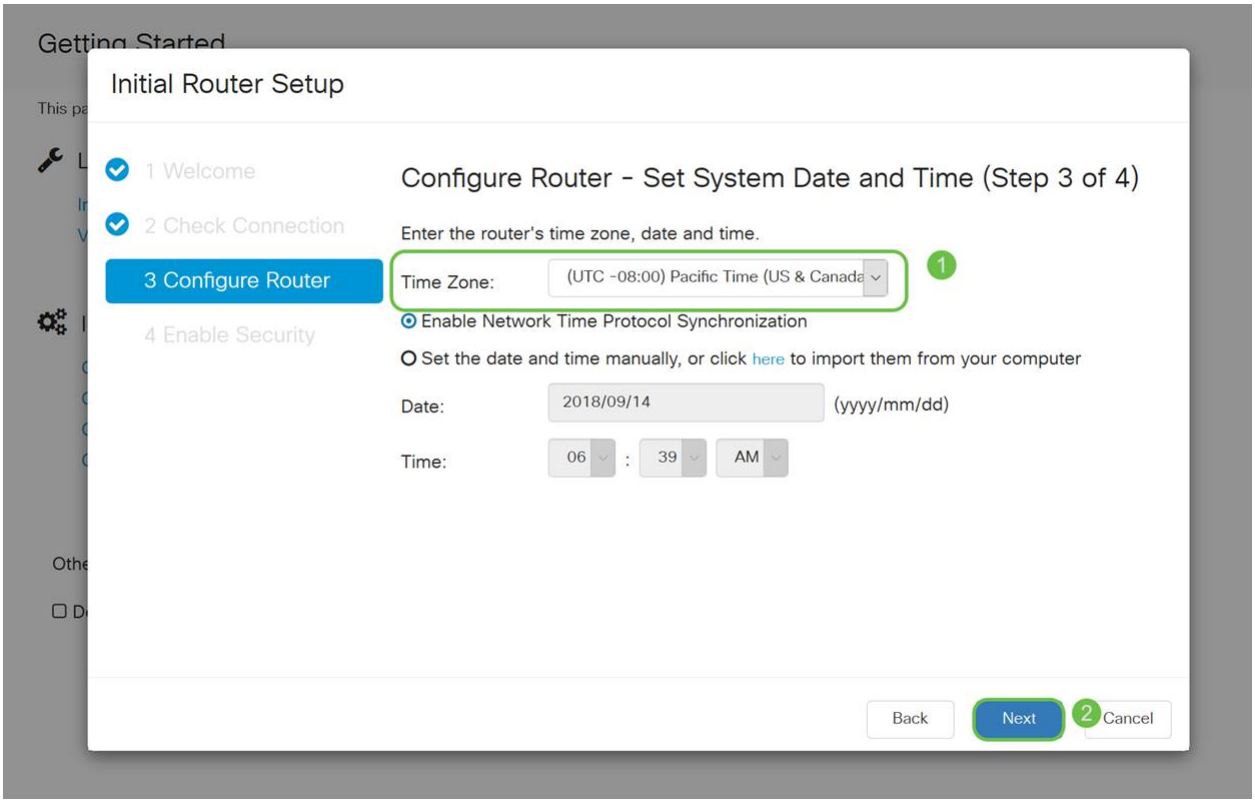
この初期設定にはDHCPを使用する必要がありますが、今後の参考として、画面下部に表示される各種の接続の種類に関する詳細を確認するように選択できます。詳細については、次を参照してください。

- 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



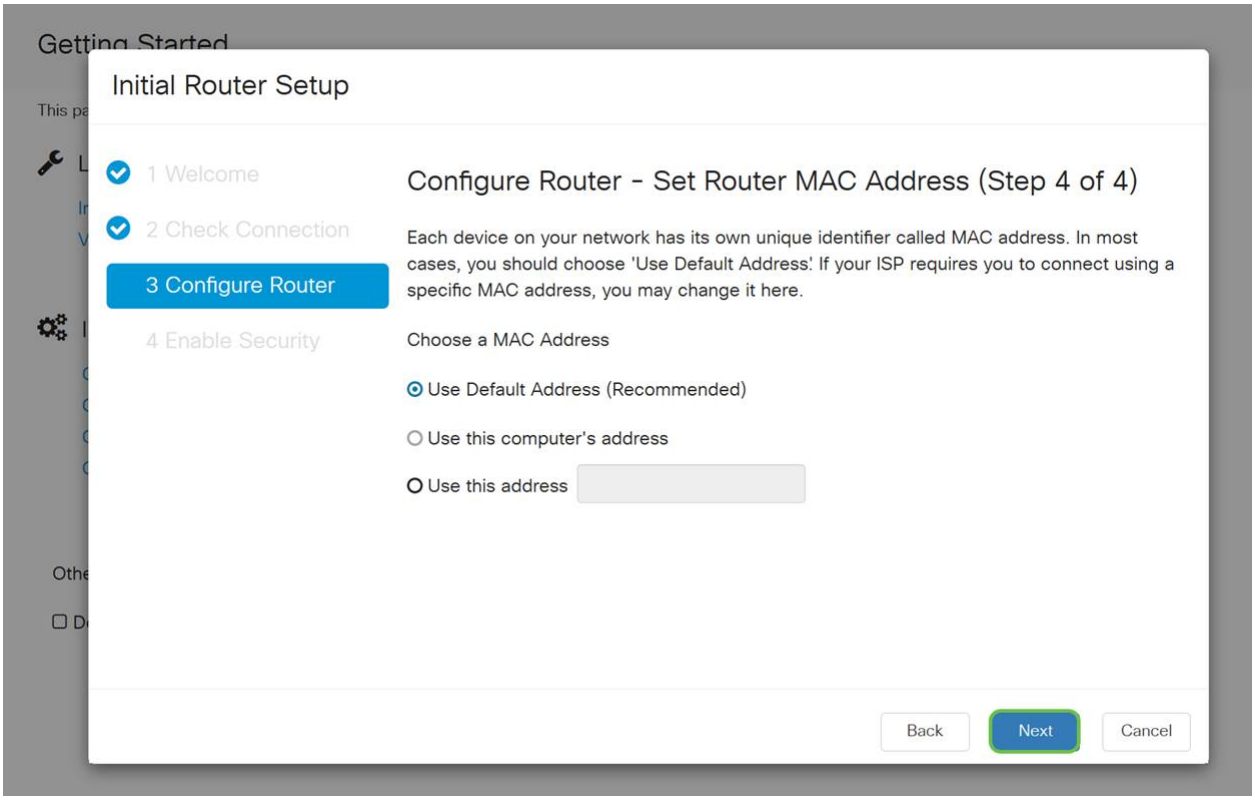
手順 5

次に、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。



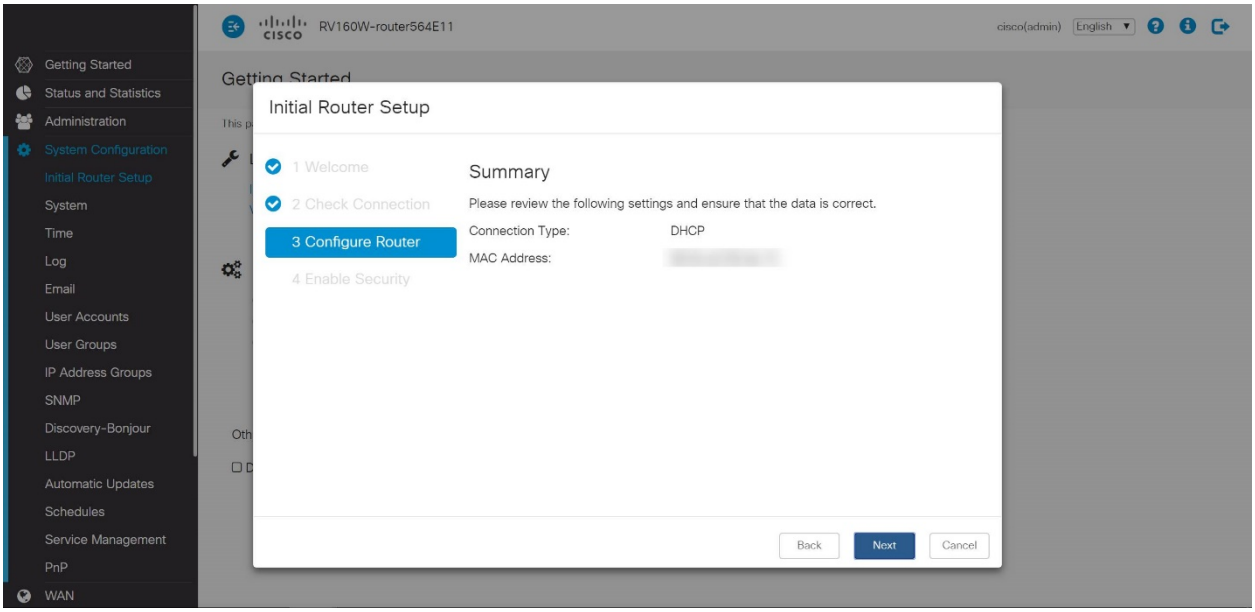
手順 6

次に、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。



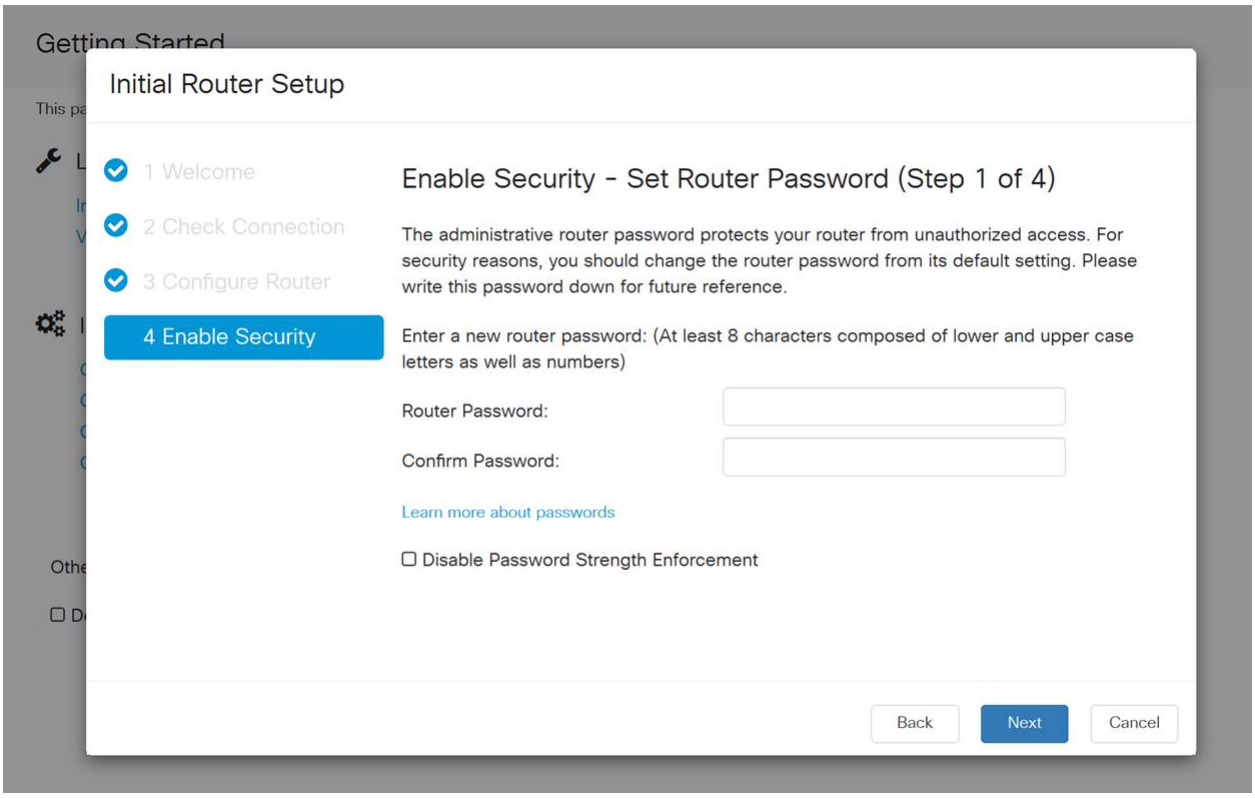
ステップ7

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）と数字を含めることです。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。今後の口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

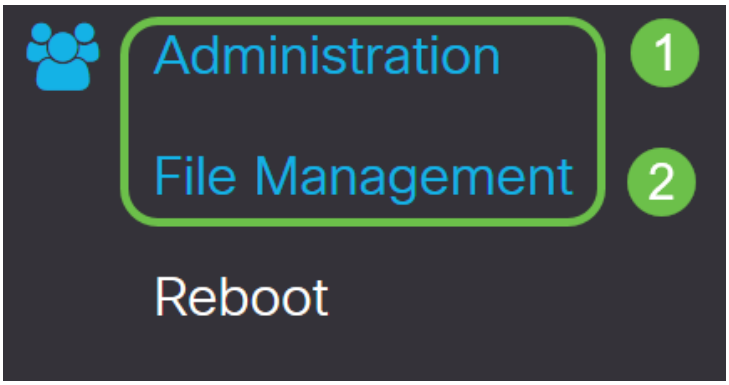
[保存]アイコンをクリックします。

必要に応じたファームウェアのアップグレード

これは重要だ飛ばすな！

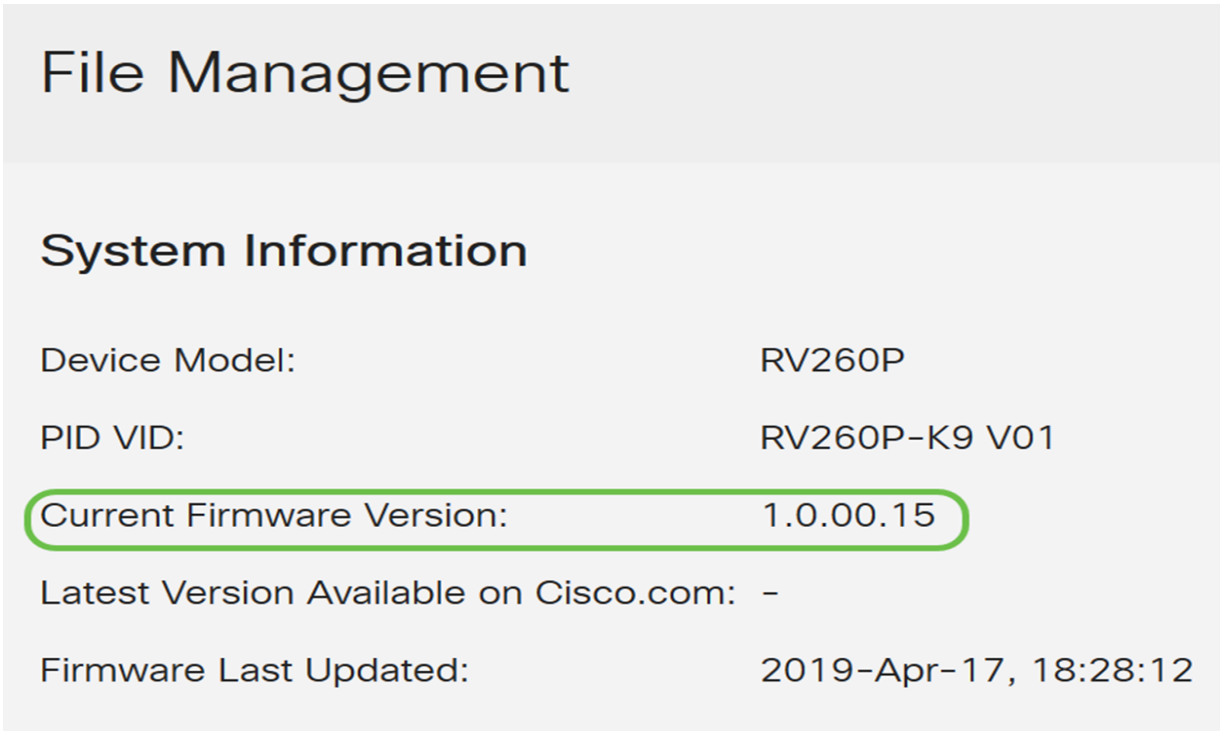
手順 1

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



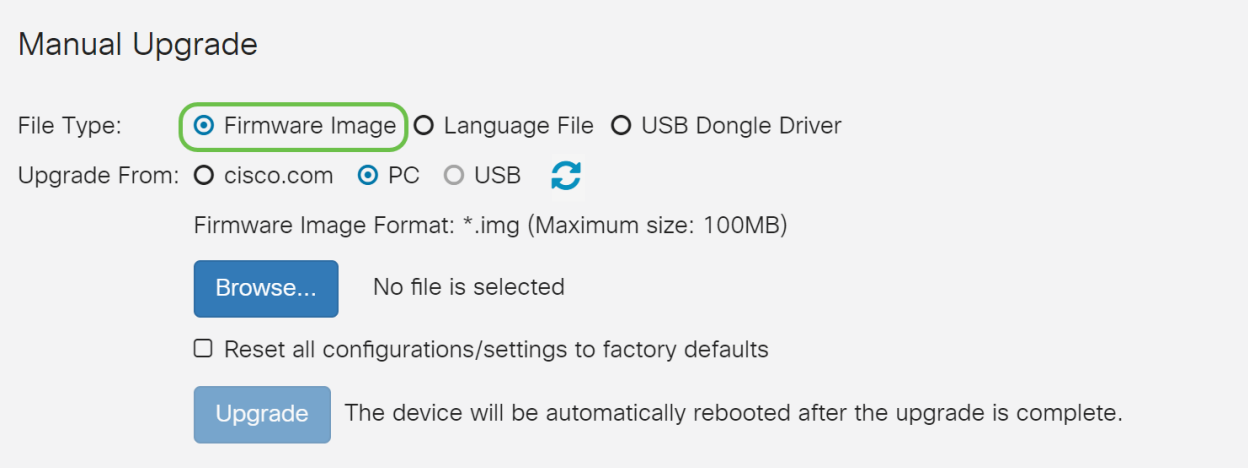
[システム情報]領域で、次のサブエリアで説明します。

- [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

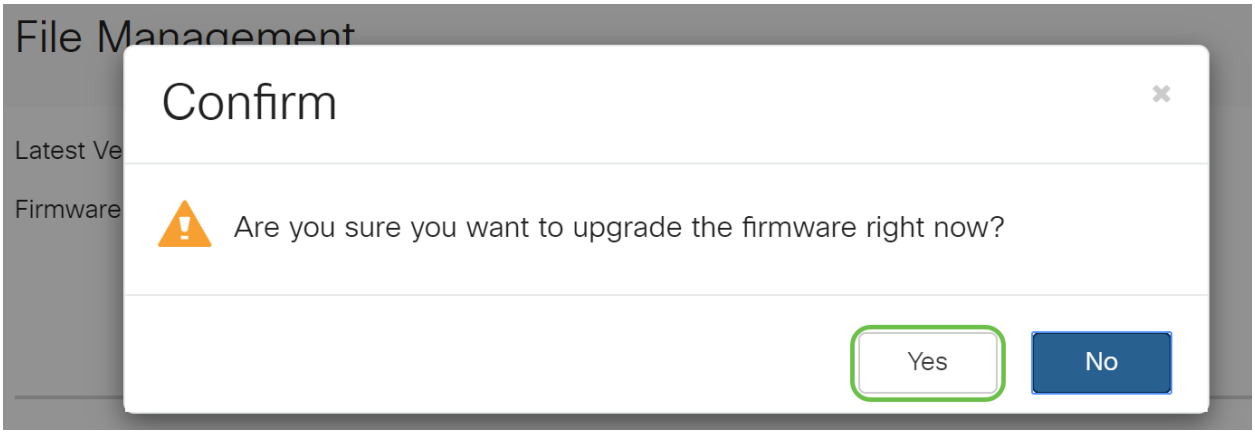
[マニュアルアップグレード]ページで、オプションボタンをクリックして*cisco.com*を選択します。これには他にもいくつかのオプションがありますが、これはアップグレードを行う最も簡単な方法です。このプロセスでは、最新のアップグレードファイルをCisco Software Downloads Webページから直接インストールします。

手順 4

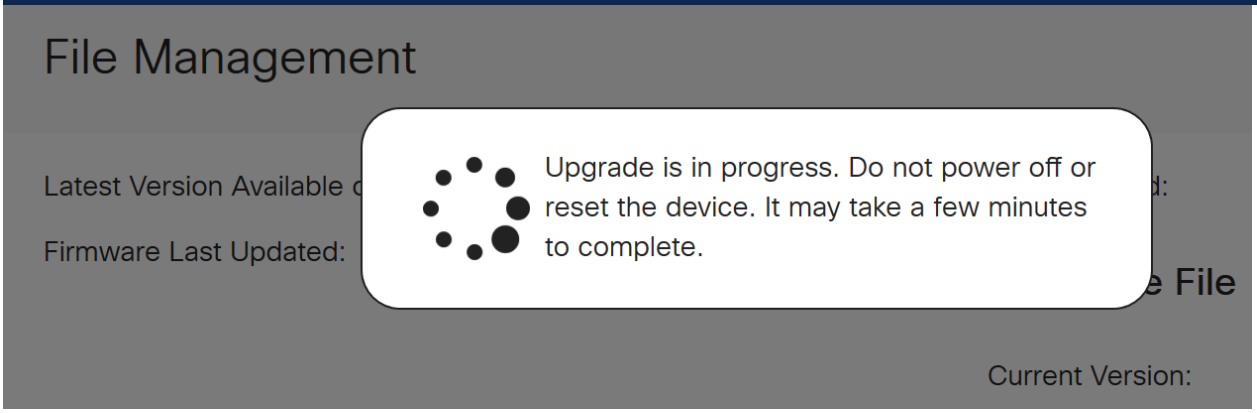
[Upgrade]をクリックします。

手順 5

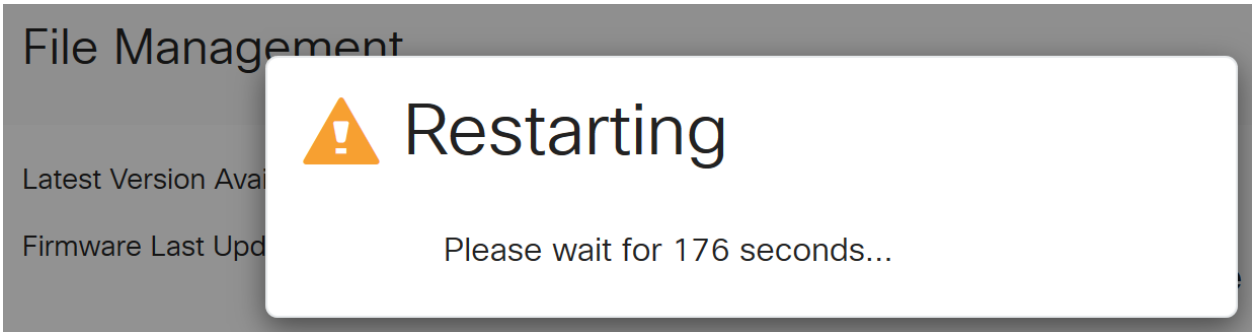
確認ウィンドウで[はい]をクリックして続行します。



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。

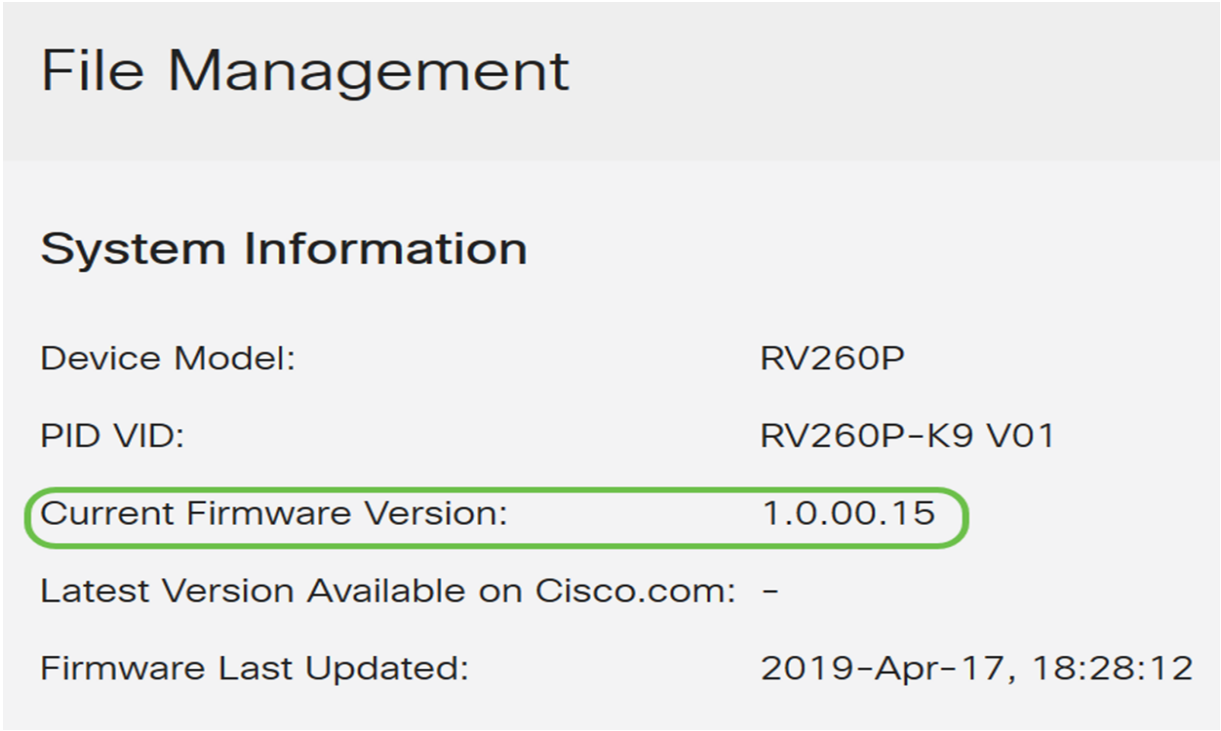


アップグレードが完了すると、通知ウィンドウがポップアップ表示され、プロセスが終了するまでの推定時間をカウントダウンしてルータが*再起動*することを通知します。その後、ログアウトされます。



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り、該当する場合は記事をスクロールし続けることを推奨します。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。

- 仮想ローカル エリア ネットワーク（VLAN）
- IPアドレスの編集
- スタティックIPアドレスの追加
- 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）

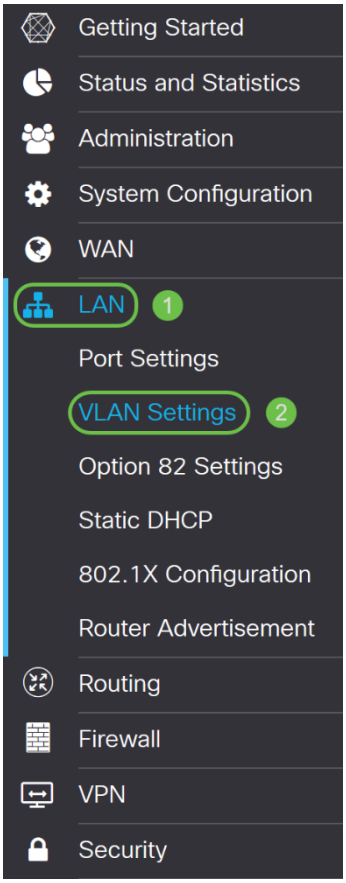
仮想ローカルエリアネットワーク(VLAN)を使用すると、ローカルエリアネットワーク(LAN)を論理的に異なるブロードキャストドメインにセグメント化できます。機密データがネットワーク上でブロードキャストされるシナリオでは、特定のVLANにブロ

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。

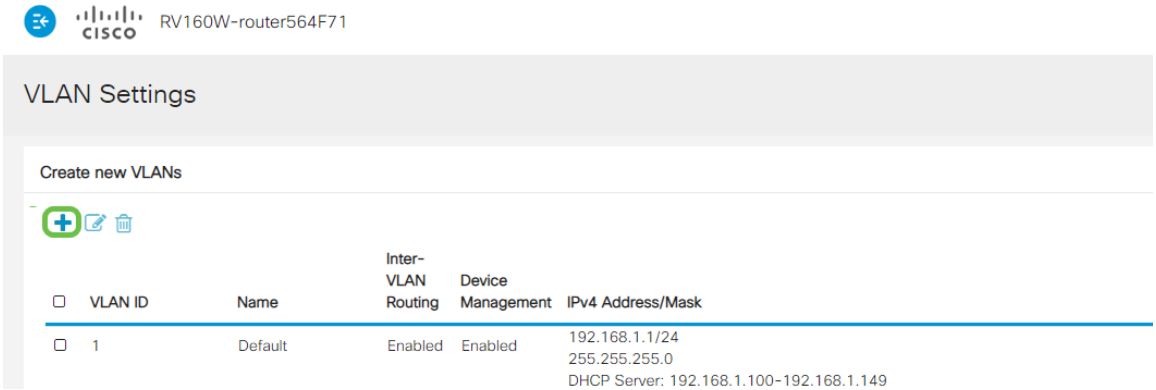
手順 1

[LAN] > [VLAN Settings]に移動します。



手順 2

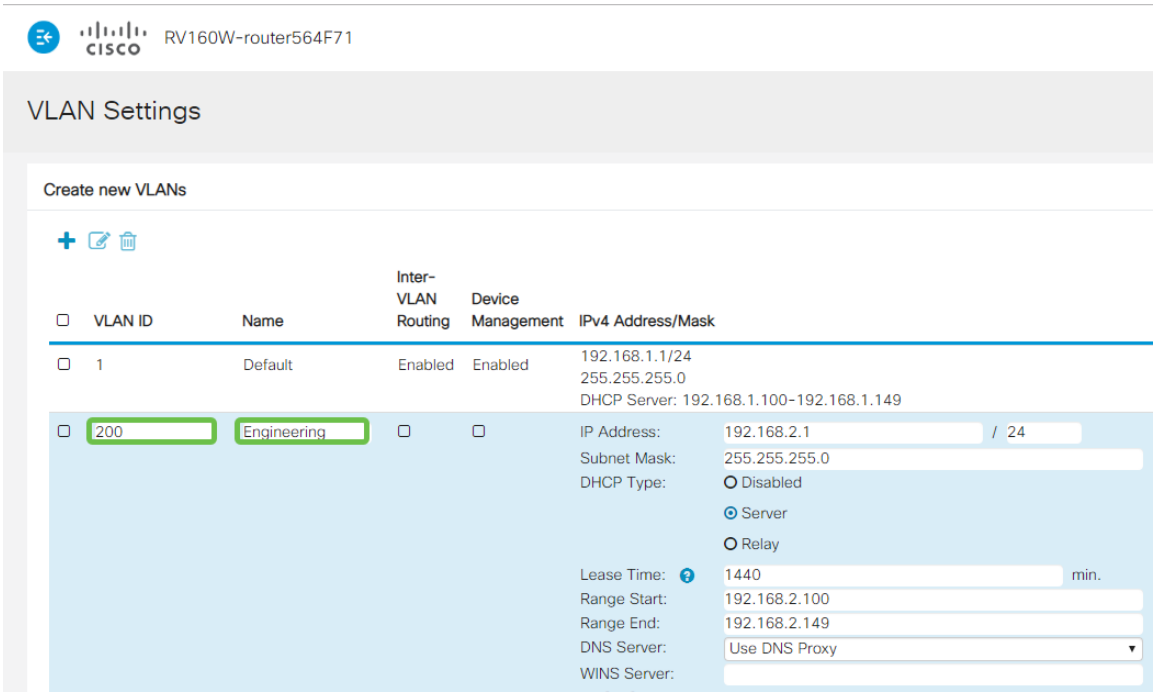
[Add]をクリックし、新しいVLANを作成します。



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。



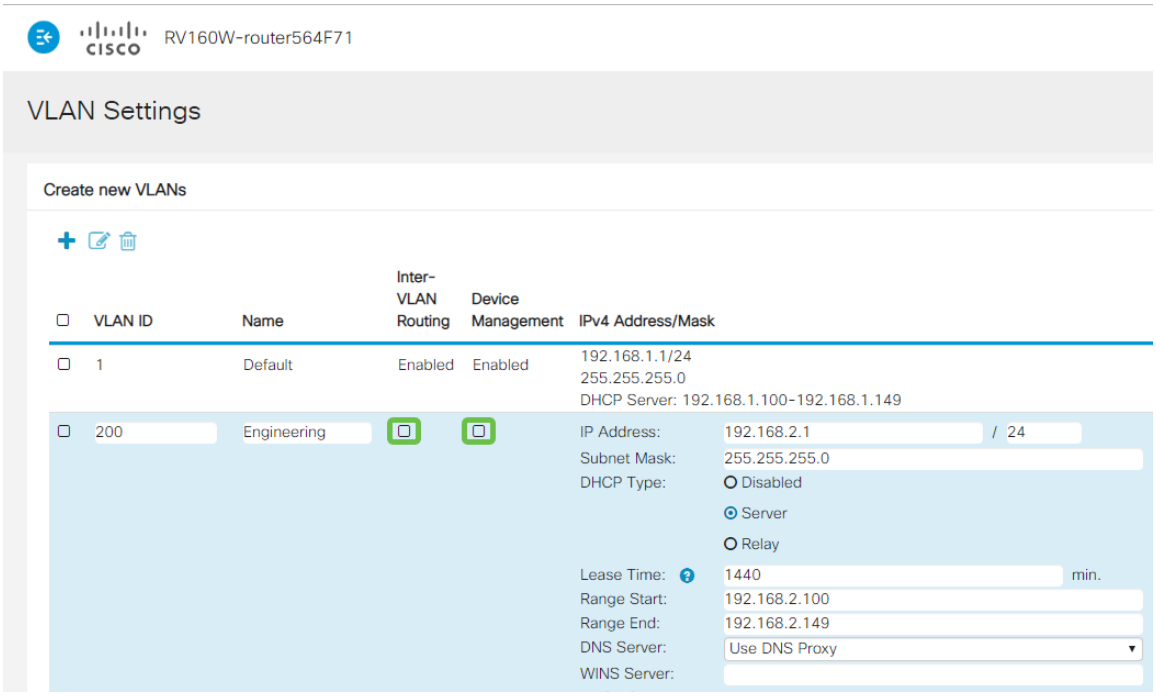
手順 4

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。

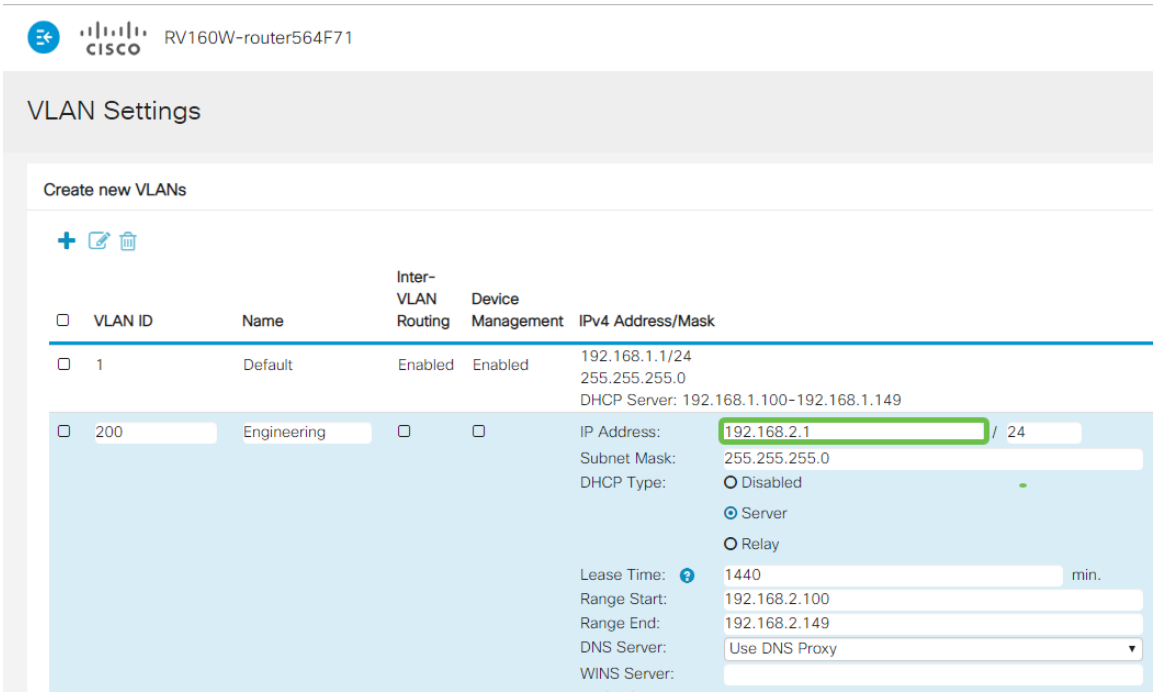
Device Managementは、ブラウザを使用してVLANからRV260PのWeb UIにログインし、RV260Pを管理できるソフトウェアです。これは、ゲストネットワークでも無効にする必要があります。

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

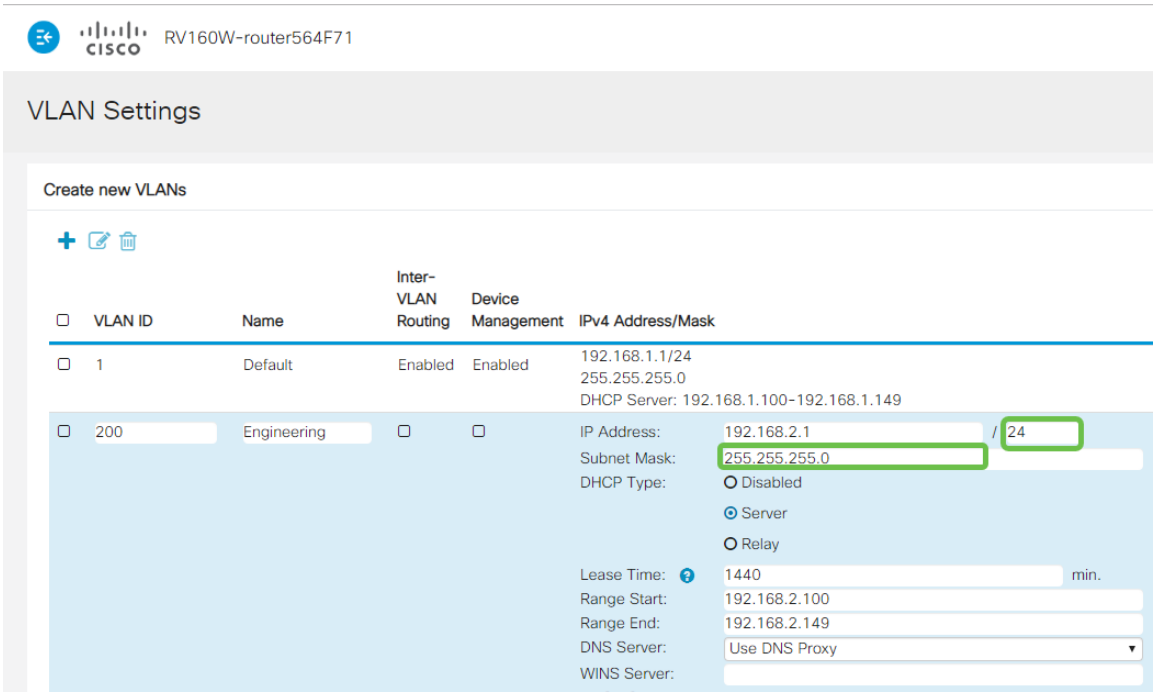
プライベートIPv4アドレスが[IPアドレス]フィールドに自*動的に入力*されます。これを調整するには、次を選択します。この例では、サブネットに192.168.2.100 ~ 192.168.2.149のIPアドレスがDHCPで使用可能です。192.168.2.1 ~ 192.168.2.99および192.168.2.150 ~ 192.168.2.254は、スタティックIPアドレスに使用できます。



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。**



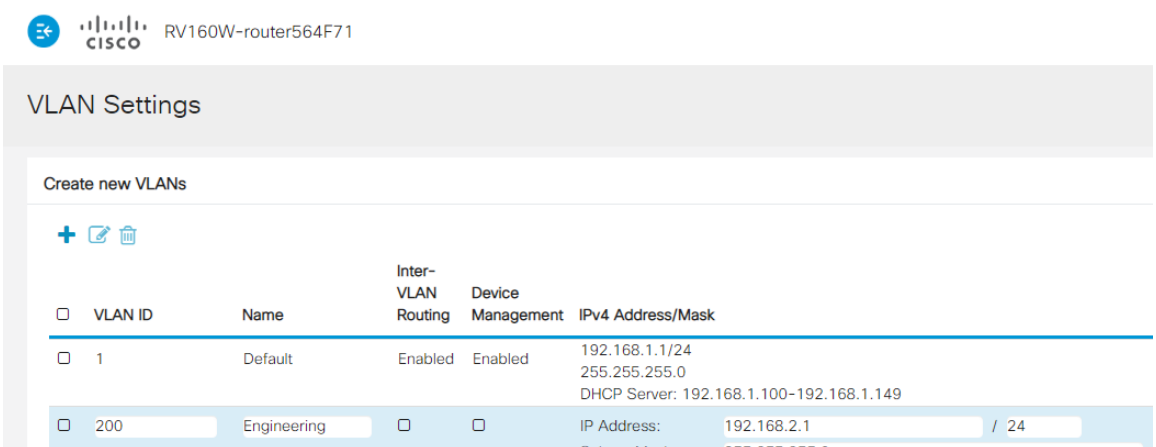
ステップ7

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。

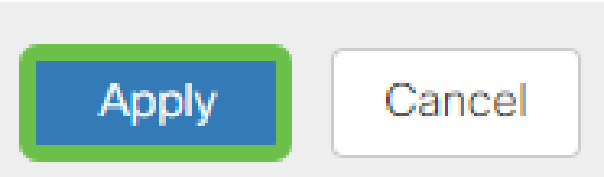
Server : これは最もよく使用されるオプションです。

- [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:

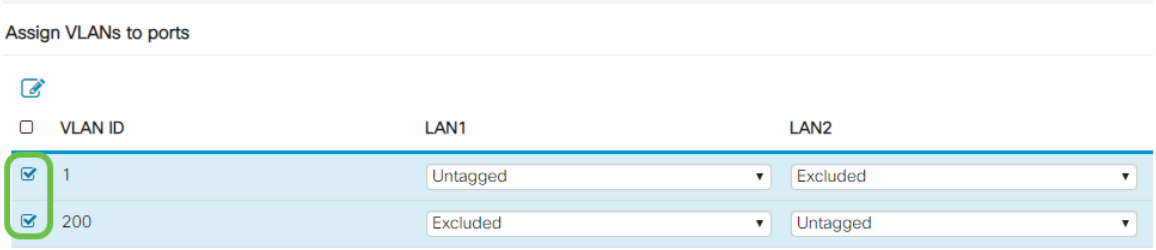
- トランクポートと見なされます。
- いずれかのVLANに[Untagged]というラベルを付けることができます。
- トランクポートの一部である残りのVLANには、[Tagged]というラベルを付ける必要があります。
- トランクポートの一部ではないVLANには、そのポートに対して[Excluded]というラベルを付ける必要があります。

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。

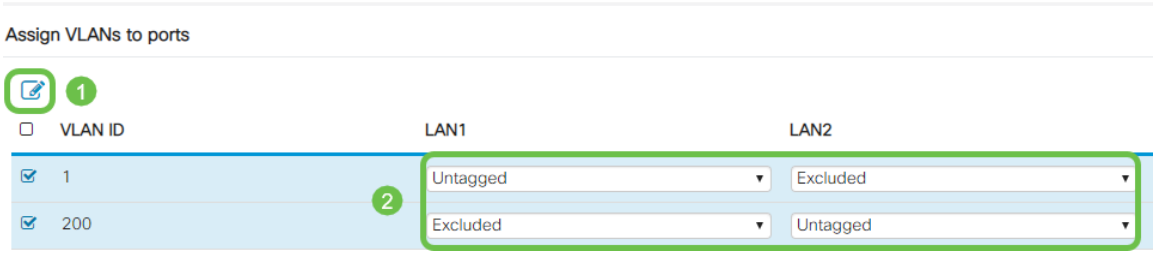
この例では、VLAN 1と*VLAN* 200を*選択*しています。



手順 10

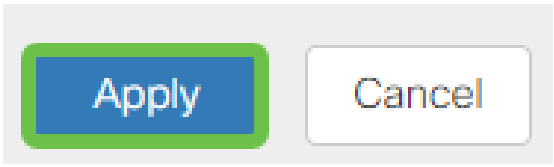
VLANをLANポートに割り当て、[Edit]をクリックし、それぞれの設定を[*Tagged*]、[*Untagged*]、または[*Excluded*]に指定します。

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](#)。

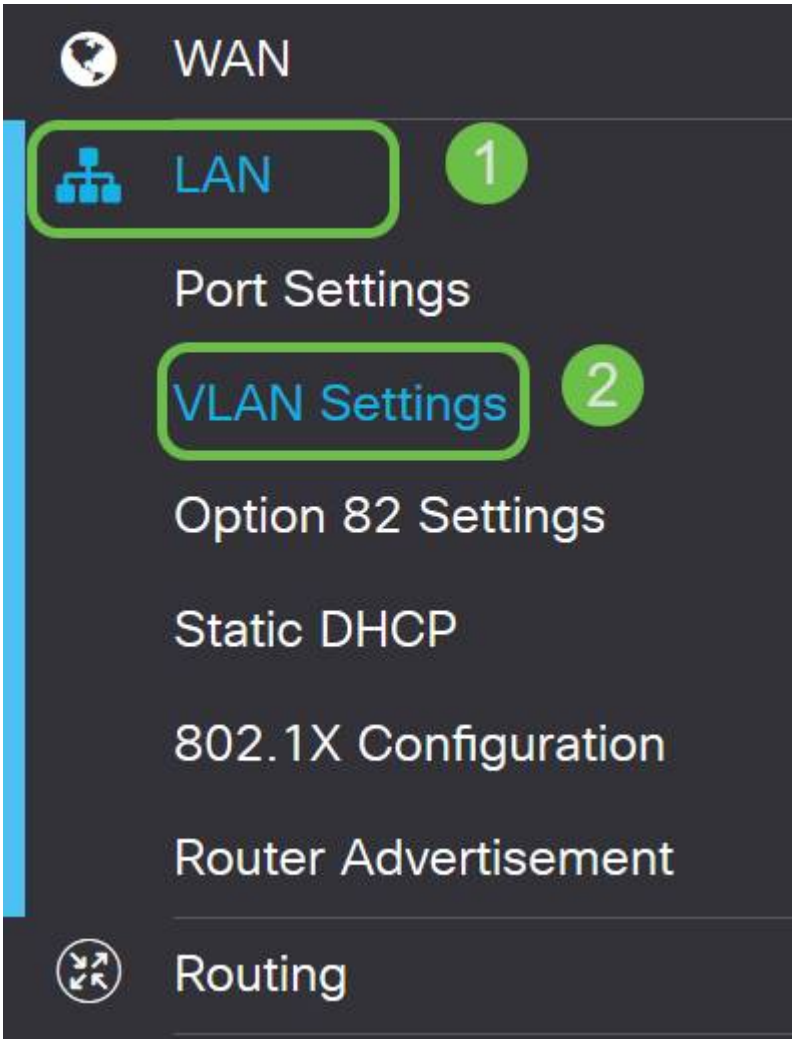
IPアドレスの編集（オプション）

*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。

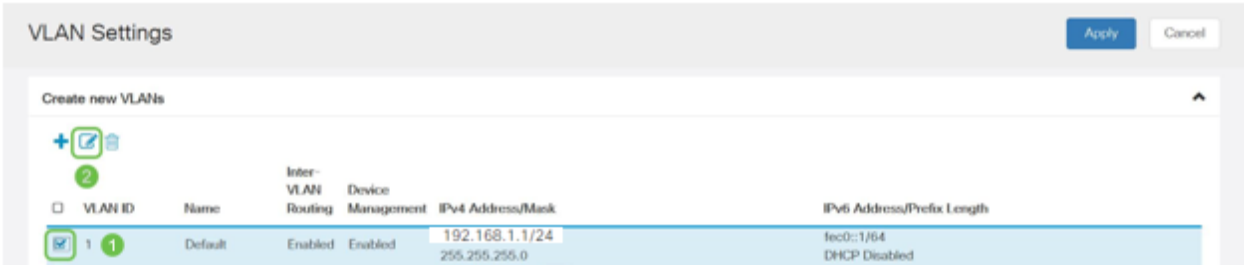
手順 1

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



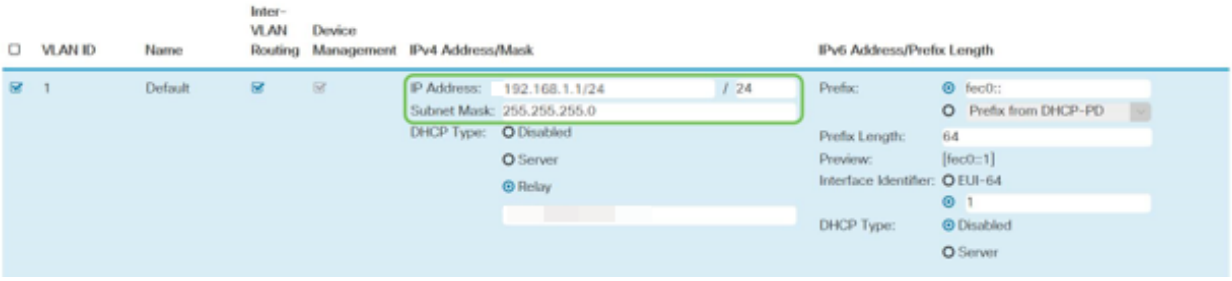
手順 2

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。



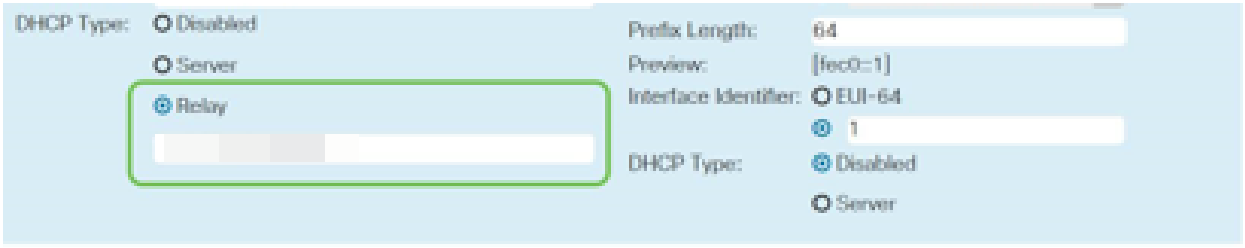
手順 3

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。



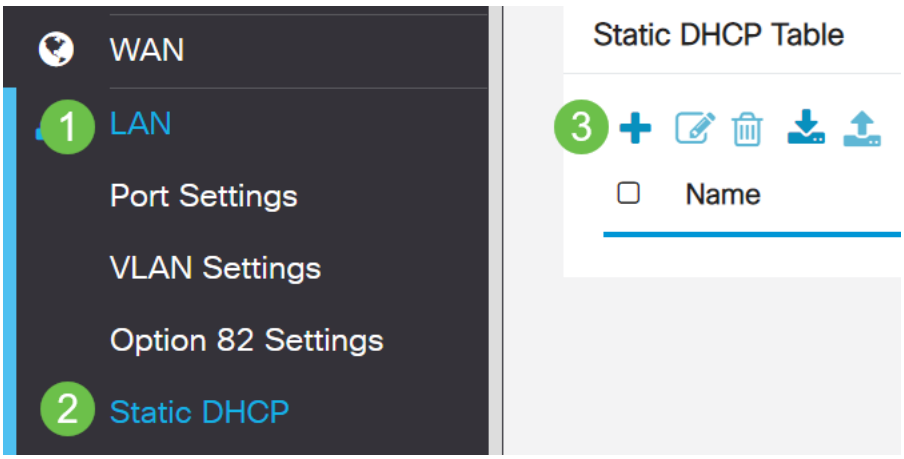
スタティックIPの追加 (オプション)

特定のデバイスを他のVLANに到達可能にするには、そのデバイスにスタティックIPアドレスを割り当て、アクセスルールを作成してアクセスできるようにします。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。

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。

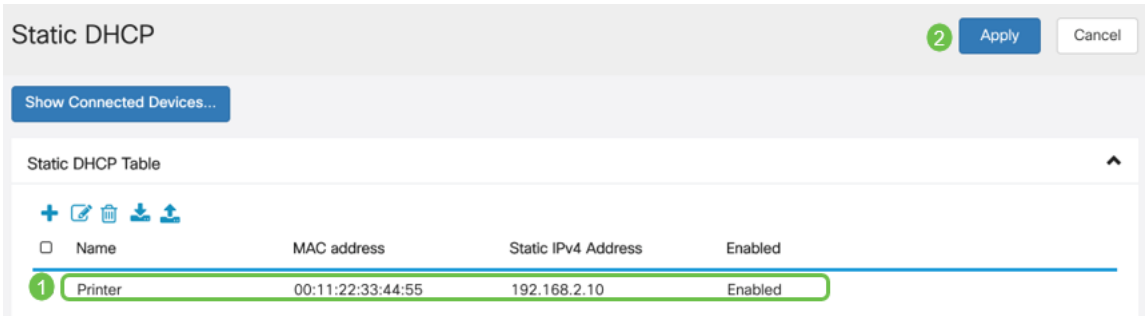
手順 1

[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。



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でのスタティックIPアドレスの設定のベストプラクティス』を参照してください。

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、『RV160およびRV260ルータのリブートおよび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。

140ACモバイルアプリケーションワイヤレスアクセスポイントのセットアップ

このセクションでは、モバイルアプリケーションを使用してモバイルアプリケーションワイヤレスアクセスポイントを設定します。

アプリケーションの更新が頻繁に行われ、外観/レイアウトが時間とともに変化する可能性があることに注意してください。

140ACの背面で、APに付属のケーブルを140 ACの黄色いPoEプラグに差し込みます。もう一方の端をRV260P LANポートの1つに差し込みます。

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

Google PlayまたはApple App Storeで入手できるCisco Business Wireless Appをモバイルデバイスにダウンロードしてください。次のいずれかのオペレーティングシステムが必要です。

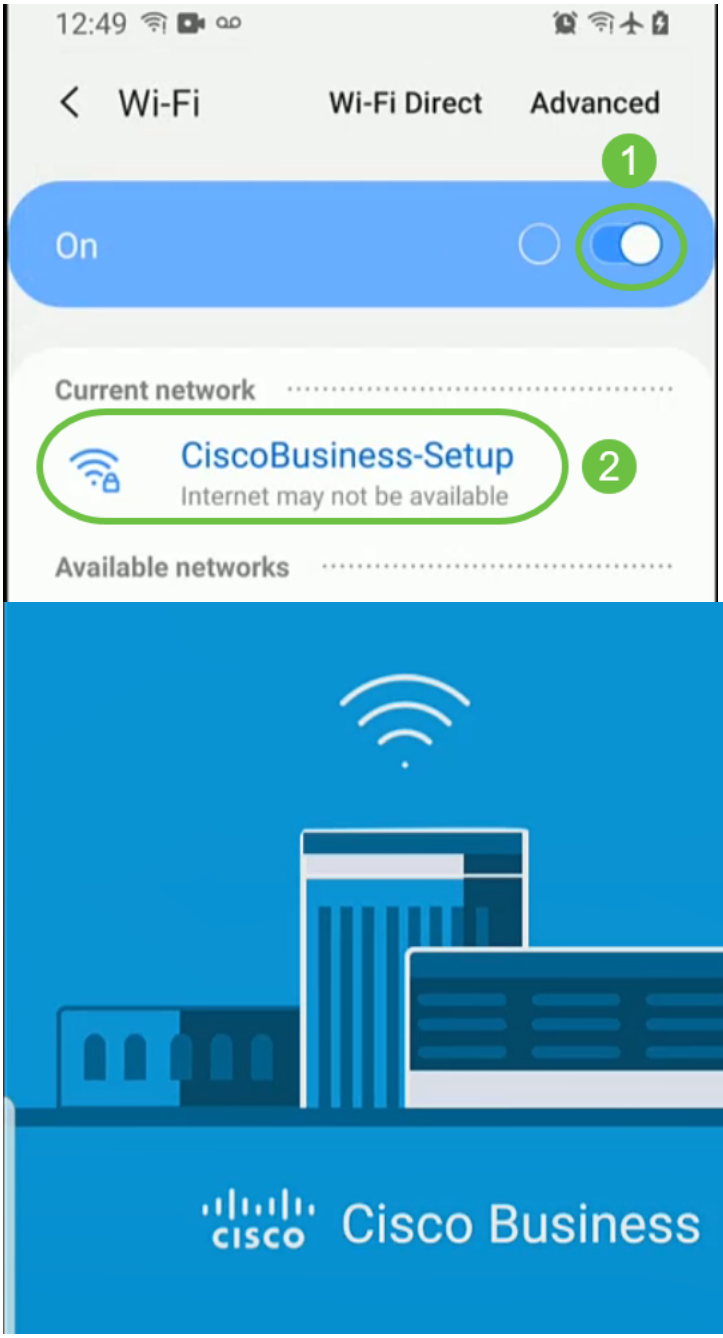
- Androidバージョン5.0以降
- iOSバージョン8.0以降

手順 2

モバイルデバイスでCisco Business Wirelessアプリケーションを開きます。

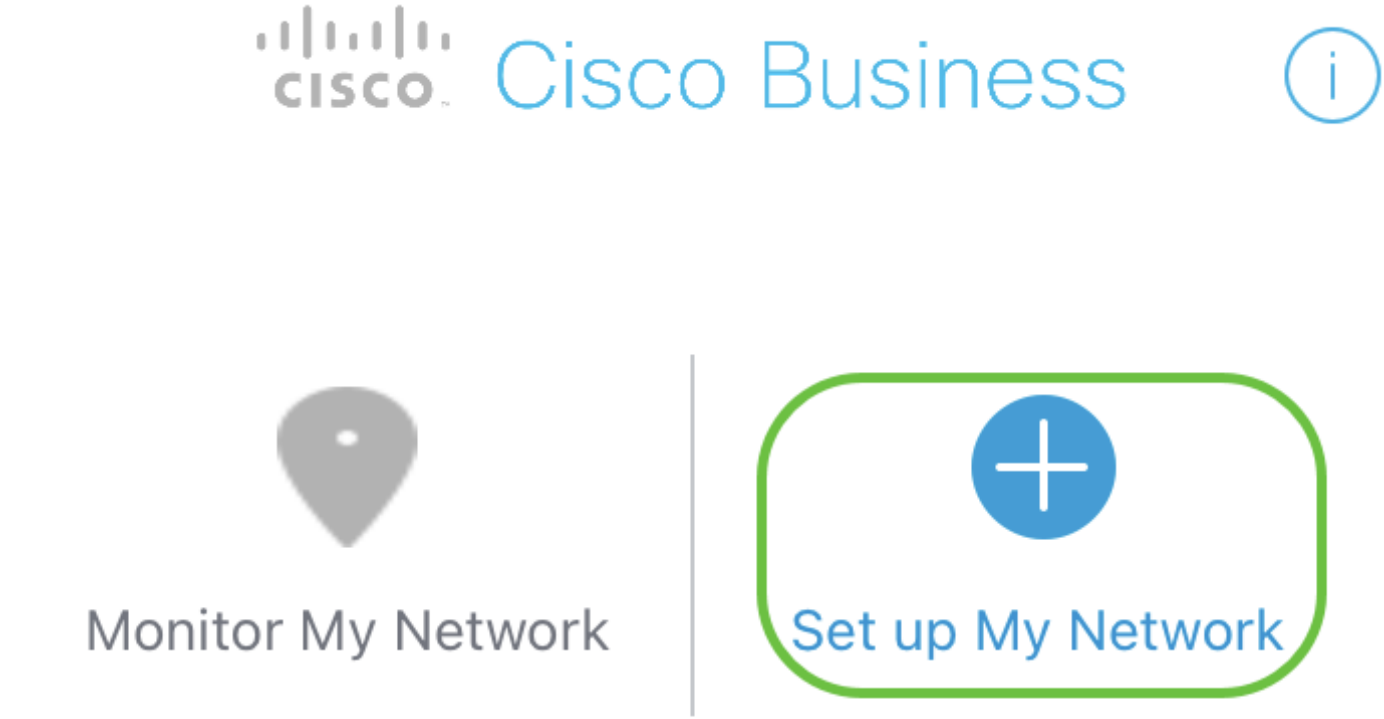
手順 3

モバイルデバイスのCiscoBusiness-Setupワイヤレスネットワークに接続します。パスフレーズはcisco123です。



手順 4

アプリがモバイルネットワークを自動的に検出します。[マイネットワークの設定]を選択します。



手順 5

ネットワークをセットアップするには、次のように入力します。

- *管理者ユーザ名の作成*
- *管理者パスワードの作成*
- *管理者パスワードを再入力*して確認します。
- （オプション）[パスワードの表示]チェックボックスをオンにします。

[はじめに]を選択します。

1 Name and Place

Primary AP Name

1 TestAP

Country

2 United States (US)

Date and Time

3 04/09/2021 05:05:37 PM

Timezone

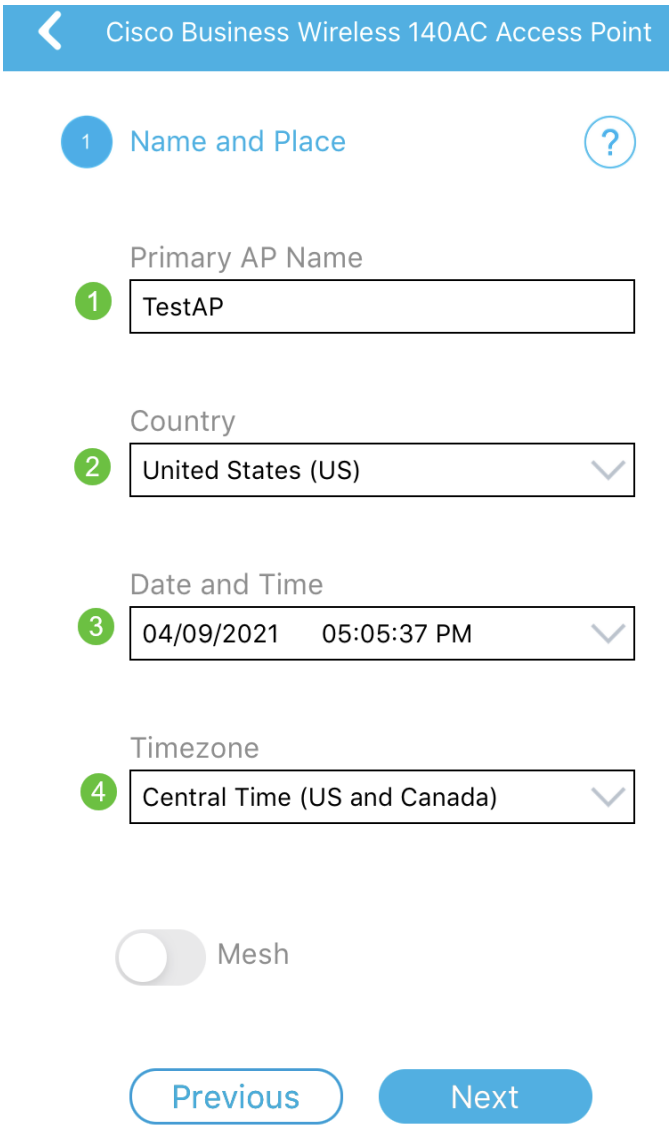
4 Central Time (US and Canada)

Mesh

手順 6

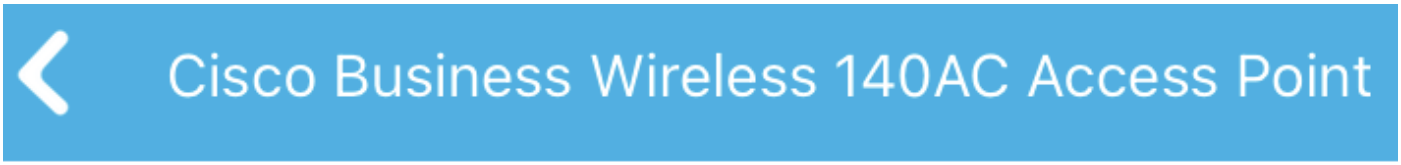
名前と場所を設定するには、次の情報を正確に入力します。競合する情報を入力すると、予期しない動作が発生する可能性があります。

- *ワイヤレスネットワークのモバイルアプリケーションAP名。*
- *Country*
- *日付*
- *時間*
- *TimeZone*



ステップ7

[メッシュ]の切り替えをオンにします。[next] をクリックします。



1 Name and Place

Primary AP Name

TestAP

Country

United States (US)

Date and Time

04/09/2021 05:05:37 PM

Timezone

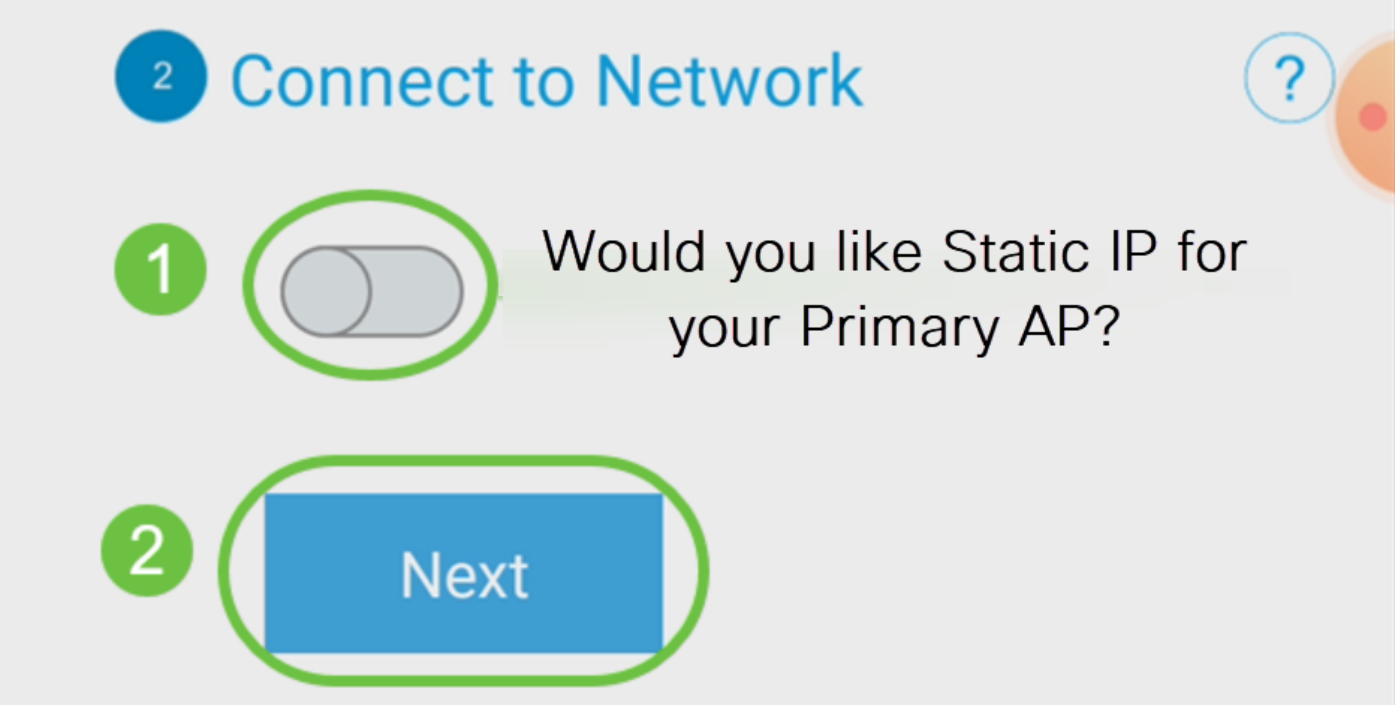
Central Time (US and Canada)

1

Mesh

手順 8

（オプション）管理のために、モバイルアプリケーション*APのスタティックIPを有効にすることもできます。*そうでない場合、DHCPサーバはIPアドレスを割り当てます。アクセスポイントのスタティックIPを設定しない場合は、[**Next**]をクリックします。

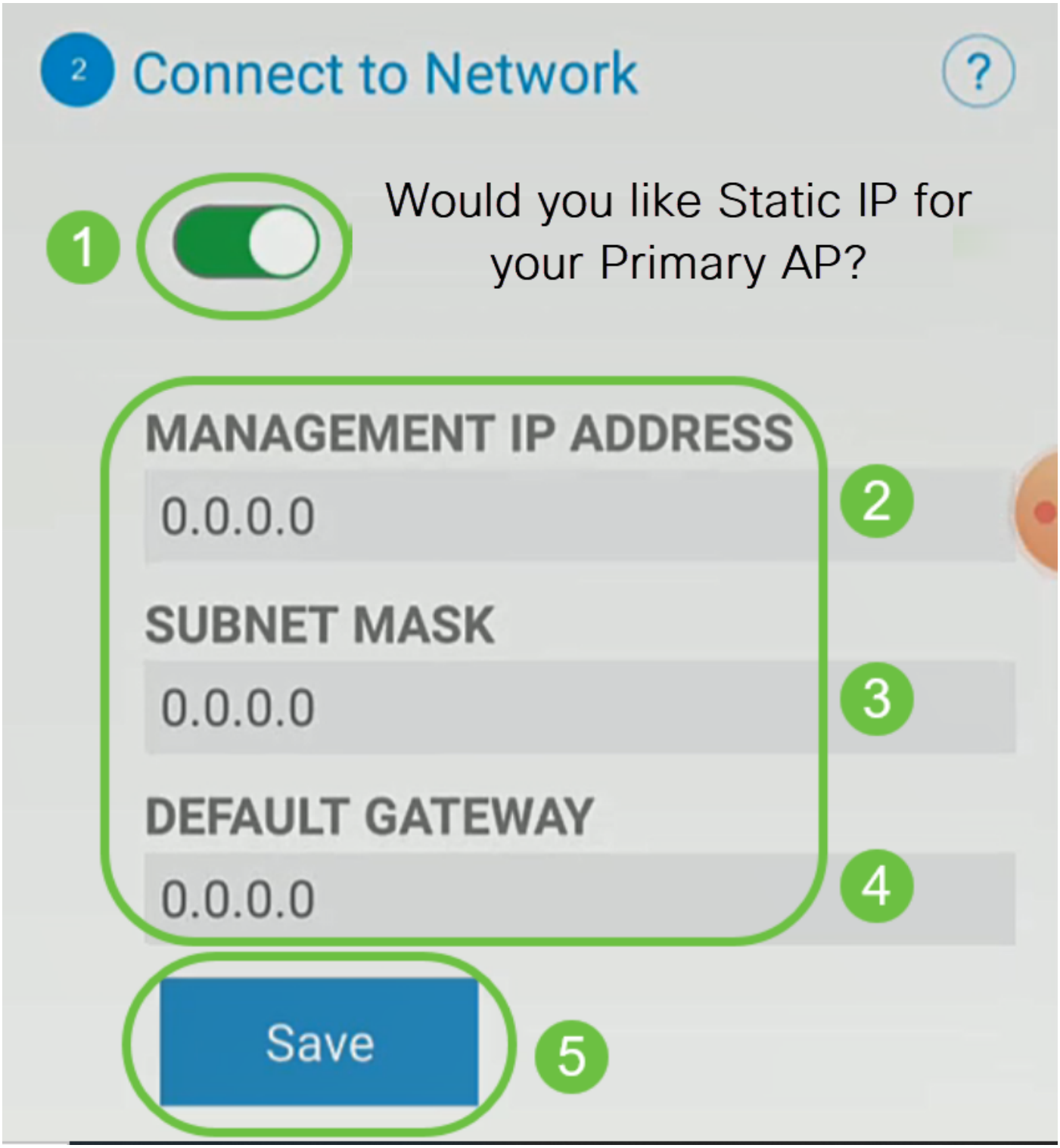


または、ネットワークに*接続するには*:

モバイルアプリケーション*APの[Static IP]を選択します。*デフォルトでは、このオプションは**無効です。**

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

[Save] をクリックします。

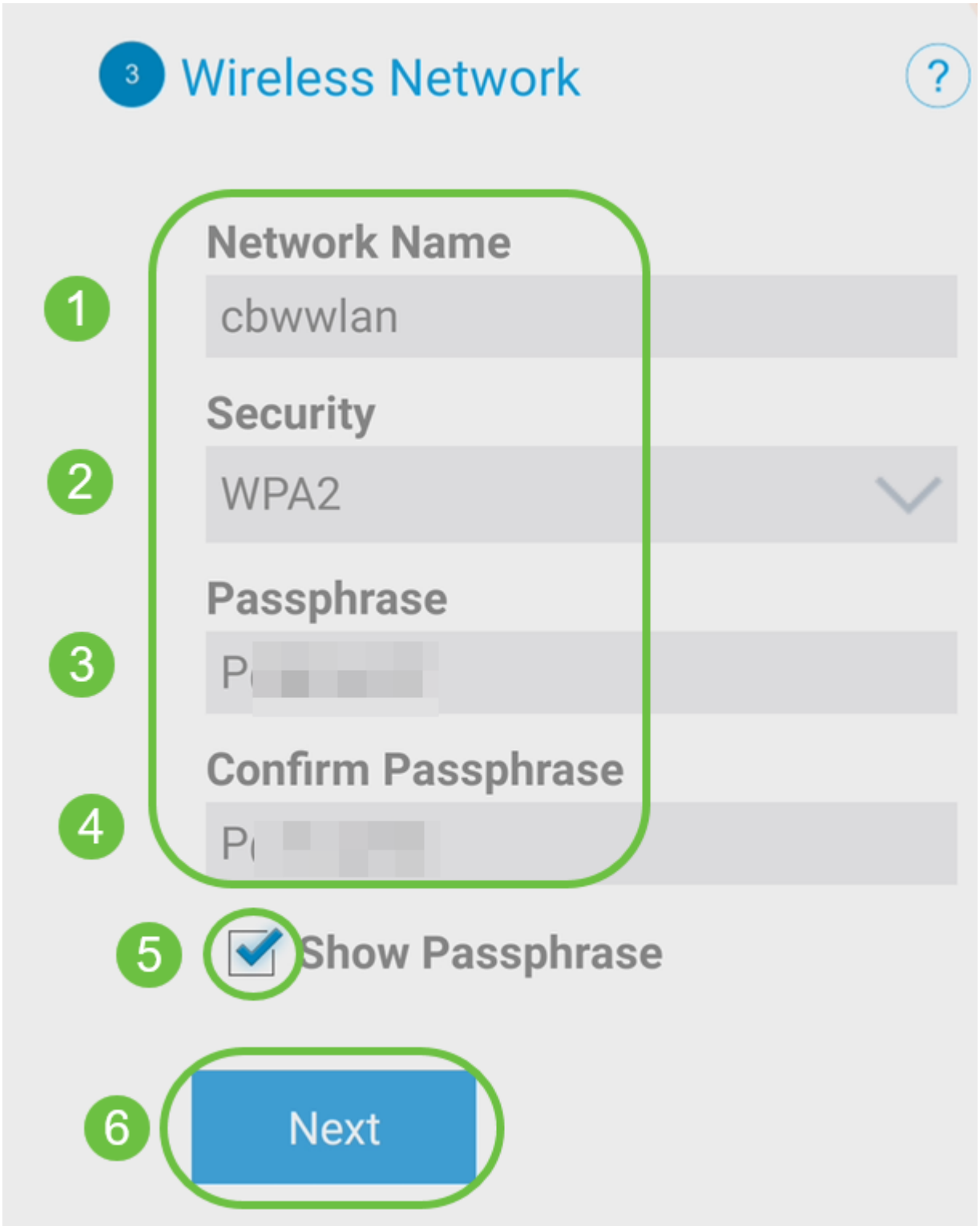


手順 9

次のコマンドを入力して、ワイヤレス・ネットワークを構成します。

- *ネットワーク名/SSID*
- *セキュリティ*
- *パスフレーズ*
- *パスフレーズの確認*
- （オプション）*Show Passphraseをオンにします*

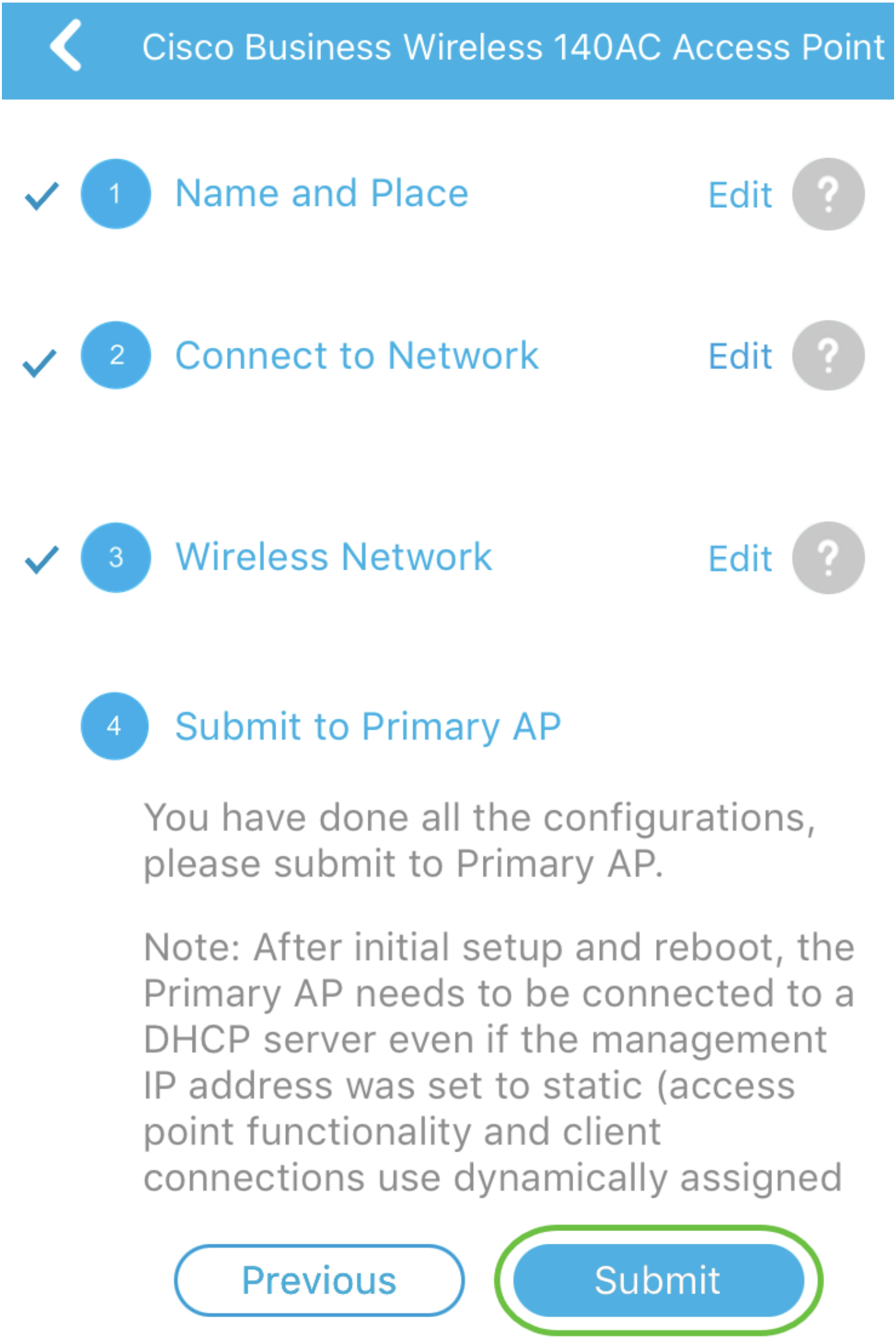
[next] をクリックします。



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。

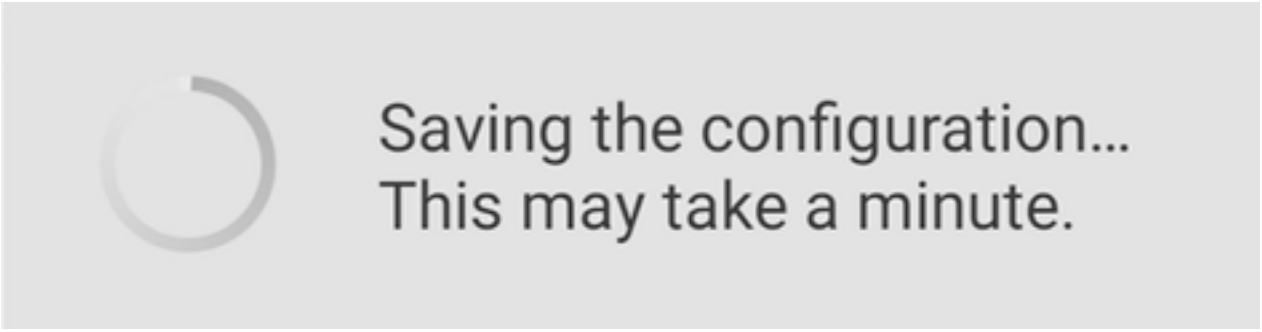
手順 10

[Submit to *Mobile Application AP*]画面の設定を*確認するには、*[Submit]をクリックします。


Cisco Business Wireless 140AC Access Point
1
Name and Place
Edit
2
Connect to Network
Edit
3
Wireless Network
Edit
4
Submit to Primary AP
You have done all the configurations, please submit to Primary AP.
Note: After initial setup and reboot, the Primary AP needs to be connected to a DHCP server even if the management IP address was set to static (access point functionality and client connections use dynamically assigned
Previous
Submit

手順 11

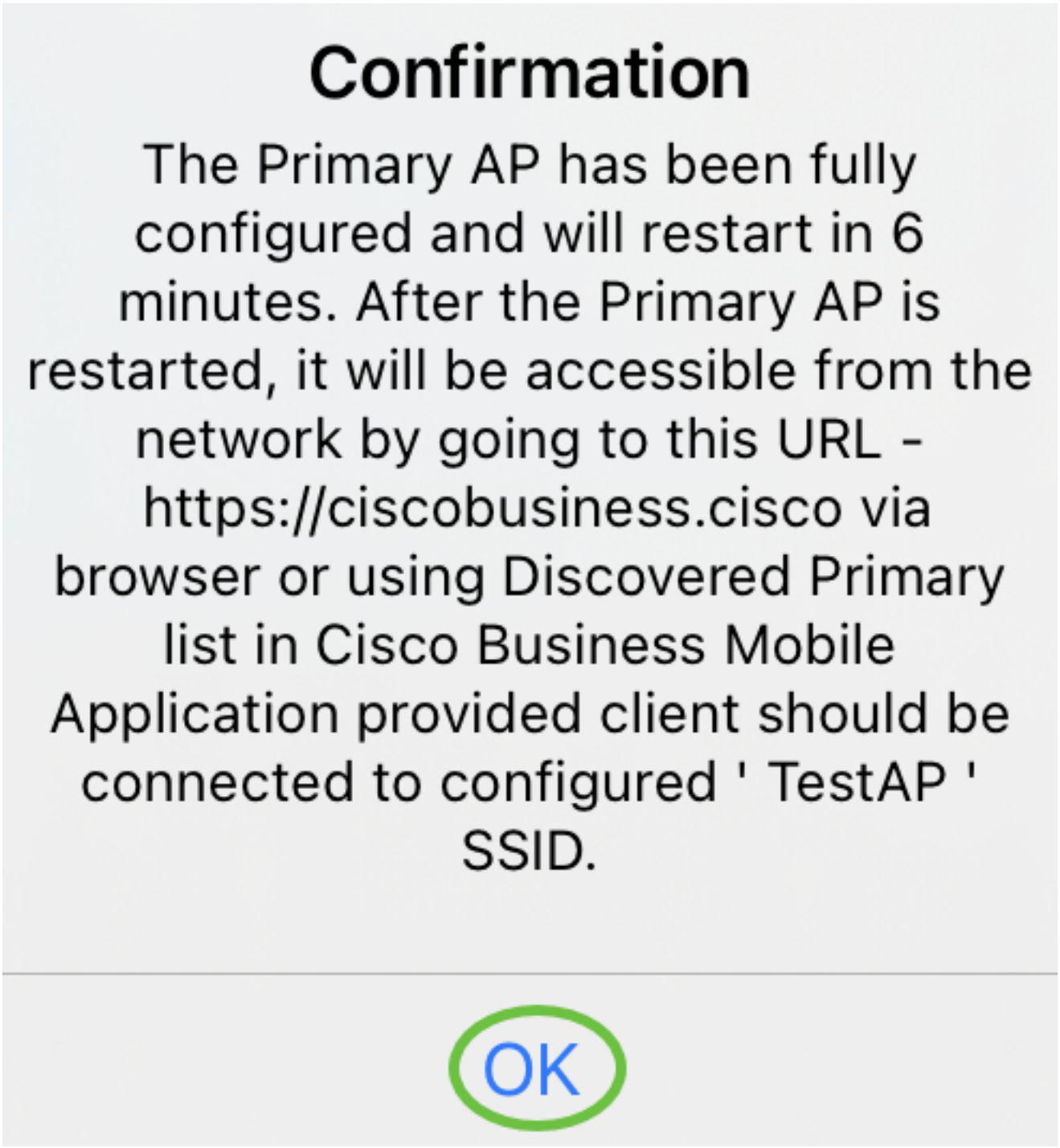
リブートが完了するまで待ちます。



リブートには最大10分かかります。リブート中に、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。

ステップ 12

次の[確認]画面が表示されます。[OK] をクリックします。



手順 13

アプリを閉じ、新しく作成したワイヤレスネットワークに接続し、再起動してワイヤレスネットワークの最初の部分を正常に完了します。

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。モバイルアプリケーションAPを見つけるには、これを無効にする必要があります。

- https://<モバイルアプリケーションAPのIPアドレス>を使用して、モバイルアプリケーションAPにログインします。
- 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、[開く]メニューをクリックし、*[Help] > [Troubleshooting Information]を選択し*ます。

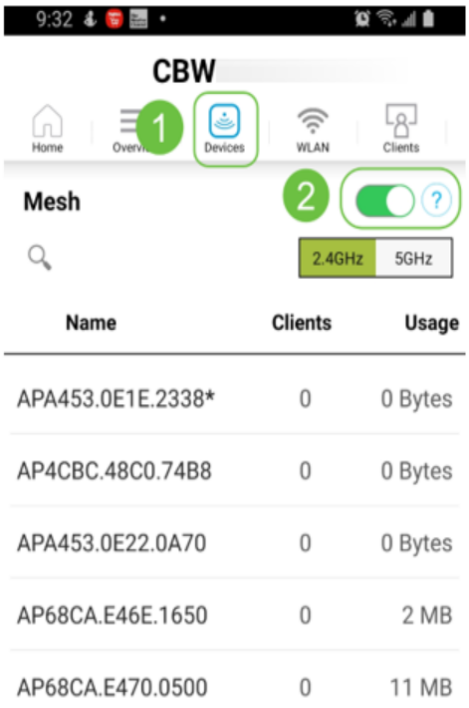
CBW142ACMメッシュエクステンダの設定

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。

モバイルデバイスでCisco Businessアプリにログインします。

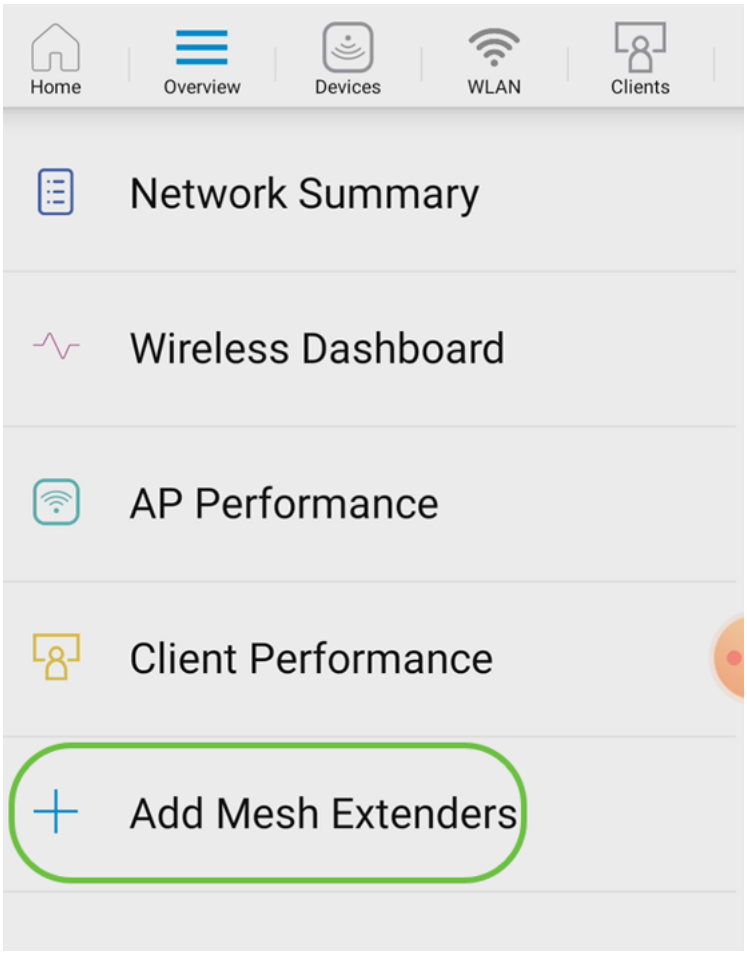
手順 1

[デバイス]に**移動します**。[メッシュ]が有効になっていることを*ダブルチェック*してください。



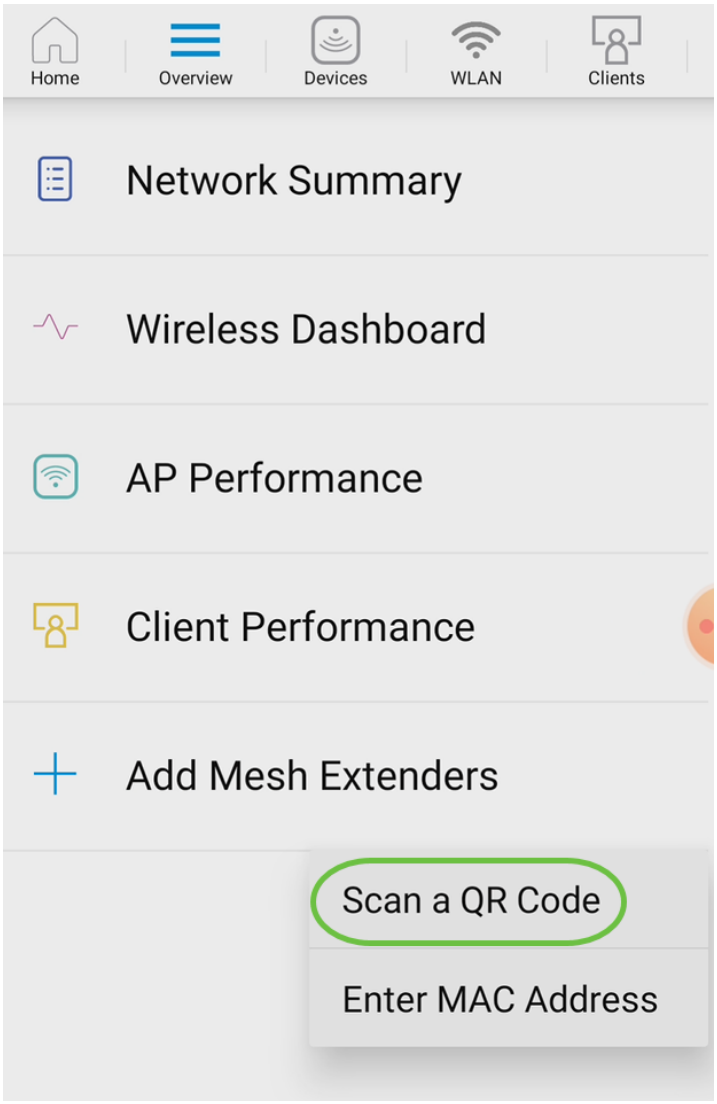
手順 2

モバイルアプリケーションAPのメッシュネットワークで使用するすべてのメッシュエクステンダのMACアドレスを入力する必要があります。MACアドレスを追加するには、メニューから**Add Mesh Extendersを**クリックします。



手順 3

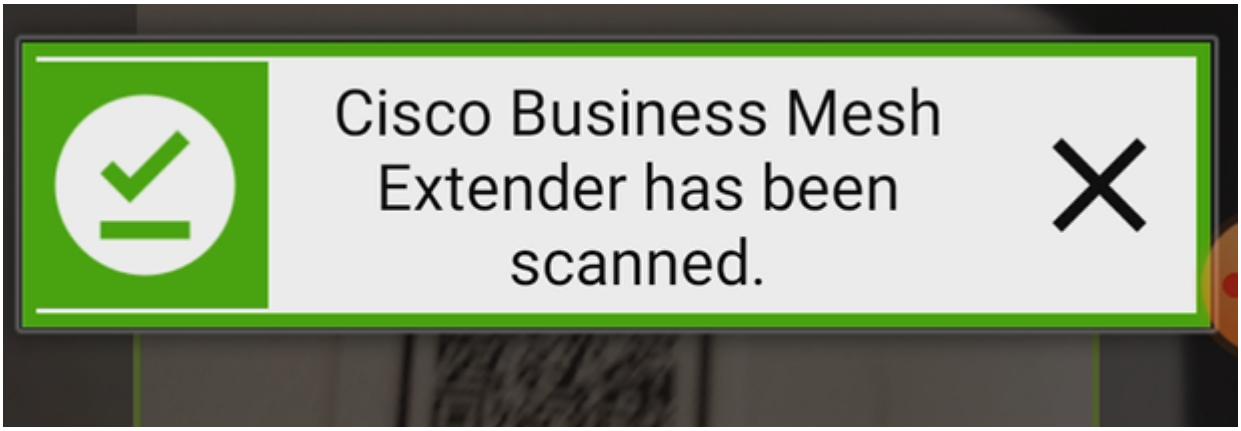
MACアドレスを追加するには、QRコードをスキャンするか、MACアドレスを手動で入力します。この例では、[QRコードのスキャン]が選択されています。



手順 4

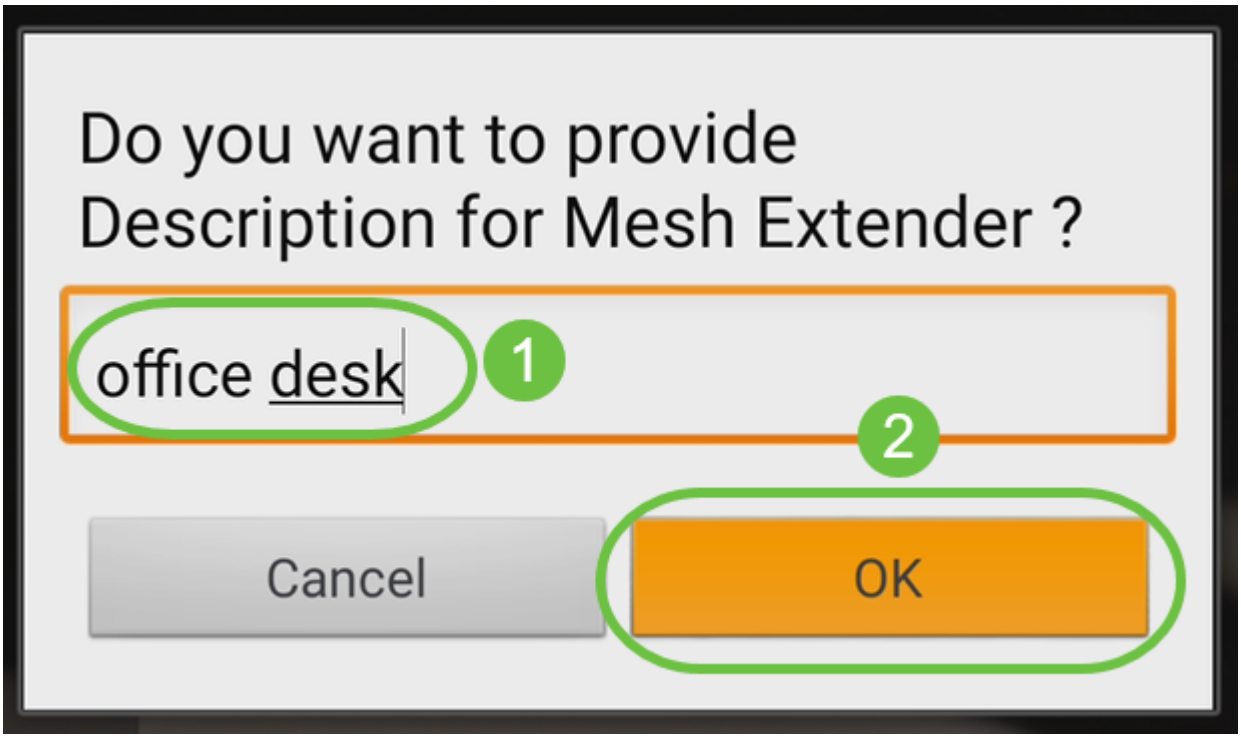
QRコードリーダーがQRコードをスキャンするように表示されます。

Mesh ExtenderのQRコードがスキャンされると、次の画面が表示されます。



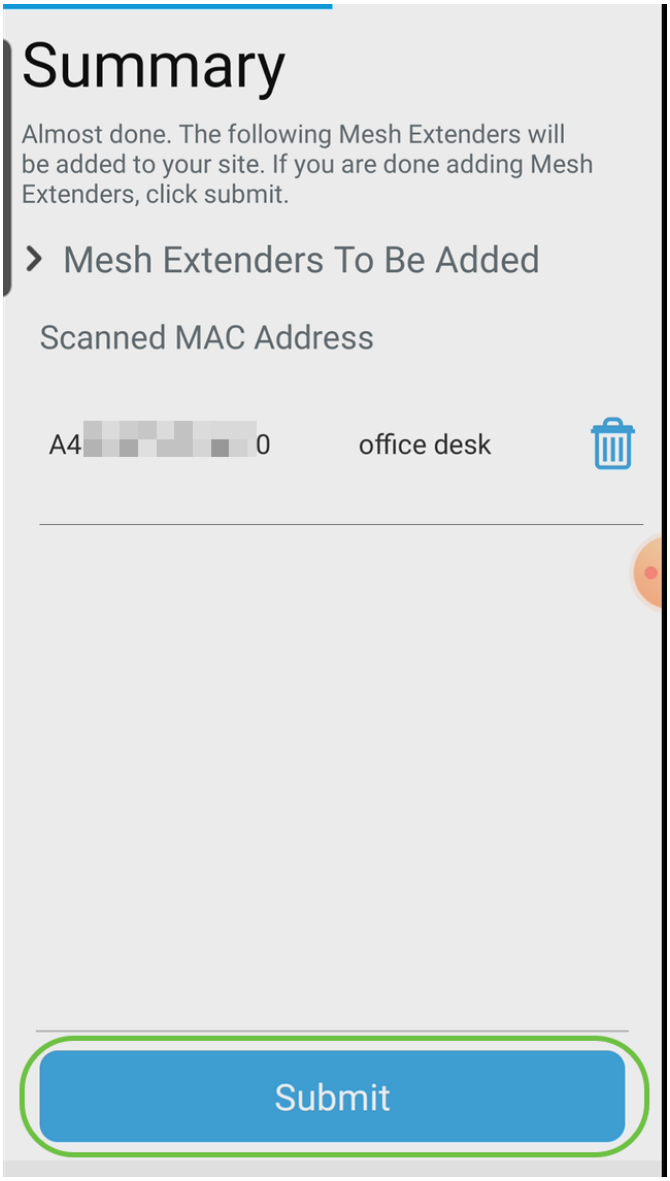
手順 5 (オプション)

必要に応じて、メッシュエクステンダの*説明を入力します*。[OK] をクリックします。



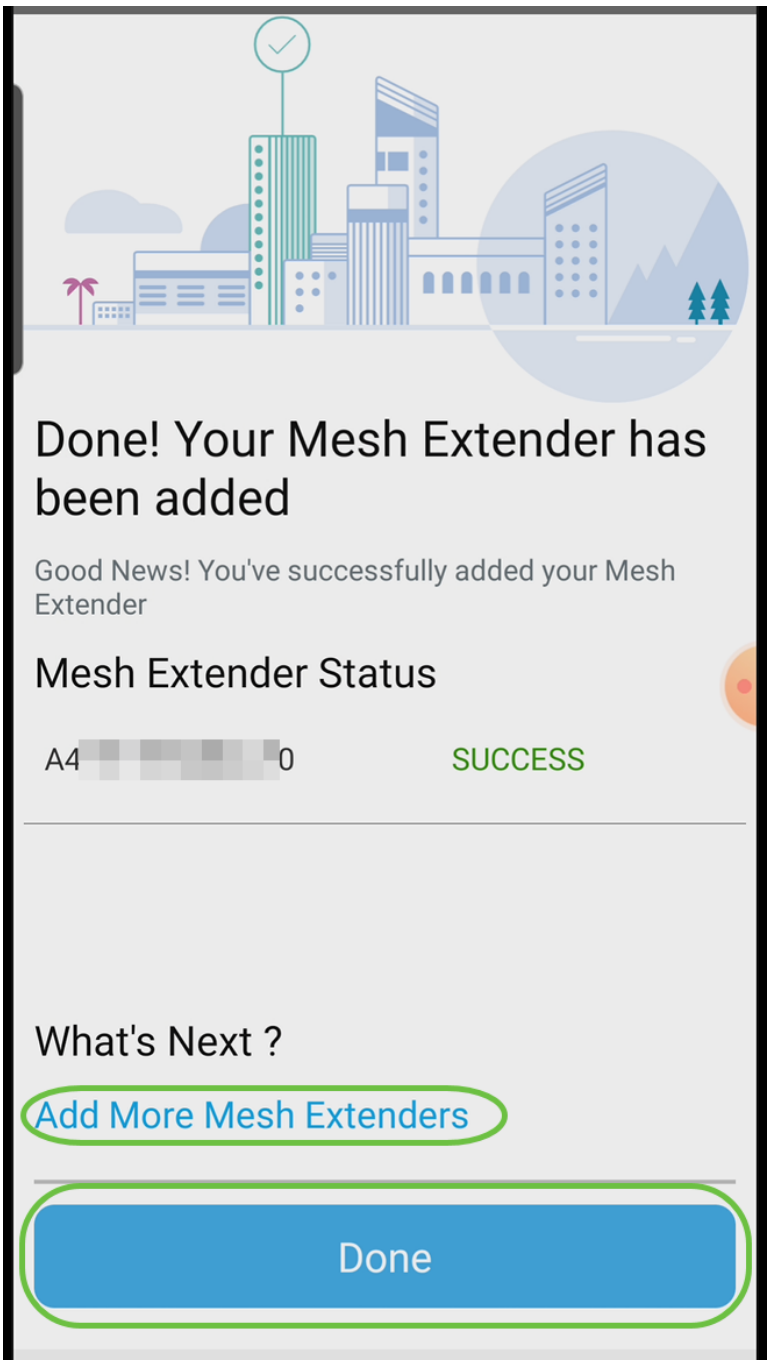
手順 6

サマリーを確認し、*[*送信]をクリックします。



ステップ7

他のメッシュエクステンダをネットワークに*追加*するには、[Add More Mesh Extender]をクリックします。メッシュエクステンダをすべて追加したら、[完了]をクリックします。



各メッシュエクステンダについて繰り返します。

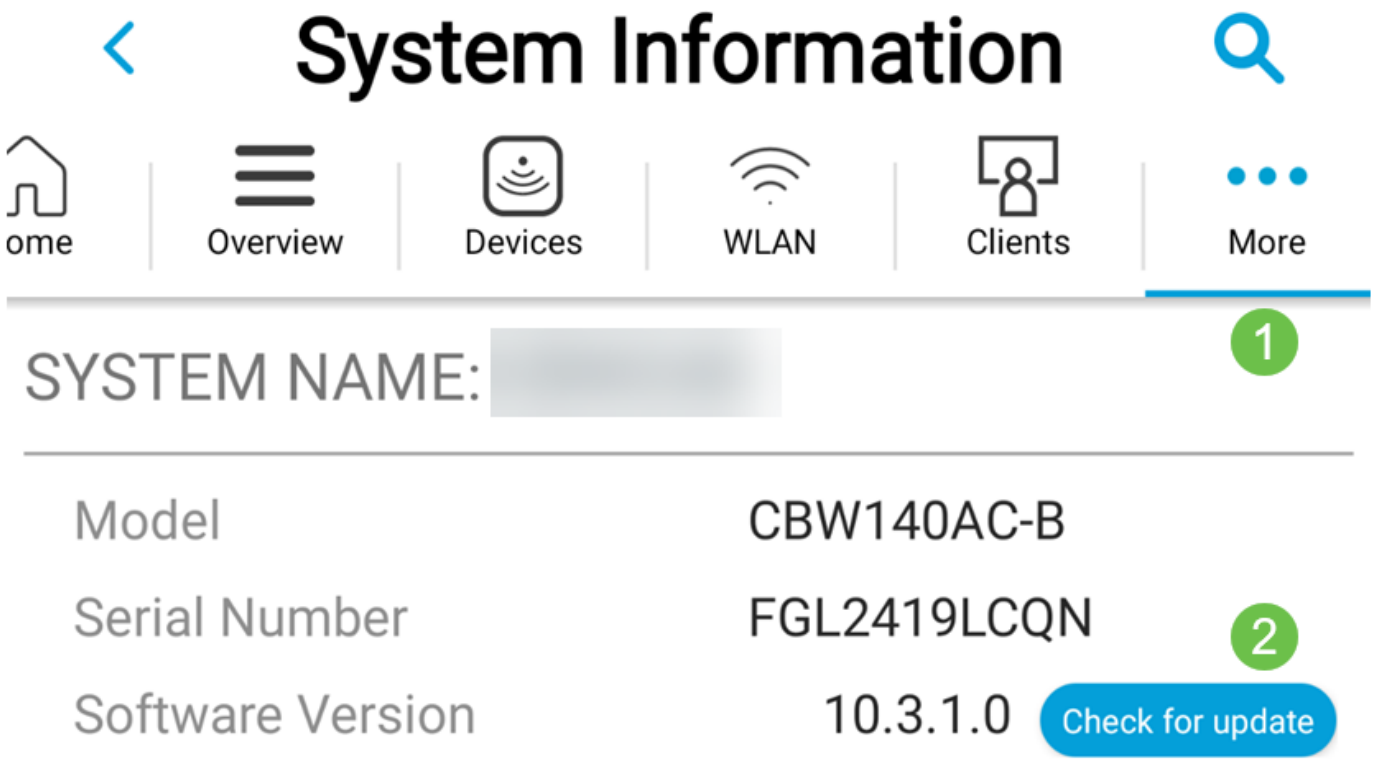
これで、基本設定を口ールする準備ができました。先に進む前に、必要に応じてソフトウェアを確認して更新してください。

モバイルアプリのソフトウェアの確認と更新

ソフトウェアのアップデートは非常に重要なので、この部分は省略しないでください。

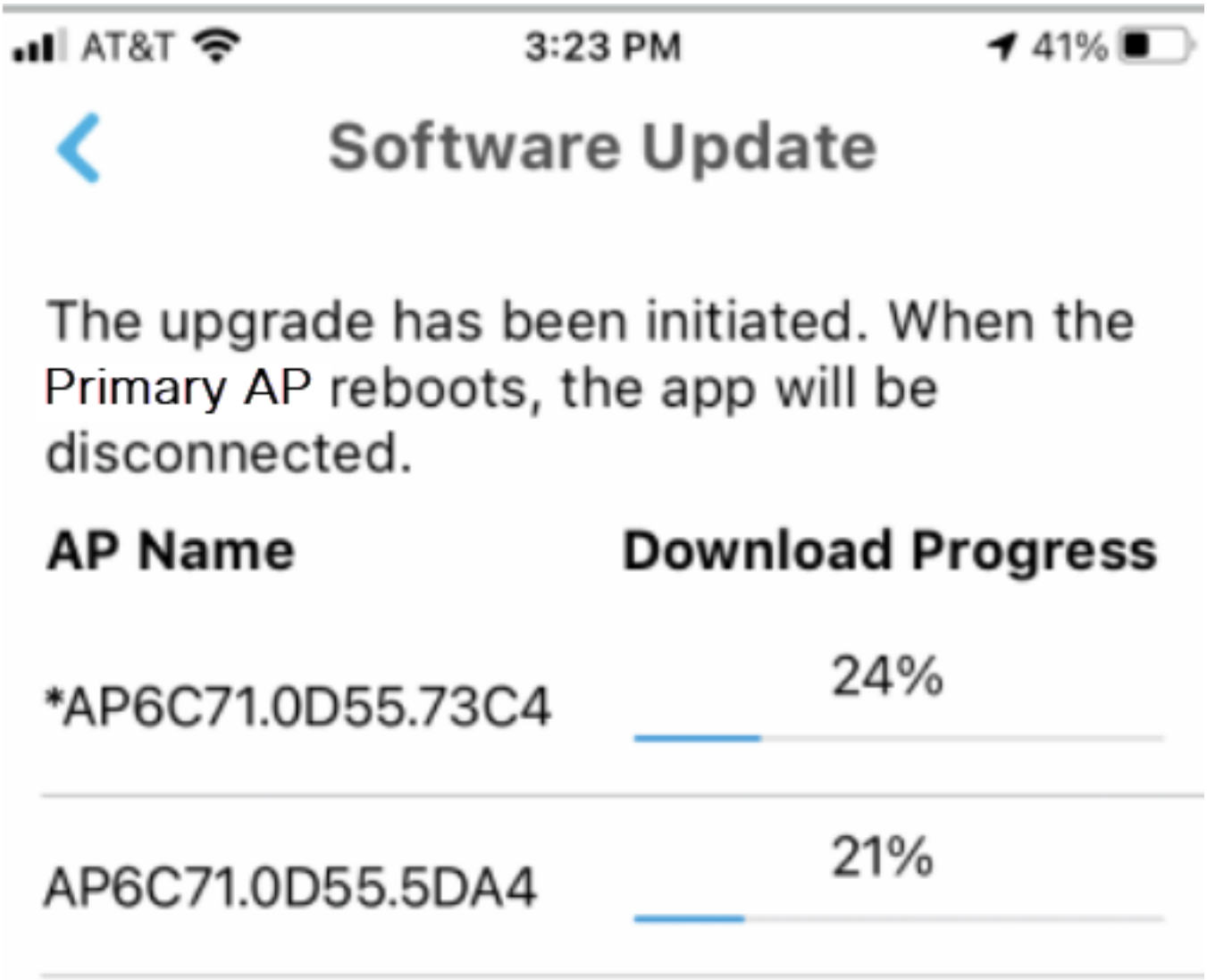
手順 1

モバイルアプリで、[詳細]タブの下**の[更**新の確認]ボタン**をクリック**します。プロンプトに従って、ソフトウェアを最新バージョンに更新します。



手順 2

ダウンロードの進行状況が表示されます。


AT&T
3:23 PM
41%
Software Update
The upgrade has been initiated. When the Primary AP reboots, the app will be disconnected.
AP Name
Download Progress
*AP6C71.0D55.73C4
24%
AP6C71.0D55.5DA4
21%

手順 3

ポップアップ確認により、ソフトウェアアップグレードの終了が通知されます。[OK]をクリックします。

モバイルアプリを使用したWLANの作成

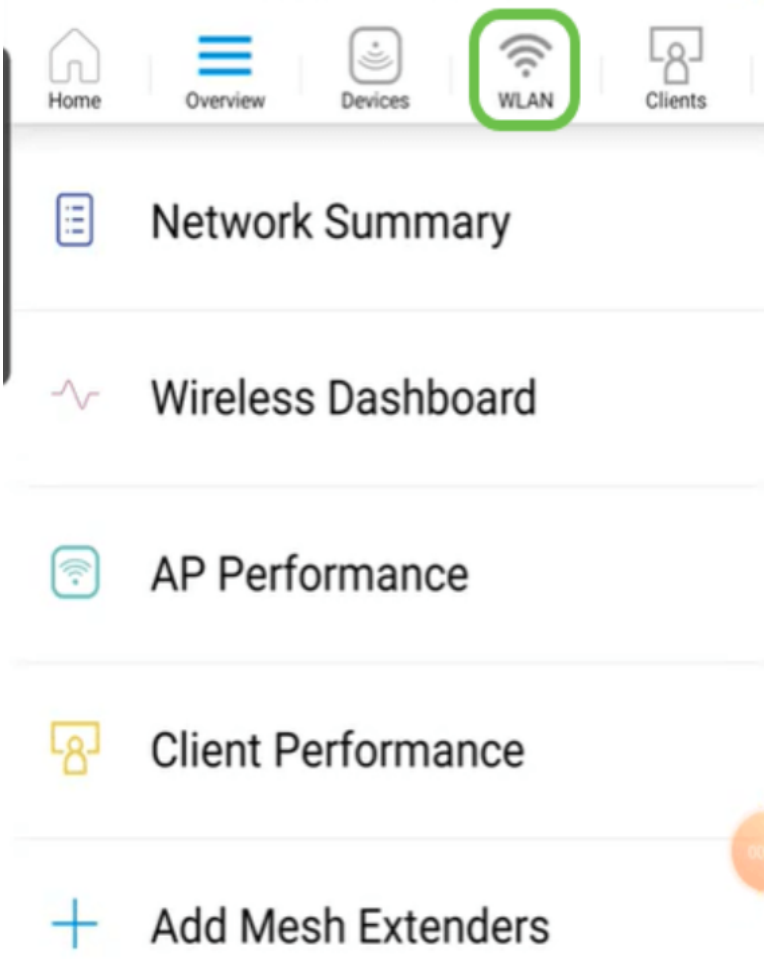
このセクションでは、ワイヤレスローカルエリアネットワーク(WLAN)を作成できます。

手順 1

Cisco Business Wireless Appを開きます。

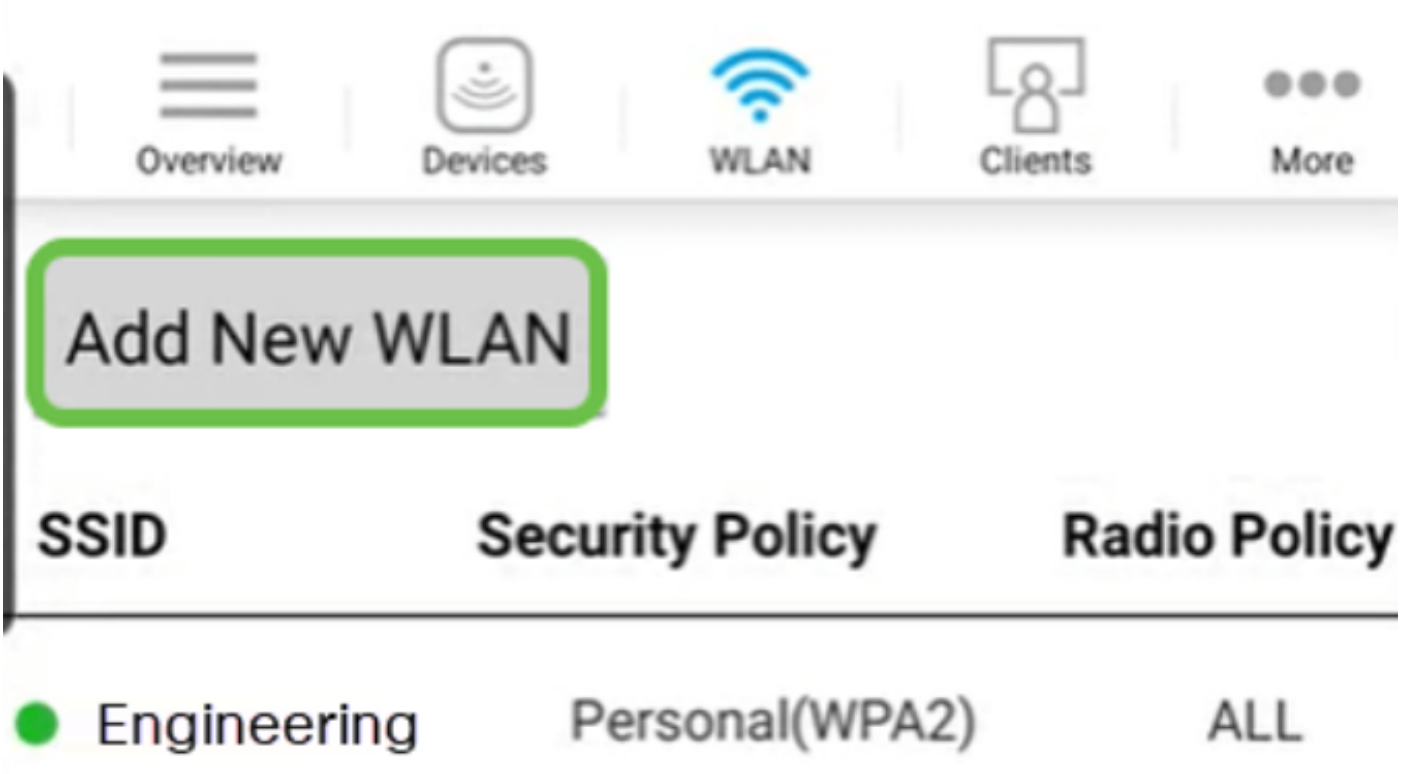
手順 2

モバイルでシスコビジネスワイヤレスネットワークに接続します。アプリケーションにログインします。ページ上部の**[WLAN]**アイコンをクリックします。



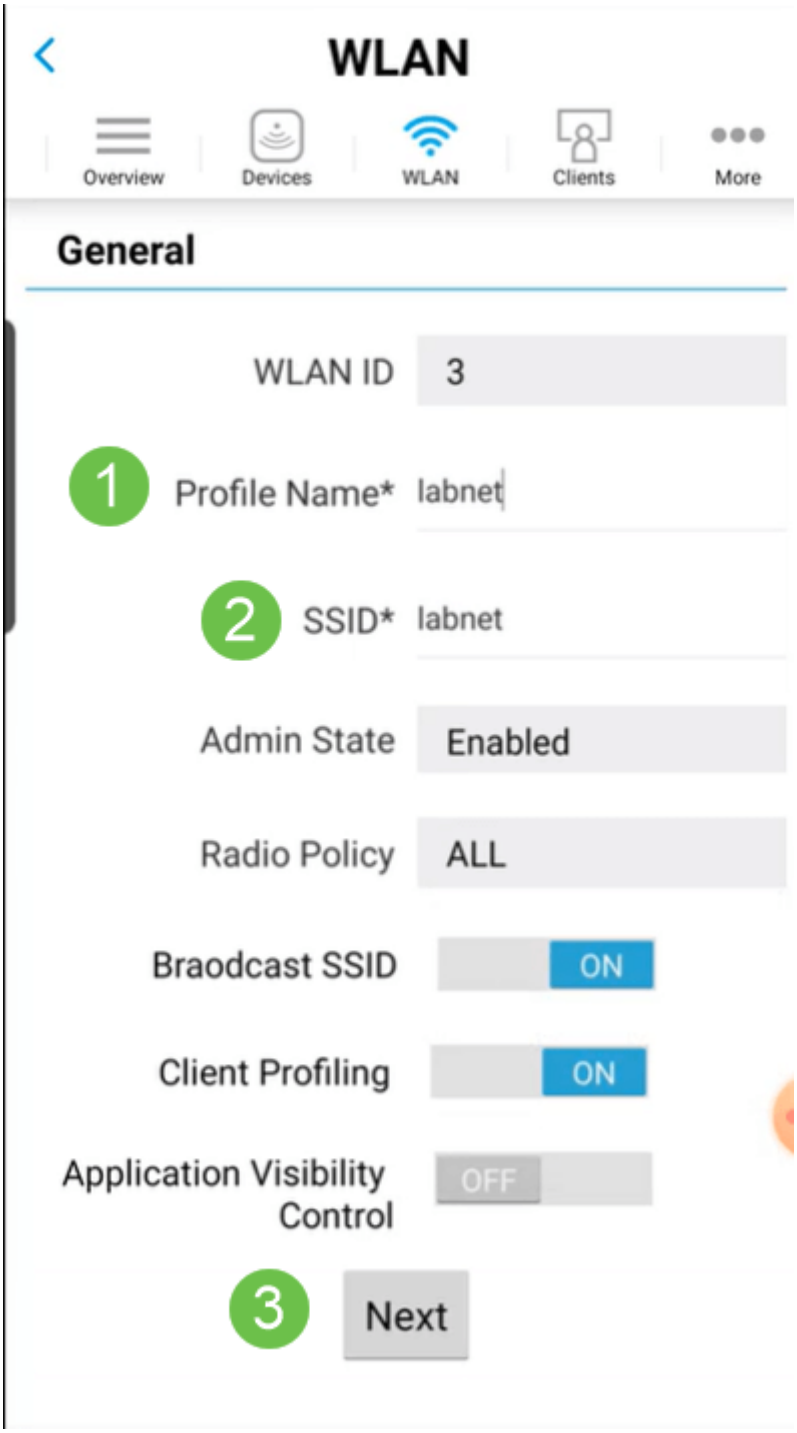
手順 3

[*Add New WLAN*]*画面が開き*ます。既存のWLANが表示されます。[**Add New WLAN**]を**選択します。**



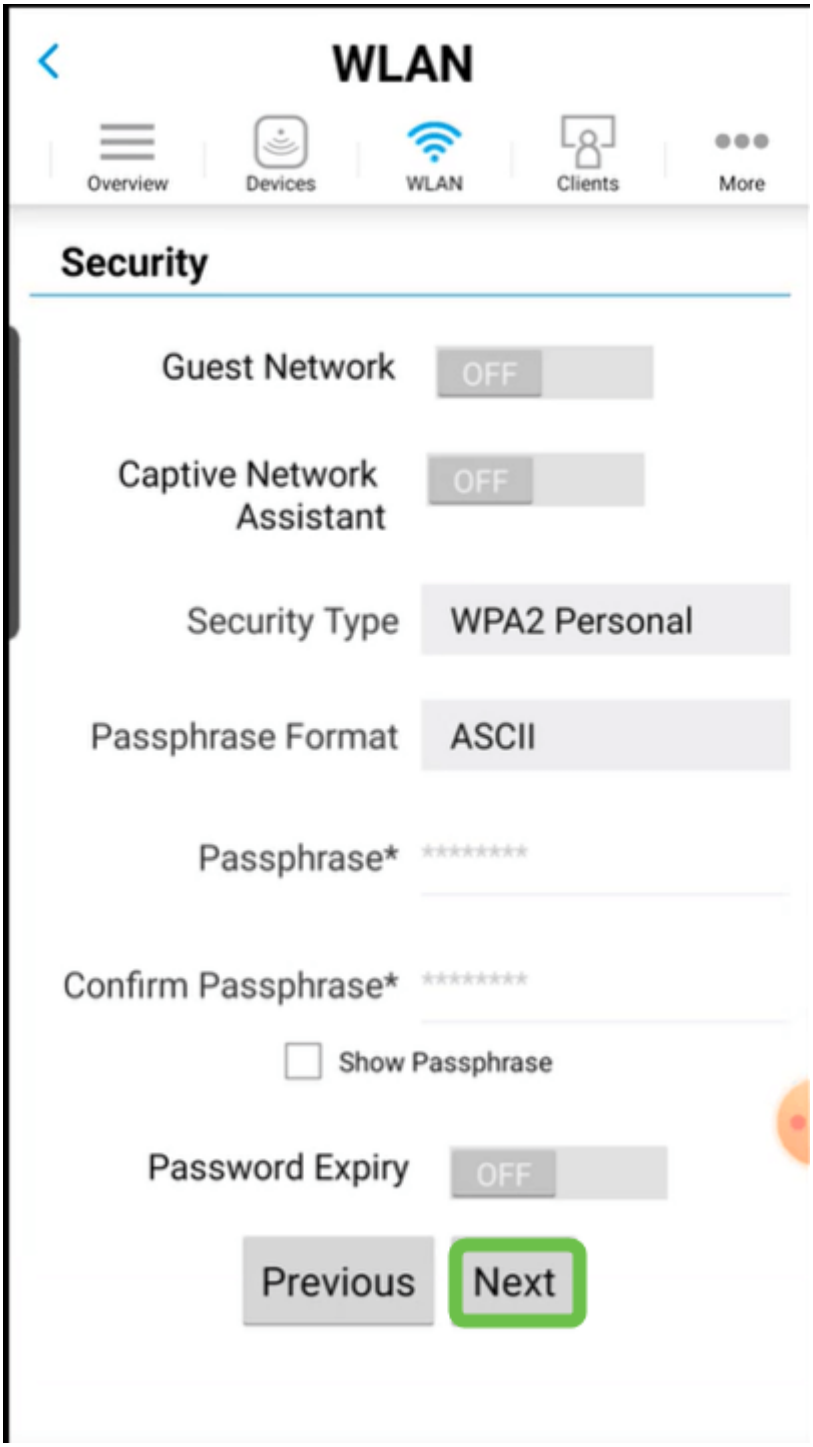
手順 4

プロファイル名とSSIDを入力します。残りのフィールドに入力するか、デフォルト設定のままにします。Application Visibility Controlを有効にした場合は、ステップ6で説明した他の設定が表示されます。[次へ]をクリックします。



手順 5 (オプション)

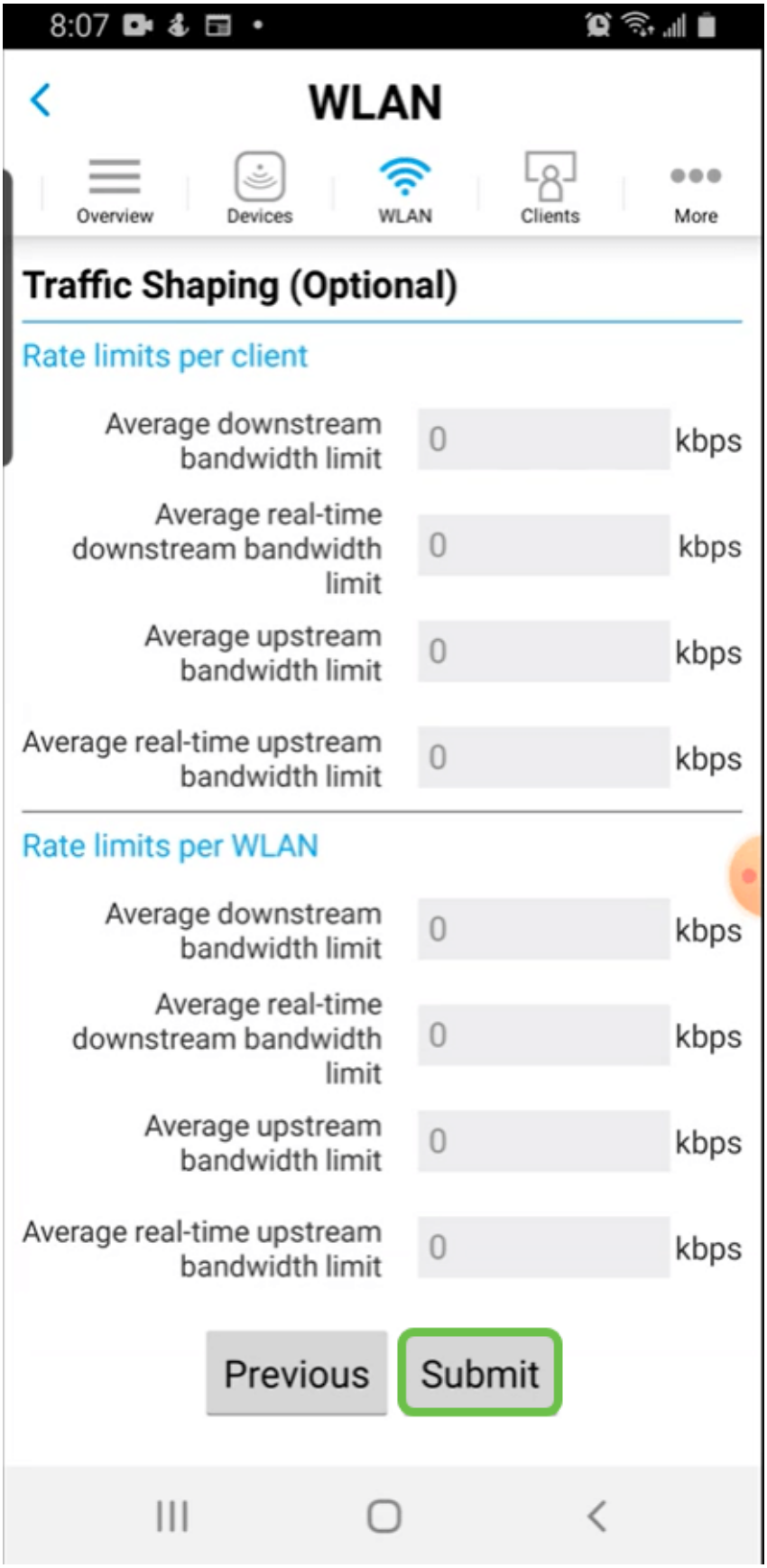
ステップ4で*Application Visibility Controlを有効にした場合*は、ゲストネットワークを含む他の設定を構成できます。詳細は次のセクションで確認できます。キャプティブネットワークアシスタント、*セキュリティタイプ*、*パスフレーズ*、*およびパスワード有効期限も追加*できます。すべての構成を追加したら、[次へ]をクリックします。



モバイルアプリケーションを使用する場合、[セキュリティの種類]のオプション*は[閉く]*または[*WPA2 Personal]*のみのみです。より高度なオプションを使用するには、代わりにモバイルアプリケーションAPのWeb UIにログインします。

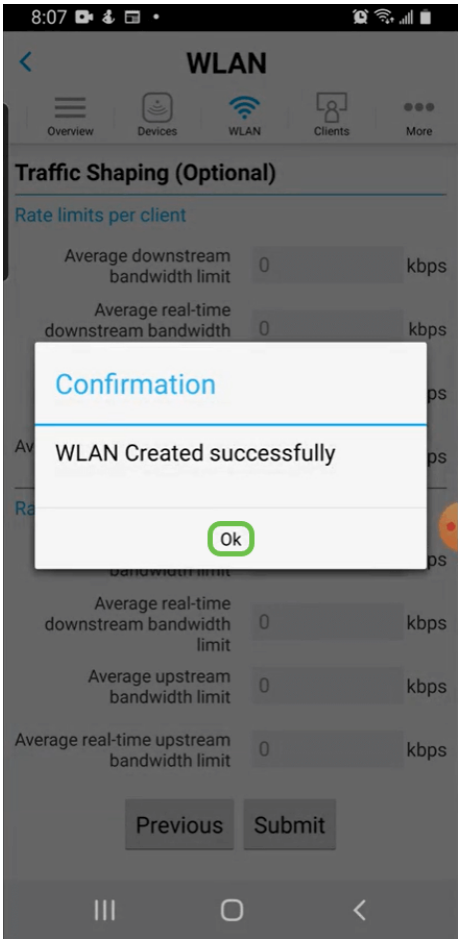
ステップ 6 (オプション)

この画面には、トラフィックシェーピングのオプション*が表示されます*。この例では、トラフィックシェーピングは設定されていません。[Submit] をクリックします。



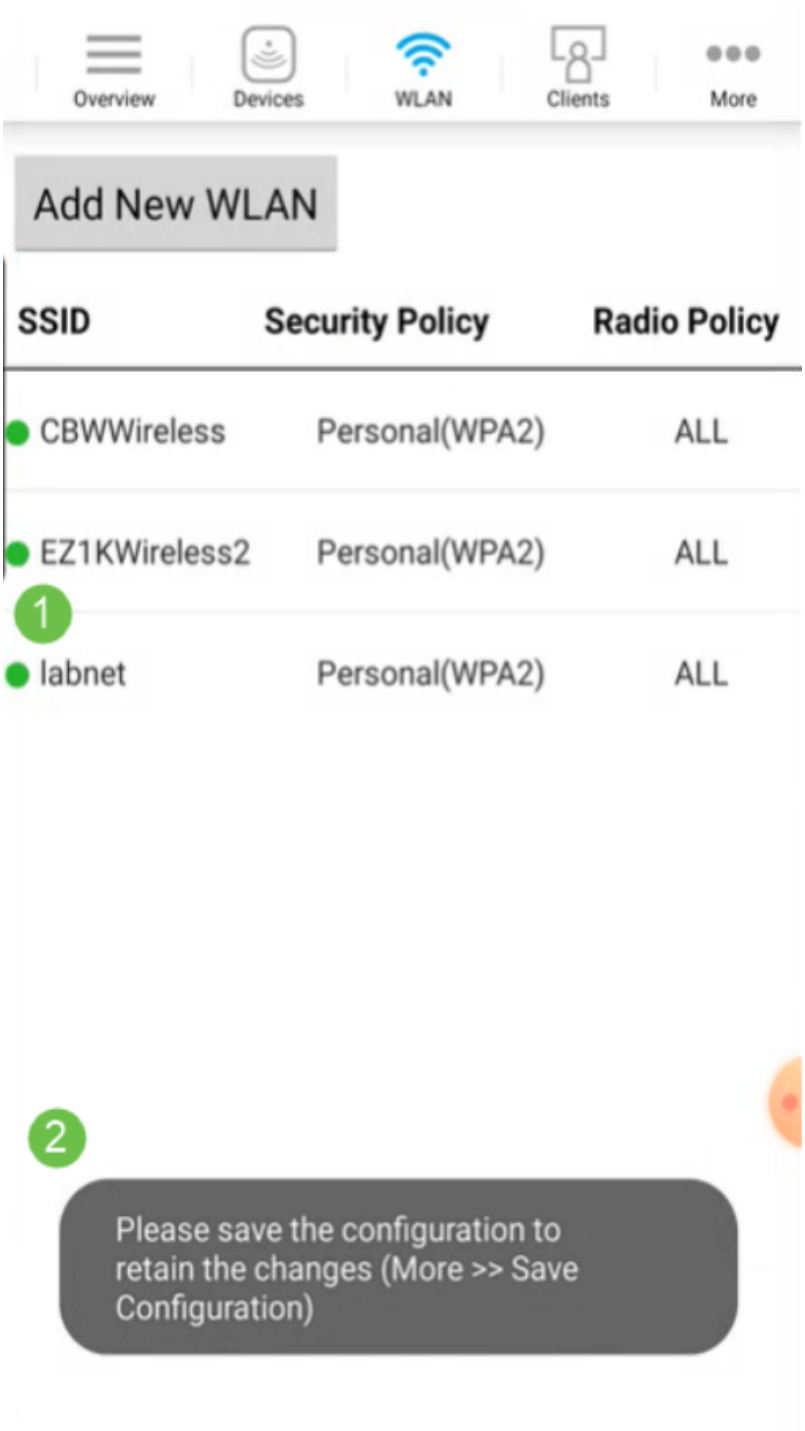
ステップ7

確認のポップアップが表示されます。[OK] をクリックします。



手順 8

ネットワークに追加された新しいWLANと、設定を保存するためのリマインダが表示されます。



手順 9

[詳細]タブをクリックして**構成を保**存し、ドロップダウン· **メニューから**[構成の保存]を選択します。

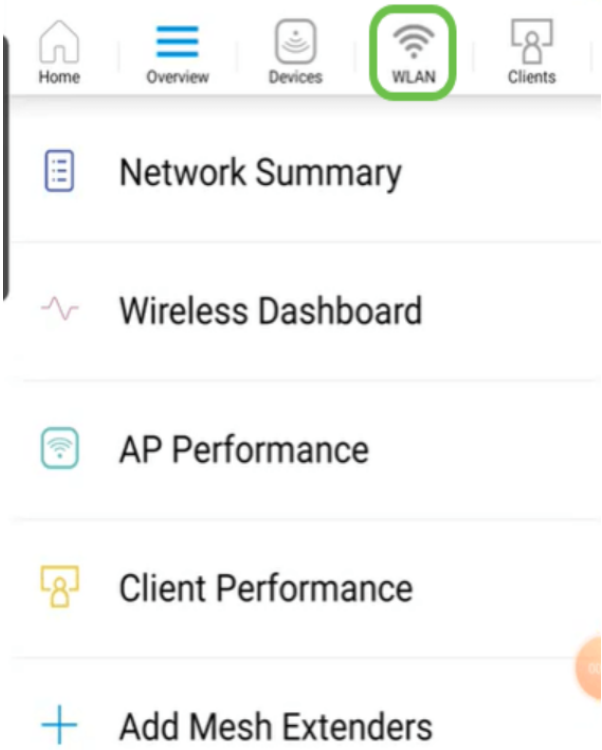
モバイルアプリを使用したゲストWLANの作成

手順 1

モバイルデバイスでシスコビジネスワイヤレスネットワークに接続します。アプリケーションにログインします。

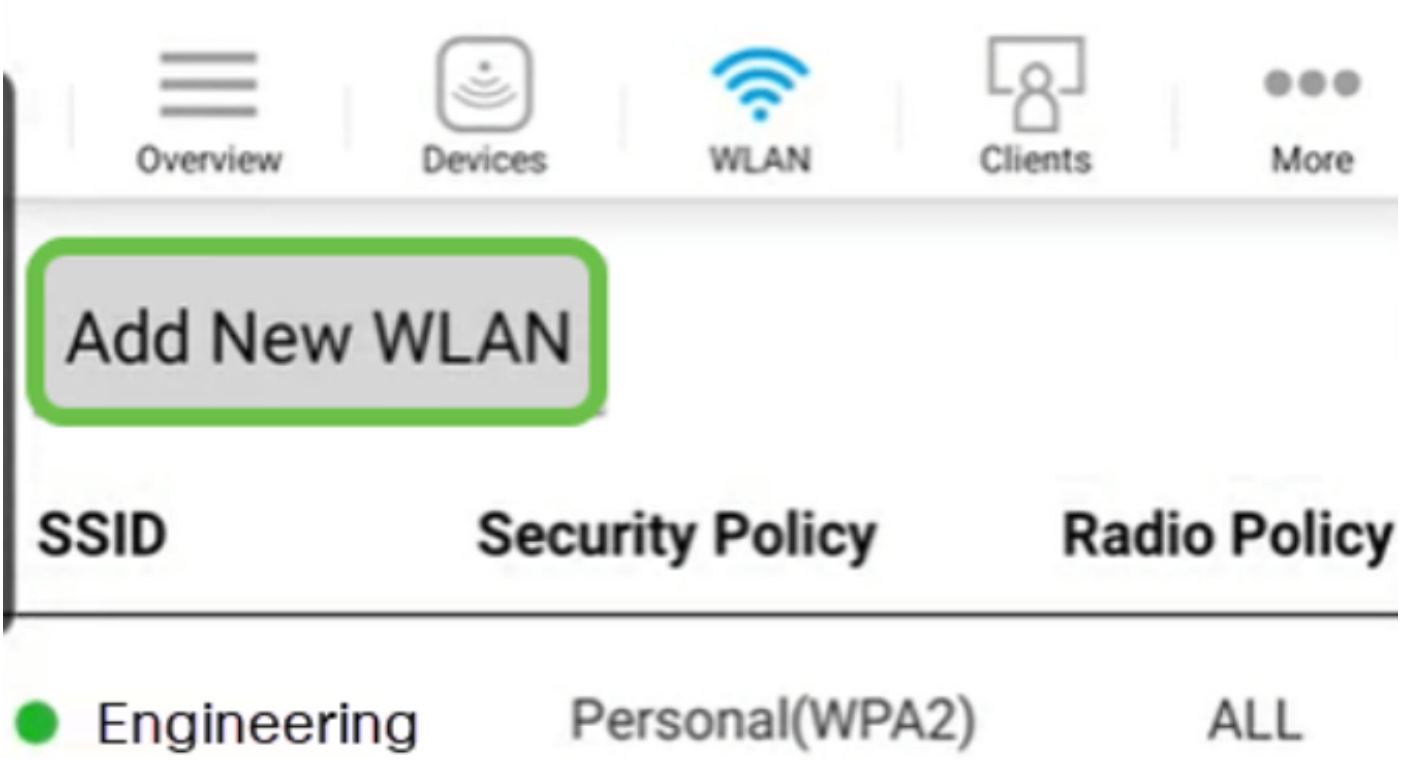
手順 2

ページ上部の**[WLAN]**アイコンをクリックします。



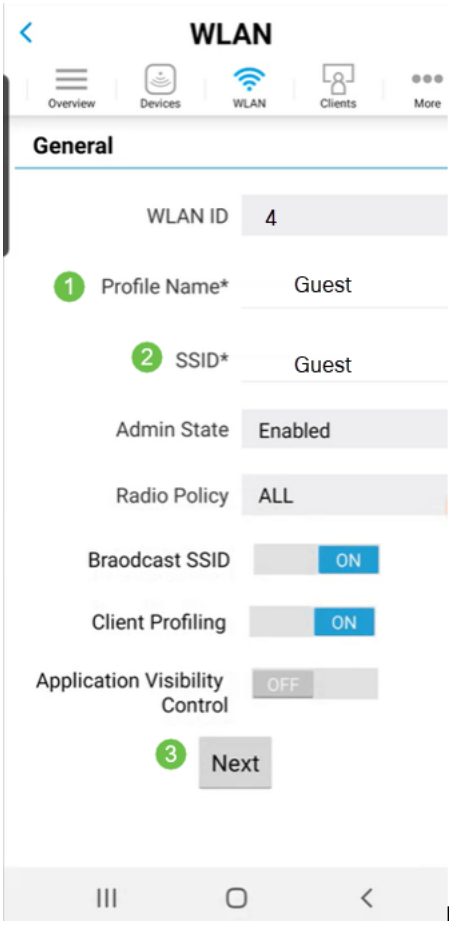
手順 3

[*Add New WLAN*]*画面が開*きます。既存のWLANが表示されます。**[Add New WLAN]を選択します。**



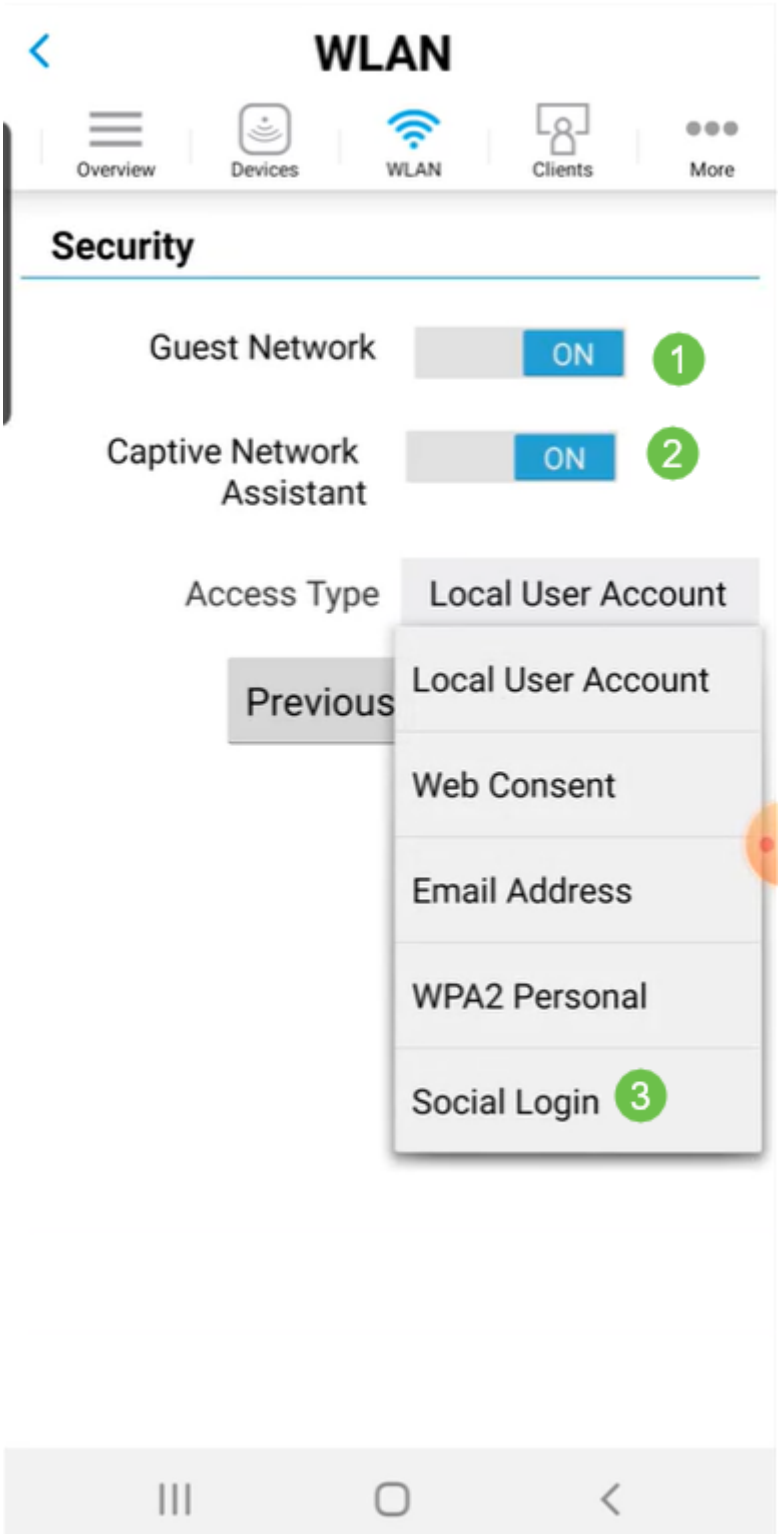
手順 4

プロファイル**名とSSIDを**入力**します**。残りのフィールドに入力するか、デフォルト設定のままにします。[next] をクリックします。



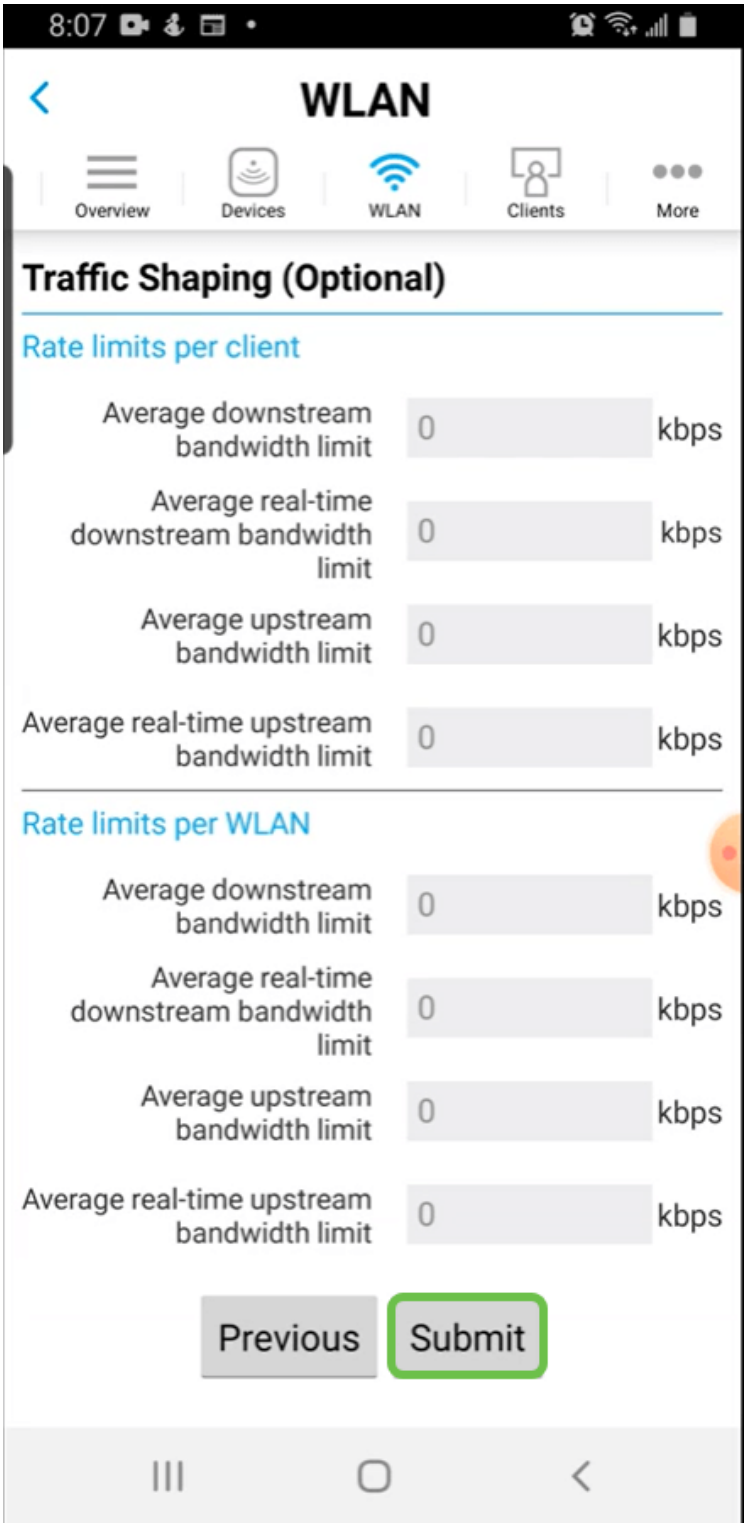
手順 5

ゲストネットワークをオンにします。この例では、キャプティブネットネットワークアシスタントもオンに切り替えられますが、これはオプションです。アクセスタイプのオプションがあります。この場合、[ソーシャルログイン]**が選択**されています。



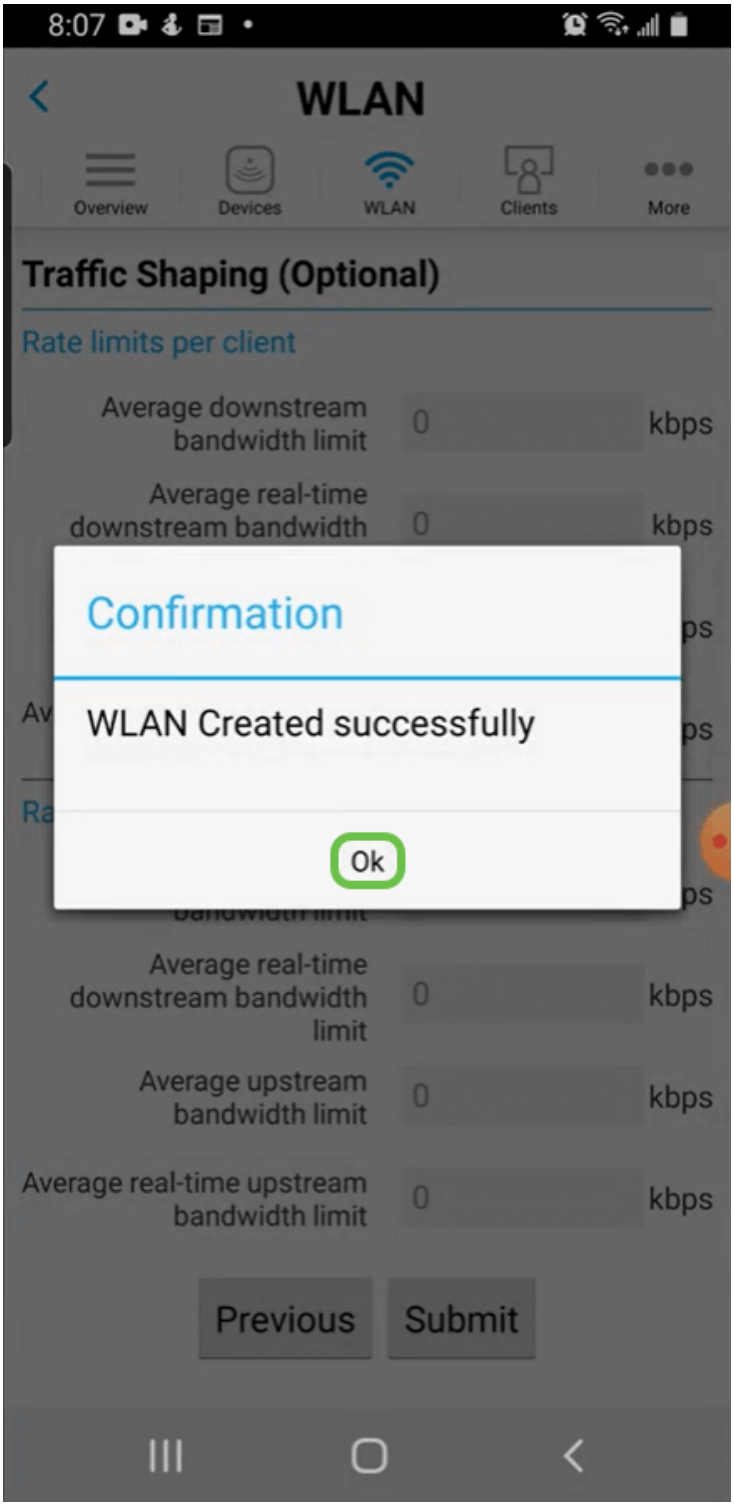
手順 6

この画面には、トラフィックシェーピング（オプション）のオプションが表示されます。 この例では、トラフィックシェーピングは設定されていません。[Submit] をクリックします。



ステップ7

確認のポップアップが表示されます。[OK] をクリックします。



手順 8

[詳細]タブをクリックし**て構成を保**存し、ドロップダウン· **メニューから**[構成の保存]を選択します。

結論

これで、ネットワークの完全なセットアップが完了しました。少し時間を取って祝っ

て仕事に行って！

アプリケーションプロファイリングまたはクライアントプロファイリングをワイヤレスメッシュネットワークに追加する場合は、Webユーザインターフェイス(UI)を使用します。 **をクリックして、これらの機能を設定します**。

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