ネットワーク構成の合計：Web UIを使用したRV345PおよびCisco Business Wireless

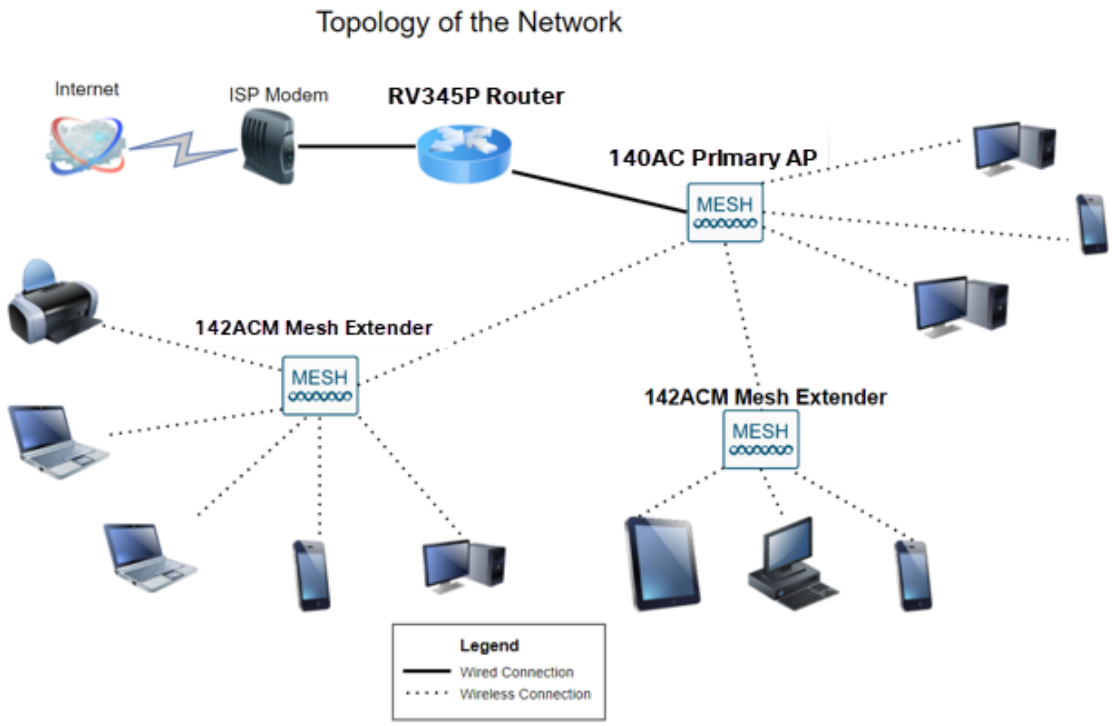
目的

このガイドでは、RV345P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。

目次

トポロジ



概要

すべての調査が統合され、シスコ機器を購入しました。とても工キサイティングです。このシナリオでは、RV345P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。

この高度なルータは、追加機能のオプションも提供します。

1. アプリケーション制御により、トラフィックを制御できます。この機能は、トラフィックを許可し、ログを記録したり、トラフィックをブロックしてログを記録したり、トラフィックをブロックしたりするように設定できます。
2. Webフィルタリングは、安全でないWebサイトや不適切なWebサイトへのWebトラフィックを防止するために使用されます。この機能を使用した口ギングはありません。
3. AnyConnectは、シスコが提供するセキュアソケットレイヤ(SSL)バーチャルプライベ

ートネットワーク(VPN)です。VPNを使用すると、インターネットを介して安全なトンネルを確立することで、リモートユーザやリモートサイトから企業オフィスやデータセンターに接続できます。

これらの機能を使用するには、ライセンスを購入する必要があります。ルータとライセンスはオンラインで登録されており、このガイドで説明します。

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

該当するデバイス |ソフトウェアバージョン

- RV345P |1.0.03.21
- CBW140AC |10.4.1.0
- CBW142ACM | 10.4.1.0（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）

前提条件

ルータの準備

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. RV345Pルータを使用する際の特別な手順については、インターネットサービスプロバイダー(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。

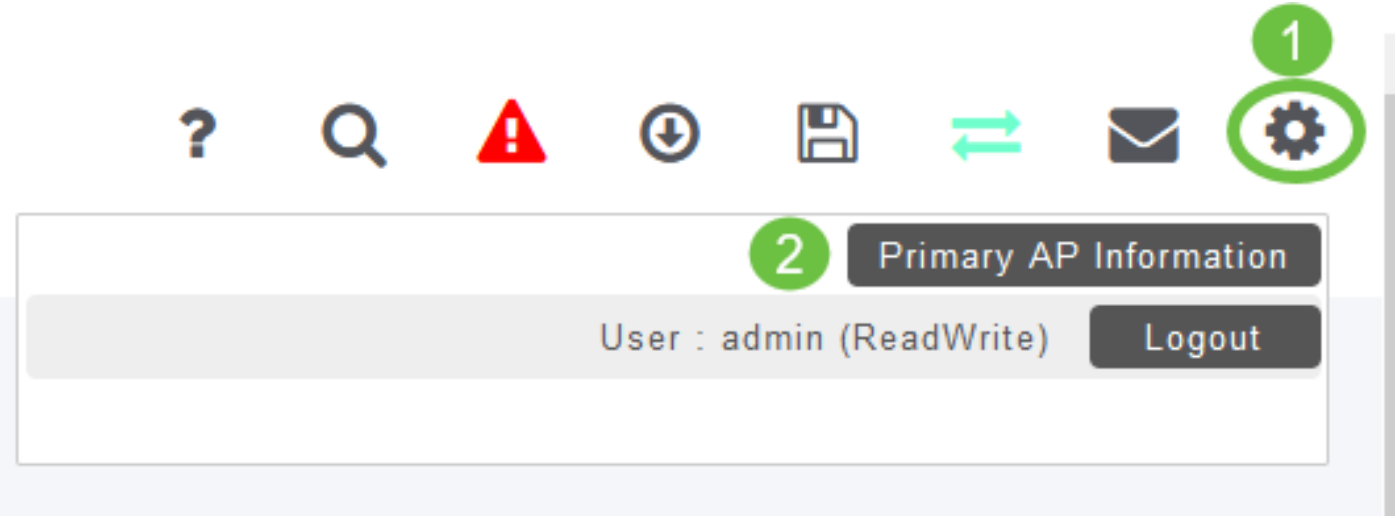
Cisco.comアカウントの取得

シスコの機器を所有しているため、Cisco.comアカウントを取得する必要があります。これは、Cisco Connection Online Identification(CCO ID)と呼ばれることもあります。 勘定は無料です。

アカウントを既に持っている場合は、この記事の次のセクションにジャンプできます。

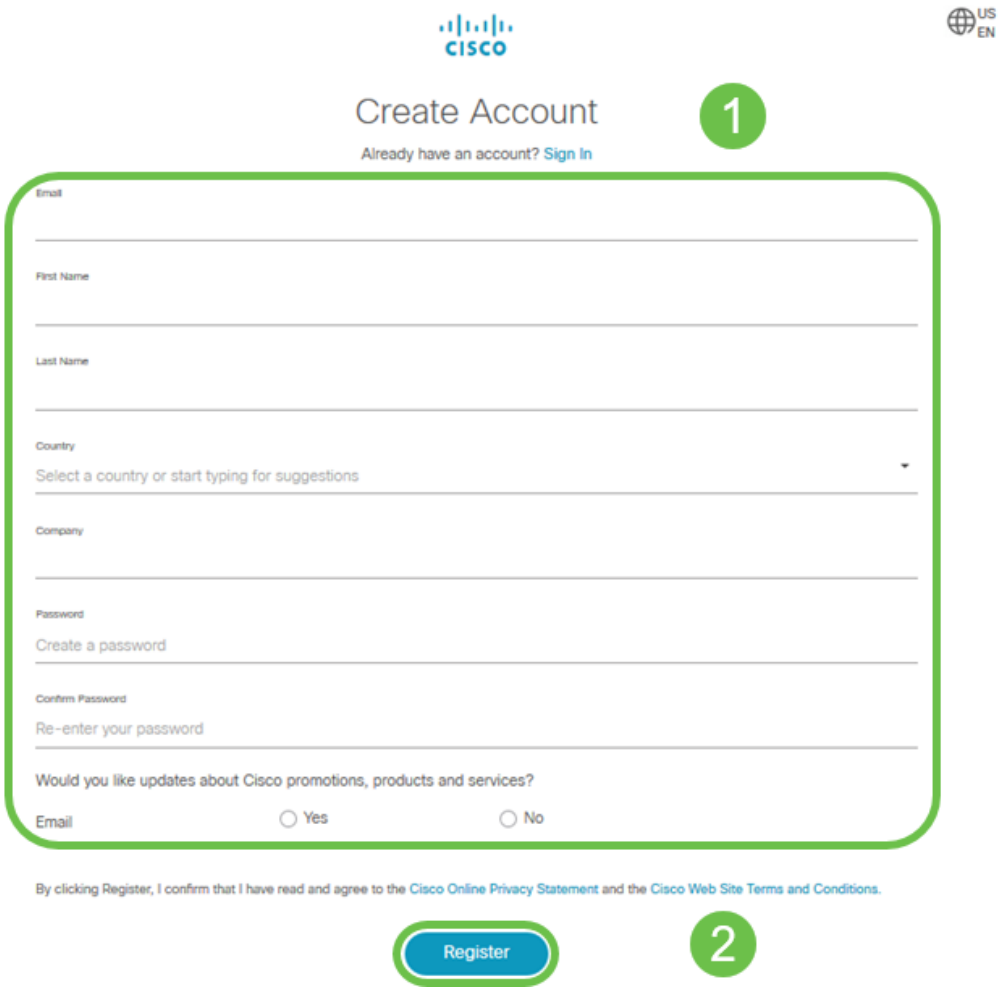
手順 1

Cisco.comに移動します。個人アイコンをクリックし、[アカウントの作成]を選択します。



手順 2

アカウントを作成するために必要な詳細を入力し、[登録]をクリックします。手順に従って、登録プロセスを完了します。



問題がある場合は、をクリックしてCisco.comアカウント登録のヘルプページに移動します。

RV345P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。

RV345P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、ネットワークの要求またはインターネットサービスプロバイダー(ISP)が、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。

準備はいいか？行こう！

RV345Pすぐに使用可能

手順 1

RV345P 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RV345Pと同じ有線サブネットワークに存在する必要があります。

手順 2

RV345P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、RV345P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RV345P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RV345PのWANポートに接続します。

手順 5

RV345Pアダプタのもう一方の端をコンセントに差し込みます。RV345Pの電源がオンになります。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、RV345P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

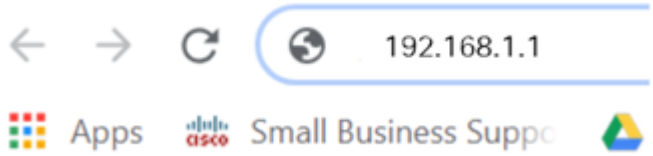
準備作業が完了しました。これで、いくつかの設定に進みます。Web UIを起動するには、次の手順を実行します。

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。

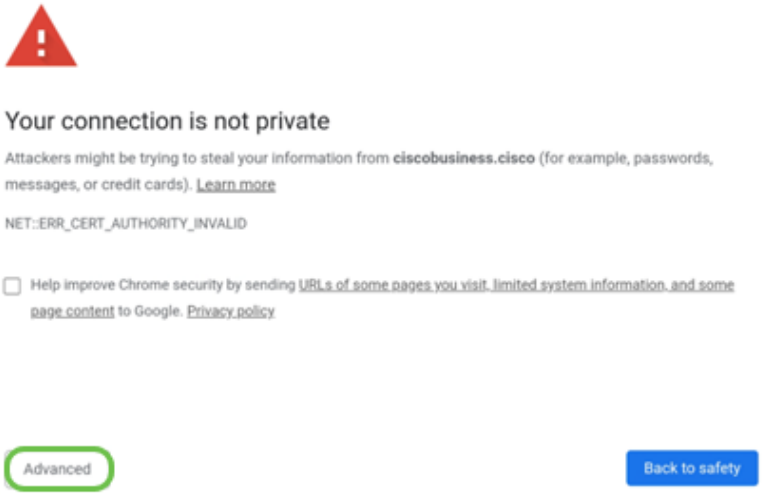
手順 2

Safari、Internet Explorer、FirefoxなどのWebブラウザを開きます。アドレスバーに、RV345P、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](#)。



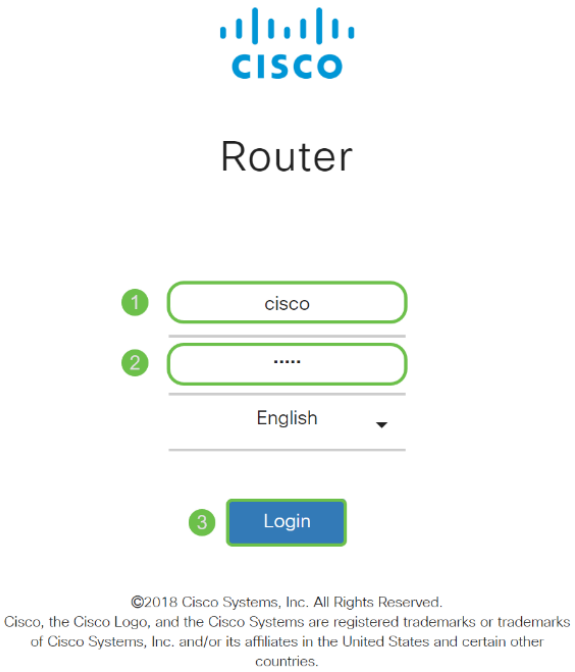
手順 4

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。

[Login] をクリックする。

詳細については、「[Cisco RV340シリーズVPNルータのWebベースセットアップペー](#)

ジへのアクセス方法」をクリックしてください。



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。ナビゲーションウィンドウが開いていない場合は、メニューアイコンをクリックして開きます。

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、このトラブルシューティングの記事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（RV345Pのデフォルト IP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、

RV345P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。

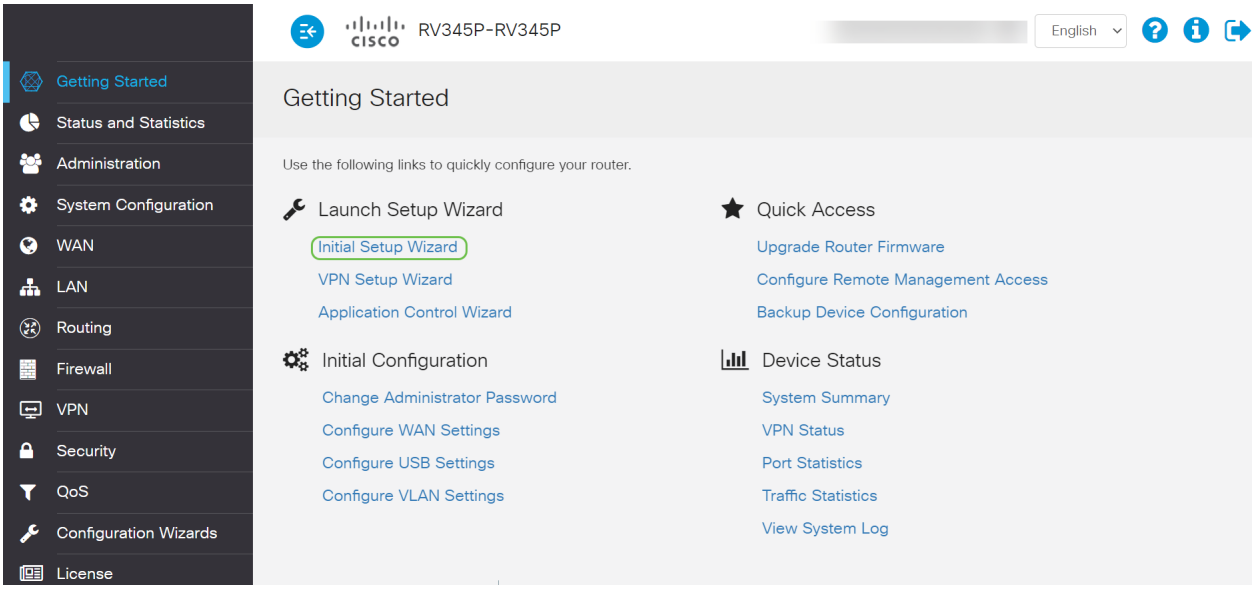
3. 192.168.1.1のIPアドレスを使用している既存の機器がある場合は、ネットワークが動作するためにこの競合を解決する必要があります。このセクションの最後に詳しく説明します。または、ここをクリックして直接説明してください。
4. 両方のデバイスの電源をオフにして、モデムとRV345Pをリセットします。次に、モデムの電源を入れ、約2分間アイドル状態にします。その後、RV345Pの電源をオンにします。これで、WAN IPアドレスが受信されます。
5. DSLモデムを使用している場合は、ISPにDSLモデムをブリッジモードにするよう依頼します。

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。

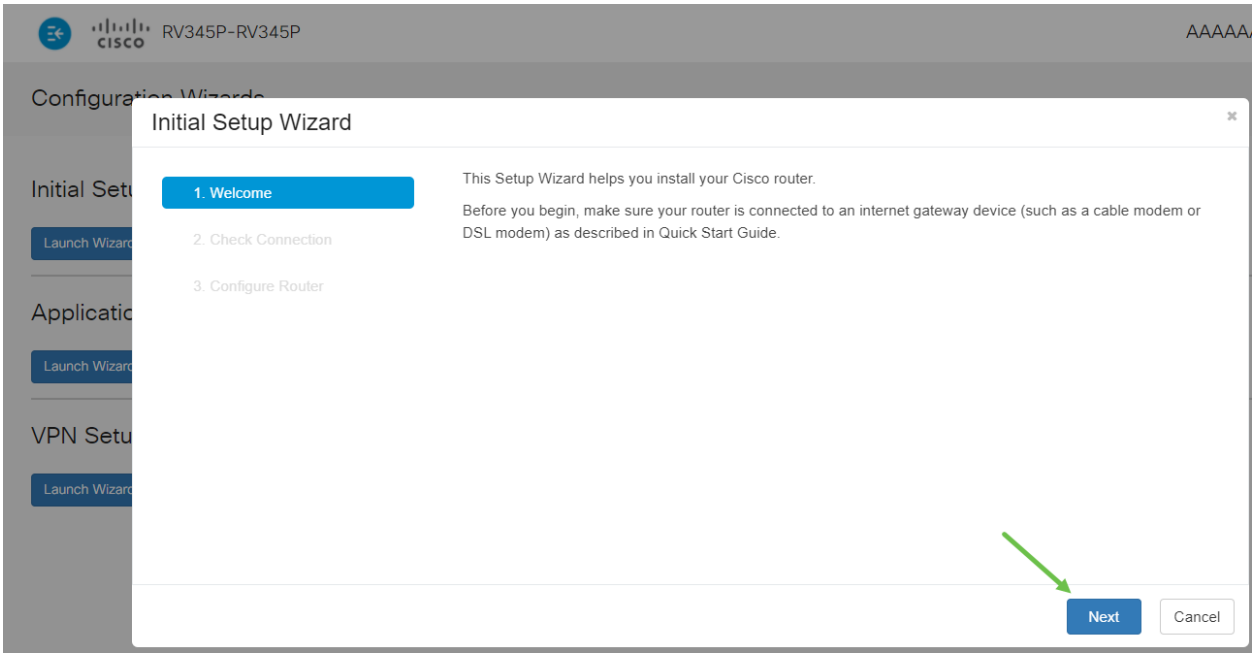
手順 1

[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。



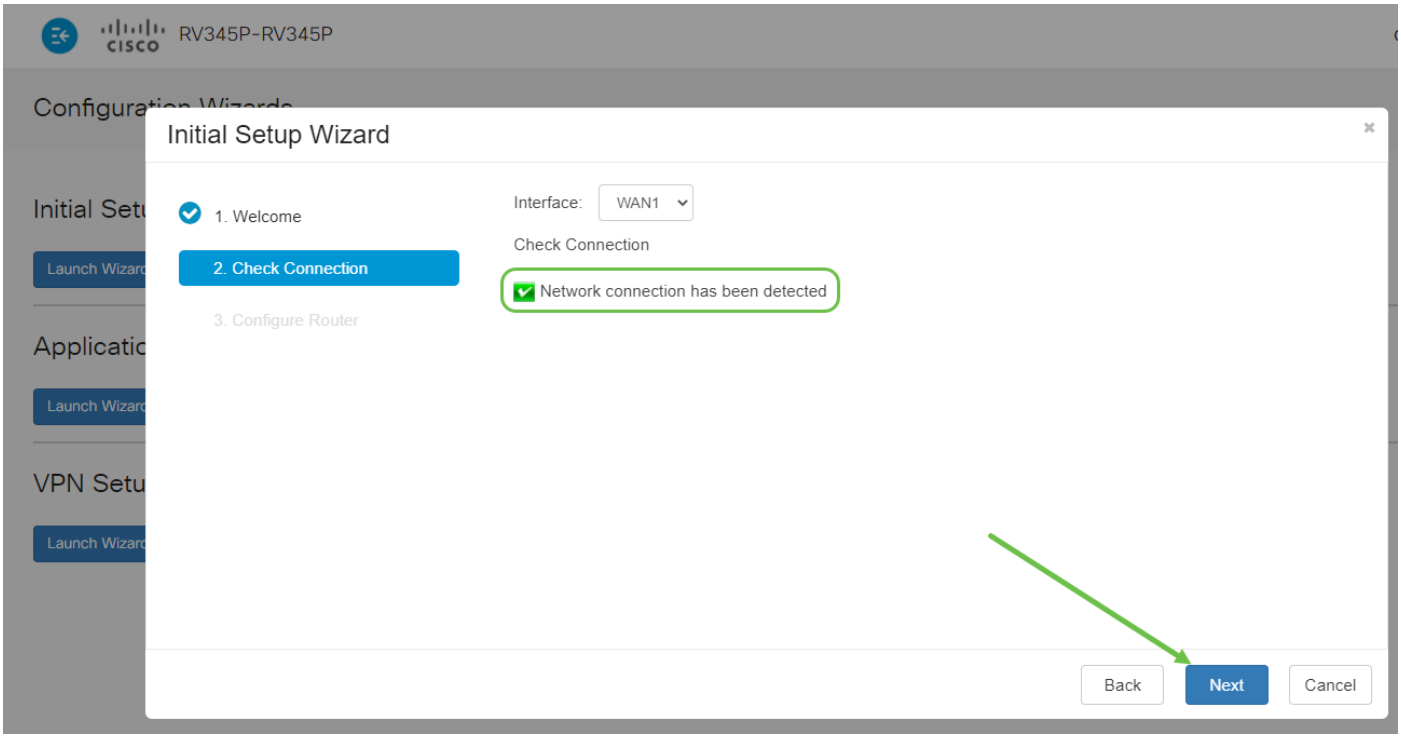
手順 2

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。



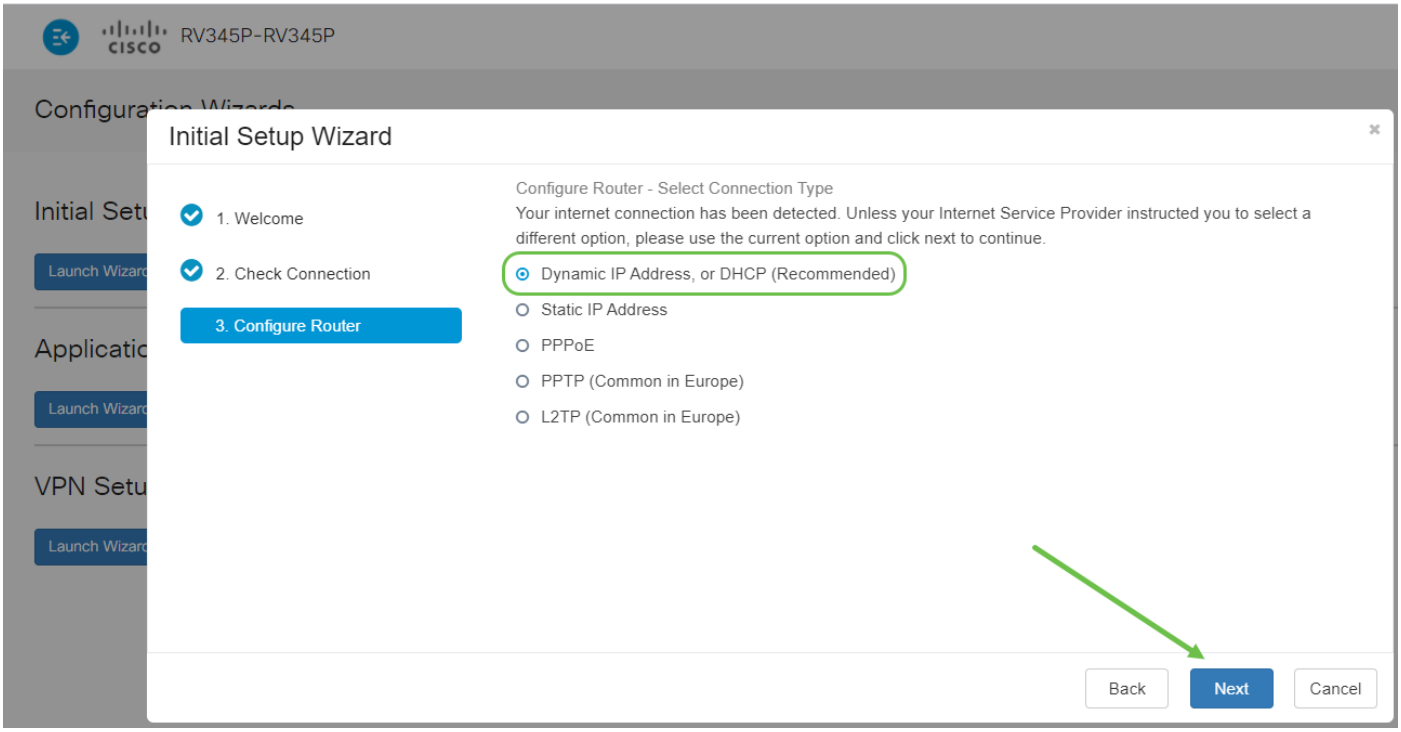
手順 3

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。



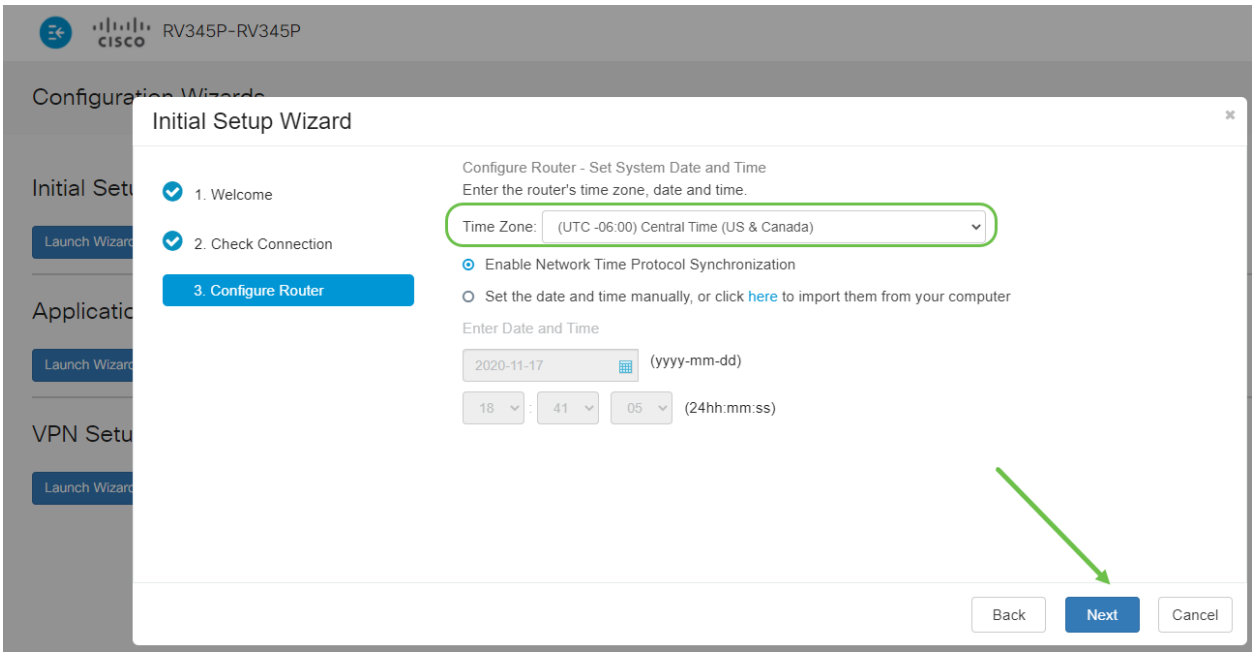
手順 4

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。



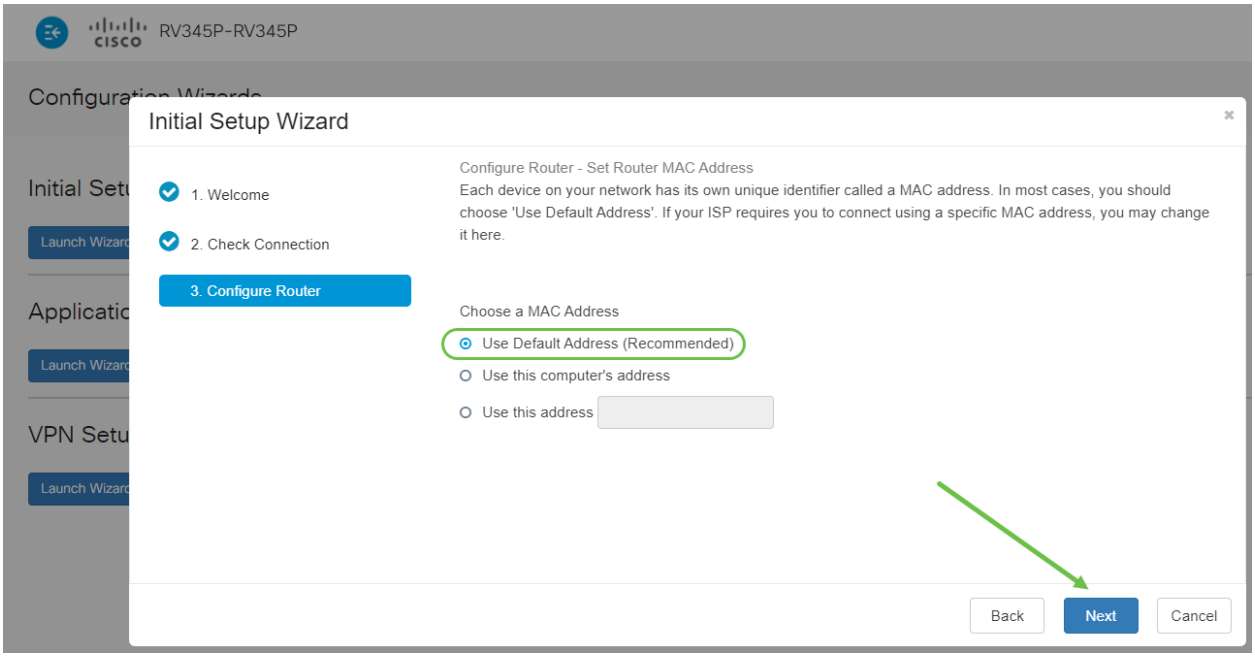
手順 5

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。**



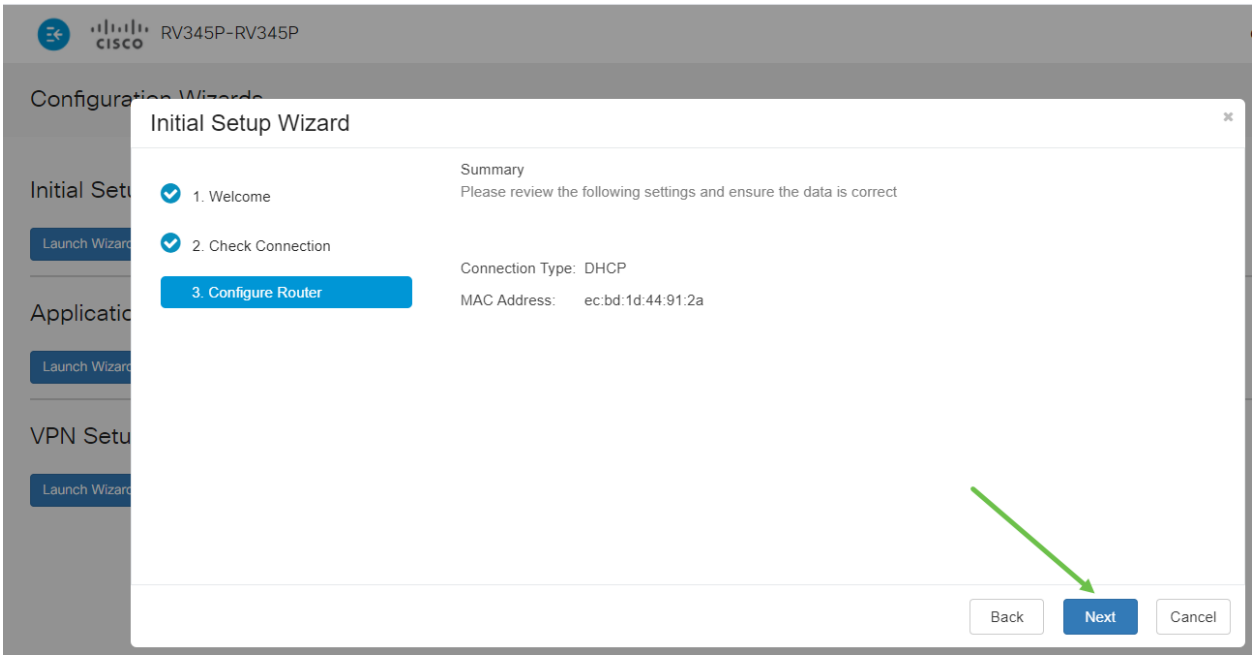
手順 6

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。



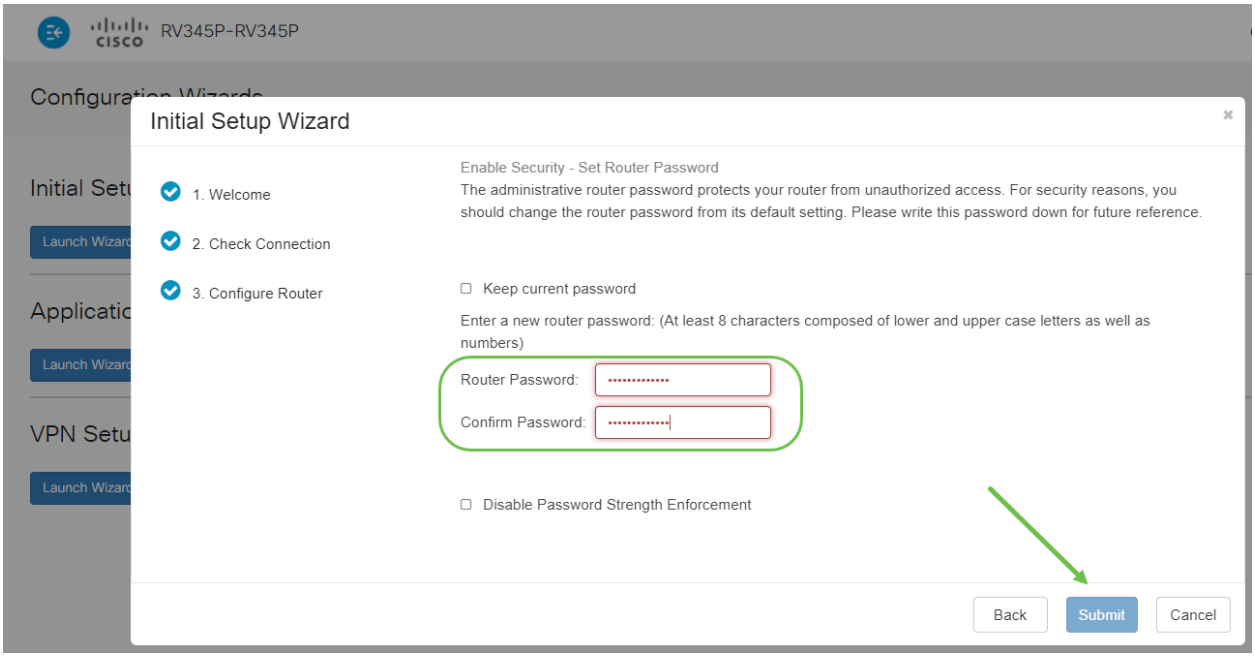
ステップ7

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。**

これらの設定の詳細については、「RV34xルータでのDHCP WAN設定の構成」を参照してください。

RV345Pでは、デフォルトでPower over Ethernet(PoE)が有効になっていますが、いくつかの調整を行うことができます。設定をカスタマイズする必要がある場合は、RV345PルータのPower over Ethernet(PoE)設定を確認してください。

必要に応じてIPアドレスを編集する（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。

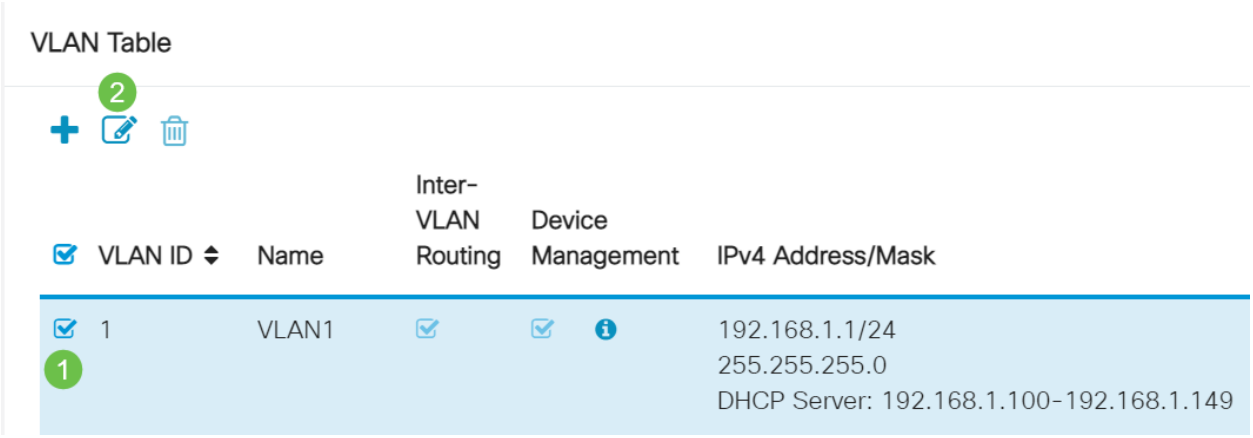
このプロセスは、ルータのIPアドレスを既存のネットワーク内の特定のアドレスに割り当てる必要がある場合にのみ必要です。IPアドレスを編集する必要がない場合は、この記事の次のセクションに移動できます。

手順 1

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

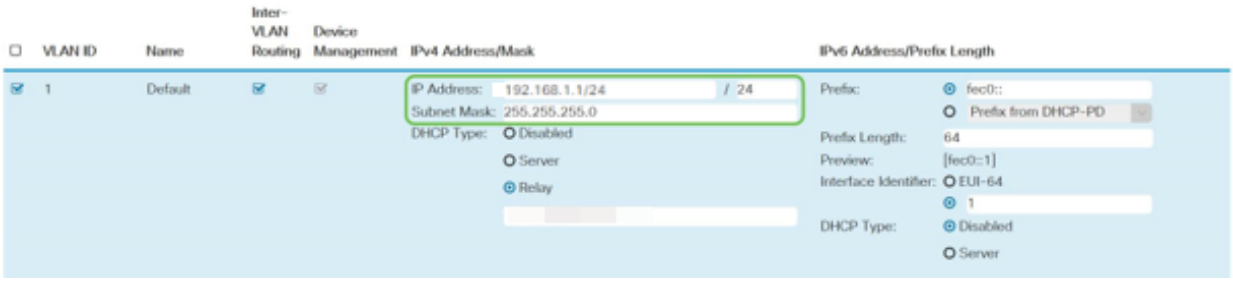
手順 2

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。



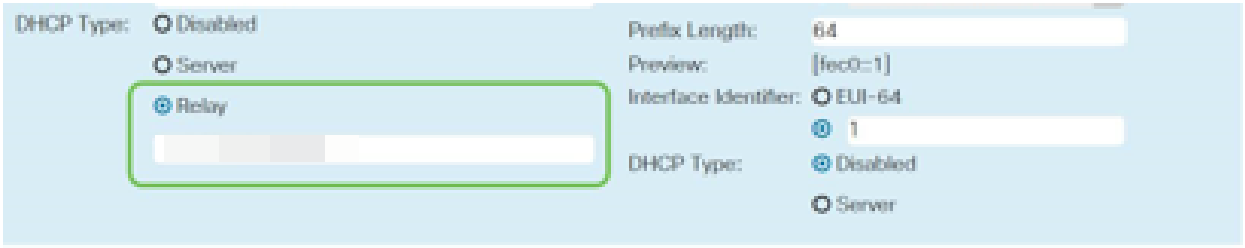
手順 3

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。

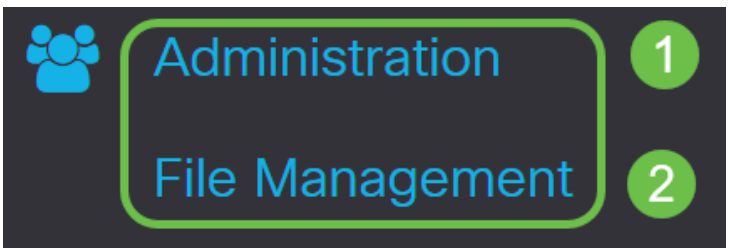


必要に応じたファームウェアのアップグレード

これは重要なステップだ、スキップしないでください！

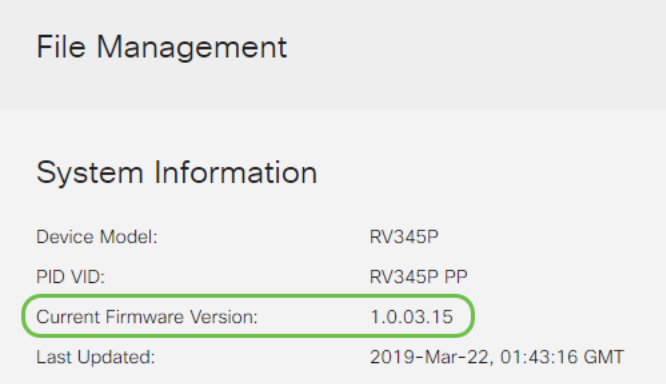
手順 1

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



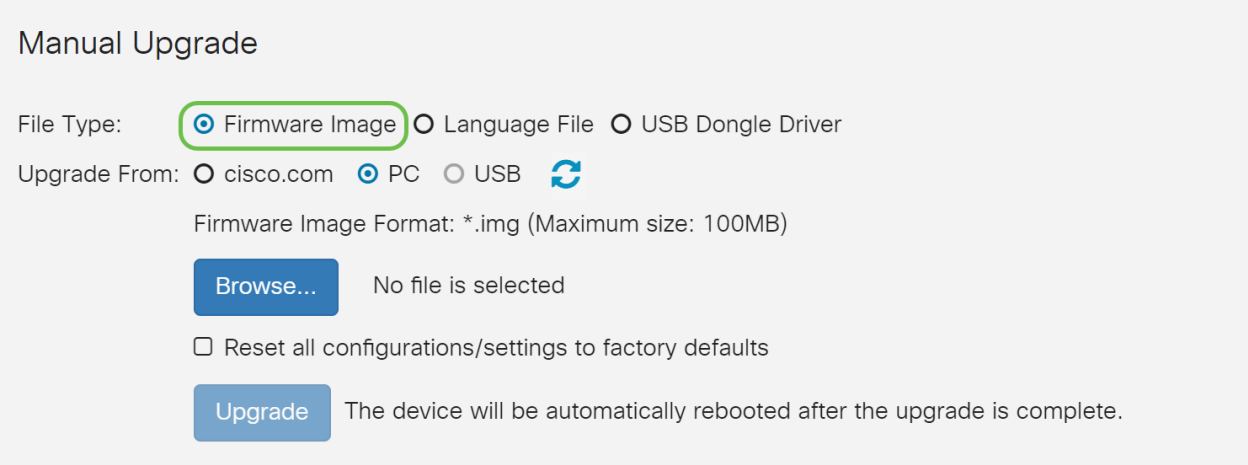
[システム情報]領域で、次のサブエリアで説明します。

- [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。

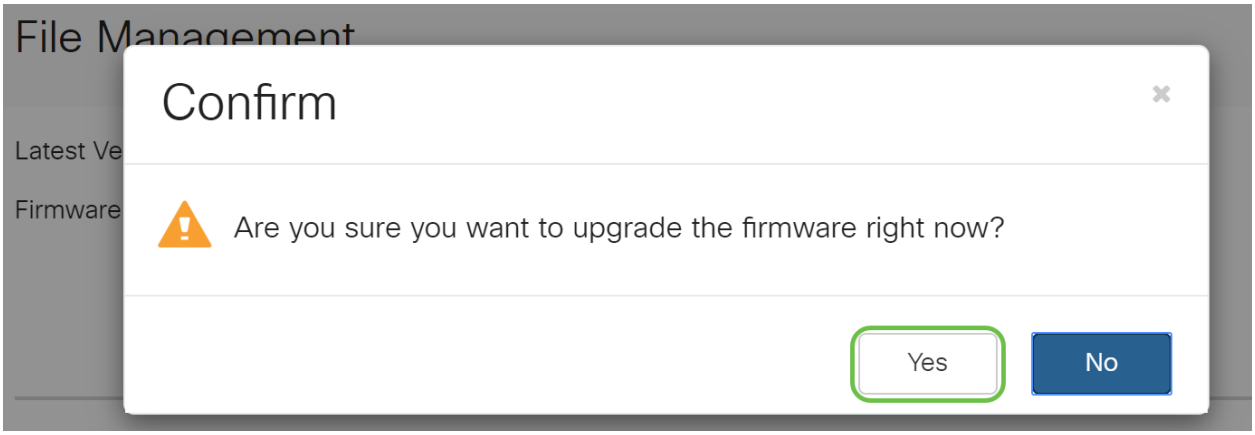
デバイスがインターネットに接続されていない場合、またはインターネットの切断が発生している場合は、cisco.comからアップグレードできません。これに関係する場合は、他のオプションを参照して ください。

手順 4

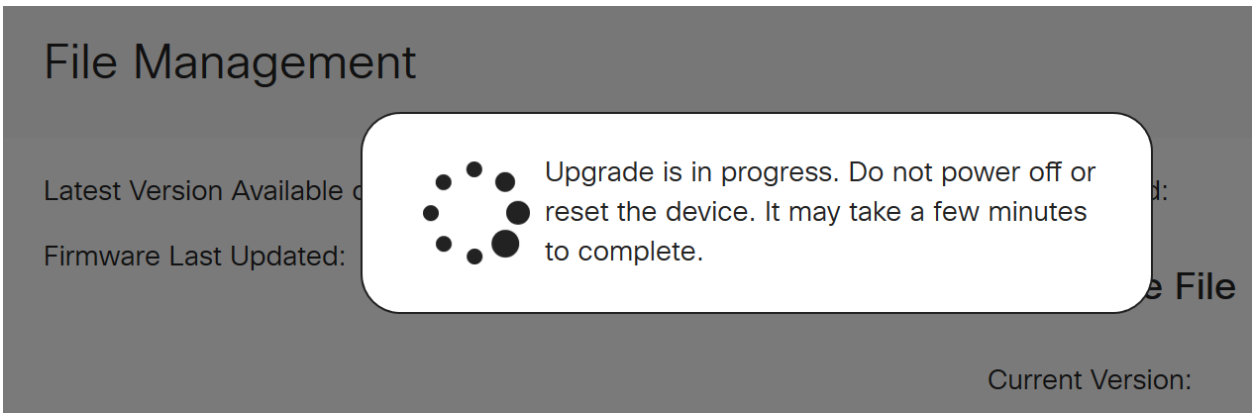
[Upgrade] をクリックします。

手順 5

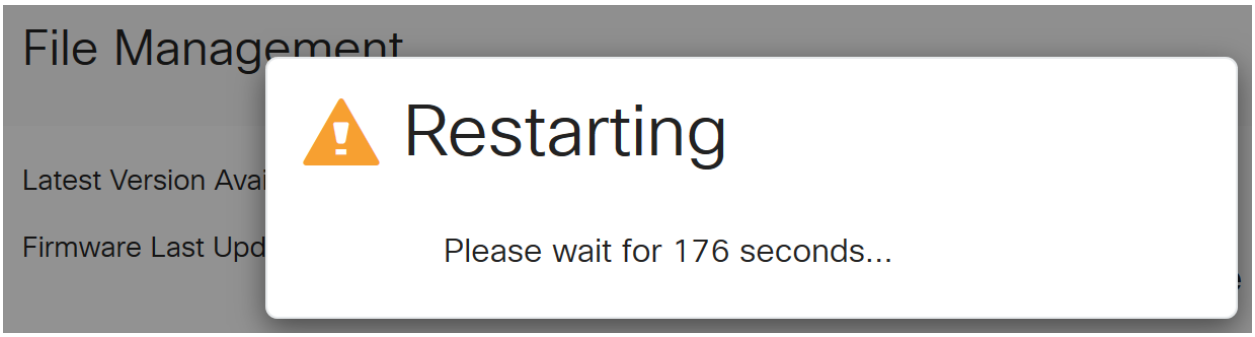
確認ウィンドウで[はい]をクリックして続行します。



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。

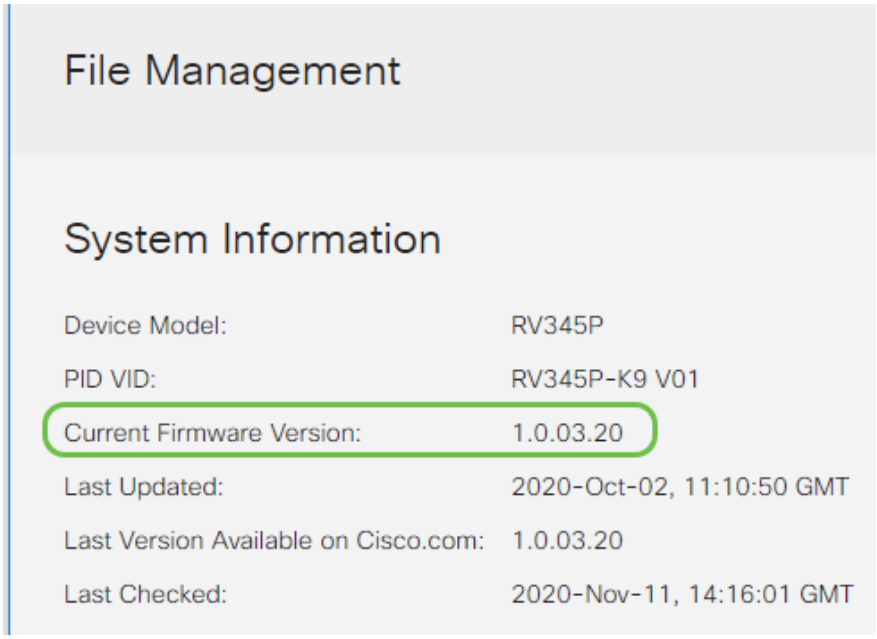


アップグレードが完了すると、通知ウィンドウがポップアップ表示され、プロセスが終了するまでの推定時間をカウントダウンしてルータが*再起動*することを通知します。その後、ログアウトされます。



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。

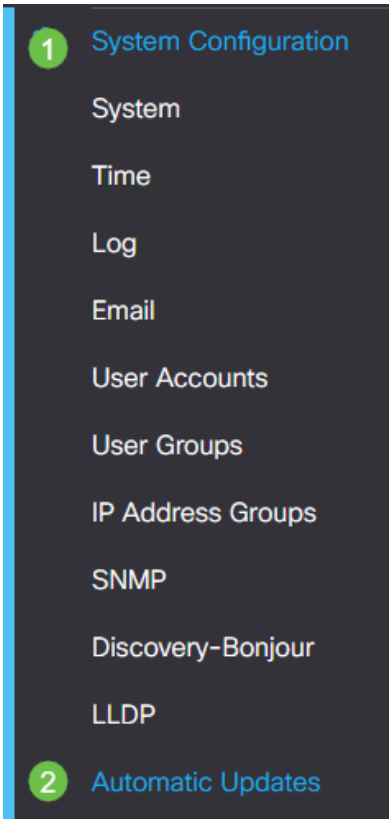


RV345Pシリーズルータの自動更新の設定

アップデートは非常に重要で、忙しい人なので、ここから先は自動更新を設定するのが理にかなっています。

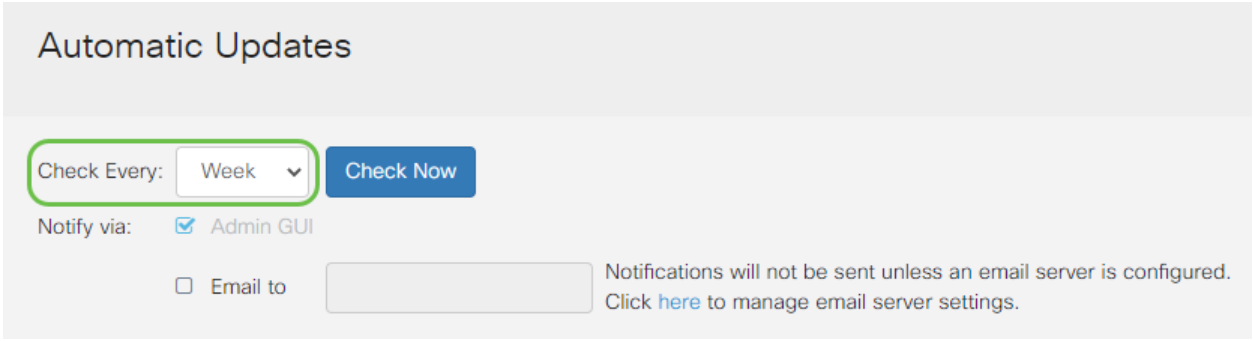
手順 1

Webベースのユーティリティにログインし、**[System Configuration] > [Automatic Updates]を選択します。**



手順 2

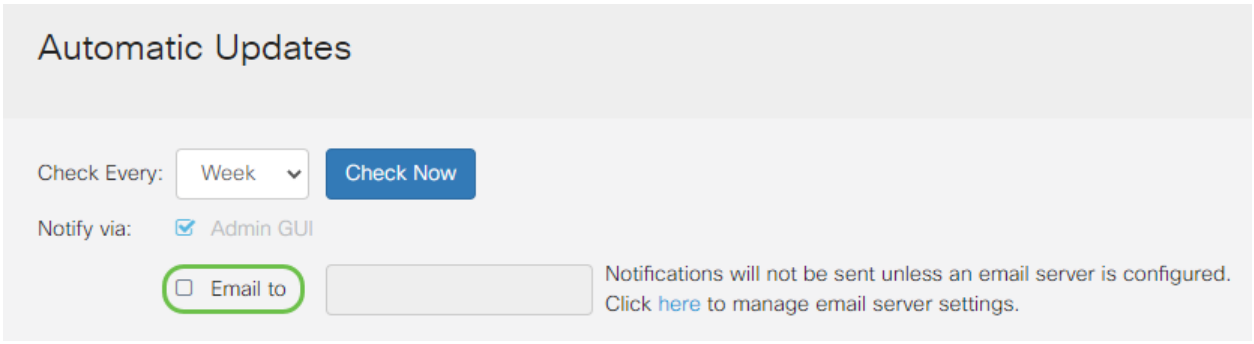
[Check Every] ドロップダウンリストから、ルータが更新をチェックする頻度を選択します。



手順 3

[Notify via]領*域で、[Email to]*チェックボックスをオンにし**て、**電子メールで更新を受信します。[管理GUI]*チェックボックス*はデフォルトで有効になっており、無効にすることはできません。更新が利用可能になると、Webベースの設定に通知が表示されます。

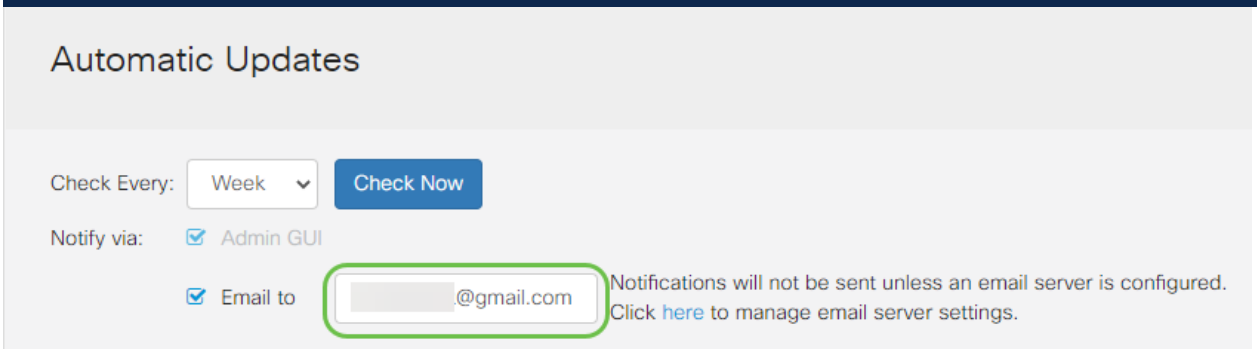
電子メールサーバの設定を行う場合は、ここをクリックして**詳細を**確認してください。



手順 4

[Email to address]フィールドに電子メール*アドレス*を入力します。

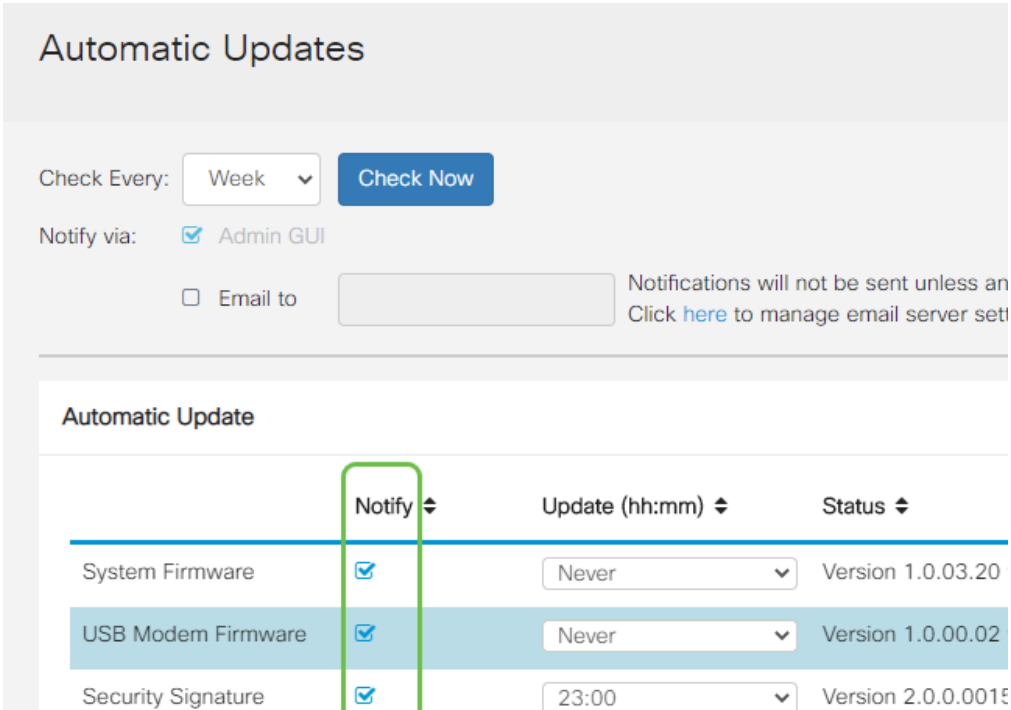
個人の電子メールを使用してプライバシーを維持するのではなく、別の電子メールアカウントを使用することを強く推奨します。



手順 5

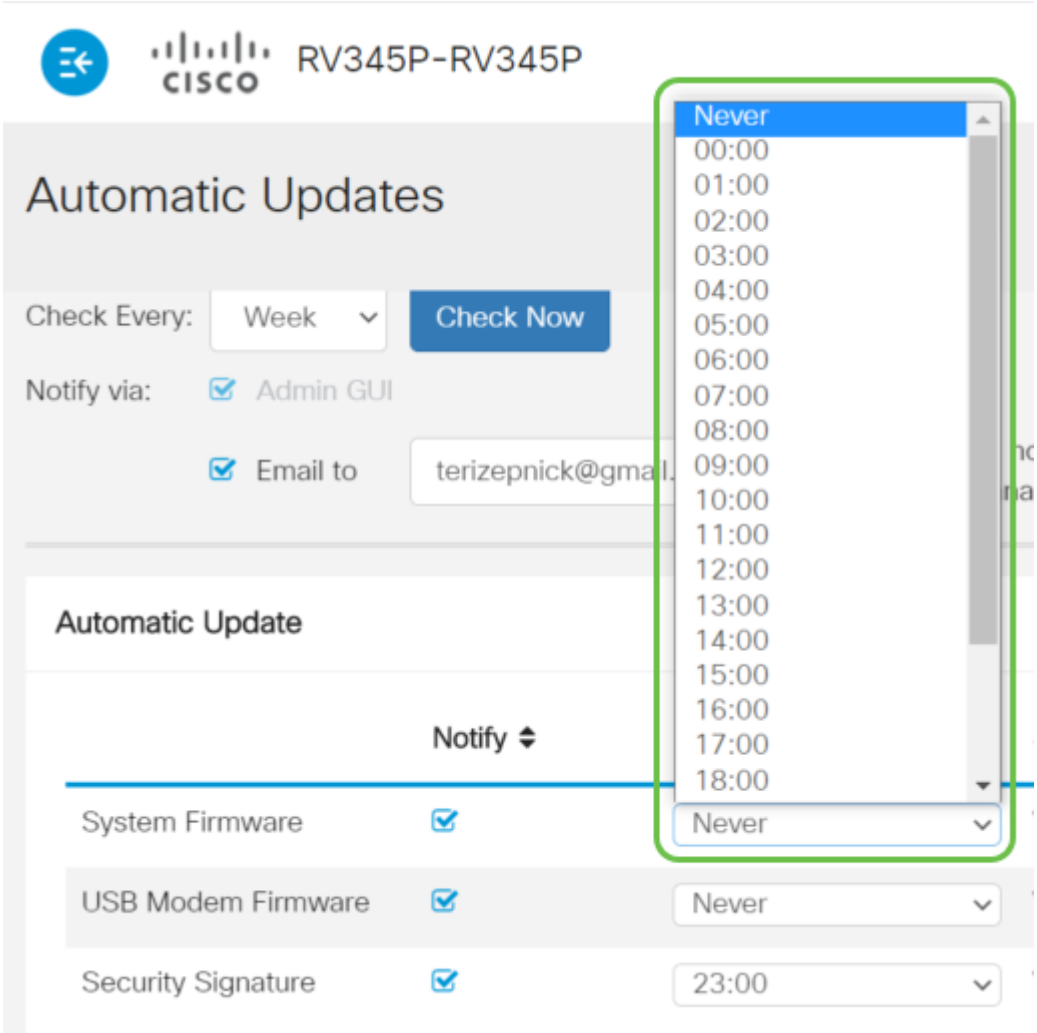
[自動更*新]領*域で、通知する更新**の種類**の[通知]チェックボックスをオンにします。次のオプションがあります。

- システムファームウェア：デバイスのメイン制御プログラム。
- USBモデムファームウェア：USBポートの制御プログラムまたはドライバ。
- セキュリティシグニチャ：アプリケーション、デバイスタイプ、オペレーティングシステムなどを識別するためのApplication Controlのシグニチャが含まれます。



手順 6

[自動更新] *ドロップ*ダウンリストから、自動更新を実行する時刻を選択します。選択した更新の種類に応じてオプションが異なる場合があります。セキュリティ署名は、即時更新を行う唯一のオプションです。オフィスを閉じる時間を設定して、サービスが不都合な時間に中断されないようにすることをお勧めします。



ステータスには、ファームウェアまたはセキュリティシグニチャの現在実行されているバージョンが表示されます。

ステップ7

[Apply] をクリックします。

手順 8

構成を永続的に保存するには、[構成のコピー/保存]ページに移動するか、ページの上部にある保**存アイコン**をクリックします。

素晴らしい、ルータの基本設定が完了しました！ここでは、いくつかの設定オプションについて説明します。

セキュリティオプション

もちろん、ネットワークを安全なものにしたいのです。複雑なパスワードを使用するなど、いくつかの簡単なオプションがありますが、セキュリティに関するセクションでは、さらに安全なネットワークの手順を確認します。

RVセキュリティライセンス (オプション)

このRVセキュリティライセンス機能は、インターネットからの攻撃からネットワークを保護します。

- 侵入防御システム(IPS):ネットワークパケットを検査し、ログを記録し、広範なネットワーク攻撃をブロックします。ネットワークの可用性の向上、迅速な修復、包括的な脅威保護を実現します。
- ウイルス対策：HTTP、FTP、SMTP電子メールの添付ファイル、POP3電子メールの添付ファイル、ルータを通過するIMAP電子メールの添付ファイルなど、さまざまなプロトコルをアプリケーションでスキャンすることにより、ウイルスから保護します。
- Webセキュリティ：インターネットに接続しながらビジネスの効率性とセキュリティを実現し、エンドデバイスとインターネットアプリケーションのインターネットアクセスポリシーを使用して、パフォーマンスとセキュリティを確保します。クラウドベースであり、分類されたドメイン数が4億5,000万を超える80以上のカテゴリが含まれています。
- アプリケーションID:ポリシーを特定し、インターネットアプリケーションに割り当てます。500個の固有のアプリケーションが自動的に特定されます。
- クライアントID:クライアントを動的に特定し、分類します。エンドデバイスカテゴリとオペレーティングシステムに基づいてポリシーを割り当てる機能。

RVセキュリティライセンスは、Webフィルタリングを提供します。Webフィルタリングは、不適切なWebサイトへのアクセスを管理できる機能です。クライアントのWebアクセス要求をスクリーニングして、そのWebサイトを許可するか拒否するかを決定できます。

ライセンスされたセキュリティ機能は、90日間無償で試用できます。評価期間終了後も、ルータの高度なセキュリティ機能を引き続き使用する場合は、ライセンスを取得してアクティブにする必要があります。

もう1つのセキュリティオプションはCisco Umbrellaです。Umbrellaセクションに移動する場合は、ここをクリックしてください。

どちらのセキュリティライセンスも必要ない場合は、をクリックして、このドキュメ

ントの「VPN」セクションに移動します。

スマートアカウントの概要

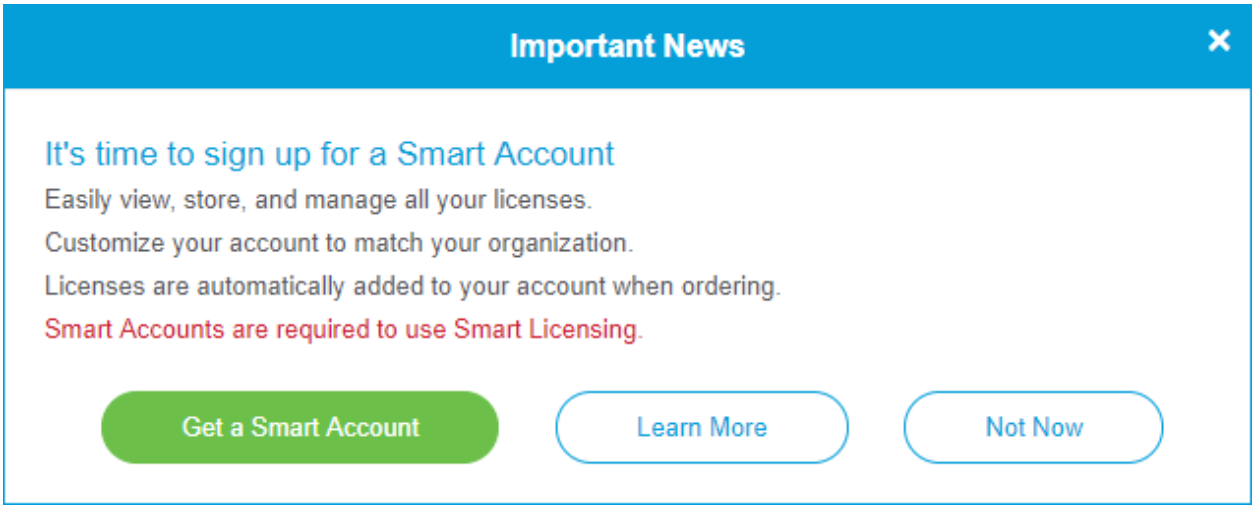
RVセキュリティライセンスを購入するには、スマートアカウントが必要です。

このスマートアカウントのアクティベーションを承認することにより、アカウントを作成し、製品およびサービスの権利、ライセンス契約、アカウントへのユーザアクセスを組織に代わって管理する権限に同意したことになります。シスコパートナーは、お客様に代わってアカウントの作成を承認することはできません。

新しいスマートアカウントの作成は1回限りのイベントであり、その後の管理はツールを通じて提供されます。

スマートアカウントの作成

Cisco.comアカウントまたはCCO ID（このドキュメントの最初に作成したID）を使用して一般的なシスコアカウントにアクセスすると、スマートアカウントを作成するためのメッセージが表示されることがあります。



このポップアップが表示されない場合は、クリックして[スマートアカウントの作成]ページに移動できます。必要に応じて、Cisco.comアカウントの認証情報を使用してログインします。

スマートアカウントのリクエスト手順の詳細については、ここをクリックしてください。

アカウント名とその他の登録の詳細を必ずメモしておいてください。

ヒント：ドメインを入力する必要があり、ドメインがない場合は、name@domain.comの形式で電子メールアドレスを入力できます。一般的なドメインは、会社やプロバイダーによってGmail、Yahooなどです。

RVセキュリティライセンスを購入する前に、Cisco.com(CCO ID)アカウントとシスコスマ

ートアカウントを所有していることが非常に重要です。

RVセキュリティライセンスの購入

シスコディストリビュータまたはシスコパートナーからライセンスを購入する必要があります。シスコパートナーを検索するには、ここをクリックします。

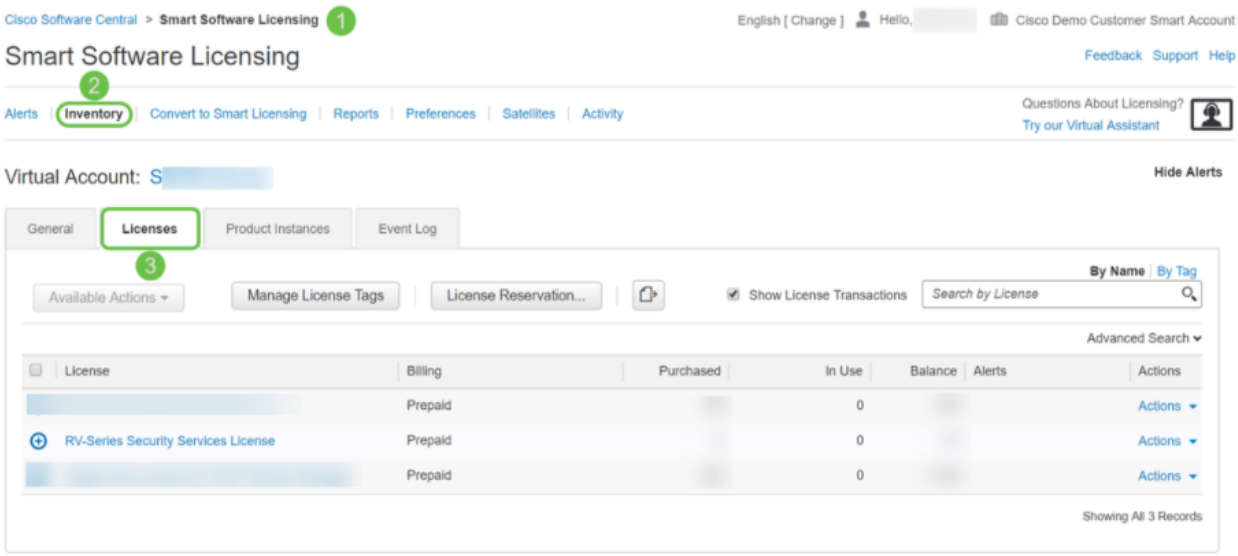
次の表に、ライセンスの製品番号を示します。

Type	製品 ID	説明
RVセキュリティライセンス	LS-RV34X-SEC-1YR=	RVセキュリティ：1年：Dynamic Web Filter、Application Visibility、Client Identification and Statistics、Gateway Antivirus、およびIntrusion Prevention System IPS。

ライセンスキーはルータに直接入力されませんが、ライセンスの発注後にシスコスマートアカウントに割り当てられます。ライセンスがアカウントに表示されるまでに要する時間は、パートナーが注文を受け入れる時期、およびリセラーがライセンスをアカウントにリンクする時期（通常は24 ～ 48時間）によって異なります。

ライセンスがスマートアカウントにあることを確認する

スマートライセンスアカウントページに移動し、[スマートソフトウェアライセンスページ] > [インベントリ] > [ライセンス]をクリックします。

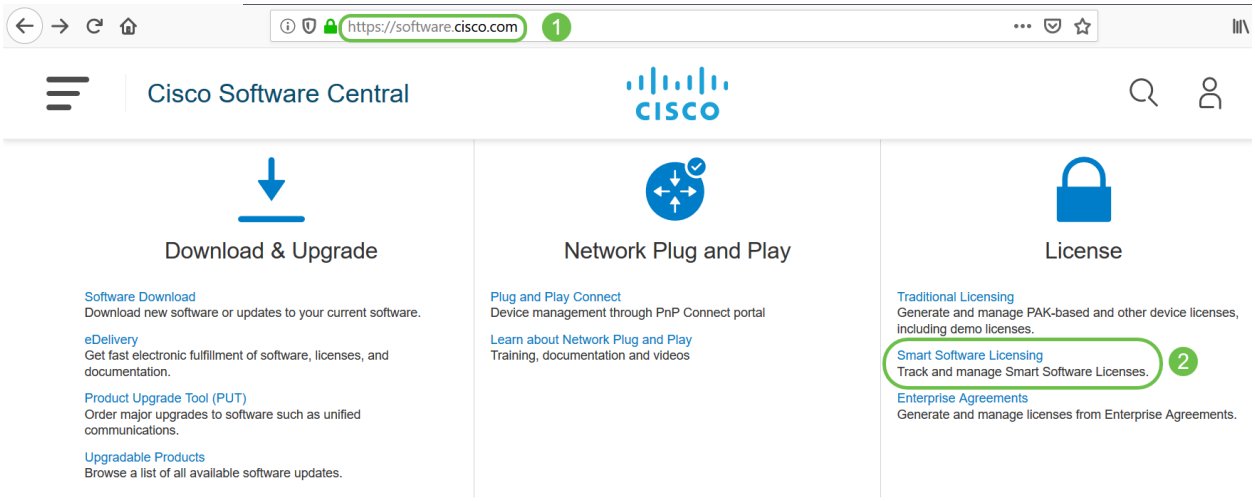


スマートアカウントにライセンスが表示されない場合は、シスコパートナーにお問い合わせください。

RV345Pシリーズルータでの RVセキュリティライセンスの設定

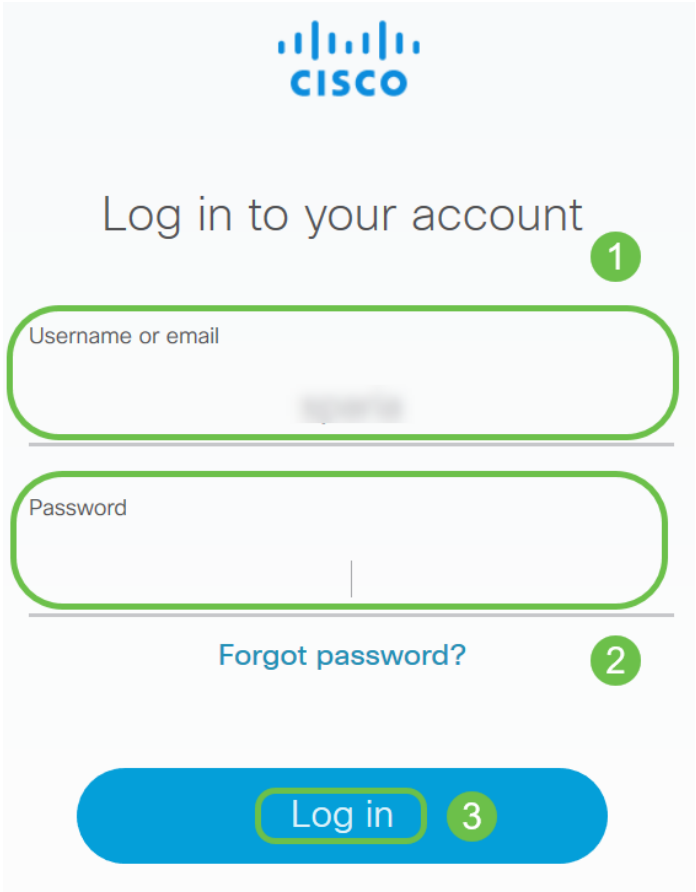
手順 1

シスコのソフトウェアにアクセスし、[Smart Software Licensing]に移動します。



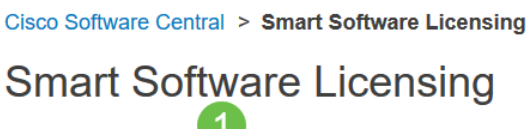
手順 2

スマートアカウントにログインするには、ユーザ名または電子メールとパスワードを入力します。[Log In] をクリックします。



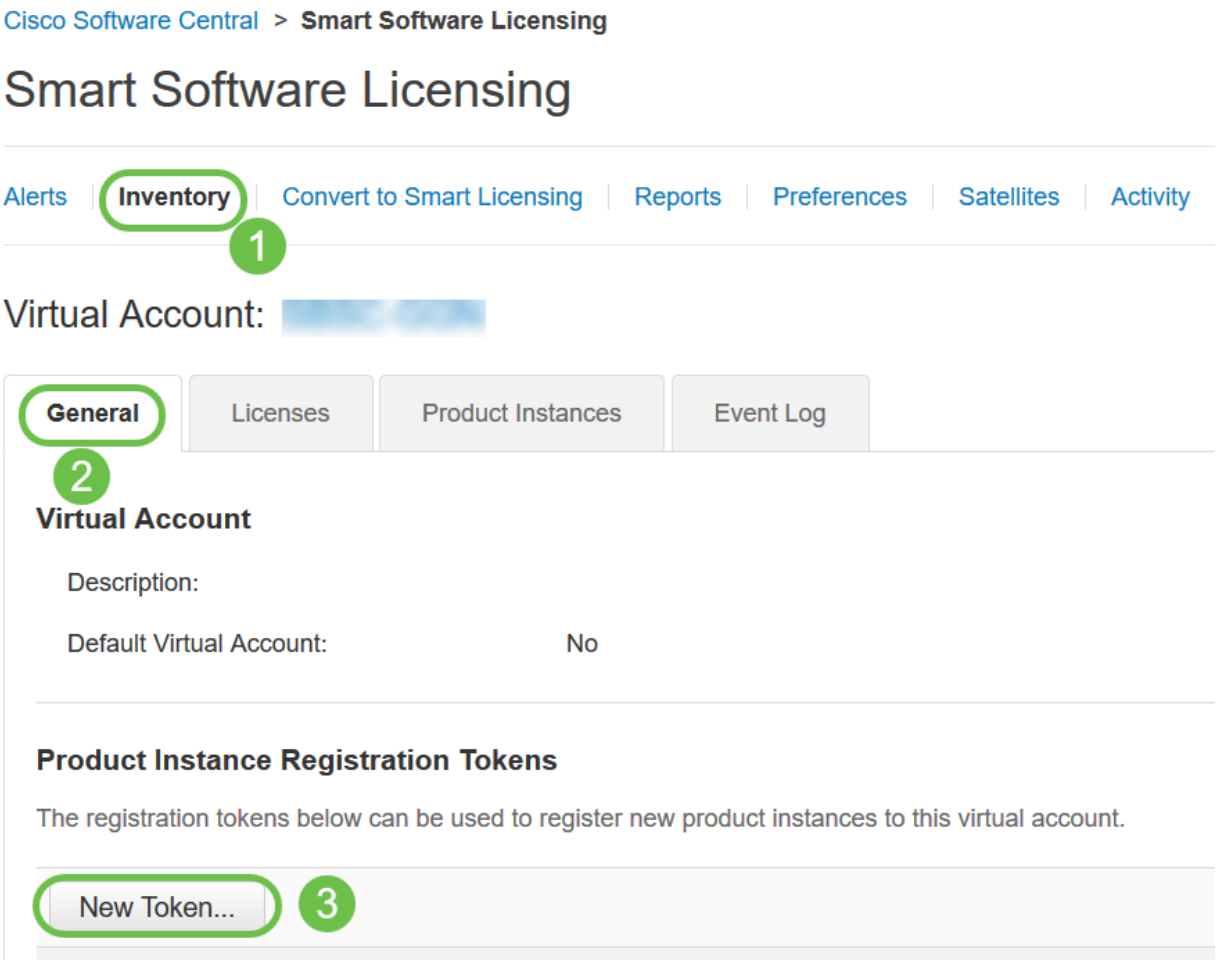
手順 3

[Inventory] > [Licenses]に移動し、*RV-Series Security Services License*がスマートアカウントにリストされていることを確認します。ライセンスが表示されない場合は、シスコパートナーにお問い合わせください。



手順 4

[インベントリ] > [一般]に移動します。[*Product Instance Registration Tokens*]で、[New Token]をクリックします。



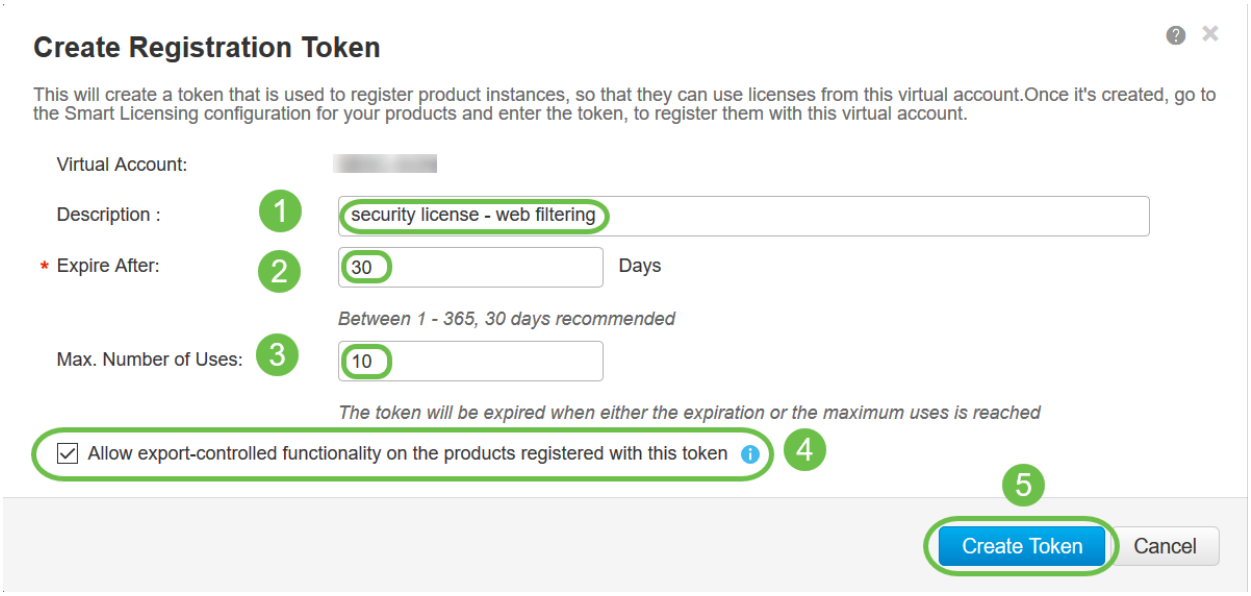
手順 5

[Create Registration Token]ウィンドウが表示されます。[仮想アカウント]領域には、登録トークンが作成される仮想アカウントが表示されます。[登録トークンの*作成*]ページで、次の手順を実行します。

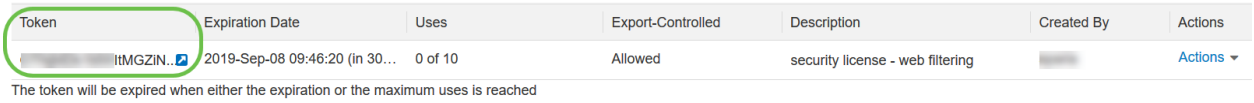
- [説明]フィールドに、トークンの一意の説明を入力します。この例では、セキュリティライセンス – Webフィルタリングが入力されています。
- [有効期限]フィールドに、1 ~ 365日の範囲の値を入力します。このフィールドの値は30日にすることを推奨します。ただし、必要に応じて値を編集することもできます。
- 最大[Number of Uses]フィールドには、そのトークンを使用する回数を定義する値を入力します。日数または最大使用回数に達すると、トークンは期限切れになります。
- 仮想アカウントの製品インスタンスのトークンに対してエクスポート制御の機能を有効にするには、[このトークンに登録された製品でエクスポート制御の機能を許可する]チェックボックスをオンにします。エクスポート制御の機能をこのトークンで使用できるようにするには、このチェックボックスをオフにします。このオプションは、輸出規制機能に準拠している場合にのみ使用してください。一部の輸出規制機能は、米国商務省によって制限されています。このトークンを使用して登録された製品のチェックボックスをオフにすると、これらの機能は制限されます。違反は罰金と管理料の対象となりま

す。

- 「トークンの**作成」をクリック**して、トークンを生成します。

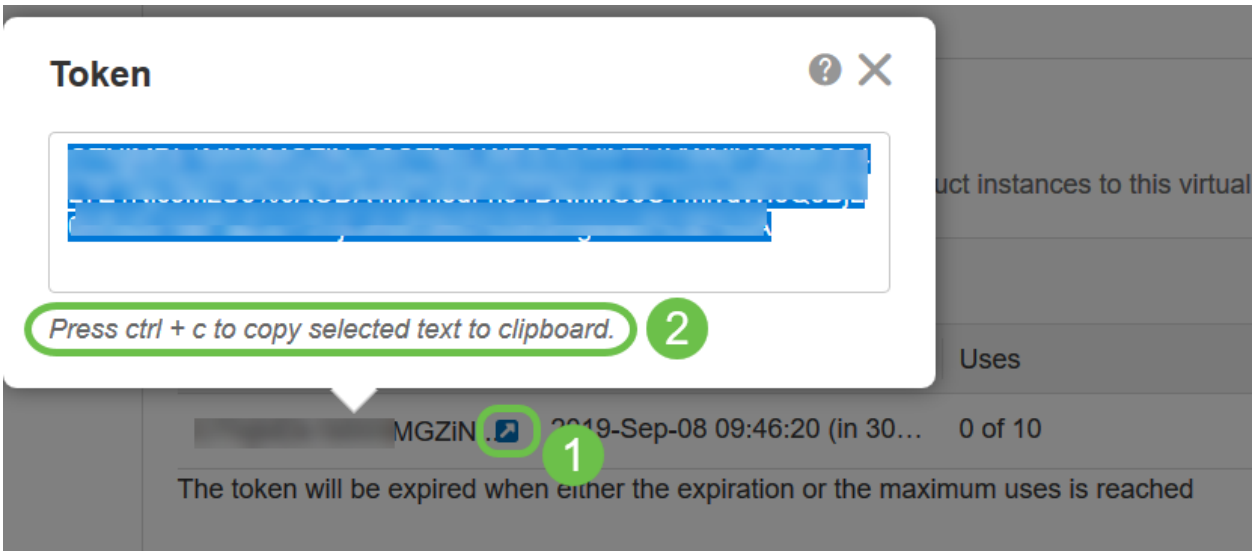


製品インスタンス登録トークンが正常に生成されました。



手順 6

[トークン]列**の矢印アイコンを**クリックし、キーボードのCtrlキーを押しながらCキーを押して**クリップボードにトークンをコピー**します。

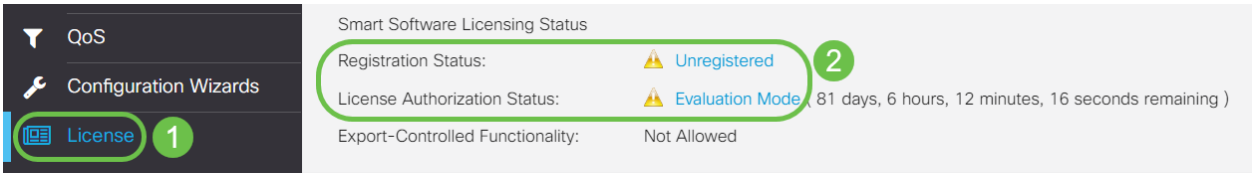


ステップ 7 (オプション)

[アクション]ドロップ**ダウン**メニューをクリックし、[コピー]**を選択**してトークンをクリップボードにコピーするか、[ダウン**ロード…**]を選択して、コピー元のトークンのテキストファイルのコピーをダウンロードします。

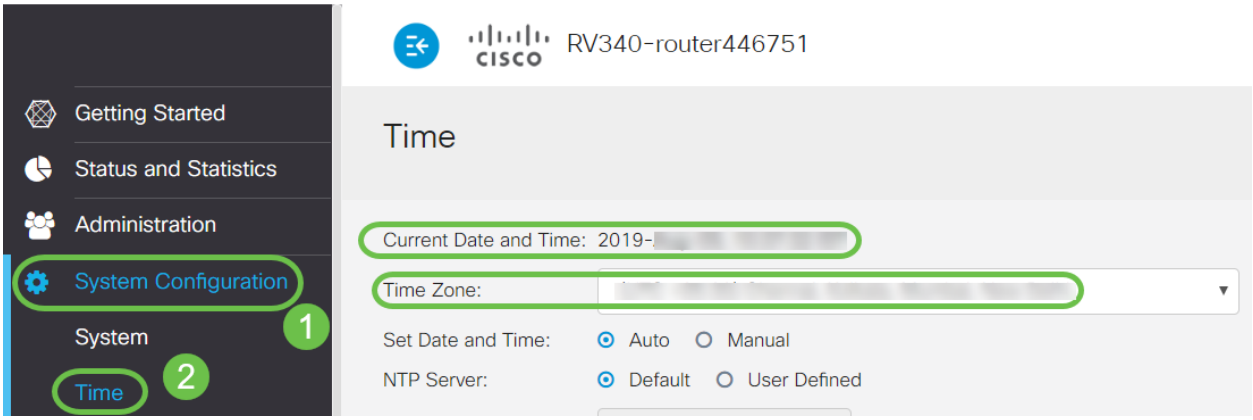
手順 8

[License]に移動し、[*Registration Status*]が[*Unregistered*]に表示され、[*License Authorization Status*]が[*Evaluation Mode*]に表示されていることを確認します。



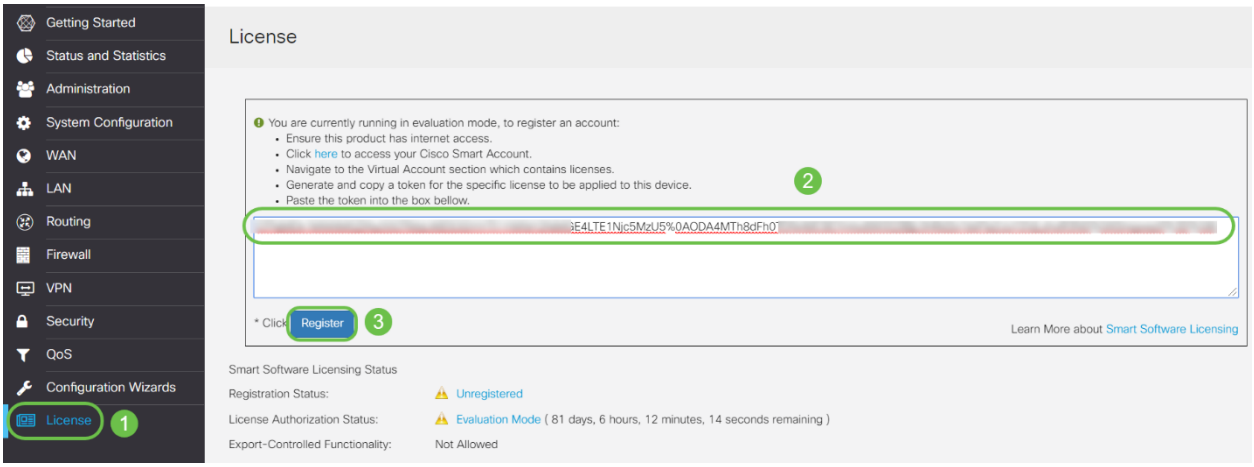
手順 9

[システム構成(**System Configuration**)] > **[時刻(Time)]に移動**し、[現在の*日付と時刻(Current Date and Time)*]と[タイムゾーン(*Time Zone*)]がタイムゾーンごとに正しく反映されていることを確認します。



手順 10

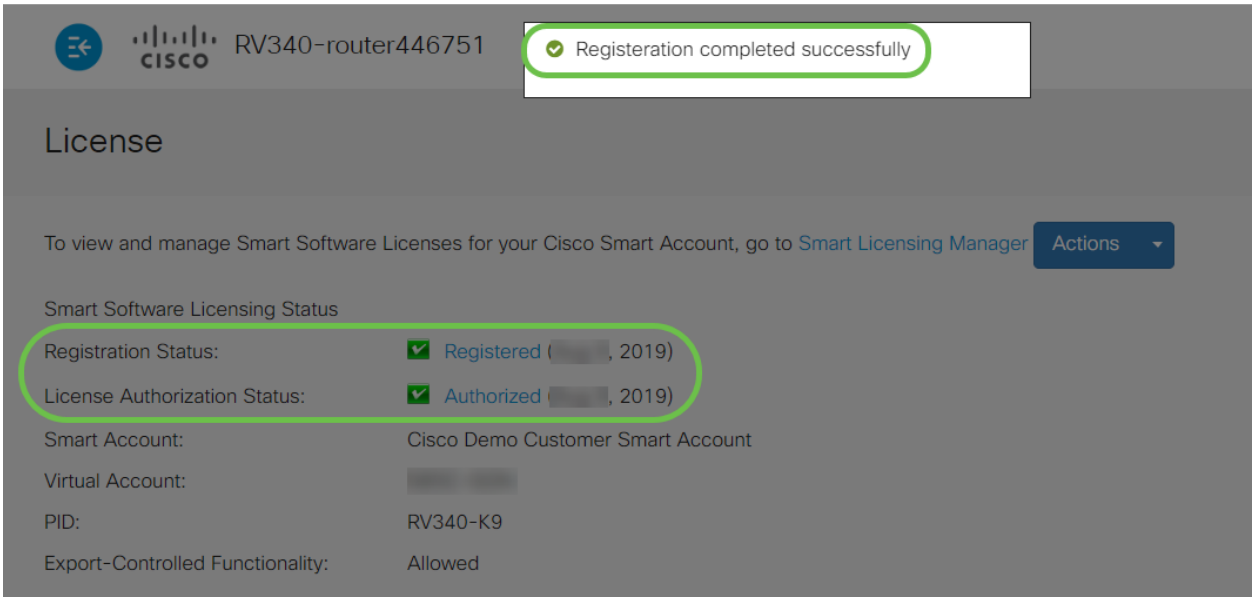
[License]に移動**します**。ステップ6でコピーしたトークンを[ライセンス]タブのテキストボックスに貼り付けます。キーボードで**ctrl + vを**選択します。[Register] をクリックします。



登録には数分かかることがあります。ルータがライセンスサーバに接続しようとするため、ページを離れないでください。

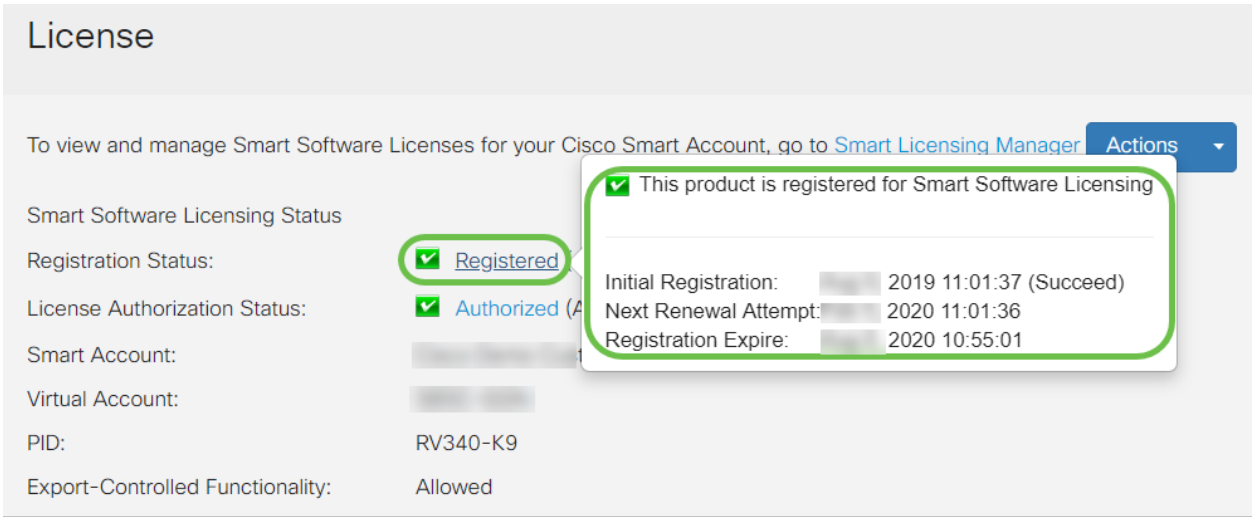
手順 11

これで、RV345Pシリーズルータのスマートライセンスの登録と承認が正常に完了したはずです。登録完了の画面に通知が表示されます。また、[Registration Status]が[*Registered*]と表示され、[*License Authorization Status*]が[*Authorized*]と表示されます。



手順 12 (オプション)

ライセンスの登録ステータスの詳細を表示するには、[登録済み]ステータスの上にポインタを置きます。次の情報を含むダイアログメッセージが表示されます。

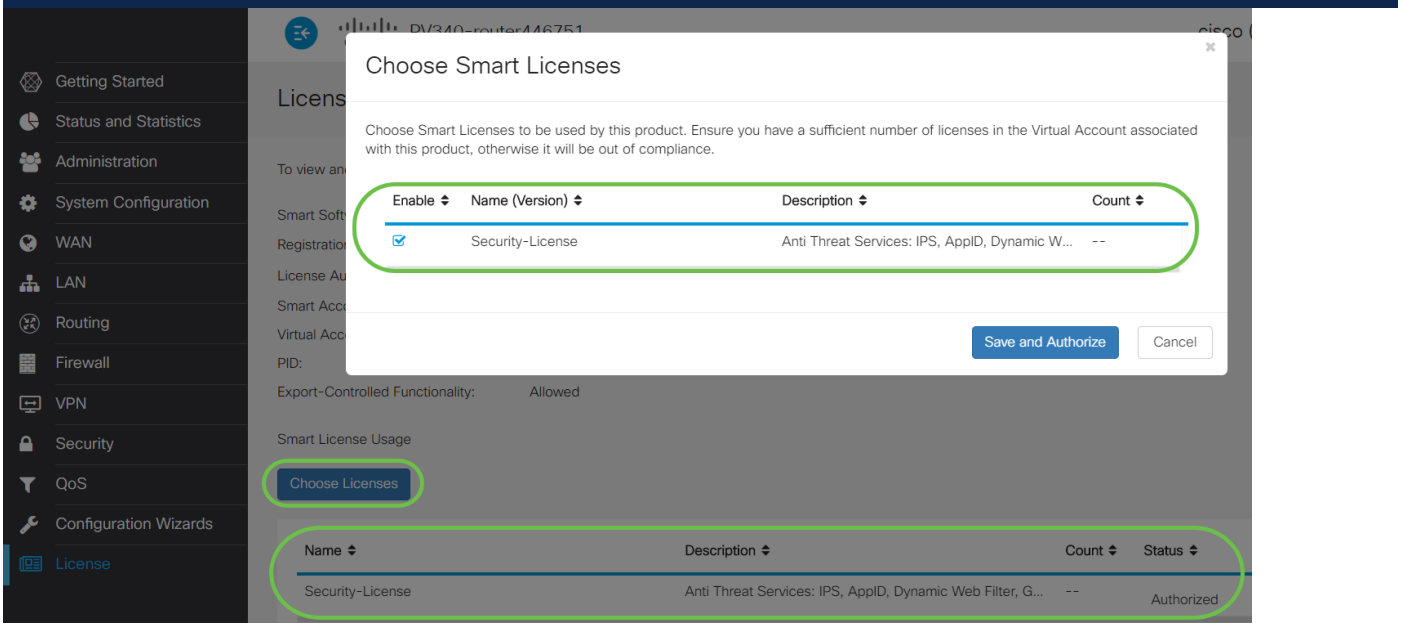


- [初期登録(Initial Registration)]：このエリアは、ライセンスが登録された日時を示します。
- [Next Renewal Attempt]：このエリアは、ルータがライセンスの更新を試行する日時を示します。
- [Registration Expire]：このエリアは、登録が期限切れになる日時を示します。

手順 13

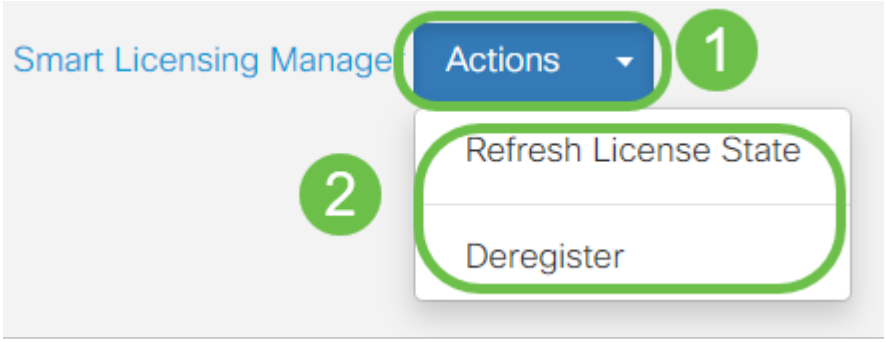
[ライセンス]ページで、[セキュリティ-ライセンス]のステータスが*[認*可]になっていることを*確認*します。[Choose License]ボタンをクリックして、[*Security-License*]が有効になっていることを*確認*することもできます。

この手順で問題が発生した場合は、ルータをリブートする必要があります。



手順 14 (オプション)

ライセンスの状態を更*新*するまたはルータからライセンスを登録解除するには、[*Smart Licensing Manager* **Actions**]ドロップダウンメニューをクリックし、アクション項目を選択します。



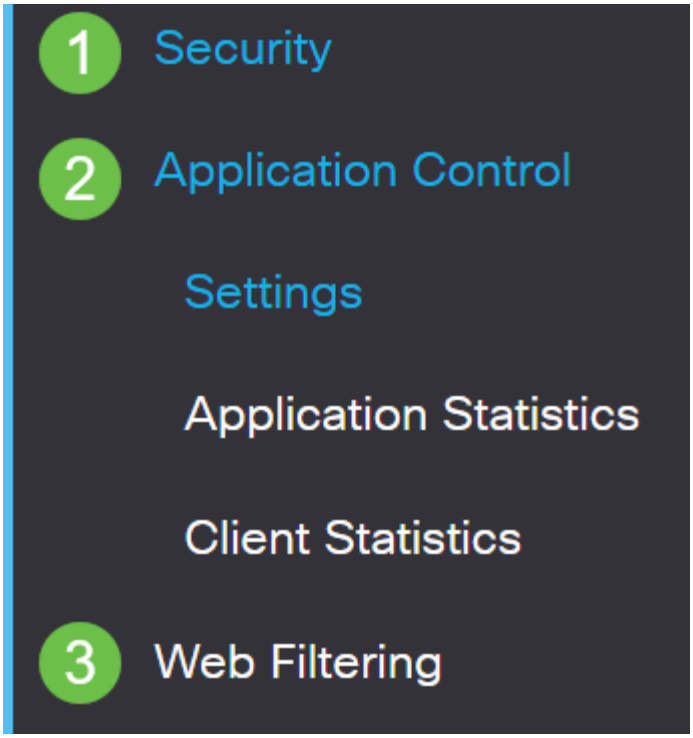
ルータにライセンスが付与されたら、次のセクションの手順を実行する必要があります。

RV345PルータのWebフィルタリング

アクティベーションから90日後に、Webフィルタリングを無料で使用できます。無料試用版の後、この機能を引き続き使用する場合は、ライセンスを購入する必要があります。クリックすると、そのセクションに戻ります。

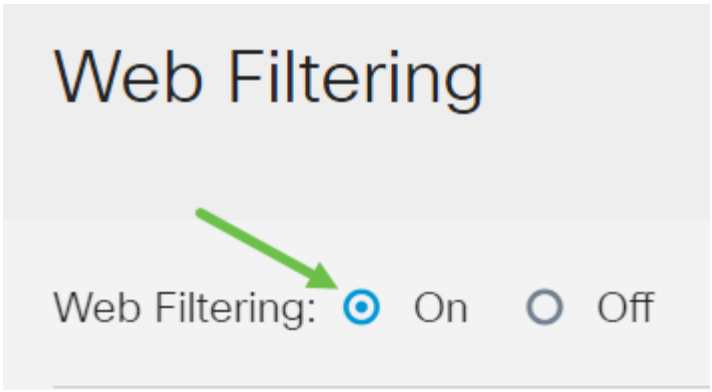
手順 1

Webベースのユーティリティにログインし、**[Security] > [Application Control] > [Web Filtering]を選択します。**



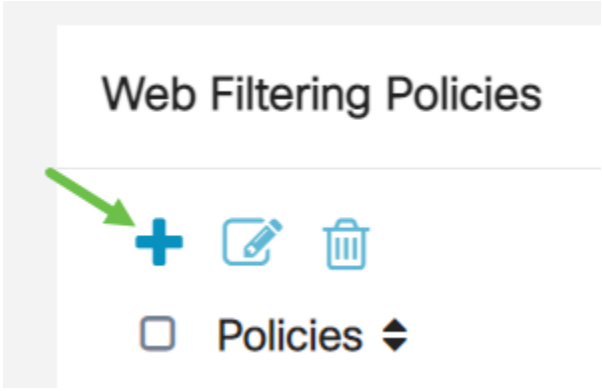
手順 2

「オン」ラジオ・**ボタン**を選択します。



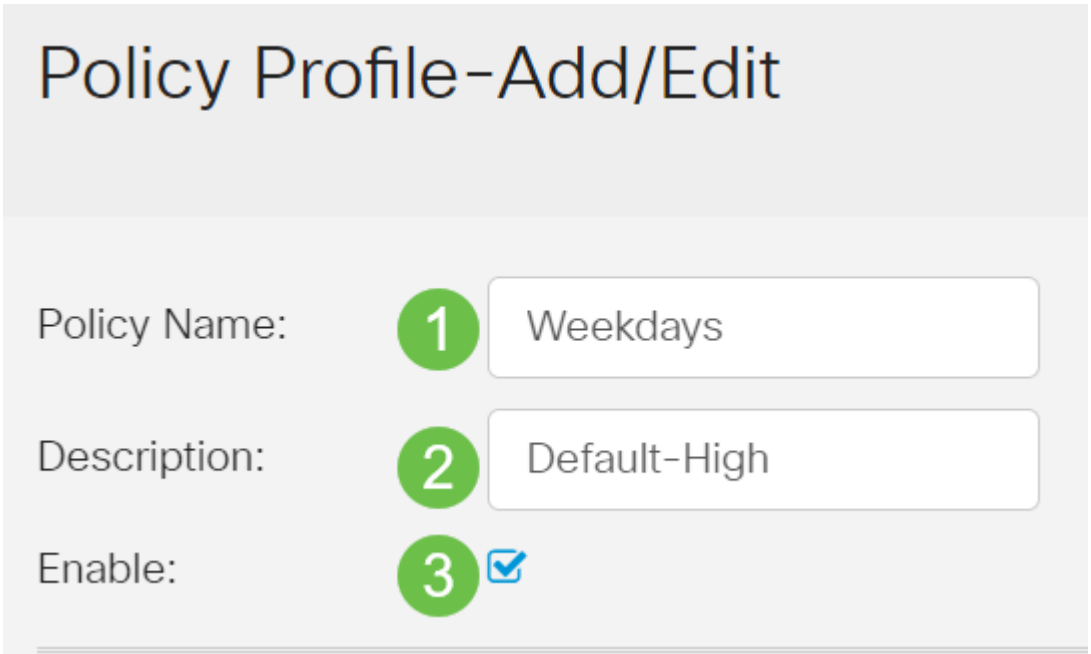
手順 3

追加アイコンを**クリックします。**



手順 4

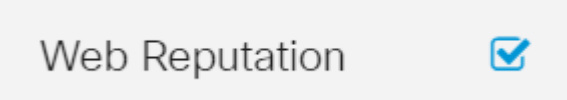
[Policy Name]、[*Description*]、および*[Enable]*チェックボックスを入力してください。



コンテンツフィルタリングがルータで有効になっている場合、コンテンツフィルタリングが無効になっており、2つの機能を同時に有効にできないことを通知する通知が表示されます。[Apply]をクリックし、設定を続行します。

手順 5

[Web Reputation]チェックボックスをオンにして、Webレピュテーションインデックスに基づくフィルタリングを有効にします。

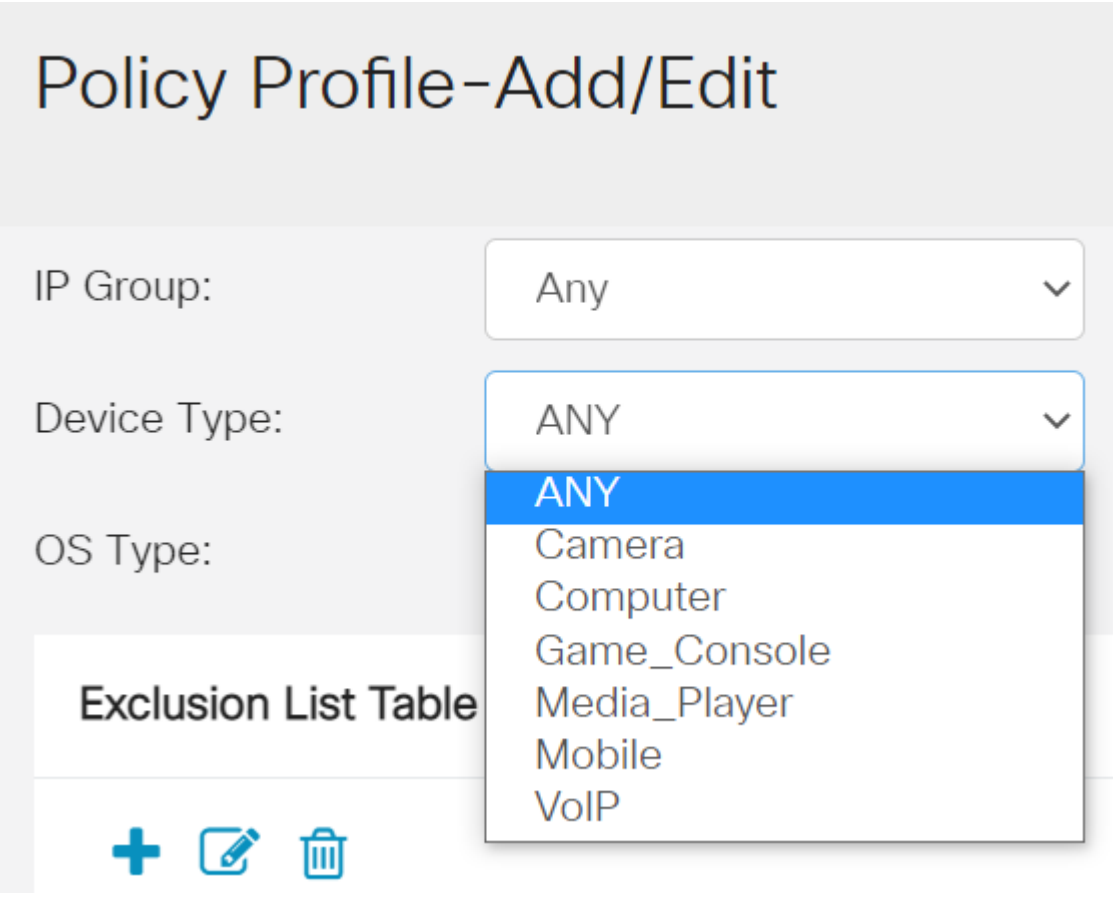


コンテンツは、Webレピュテーションインデックスに基づくWebサイトまたはURLの認知度に従ってフィルタリングされます。スコアが40を下回ると、Webサイトはブロックされます。Webレピュテーションテクノロジーの詳細については、ここをクリックして詳細を確認してください。

手順 6

[デバイスタイプ*(Device Type)*]ドロップダウンリストから、フィルタリングするパケットの送信元/宛先を選択します。一度に選択できるオプションは1つだけです。次のオプションがあります。

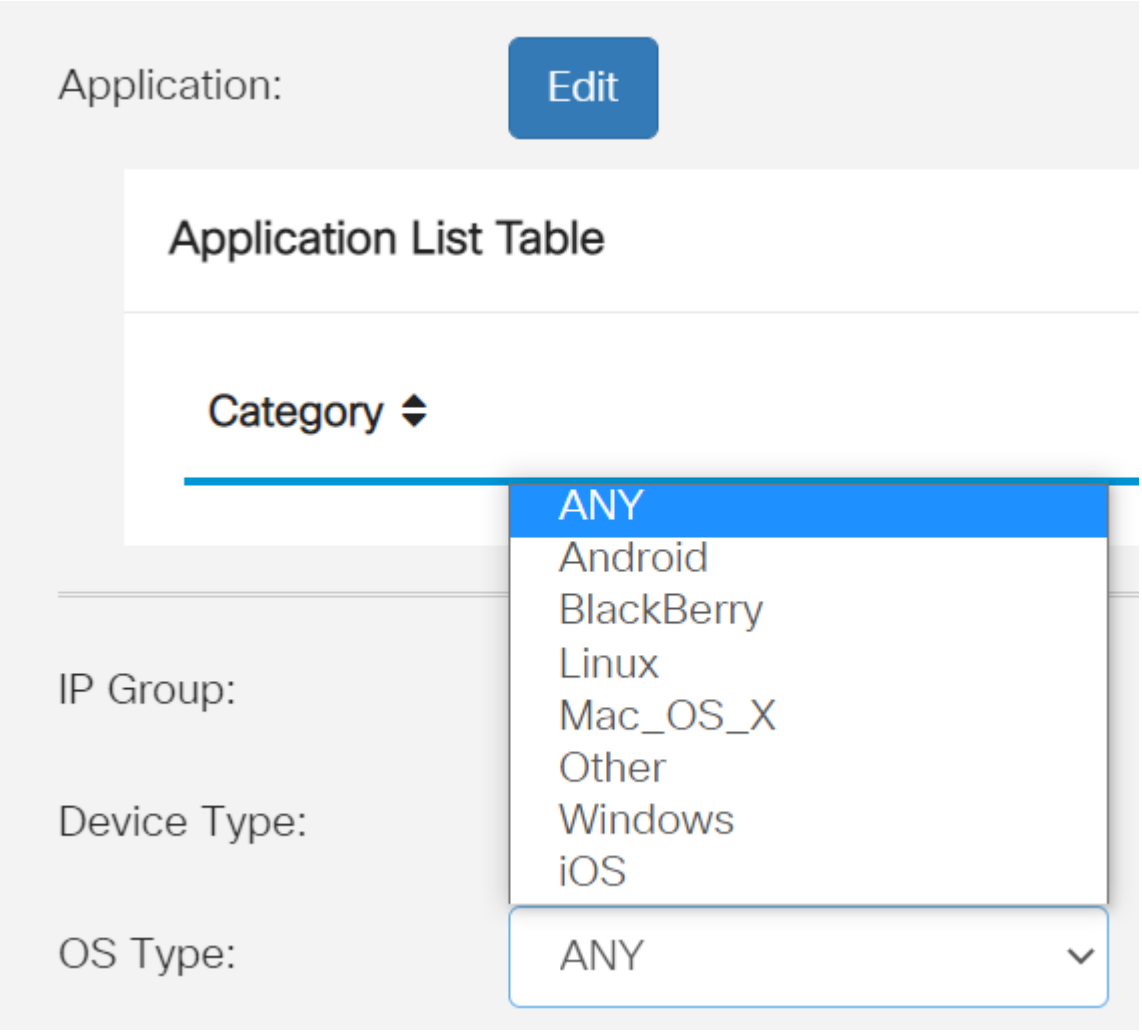
- [ANY]：任意のデバイスにポリシーを適用するには、これを選択します。
- [カメラ(Camera)]：カメラ（IPセキュリティカメラなど）にポリシーを適用します。
- [コンピュータ]：ポリシーをコンピュータに適用するには、これを選択します。
- [Game_Console]：このポリシーをゲームコンソールに適用します。
- Media_Player：ポリシーをMedia Playerに適用するには、これを選択します。
- [モバイル(Mobile)]：このポリシーをモバイルデバイスに適用します。
- [VoIP]：ポリシーをVoice over Internet Protocol(VOIP)デバイスに適用するには、これを選択します。



ステップ7

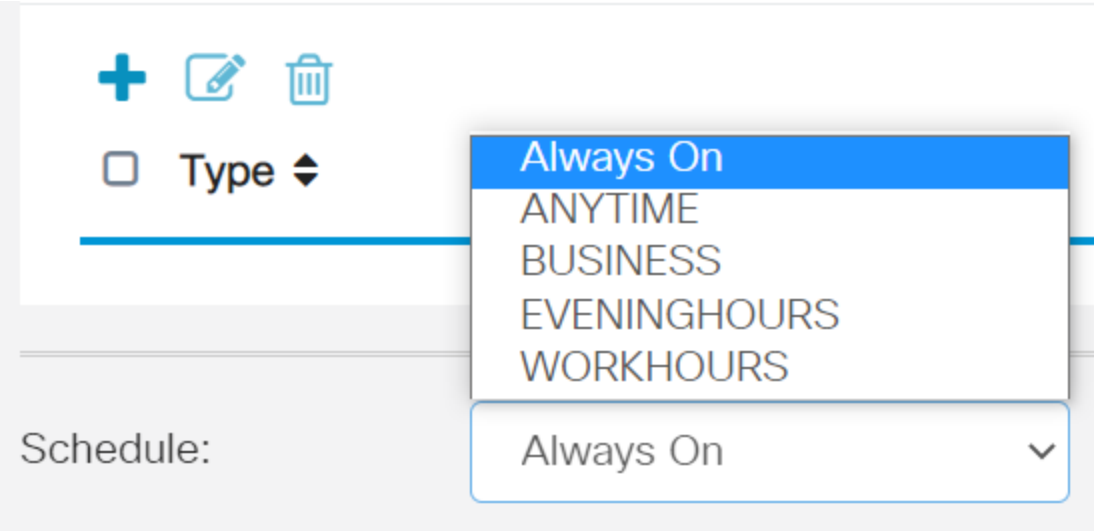
[OSタイプ]ドロップダウンリストから、ポリシーを適用するオペレーティングシステム(OS)を選択します。一度に選択できるオプションは1つだけです。次のオプションがあります。

- [ANY]：任意のタイプのOSにポリシーを適用します。これはデフォルトです。
- [Android]:Android OSだけにポリシーを適用します。
- BlackBerry：ポリシーをBlackberry OSのみに適用します。
- Linux:Linux OSだけにポリシーを適用します。
- Mac_OS_X：ポリシーをMac OSのみに適用します。
- [その他]：リストにないOSにポリシーを適用します。
- Windows：ポリシーをWindows OSに適用します。
- iOS：ポリシーをiOS OSのみに適用します。



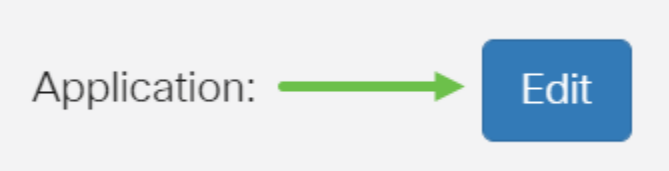
手順 8

[スケジュール]セクションまでスクロールし、ニーズに最適なオプションを選択します。



手順 9

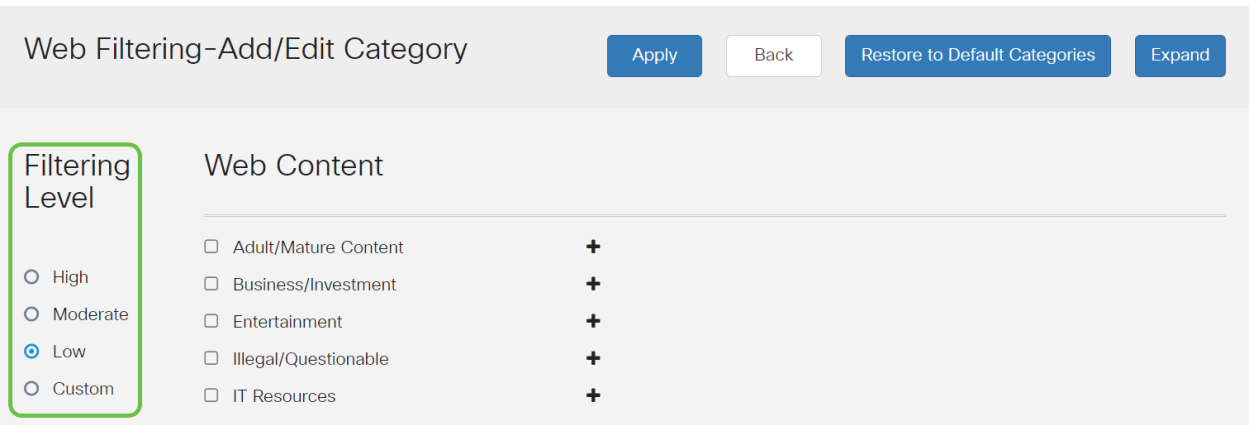
編集アイコンをクリックします。



手順 10

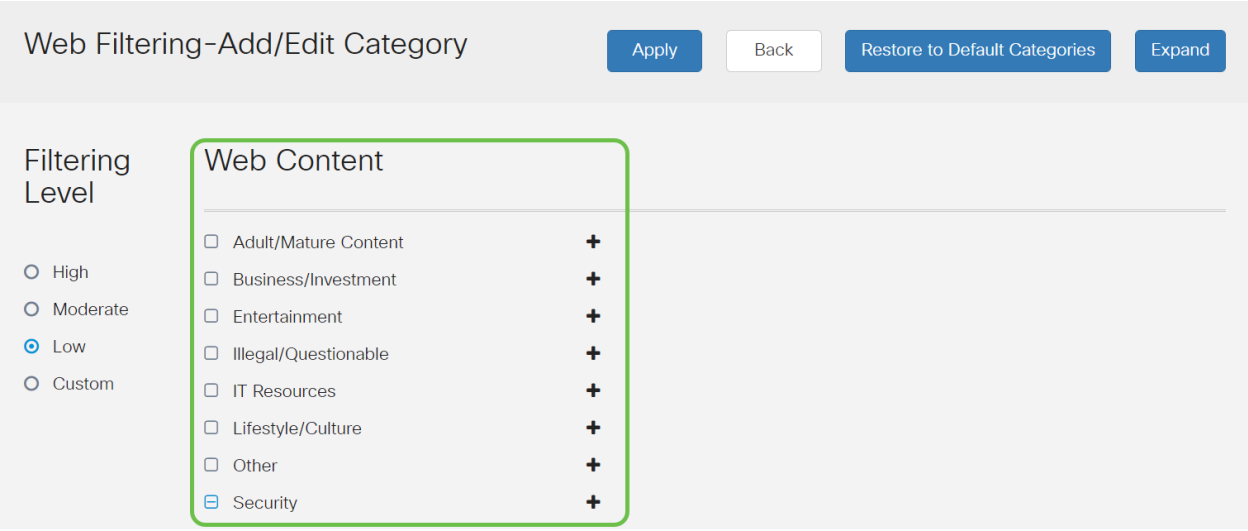
[Filtering Level]列で、オプションボタンをクリックして、ネットワークポリシーに最も適したフィルタリング範囲をすばやく定義します。オプションは、[高]、[中]、[低]、および[カスタム]です。次のいずれかのフィルタリングレベルをクリックすると、有効な各Webコンテンツカテゴリにフィルタされた特定の定義済みサブカテゴリを確認できます。事前定義されたフィルタは、これ以上変更できず、グレー表示されます。

- Low：これはデフォルトのオプションです。このオプションを使用すると、セキュリティが有効になります。
- [Moderate]:[Adult/Mature Content]、[Illegal/Againable]、および[Security]は、このオプションで有効にします。
- 高：成年/成熟度の高いコンテンツ、ビジネス/投資、不正/疑わしい、ITリソース、セキュリティがこのオプションで有効になります。
- カスタム：ユーザ定義フィルタを許可するようにデフォルトが設定されていません。



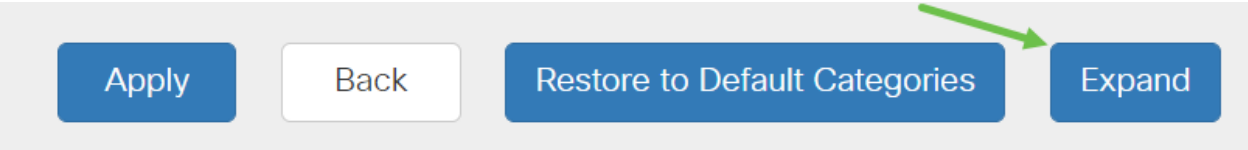
手順 11

フィルタするWebコンテンツを入力します。1つのセクションの詳細を表示するには、[+]アイコンをクリックします。



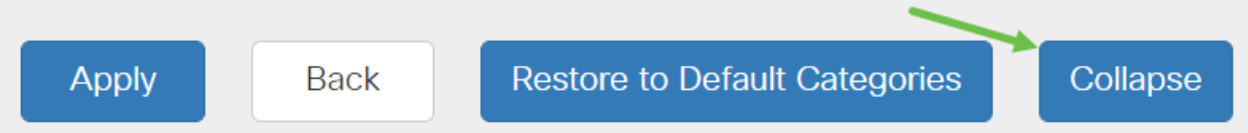
手順 12 (オプション)

すべてのWebコンテンツのサブカテゴリと説明を表示するには、[展開]ボタンをクリックします。



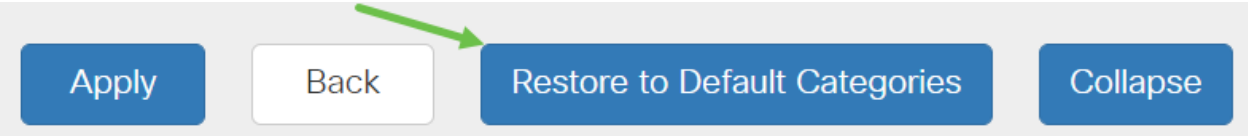
手順 13 (オプション)

[折りたたむ]をクリックして、サブカテゴリと説明を折りたたみます。



手順 14 (オプション)

既定の分類に戻るには、[既定の分類に戻す]をクリックしてください。



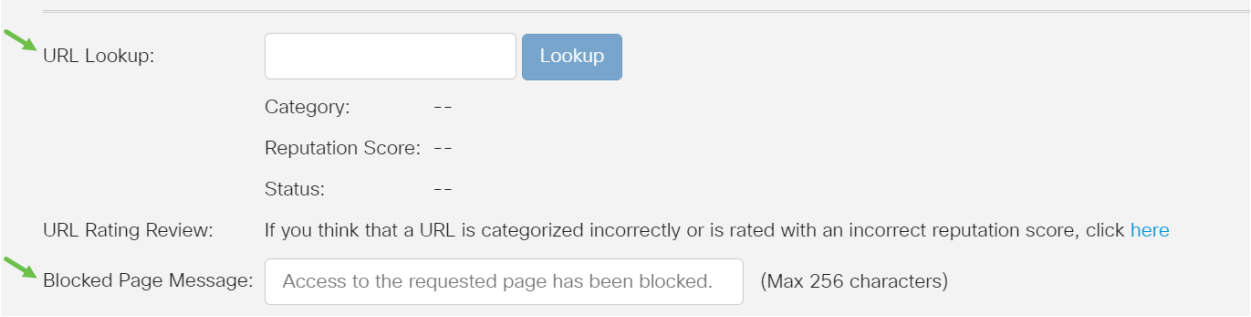
ステップ 15

[Apply]をクリックして設定を保存し、[Filter]ページに戻ってセットアップを続行します。

[Application List Table]では、選択したフィルタリングレベルに基づく対応するサブカテゴリがテーブルに入力されます。

手順 16 (オプション)

その他のオプションには、URLルックアップや、要求されたページがブロックされたときに表示されるメッセージなどがあります。



手順 17 (オプション)

[Apply] をクリックします。

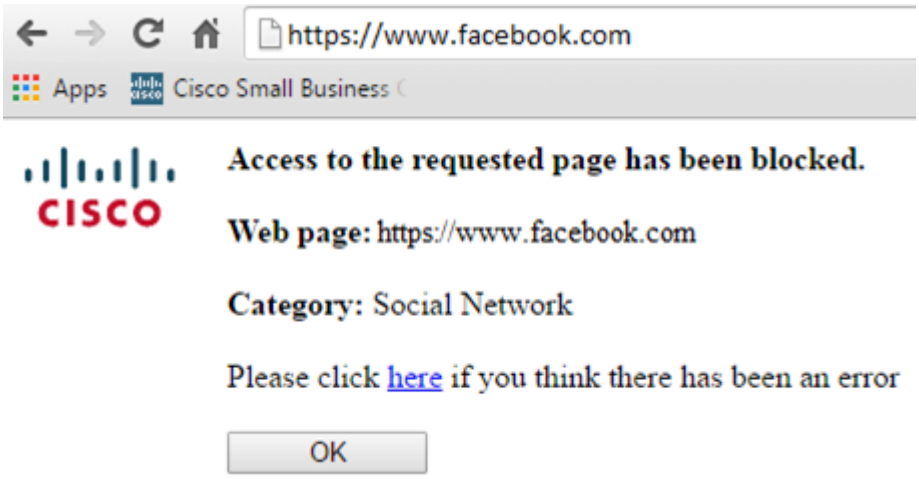
ステップ 18

構成を永続的に保存するには、[構成のコピー/保存]ページに*移動*するか、ページの上部にある**保存アイ**コンをクリックします。

手順 19 (オプション)

WebサイトまたはURLがフィルタリングまたはブロックされていることを確認するには、Webブラウザを起動するか、ブラウザで新しいタブを開きます。ブロックがリストされている、またはブロックまたは拒否するようにフィルタされたドメイン名を入力します。

この例では、www.facebook.comを使用しました。



これで、RV345PルータでWebフィルタリングが正常に設定されました。Webフィルタリングにセキュリティライセンスを使用しているため、おそらくUmbrellaは必要ありません。Umbrellaも必要な場合は、ここをクリックしてください。セキュリティが十分な場合は、をクリックして次のセクションにスキップします。

トラブルシューティング

ライセンスを購入したが、仮想アカウントに表示されない場合は、次の2つのオプションがあります。

1. リセラーに転送を依頼するには、リセラーにフォローアップしてください。
2. お問い合わせいただければ、リセラーにお問い合わせください。

理想的には、どちらでもする必要はありませんが、この交差点に到着すれば、私たちは喜んで助けます！このプロセスを可能な限り適切なものにするには、上記の表および次に示す認証情報が必要です。

必要な情報	
ライセンス請求書	ライセンスの購入が完了したら、電子メール
Cisco セールス オーダー番号	これを入手するには、リセラーに戻る必要が
スマートアカウントライセンスページのスクリーンショット	スクリーンショットを撮ると、画面の内容が

スクリーンショット

トークンを入手した後、またはトラブルシューティングを行う場合は、画面の内容をキャプチャするスクリーンショットを撮影することをお勧めします。

スクリーンショットのキャプチャに必要な手順の違いを考慮して、使用しているオペレーティングシステムに固有のリンクについては、次を参照してください。

- Windows
- MAC
- iPhone/iPad
- Android

Umbrella RV Branchライセンス（オプション）

Umbrellaは、シスコのシンプルで非常に効果的なクラウドセキュリティプラットフォームです。

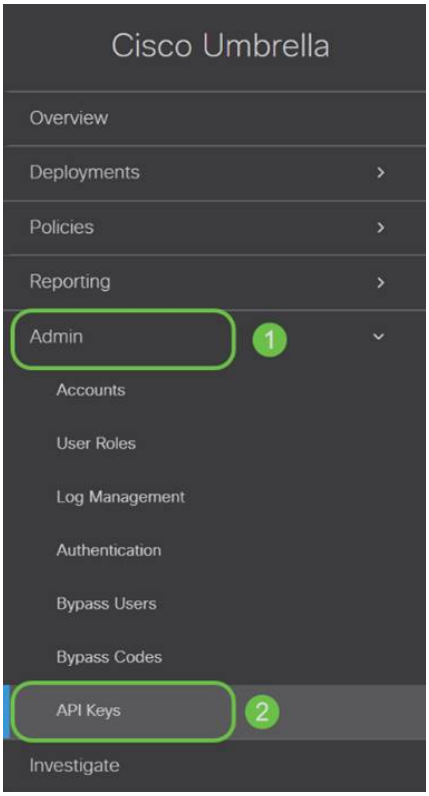
Umbrellaはクラウドで動作し、セキュリティ関連の多くのサービスを実行します。緊急脅威からイベント後の調査まで。Umbrellaは、すべてのポートとプロトコルに対する攻撃を検出し、防止します。

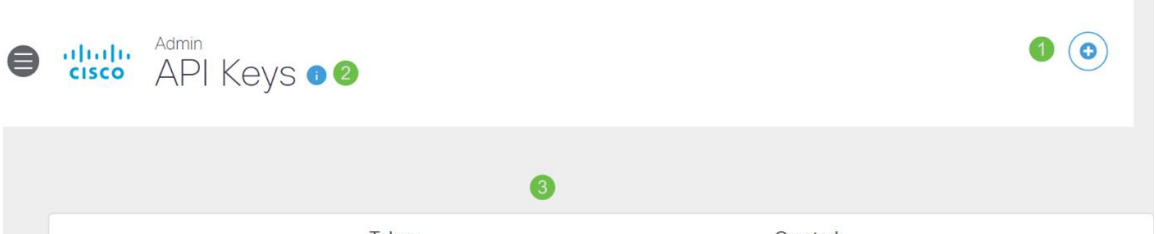
Umbrellaは、防御用のメインベクトルとしてDNSを使用します。ユーザーがブラウザーのバーにURLを入力してEnterキーを押すと、*Umbrella*が転送に参加します。このURLはUmbrellaのDNSリゾルバに渡され、セキュリティ警告がドメインに関連付けられている場合、要求はブロックされます。このテレメトリデータはマイクロ秒単位で転送および分析され、遅延はほとんど発生しません。テレメトリデータは、ログと機器を使用して、世界中の数十億のDNS要求を追跡します。このデータが広がれば、世界中に関連付けることで、攻撃の開始時に迅速に対応できるようになります。詳細については、シスコのプライバシーポリシーを参照してください。フルポリシー、サマリバージョンをご覧ください。テレメトリデータは、ツールとログから得られたデータと考えてください。

詳細とアカウントの作成については、Cisco Umbrellaをご覧ください。問題が発生した場合は、ここをチェックしてドキュメントを参照し、Umbrella Supportオプションを確認してください。

手順 1

Umbrellaアカウントにログインした後、ダッシュボード画面 で**[Admin] > [API Keys]をクリックします。**



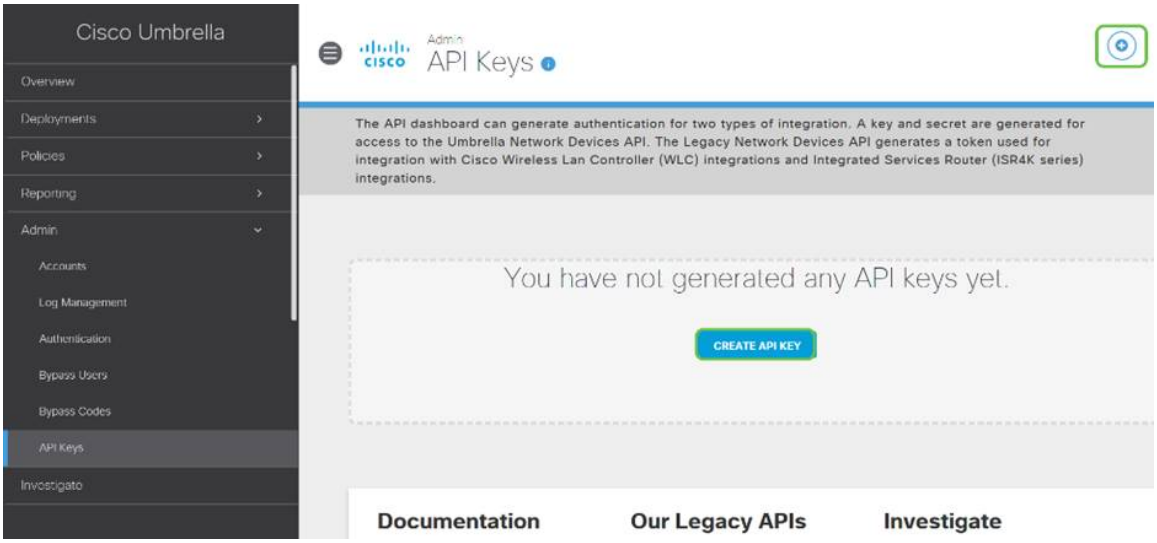


API Keys画面の構造（既存のAPIキーを使用）

1. APIキーの追加 – Umbrella APIで使用する新しいキーの作成を開始します。
2. 追加情報 – この画面の説明者と一緒に下/上にスライドします。
3. Token Well：このアカウントによって作成されたすべてのキーとトークンが含まれます。（キーが作成されると入力されます）
4. サポートドキュメント：各セクションのトピックに関するUmbrellaサイトのドキュメントへのリンク。

手順 2

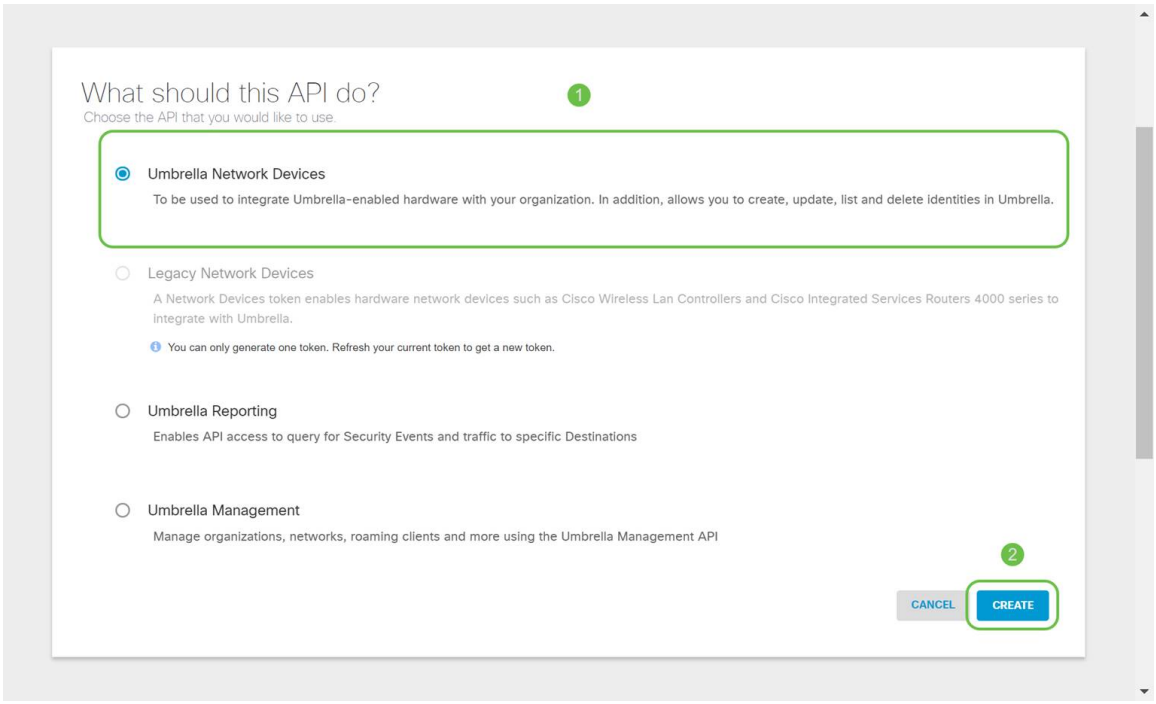
右上隅の[Add API Key]ボタンをクリックするか、[Create API Key]ボタンをクリックします。どちらも同じ機能を持ちます。



上のスクリーンショットは、このメニューを初めて開く画面に似ています。

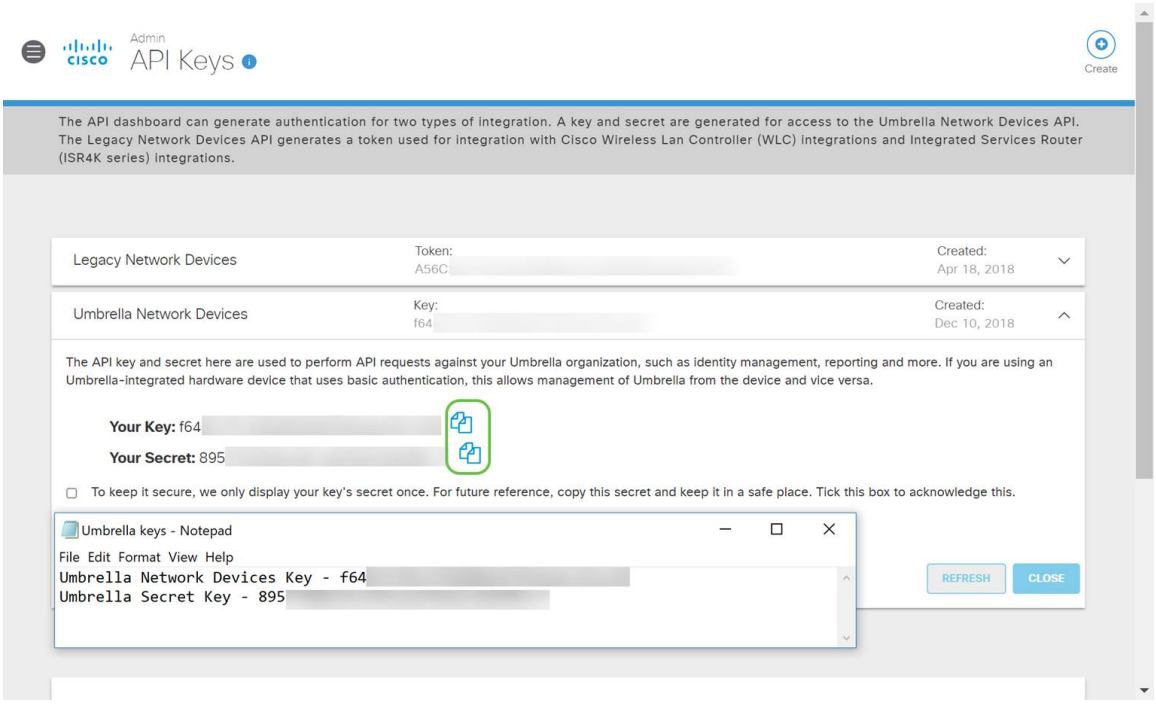
手順 3

[Umbrella Network Devices]を選択し、[Create]ボタンをクリックします。



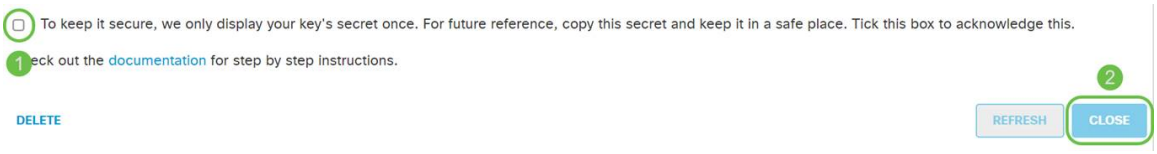
手順 4

メモ帳などのテキストエディタを開き、APIとAPI秘密キーの右側にあるコピーアイコンをクリックします。ポップアップ通知により、キーがクリップボードにコピーされたことが確認されます。一度に1つずつ、秘密とAPIキーをドキュメントに貼り付け、後で参照できるようにラベルを付けます。この場合、ラベルは「Umbrella network devices key」です。その後、テキストファイルを後でアクセスしやすい安全な場所に保存します。



手順 5

キーと秘密キーを安全な場所にコピーした後、[*Umbrella API*]*画面*でチェックボックスをクリックして、秘密キーの一時的な表示の確認を確認して、[閉じる]ボタンをクリックします。



秘密キーを紛失または誤って削除した場合、このキーを取得するためにコールする機能やサポート番号はありません。紛失した場合は、キーを削除し、Umbrellaで保護する各デバイスで新しいAPIキーを再承認する必要があります。

RV345Pの傘の設定

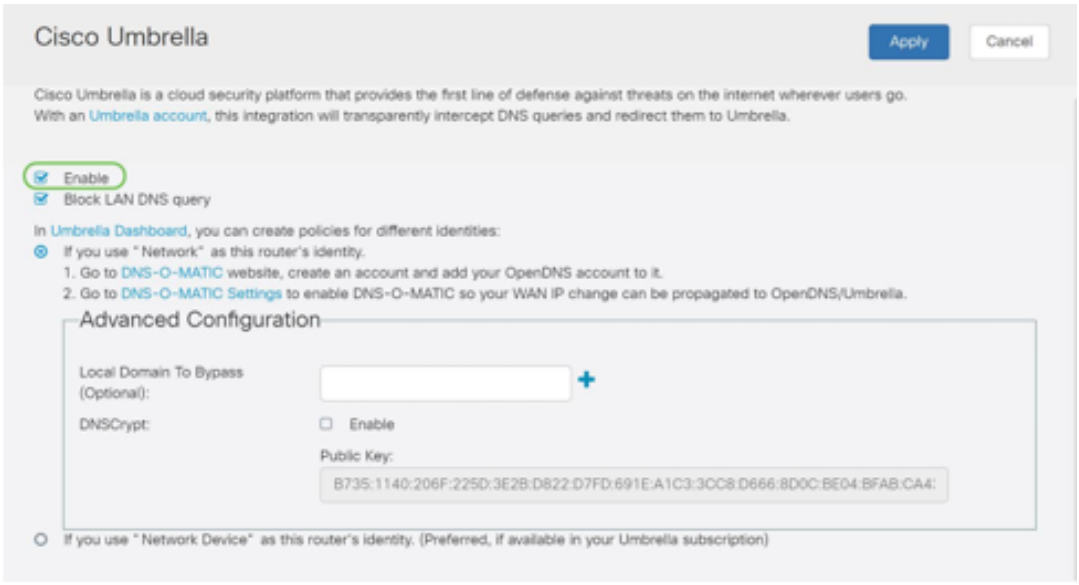
Umbrella内にAPIキーを作成したので、これらのキーをRV345Pにインストールできます。

手順 1

RV345Pルータにログインした後、サイドバーメニューの**[Security] > [Umbrella]**をクリックします。

手順 2

[Umbrella API]画面にはオプションが用意されています。[有効]チェックボックスをクリックしてUmbrellaの有効**化を開始**します。

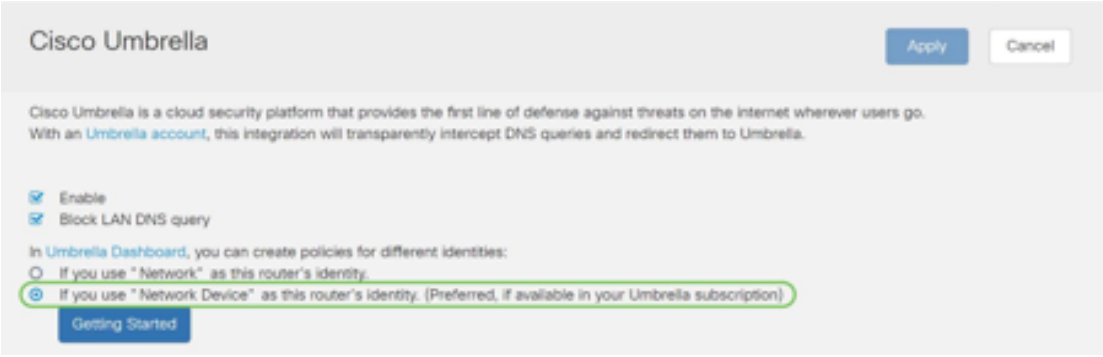


手順 3 (オプション)

既定では、[LAN DNSクエリをブロックする]ボックスが*選択*されています。この優れた機能により、ルータにアクセスコントロールリストが自動的に作成され、DNSトラフィックがインターネットに送信されなくなります。この機能により、すべてのドメイン変換要求が強制的にRV345P経由で送信されます。これは、ほとんどのユーザにとって良い考えです。

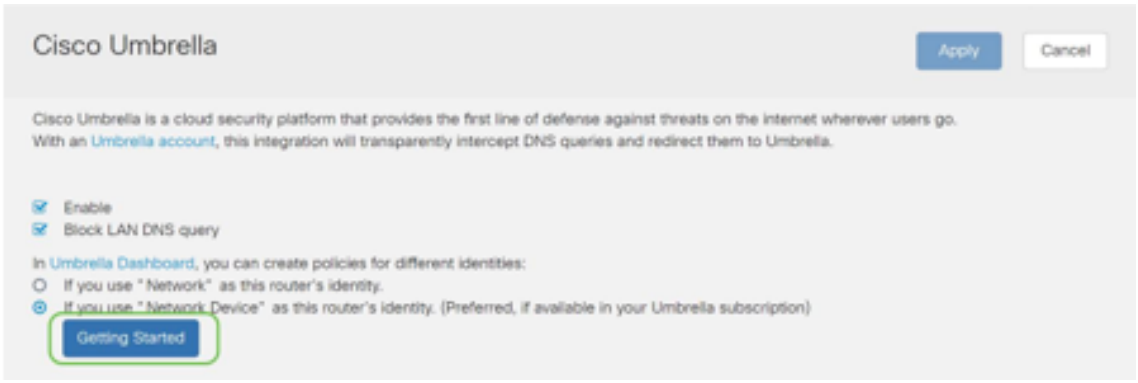
手順 4

次のステップは、2つの異なる方法で再生されます。どちらもネットワークのセットアップによって異なります。DynDNSやNoIPなどのサービスを使用する場合は、デフォルトの名前付け方式である「Network」のままにします。これらのアカウントにログインして、Umbrellaが保護を提供するサービスとのインターフェイスを確保する必要があります。目的は「ネットワークデバイス」に依存しているため、下部のオプションボタンをクリックします。



手順 5

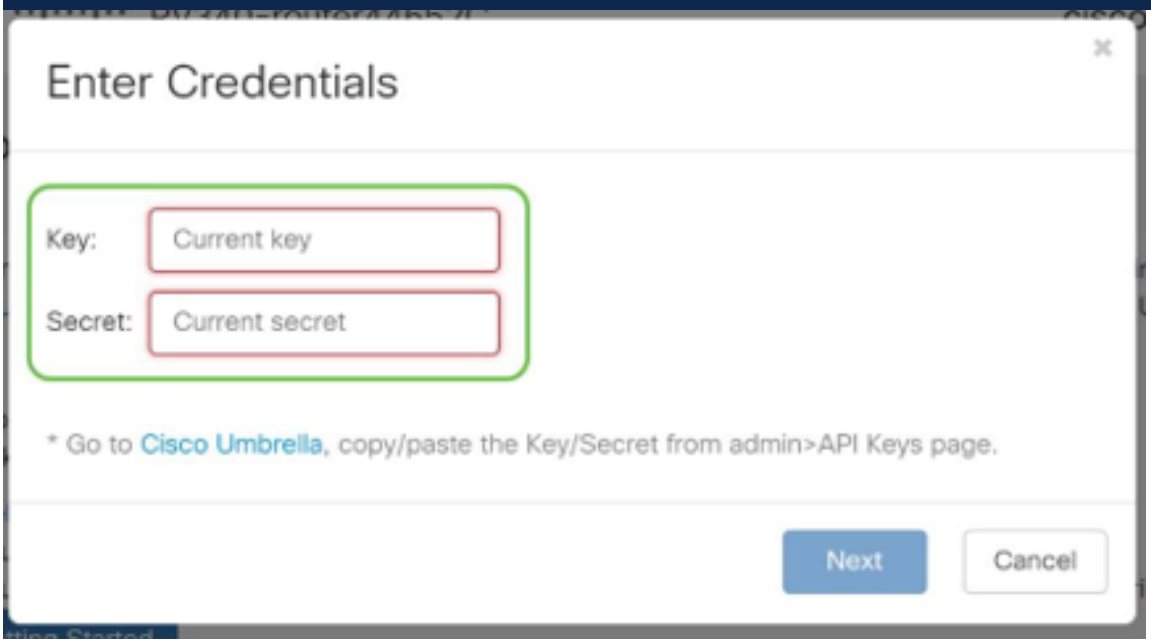
[はじめに]**をクリックします。**



手順 6

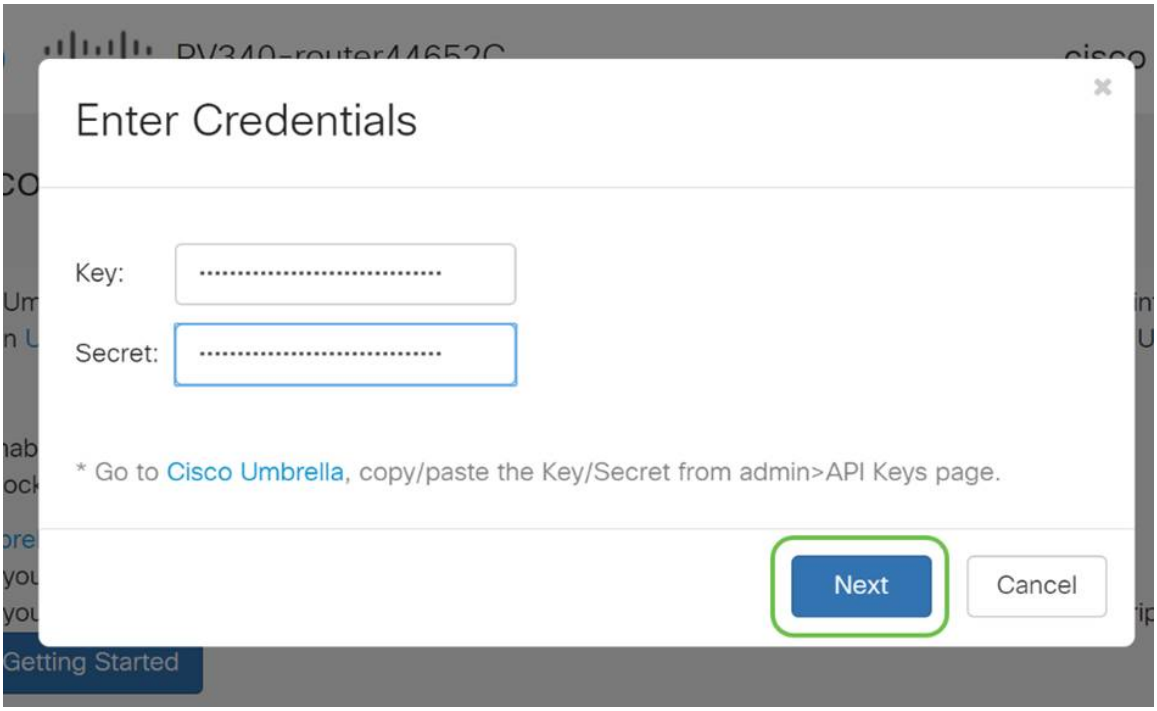
テキスト・ボックスにAPIキーおよびシークレット・キーを入力します。

2回呼ぶから大事だと分かってる！秘密キーを紛失または誤って削除した場合、このキーを取得するために呼び出す機能またはサポート番号はありません。秘密にして安全にしてください。紛失した場合は、キーを削除し、Umbrellaで保護する各デバイスで新しいAPIキーを再承認する必要があります。



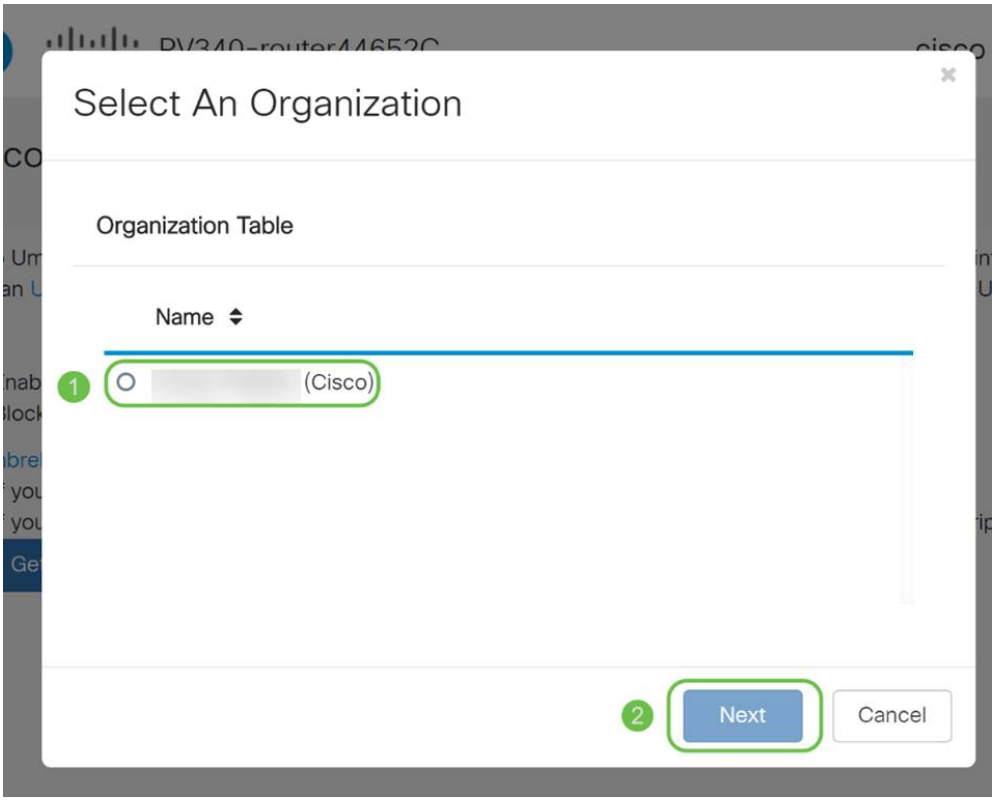
ステップ7

APIと秘密キーを入力したら、[次へ]ボタンをクリックします。



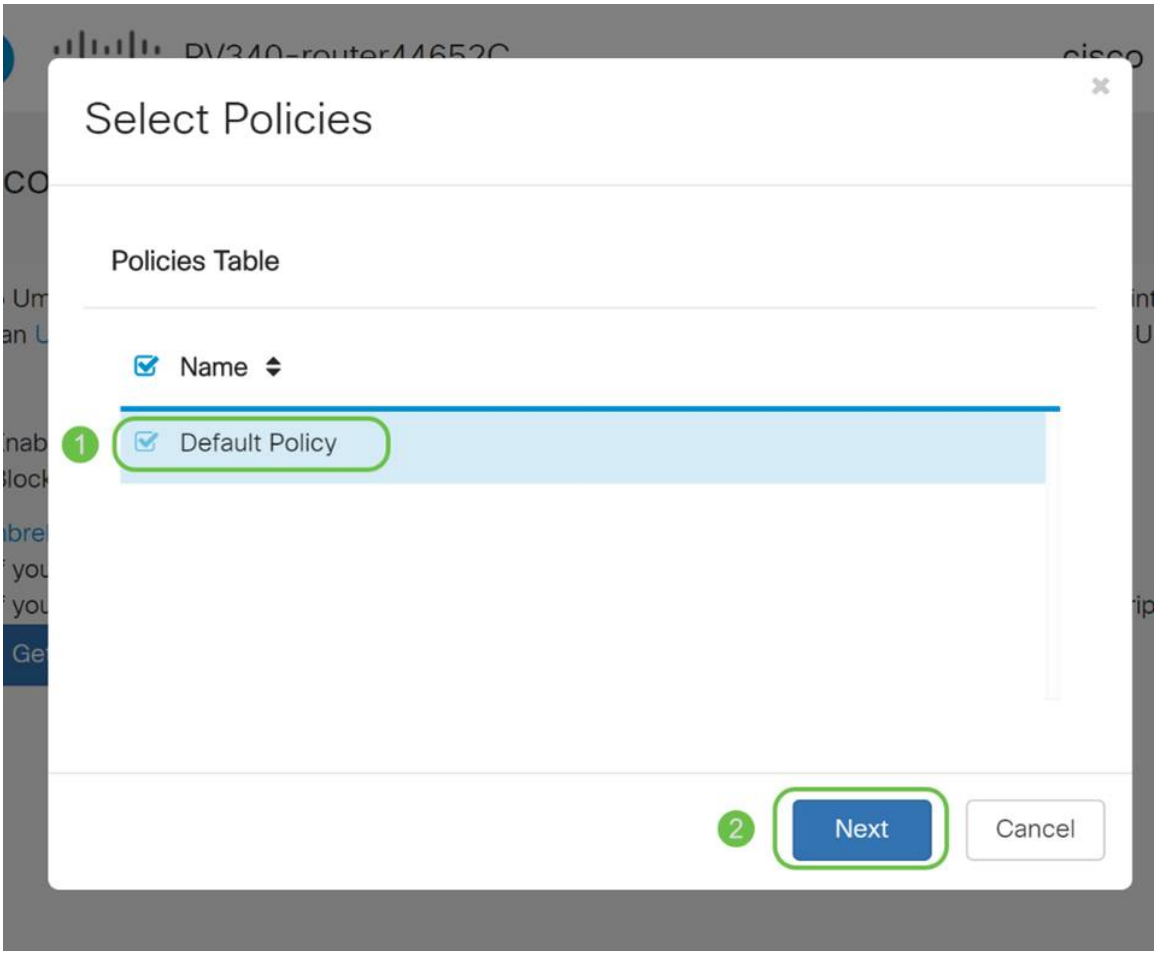
手順 8

次の画面で、ルータに**関連付ける**組織を選択します。[next] をクリックします。



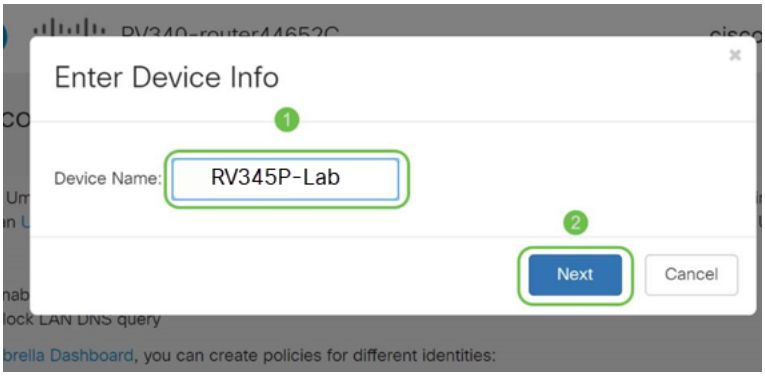
手順 9

RV345Pによってルーティングされるトラフィックに適用するポリシーを選択します。ほとんどのユーザに対して、デフォルトポリシーは十分なカバレッジを提供します。



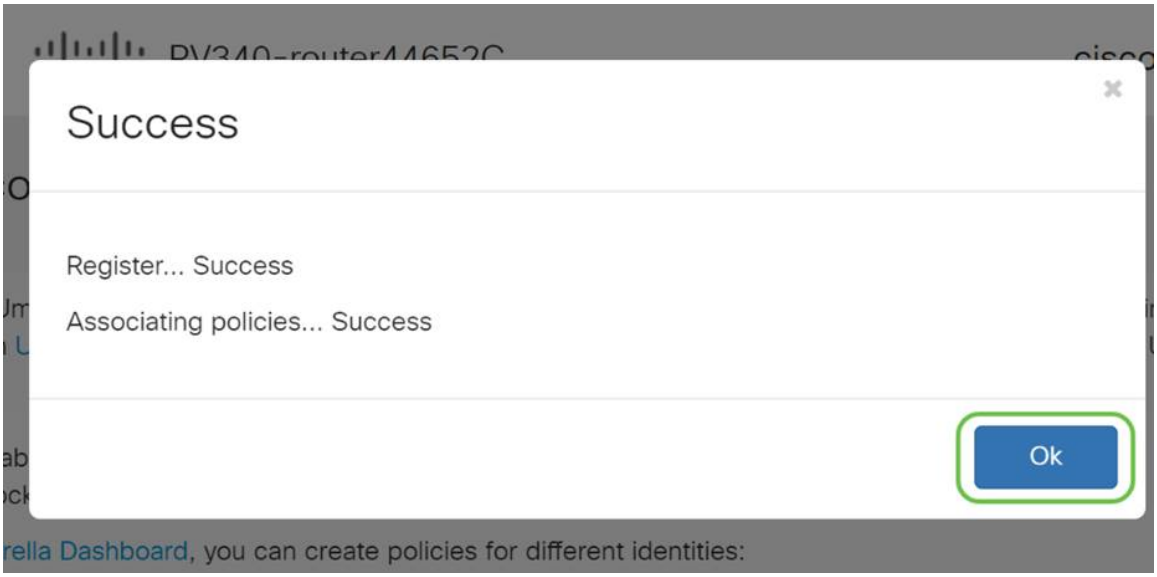
手順 10

Umbrellaレポートで指定できるように、デバイスに名前を割り当てます。セットアップでは、*RV*345P-Labという名前を付けています。



手順 11

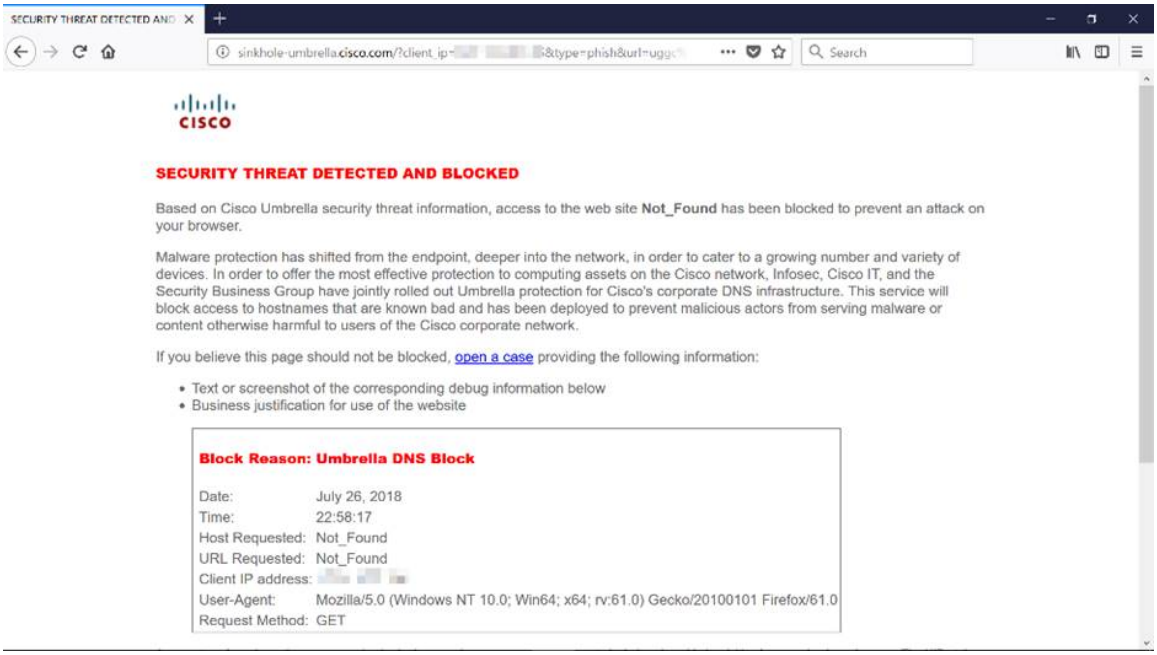
次の画面では、選択した設定を検証し、関連付けが正常に行われたときに更新を行います。[OK] をクリックします。



確認

これで、Cisco Umbrellaによって保護されました。それともあなたは？実際の例を使用して再確認し、ページのロードと同時に、これを決定するための専用Webサイトを作成しました。ここをクリックするか、https://InternetBadGuys.comと入力します。

Umbrellaが正しく設定されている場合、次のような画面が表示されます。



その他のセキュリティオプション

ネットワークデバイスからイーサネットケーブルを抜いて接続することで、誰かがネットワークへの不正アクセスを試みることを心配していますか。この場合、ルータに直接接続できるホストのリストを、それぞれのIPアドレスとMACアドレスで登録することが重要です。手順については、『RV34xシリーズルータでのIPソースガードの設定』を参照してください。

VPNオプション

バーチャルプライベートネットワーク(VPN)接続を使用すると、インターネットなどのパブリックネットワークまたは共有ネットワークを介してプライベートネットワークとの間でデータのアクセス、送受信が可能になりますが、基盤となるネットワークインフラストラクチャへの安全な接続を確保してプライベートネットワークとそのリソースを保護します。

VPNトンネルは、暗号化と認証を使用してデータを安全に送信できるプライベートネットワークを確立します。企業オフィスはVPN接続を主に使用します。これは、従業員がオフィスの外からでもプライベートネットワークにアクセスできるようにするために便利で必要な機能です。

VPNを使用すると、リモートホストを同じローカルネットワーク上に配置されているかのように動作させることができます。ルータは最大50のトンネルをサポートします。ルータがインターネット接続用に設定された後、ルータとエンドポイントの間にVPN接続を設定できます。VPNクライアントは、接続を確立できるVPNルータの設定に完全に依存しています。

どのVPNがニーズに最適なのかがわからない場合は、『Cisco Business VPN Overview』および『Best Practices』を参照してください。

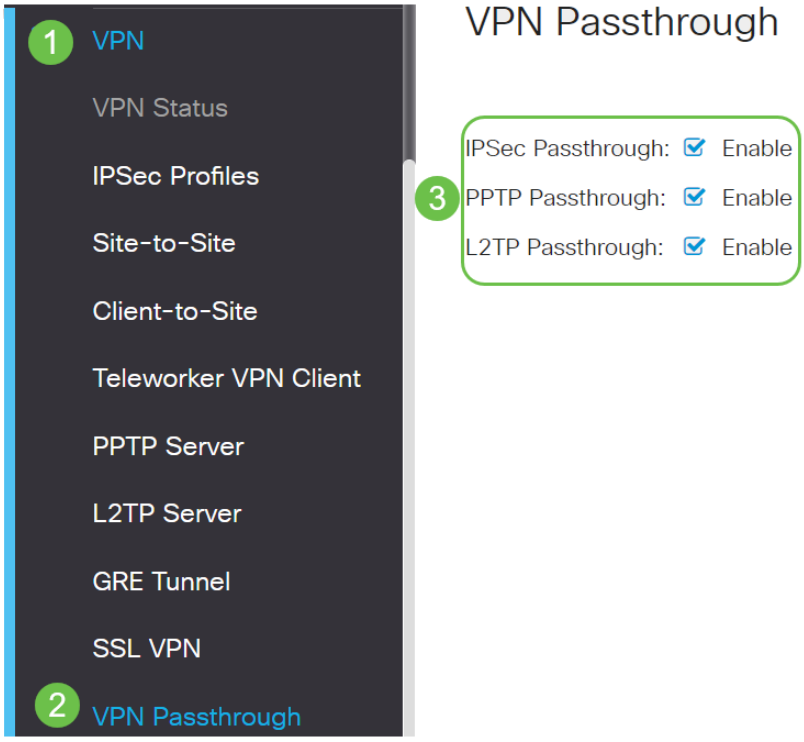
AnyConnect VPNは、この設定ガイドに記載されている唯一のCisco VPNサポート製品です。TheGreenBowやShrew Softなどのシスコ以外のサードパーティ製品は、シスコではサポートされていません。これらはガイダンスの目的でのみ含まれています。この記事を超えてサポートが必要な場合は、サードパーティにサポートを依頼してください。

VPNのセットアップを計画していない場合は、クリックして次のセクションに移動できます。

VPN パススルー

通常、すべてのルータは、同じインターネット接続を持つ複数のクライアントをサポートする場合にIPアドレスを節約するために、ネットワークアドレス変換(NAT)をサポートします。ただし、Point-to-Point Tunneling Protocol(PPTP)およびInternet Protocol Security(IPsec)VPNはNATをサポートしていません。ここで、VPNパススルーが表示されます。VPNパススルーは、このルータに接続されたVPNクライアントから生成されたVPNトラフィックがこのルータを通過し、VPNエンドポイントに接続できるようにする機能です。VPNパススルーでは、PPTPとIPSec VPNは、VPNクライアントから開始されたインターネットへのパススルーのみが許可され、リモートVPNゲートウェイに到達します。この機能は、NATをサポートするホームルータで一般的に見られます。

デフォルトでは、IPsec、PPTP、およびL2TPパススルーが有効になっています。これらの設定を表示または調整する場合は、**[VPN] > [VPN Passthrough]を選択します**。必要に応じて表示または調整します。



AnyConnect VPN

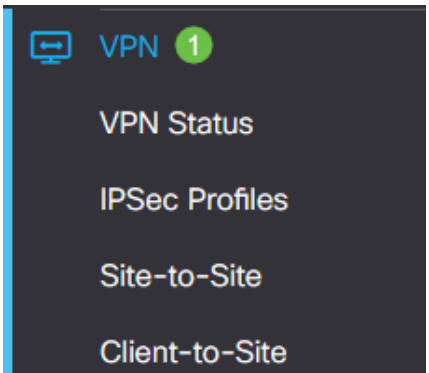
Cisco AnyConnectを使用する利点はいくつかあります。

1. セキュアで持続的な接続
2. 永続的なセキュリティとポリシーの適用
3. 適応型セキュリティアプライアンス(ASA)またはエンタープライズソフトウェア導入システムから導入可能
4. カスタマイズおよび翻訳可能
5. 簡単な設定
6. インターネットプロトコルセキュリティ(IPsec)とセキュアソケットレイヤ(SSL)の両方をサポート
7. インターネットキーエクスチェンジバージョン2.0(IKEv2.0)プロトコルをサポート

RV345PでのAnyConnect SSL VPNの設定

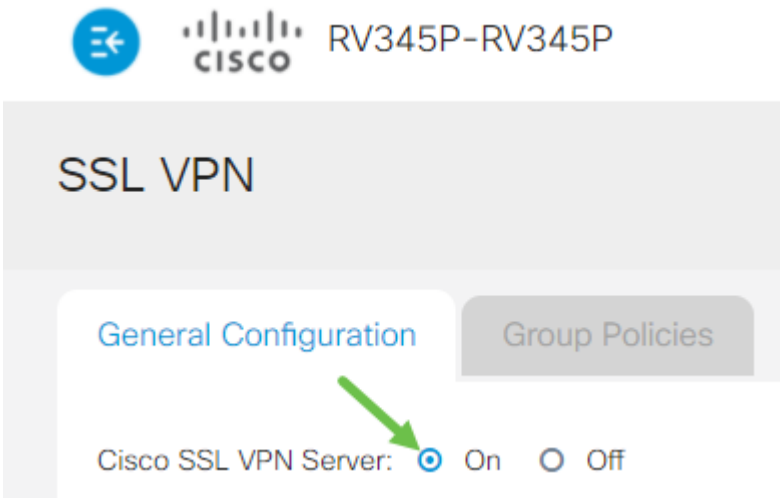
手順 1

ルータのWebベースのユーティリティにアクセスし、**[VPN] > [SSL VPN]を選択します**。



手順 2

[On] オプションボタンをクリックして、Cisco SSL VPN Serverを有効にします。



必須ゲートウェイ設定

手順 1

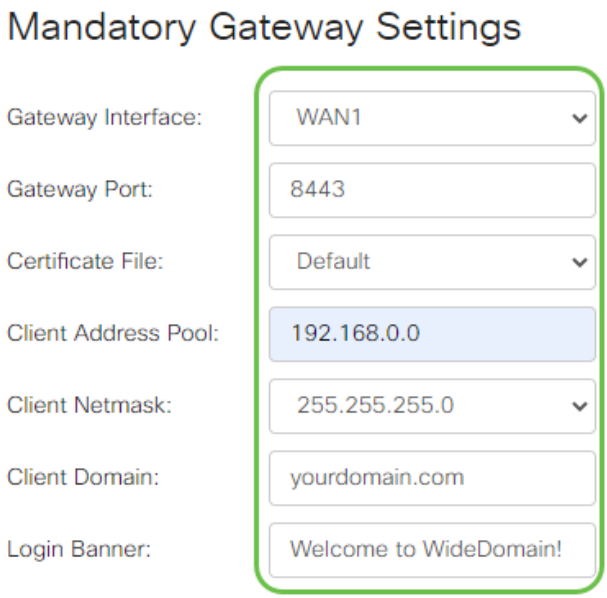
次の設定は必須です。

1. ドロップダウンリストから[ゲートウェイインターフェイス(Gateway Interface)]を選択します。これは、SSL VPNトンネルを通過するトラフィックに使用されるポートです。オプションは次のとおりです。WAN1、WAN2、USB1、USB2
2. [Gateway Port]フィールドに、SSL VPNゲートウェイに使用するポート番号を1 ~ 65535の範囲で入力します。
3. ドロップダウンリストから[Certificate File]を選択します。この証明書は、SSL VPNトンネルを介してネットワークリソースにアクセスしようとするユーザを認証します。ドロップダウンリストには、デフォルトの証明書と、インポートされる証明書が含まれています。
4. [クライアントアドレスプール]フィールドに、クライアントアドレスプールのIPアドレスを入力します。このプールは、リモートVPNクライアントに割り当てられるIPアドレスの範囲になります。

   IPアドレスの範囲が、ローカルネットワーク上のどのIPアドレスとも重複していないことを確認してください。

6. ドロップダウンリストから[Client Netmask]を選択します。
7. [Client Domain]フィールドにクライアントドメイン名を入力します。これは、SSL VPNクライアントにプッシュされるドメイン名です。
8. [ログインバナー]フィールドにログインバナーとして表示されるテキストを入力します

。これは、クライアントがログインするたびに表示されるバナーです。



手順 2

[Apply] をクリックします。

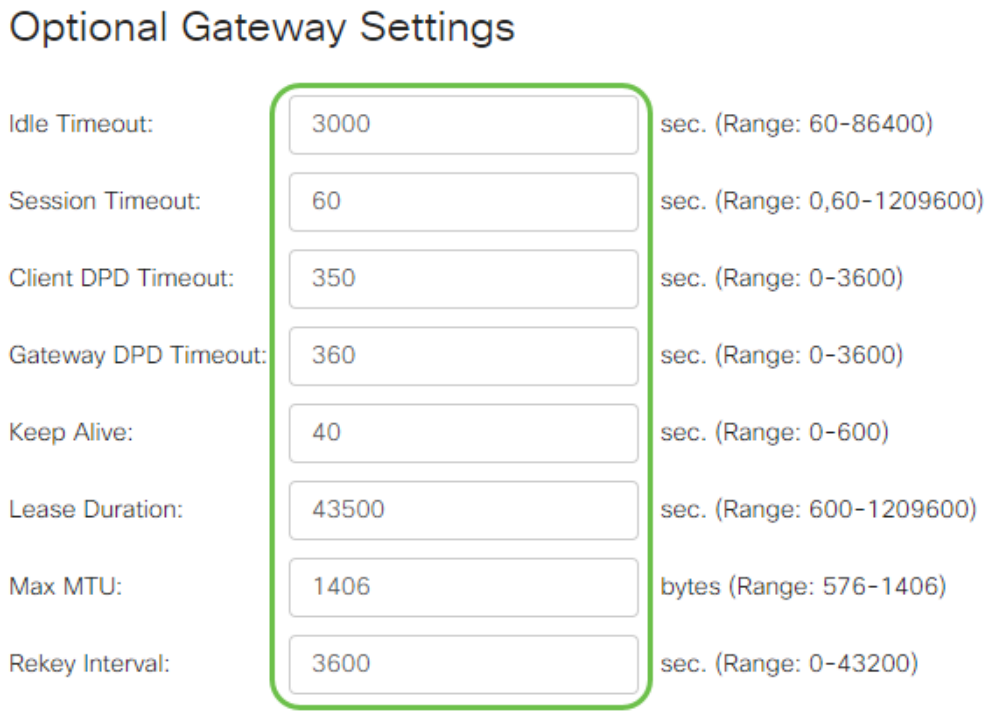
オプションのゲートウェイ設定

手順 1

次の設定値はオプションです。

1. アイドルタイムアウトの値を60 ~ 86400の範囲で秒単位で入力します。これは、SSL VPNセッションがアイドル状態を維持できる時間です。
2. [セッションタイムアウト]フィールドに値を*秒単位で入力*します。これは、Transmission Control Protocol（TCP；伝送制御プロトコル）またはUser Datagram Protocol（UDP；ユーザデータグラムプロトコル）セッションが、指定されたアイドル時間の後にタイムアウトするまでの時間です。範囲は 60 ~ 1209600 です。
3. [ClientDPD Timeout]フィールドに0 ~ 3600の*範囲*の値を秒単位で入力します。この値は、VPNトンネルのステータスを確認するためのHELLO/ACKメッセージの定期的な送信を指定します。この機能は、VPNトンネルの両端で有効にする必要があります。
4. [GatewayDPD Timeout]フィールドに0 ~ 3600の*範囲*の値を秒単位で入力します。この値は、VPNトンネルのステータスを確認するためのHELLO/ACKメッセージの定期的な送信を指定します。この機能は、VPNトンネルの両端で有効にする必要があります。
5. *Keep Alive*フィールドに0 ~ 600の範囲の値を秒単位で入力します。この機能により、ルータは常にインターネットに接続されます。VPN接続がドロップされた場合は、VPN接続の再確立を試みます。
6. [リース期間(Lease Duration)]フィールドに、接続するトンネルの期間の値（秒）を*入力*します。範囲は 600 ~ 1209600 です。

7. ネットワーク経由で送信できるパケットサイズ (バイト) を入力します。範囲は 576 ~ 1406 です。
8. [キー再生成間隔]フィールドにリレー*間隔を入力*します。キー再生成機能を使用すると、セッションの確立後にSSLキーを再ネゴシエートできます。範囲は 0 ~ 43200 です。



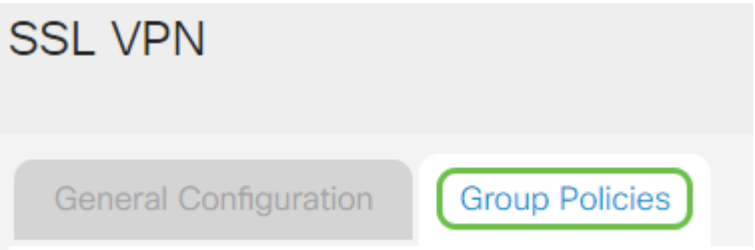
手順 2

[Apply] をクリックします。

グループポリシーの設定

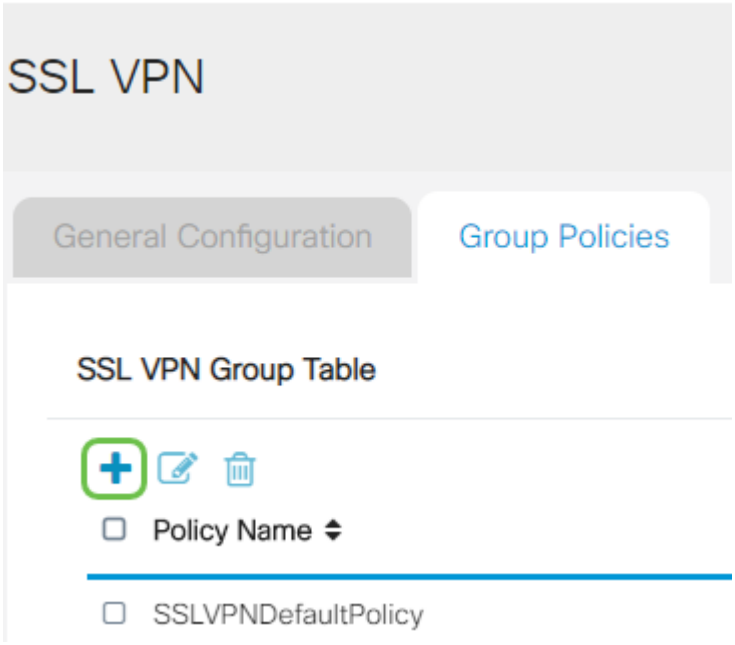
手順 1

[グループポリシー]**タブをクリック**します。



手順 2

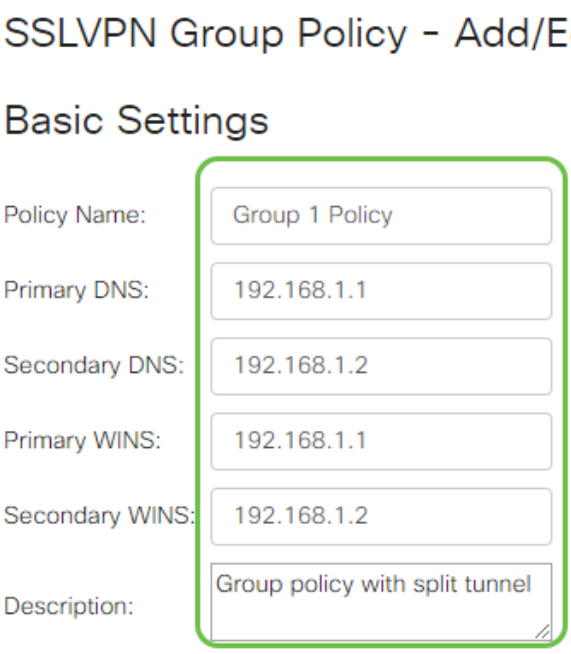
SSL VPNグループテー**ブルの下の**[Add]アイコンをクリックして、グループポリシーを追加します。



SSL VPNグループテーブルには、デバイス上のグループポリシーのリストが表示されます。リストの最初のグループポリシー(SSLVPNDefaultPolicy)を編集することもできます。これは、デバイスによって提供されるデフォルトポリシーです。

手順 3

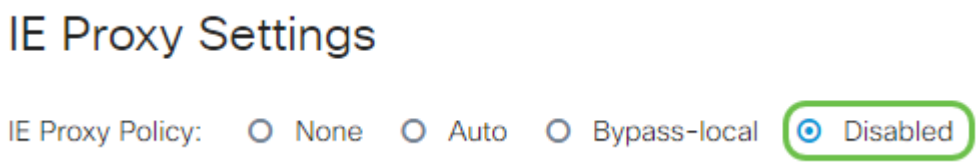
1. [ポリシー名]フィールドに優先するポリシー*名を入力*します。
2. 表示されたフィールドにプライマリDNSのIPアドレスを入力します。デフォルトでは、このIPアドレスはすでに指定されています。
3. *（オプション）表示されたフィールドにセカンダリDNSのIPアドレスを入力します。これは、プライマリDNSが失敗した場合のバックアップとして機能します。*
4. （オプション）プライマリWINSのIPアドレスをフィールドに入力します。
5. （オプション）セカンダリWINSのIPアドレスをフィールドに入力します。
6. （オプション）[説明]フィールドにポリシーの説明を入力します。



手順 4 (オプション)

オプションボタンをクリックして[IE Proxy Policy]を選択し、Microsoft Internet Explorer(MSIE)プロキシ設定を有効にしてVPNトンネルを確立します。次のオプションがあります。

- [なし(None)]：ブラウザがプロキシ設定を使用しないようにします。
- [自動(Auto)]：ブラウザがプロキシ設定を自動的に検出できるようにします。
- Bypass-local：ブラウザがリモートユーザに設定されているプロキシ設定をバイパスできるようにします。
- [無効(Disabled)]:MSIEプロキシ設定を無効にします。



手順 5 (オプション)

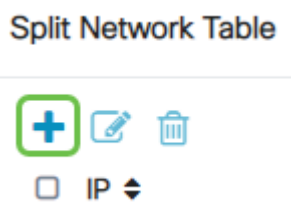
[Split Tunneling Settings]領域で、[**Enable Split Tunneling**]チェックボックスをオンにして、インターネット宛てのトラフィックを暗号化されずにインターネットに直接送信できるようにします。完全トンネリングは、すべてのトラフィックをエンドデバイスに送信し、エンドデバイスは宛先リソースにルーティングされ、Webアクセスのパスから企業ネットワークが排除されます。

ステップ 6 (オプション)

スプリットトンネリングを適用するときにトラフィックを含めるか除外するかを選択するには、オプションボタンをクリックします。

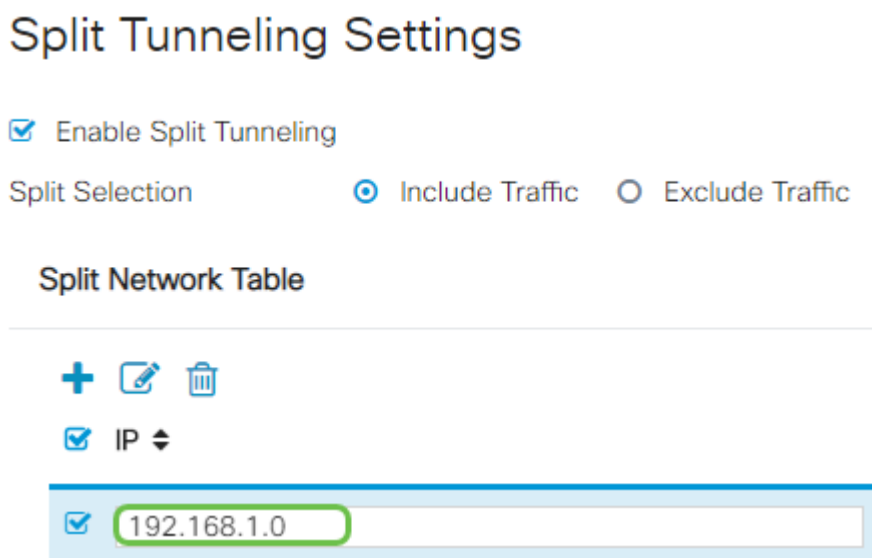
ステップ7

分割ネットワークテーブルで、[追加]アイコンをクリックして、分割ネットワーク例外を追加します。



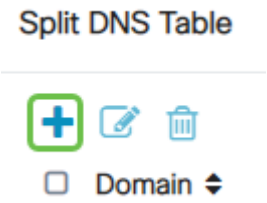
手順 8

表示されたフィールドにネットワークのIPアドレスを入力します。



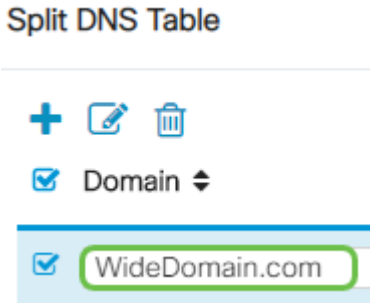
手順 9

[スプリットDNSテーブル]で、[追加]アイコンをクリックして、スプリットDNS例外を追加します。



手順 10

表示されたフィールドにドメイン名を入力し、[適用]をクリックします。



ルータには、デフォルトで2つのAnyConnectサーバライセンスが付属しています。つまり、AnyConnectクライアントライセンスを取得すると、他のRV340シリーズルータと同時に2つのVPNトンネルを確立できます。

つまり、RV345Pルータにはライセンスは必要ありませんが、すべてのクライアントには1つ必要です。AnyConnectクライアントライセンスを使用すると、デスクトップおよびモバイルクライアントからVPNネットワークにリモートでアクセスできます。

次のセクションでは、クライアントのライセンスを取得する方法について詳しく説明します。

AnyConnectモビリティクライアント

VPNクライアントは、リモートネットワークへの接続を希望するコンピュータにインストールされ、実行されるソフトウェアです。このクライアントソフトウェアは、IPアドレスや認証情報など、VPNサーバと同じ設定でセットアップする必要があります。この認証情報には、データの暗号化に使用されるユーザ名と事前共有キーが含まれます。接続するネットワークの物理的な場所に応じて、VPNクライアントをハードウェアデバイスにすることもできます。これは通常、VPN接続を使用して、別の場所にある2つのネットワークを接続する場合に発生します。

Cisco AnyConnectセキュアモビリティクライアントは、さまざまなオペレーティングシステムやハードウェア構成で動作するVPNに接続するためのソフトウェアアプリケーションです。このソフトウェアアプリケーションを使用すると、ユーザが自分のネットワークに直接接続されているかのように、他のネットワークのリモートリソースに安全にアクセスできます。

ルータがAnyConnectで登録および設定されると、クライアントは、購入した利用可能なライセンスプールからルータにライセンスをインストールできます。これについては、次のセクションで詳しく説明します。

購入ライセンス

シスコディストリビュータまたはシスコパートナーからライセンスを購入する必要があります。ライセンスを発注する際には、シスコスマートアカウントIDまたはドメインIDをname@domain.comの形式で指定する必要が***あります***。

シスコのディストリビュータまたはパートナーがいない場合は、こちらを参照してください。

このドキュメントの執筆時点で、次の製品SKUを使用して25のバンドルの追加ライセンスを購入できます。AnyConnectクライアントライセンスには、Cisco AnyConnect発注ガイドに記載されているその他のオプションがありますが、製品IDが完全な機能の最小要件です。

AnyConnectクライアントライセンスの製品SKUが最初にリストされ、1年間のライセンスが提供されます。25ライセンス以上の購入が必要です。RV340シリーズルータに適用可能な他の製品SKUも、次に示すさまざまなサブスクリプションレベルで提供されています。

- **LS-AC-PLS-1Y-S1**:1年間のCisco AnyConnect Plusクライアントライセンス
- **LS-AC-PLS-3Y-S1**:3年間のCisco AnyConnect Plusクライアントライセンス
- **LS-AC-PLS-5Y-S1**:5年間のCisco AnyConnect Plusクライアントライセンス
- **LS-AC-PLS-P-25-S**:25パックCisco AnyConnect Plus永久クライアントライセンス
- **LS-AC-PLS-P-50-S**:50パックCisco AnyConnect Plus永久クライアントライセンス

クライアント情報

クライアントが次のいずれかを設定すると、これらのリンクが送信されます。

- Windows：WindowsコンピュータのAnyConnect
- Mac:MacにAnyConnectをインストールします。
- Ubuntu Desktop:Ubuntu DesktopでのAnyConnectのインストールと使用
- 問題が発生した場合は、「Cisco AnyConnectセキュアモビリティクライアントエラーに関する基本的なトラブルシューティングのための情報の収集」を参照してください。

AnyConnect VPN接続の確認

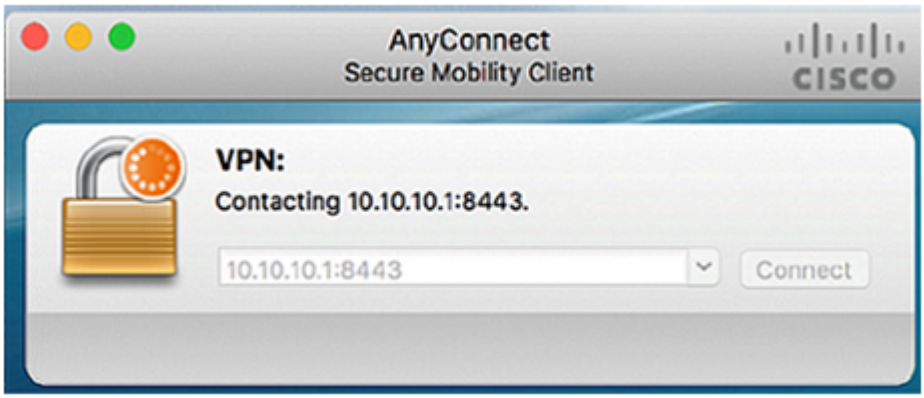
手順 1

[AnyConnect Secure Mobility Client]アイコンをクリックします。

手順 2

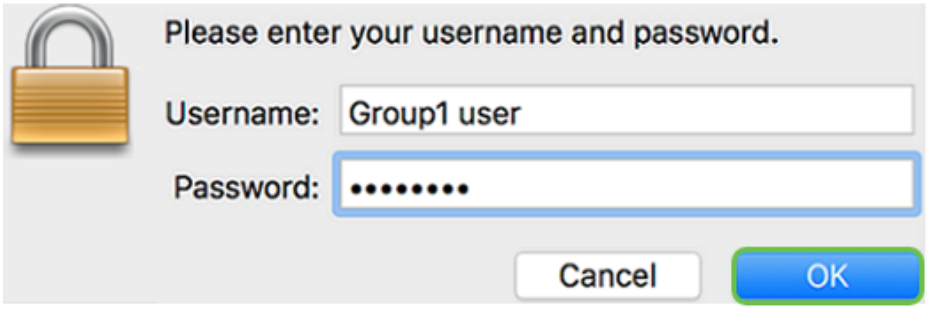
[AnyConnect Secure Mobility Client]ウィンドウで、ゲートウェイのIPアドレスとゲートウェイポート番号をコロン(:)で区切って入力し、[Connect]をクリックします。

ソフトウェアは、リモートネットワークに接続していることを示します。



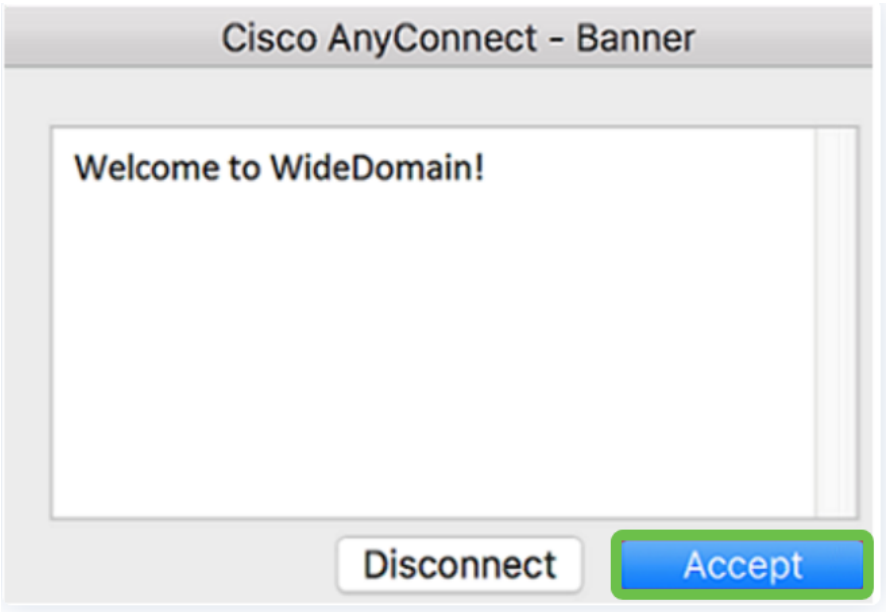
手順 3

各フィールドにサーバーのユーザー名とパスワードを入力し、「OK」をクリックします。

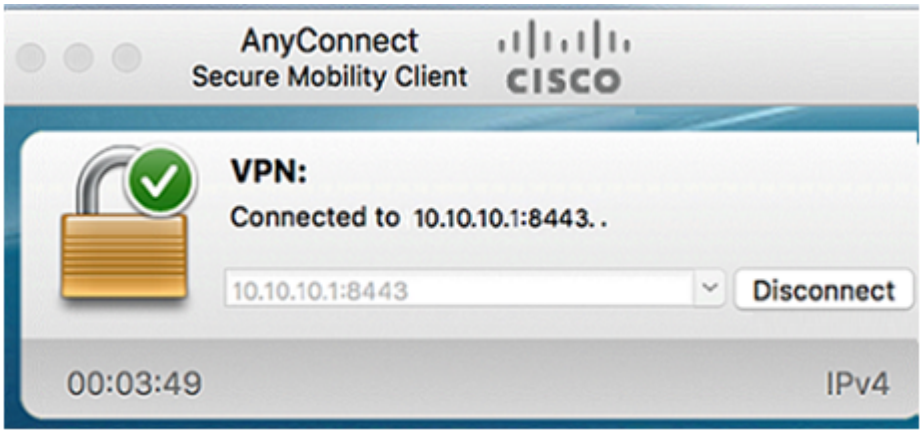


手順 4

接続が確立するとすぐに、ログインバナーが表示されます。[Accept] をクリックします。



[AnyConnect]ウィンドウに、ネットワークへのVPN接続が正常に行われたことが表示されます。



AnyConnect VPNを使用している場合は、他のVPNオプションをスキップして、次のセクションに移**動できます**。

シュレウソフトVPN

IPsec VPNでは、インターネット経由で暗号化されたトンネルを確立することで、リモートリソースを安全に取得できます。RV34Xシリーズルータは IPsec VPNサーバとして動作し、Shrew Soft VPN Clientをサポートします。このセクションでは、ルータ

とShrew Soft Clientを設定して、VPNへの接続を保護する方法について説明します。

シスコはShrew Softをサポートしていません。この例は、デモンストレーション目的でのみ提供されています。Shrew Softに問題がある場合は、サポートを依頼してください。

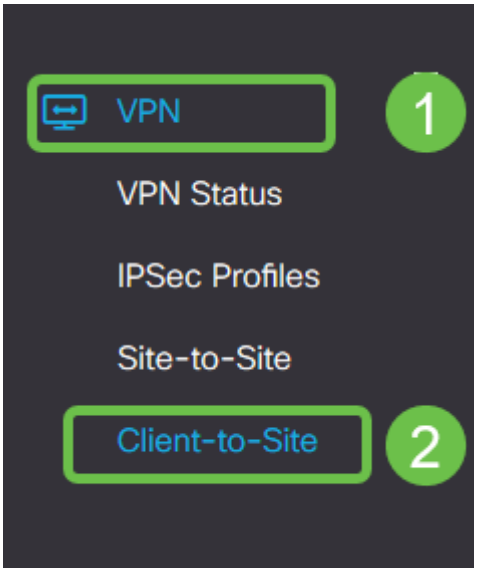
最新バージョンのShrew Soft VPN Clientソフトウェアは、次の場所からダウンロードできます。https://www.shrew.net/download/vpn

RV345PシリーズルータでのShrew Softの設定

まず、RV345Pでクライアントからサイトへの**VPN**を設定します。

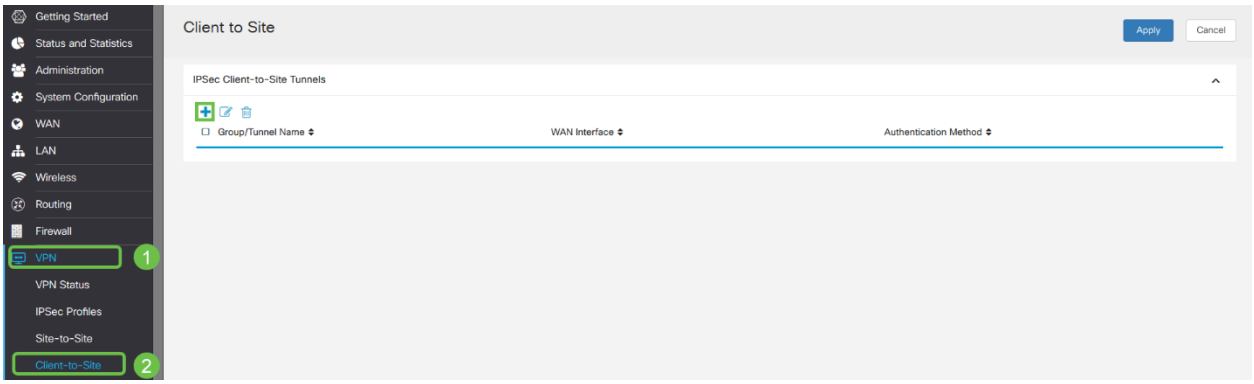
手順 1

[VPN] > [Client-to-Site]に移動します。



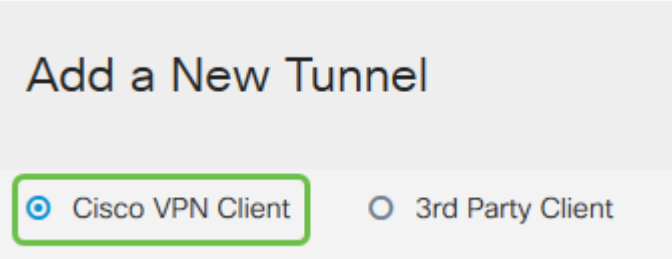
手順 2

クライアントからサイトへのVPNプロファイルを追加します。



手順 3

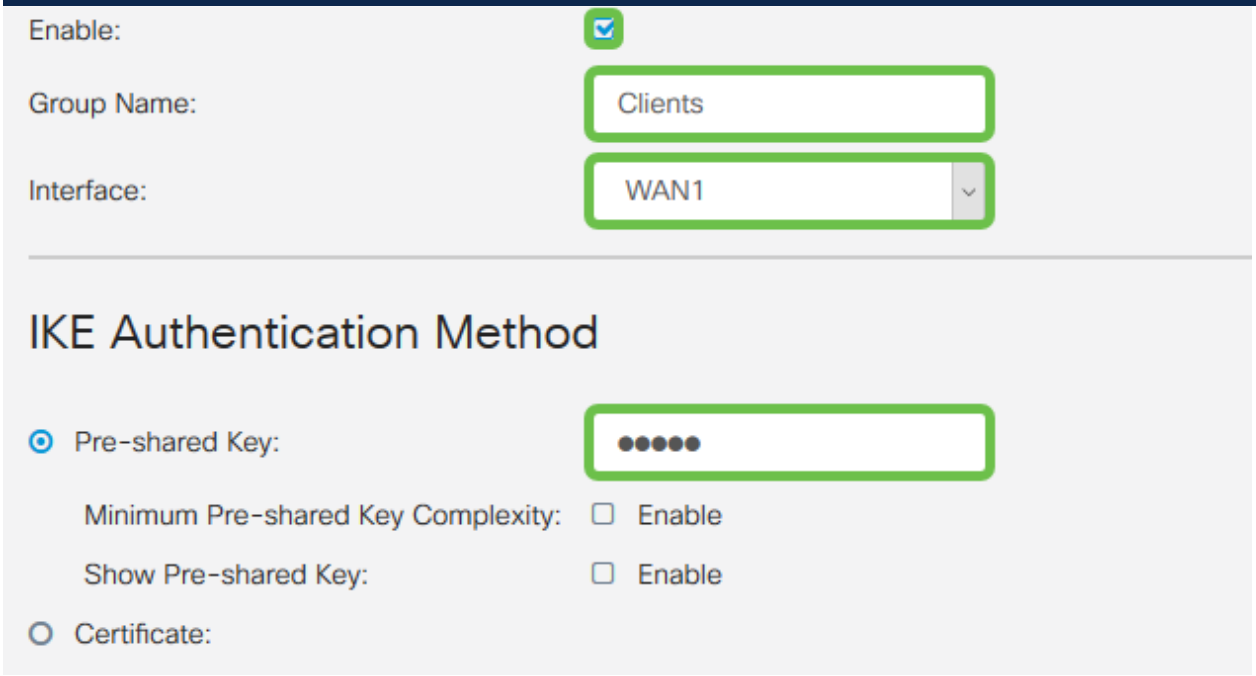
[Cisco VPN Client]オプションを選択します。



手順 4

[Enable] ボックスをオンにして、VPN Clientプロファイルをアクティブにします。グループ名を設定し、*WAN*インターフェイス**を選択**し、事前共有キー**を入力します**。

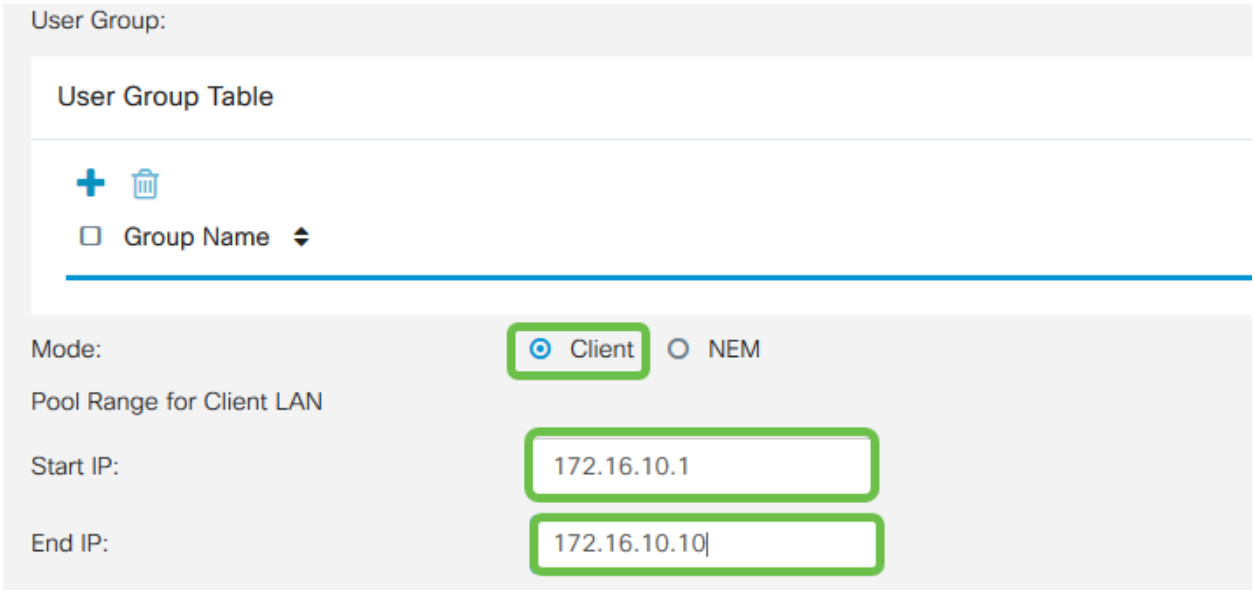
後でクライアントを構成する際に使用する *グループ名*と事前共有キーに注意してください。



手順 5

ここでは、[ユ**ーザーグループ表]は**空白のままにします。これはルータ上のユーザグループ用ですが、まだ設定していません。[Mode]が[**Client**]に**設定され**ていることを確認**します**。クライアント**LANのプール範囲を入力します**。172.16.10.1 ~ 172.16.10.10を使用します。

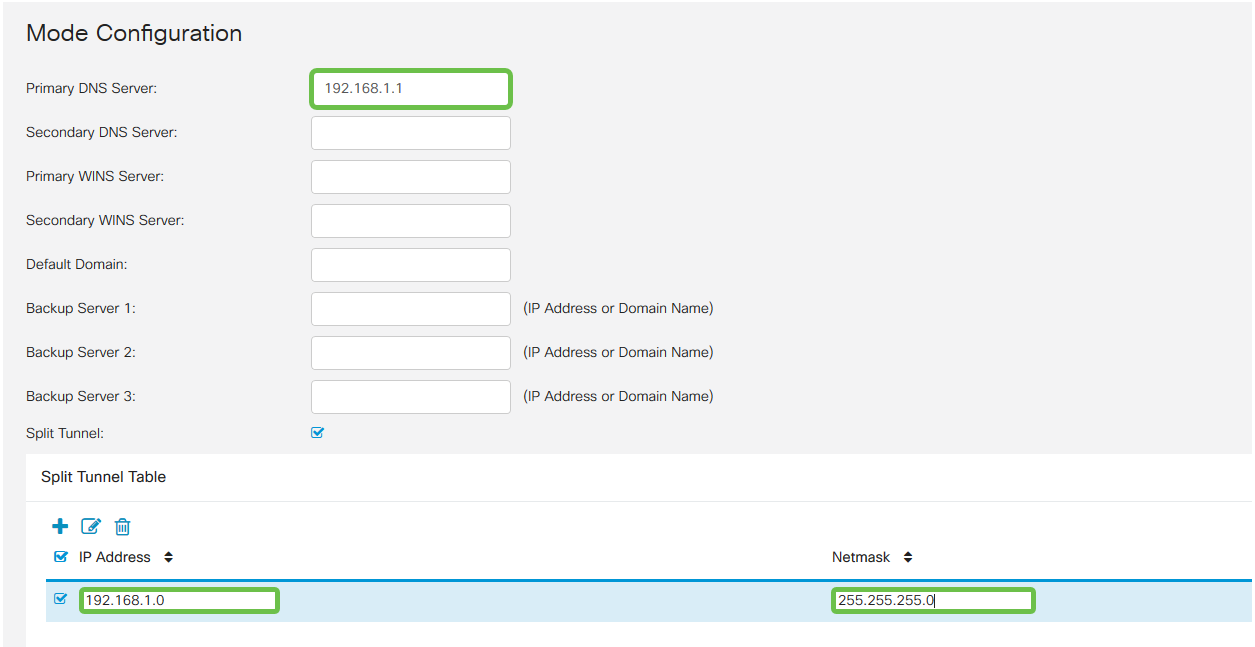
プール範囲は、ネットワーク上の他の場所では使用されない一意のサブネットを使用する必要があります。



手順 6

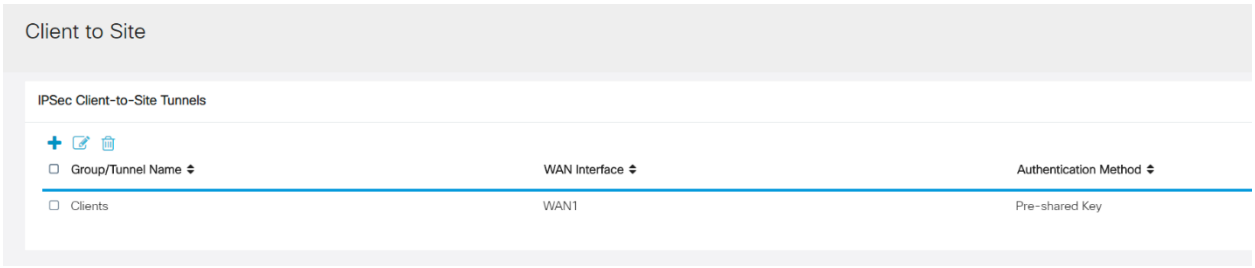
ここでは、モード設定を構成します。使用する設定は次のとおりです。

- **プライマリDNSサーバ**:内部DNSサーバがある場合、または外部DNSサーバを使用する場合は、ここに入力できます。それ以外の場合、デフォルトはRV345P LAN IPアドレスに設定されます。この例では、デフォルトを使用します。
- **スプリットトンネル：スプリ**ットトンネリングを有効にするには、オンにします。これは、VPNトンネルを通過するトラフィックを指定するために使用されます。この例では、スプリットトンネルを使用します。
- **スプリットトンネルテーブル**： VPNクライアントがVPN経由でアクセスできる必要があるネットワークを入力します。この例では、RV345P LANネットワークを使用しています。



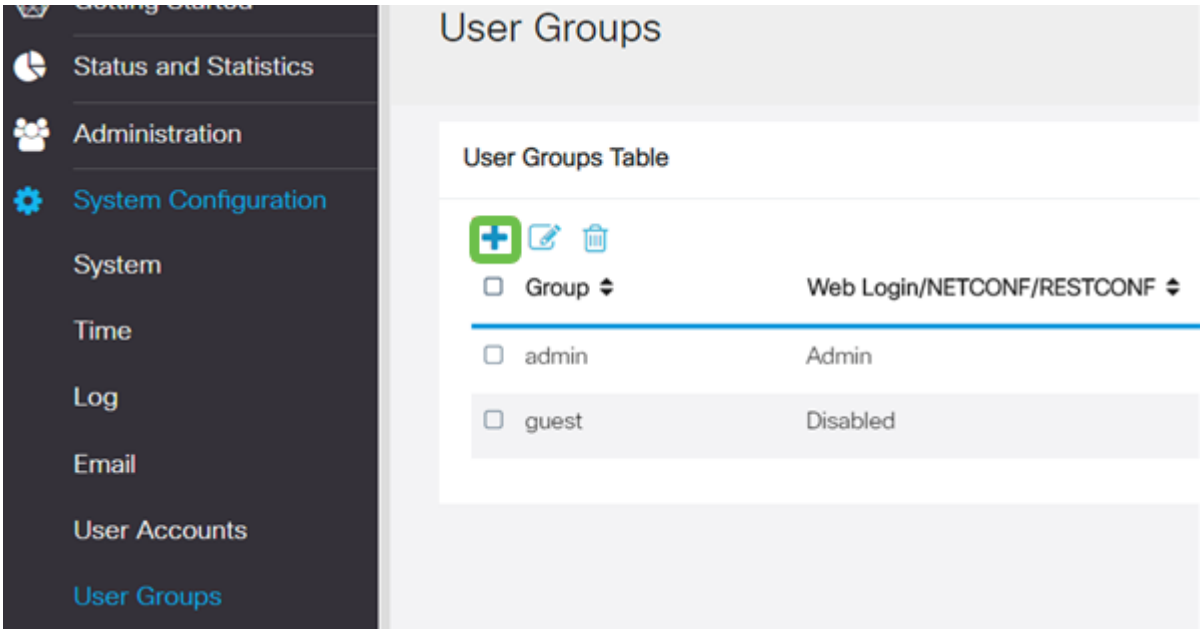
ステップ7

[保存]をクリックすると、[IPsec Client-to-Site Groups]リストにプロファイルが表示されます。



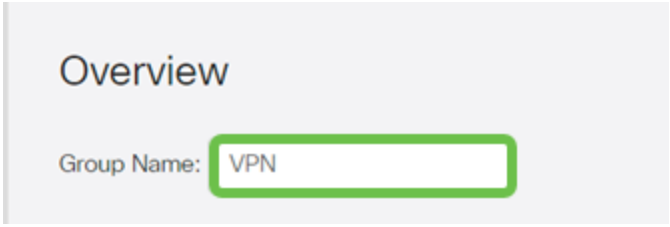
手順 8

VPN Clientユーザの**認証に使用**するユーザグループを設定します。[システム**構成**] > **[ユーザグループ]**で、プラス記号アイコン**をクリック**してユーザグループを追加します。



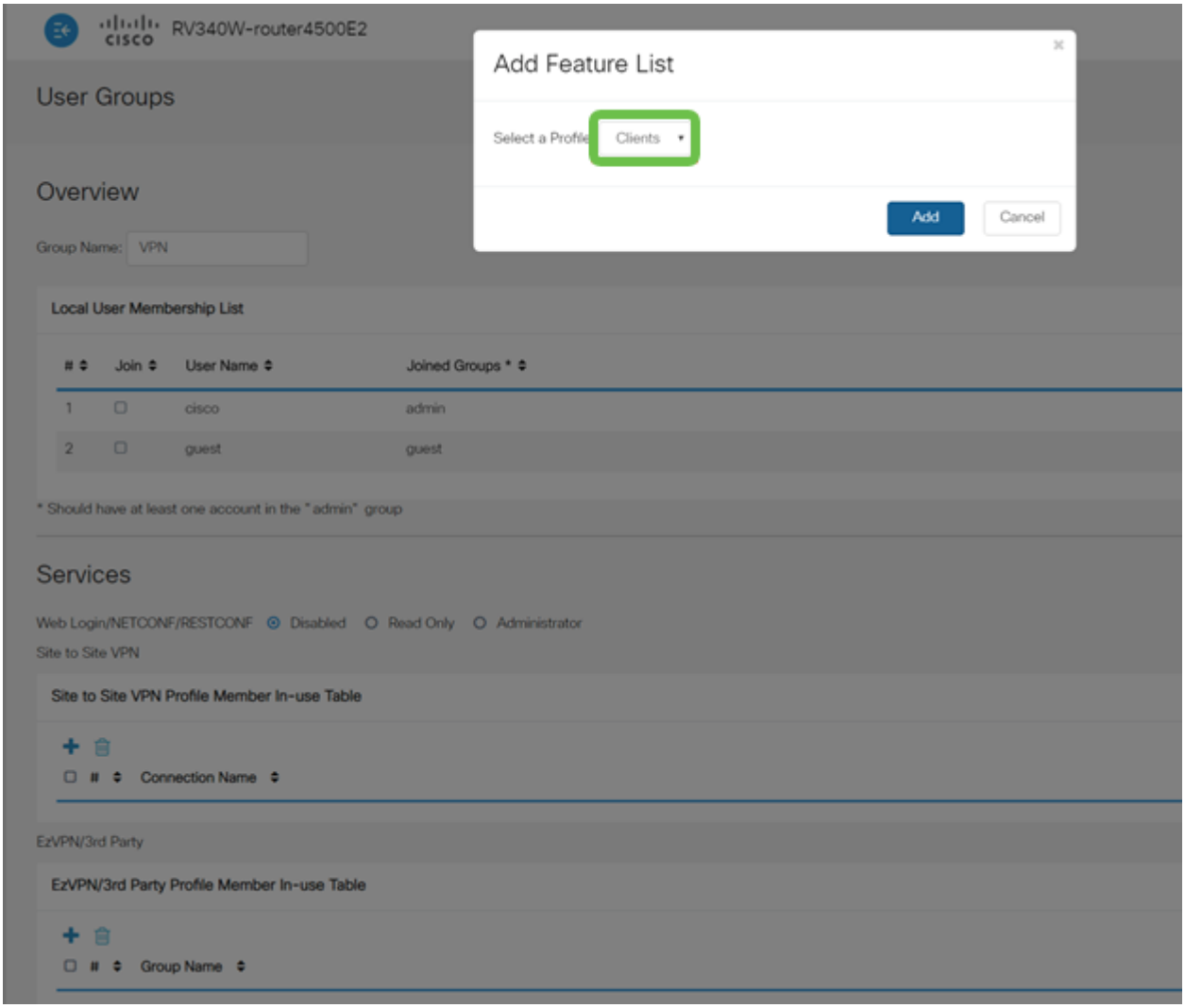
手順 9

グループ名を入力します。



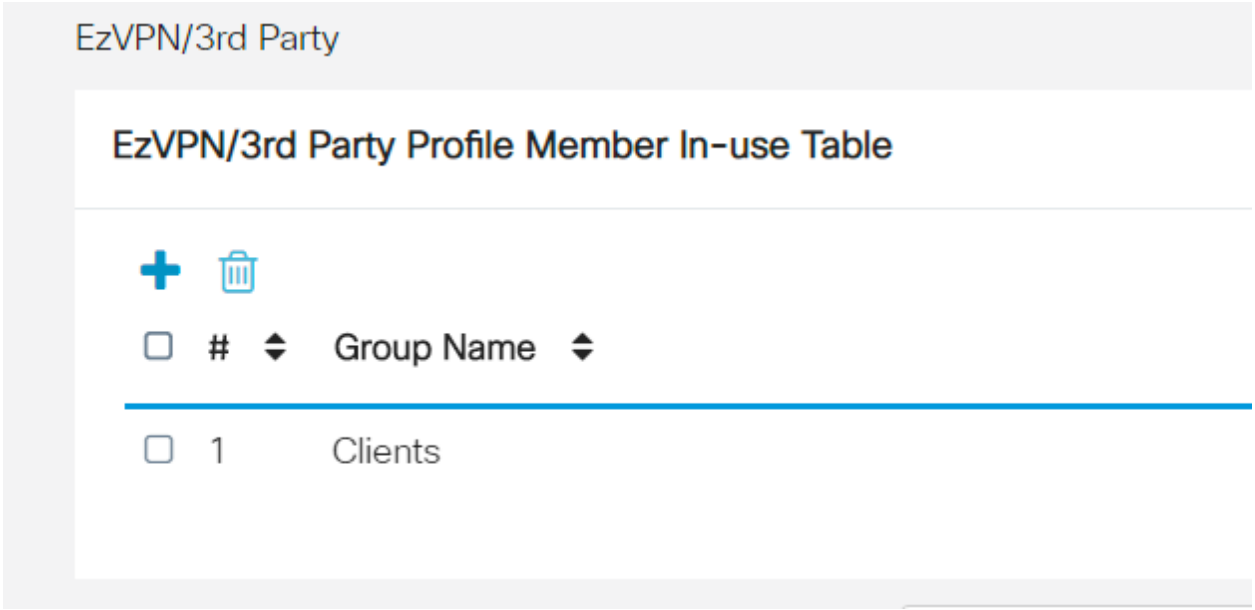
手順 10

[Services] > **[EzVPN/3rd Party]で、[Add]**をクリックし、このユーザグループを以前に設定したクライアント間プロファイルにリンクします。



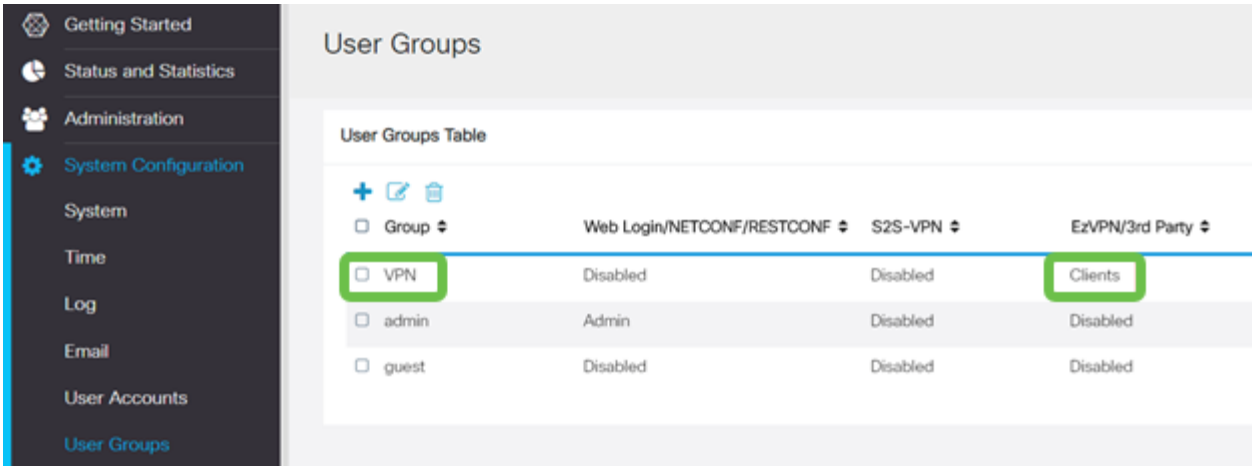
手順 11

これで、EzVPN/3rd Partyのリスト**に[Client-to-Site** Group Name]が表示**されます。**



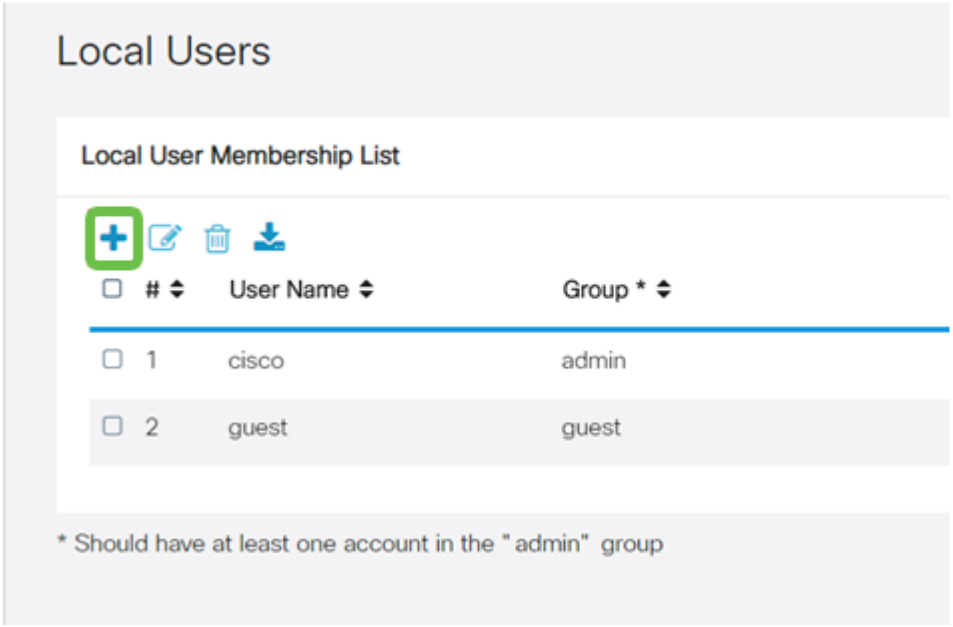
ステップ 12

ユーザグループ**の設定を**適用すると、[ユーザグループ]リストに表示され、以前に作成したクライアント間プロファイルで新しいユーザグループが使用されます。



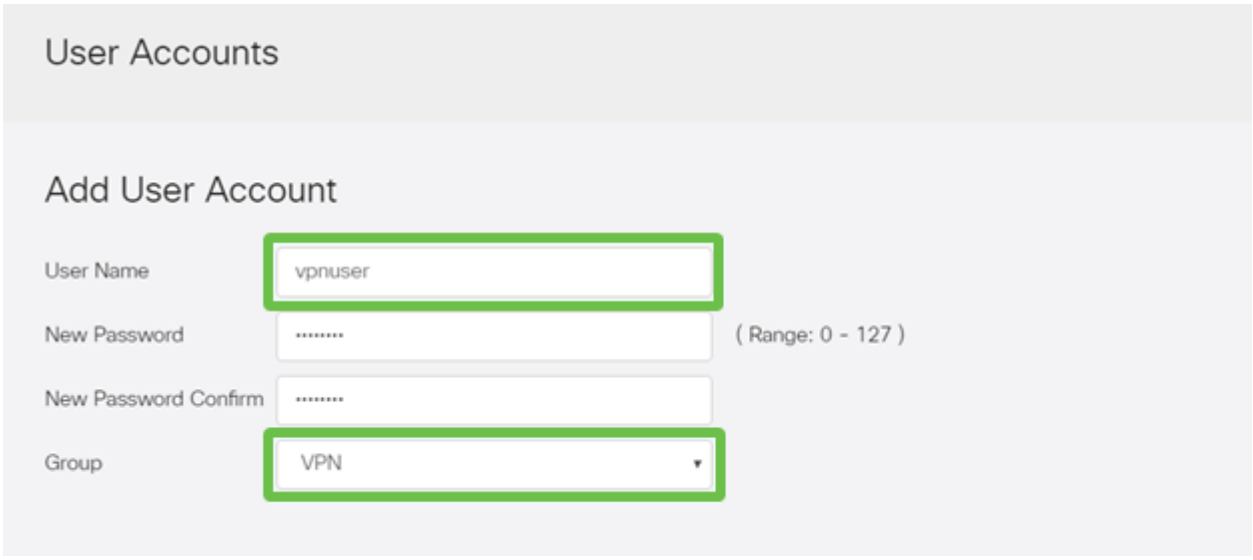
手順 13

[システムの設定(System Configuration)] > **[ユーザーアカウント(User Accounts)]で、新しいユーザーを設定します。**[+]アイコンをクリックして、新しいユーザを作成します。



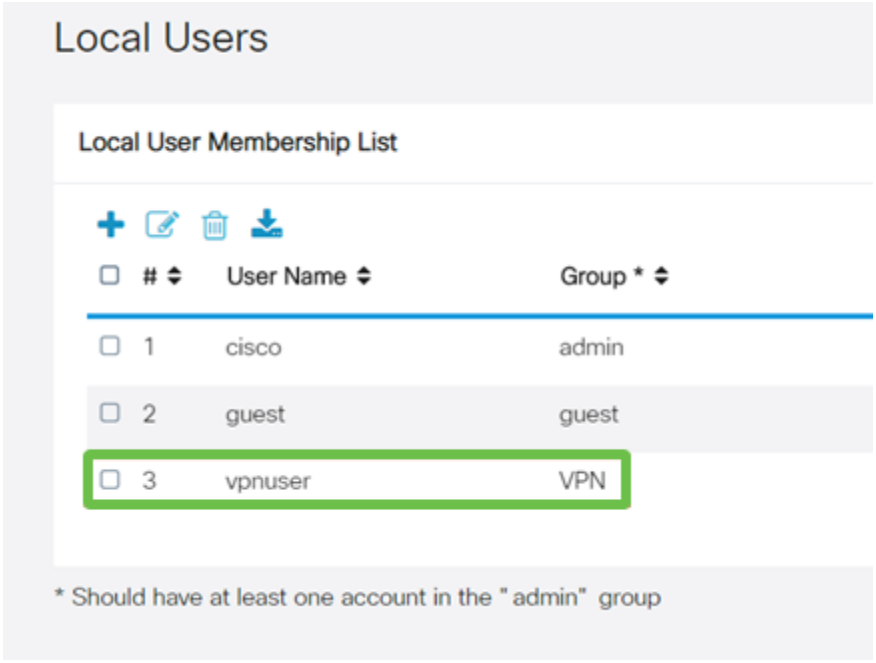
ステップ 14

新しいユーザー**名と新**しいパスワードを**入力します。**グループが、設定した**新しいユ**ーザグループに設定されている**ことを**確認してください。最後に、[Apply] をクリックします



ステップ 15

新しいユーザーがローカルユーザーのリストに表示されます。



これで、RV345Pシリーズルータの設定は完了です。次に、シュレウソフトVPNクライアントを設定します。

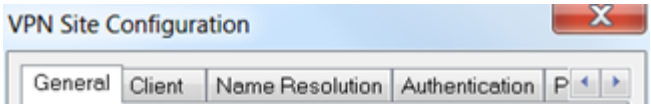
Shrew Soft VPN Clientの設定

次の手順を実行します。

手順 1

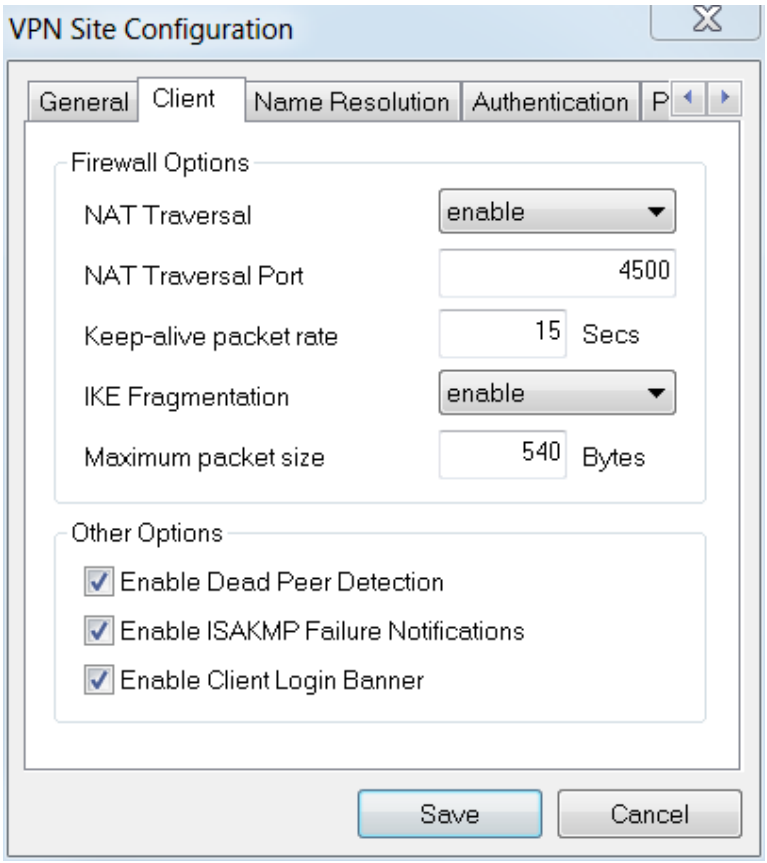
Shrew Soft *VPN Access Manager*を開き、*Add*をクリックしてプロファイルを追加します。表示される[*VPN Site Configuration*]ウィンドウで**General**タブを設定します。

- **ホスト名またはIPアドレス**:WAN IPアドレス（またはRV345Pのホスト名）を使用する
- **自動設定**:ike config pullを選択します
- **アダプタモード**:[仮想アダプタと割り当てられたアドレスを使用する]を選択します



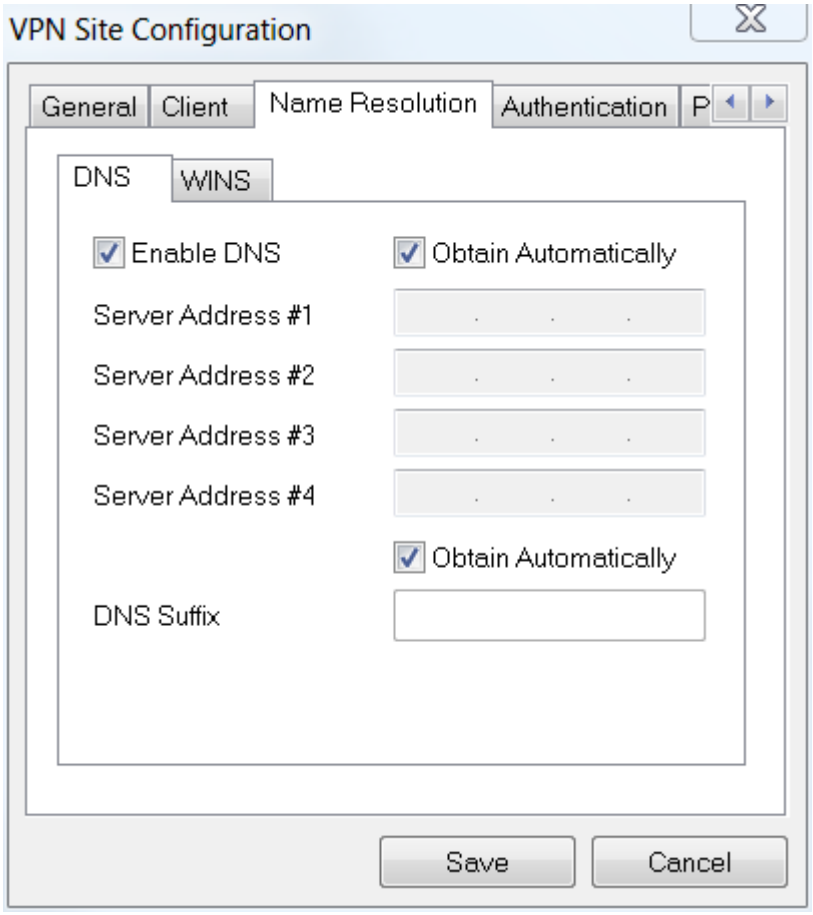
手順 2

[クライアント]**タブを設**定します。この例では、デフォルト設定を保持しています。



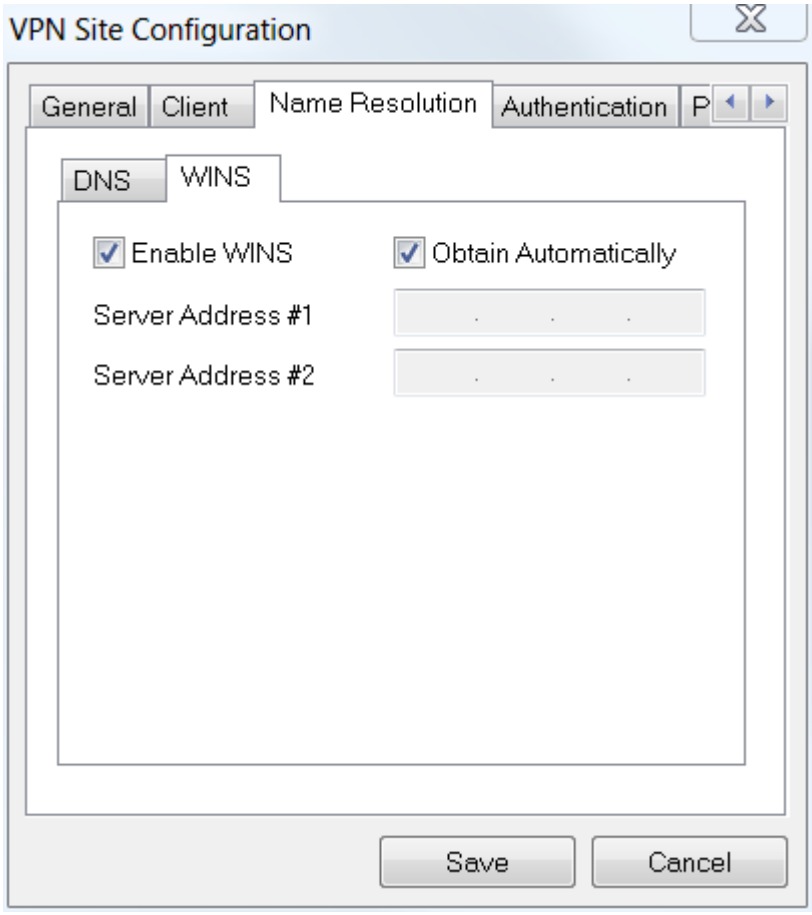
手順 3

[名前の解決] > [DNS]で、[DNSを有効にする]ボックスをオンにし、[自動的に取得]ボックス**はオンのままにして**ください。



手順 4

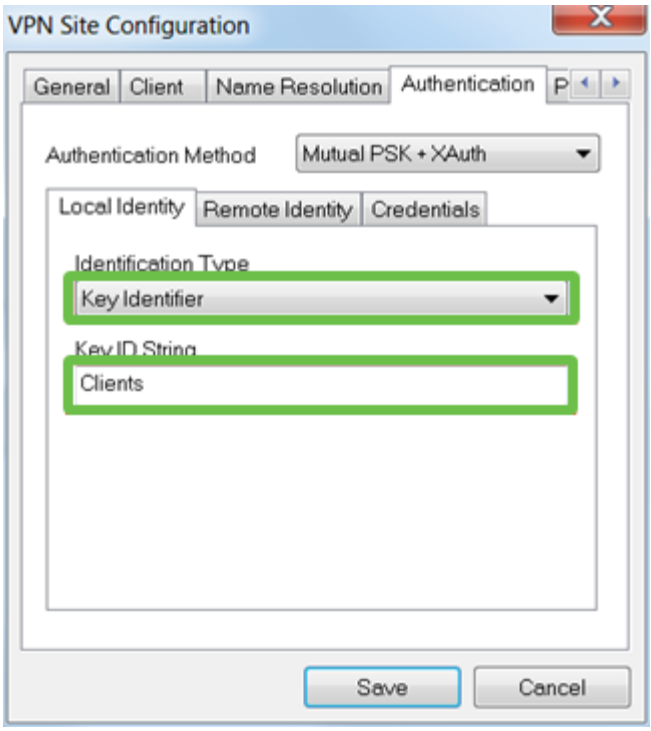
[Name Resolution] > [WINS]タブで、[Enable WINS]ボックスにチェックマークを入れ、[Obtain Automatically]ボックスにチェックマークを入れます。



手順 5

[Authentication] > [Local Identity]をクリックします。

- IDタイプ:キー識別子の選択
- キーID文字列:RV345Pで設定されたグループ名を入力します

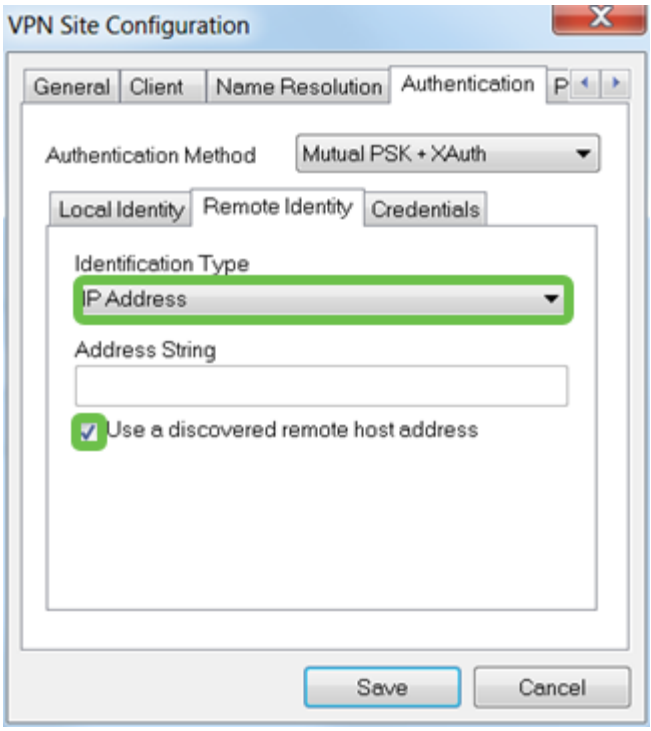


手順 6

[Authentication] > [Remote Identity]の順に選択します。この例では、デフォルト設定を

保持しています。

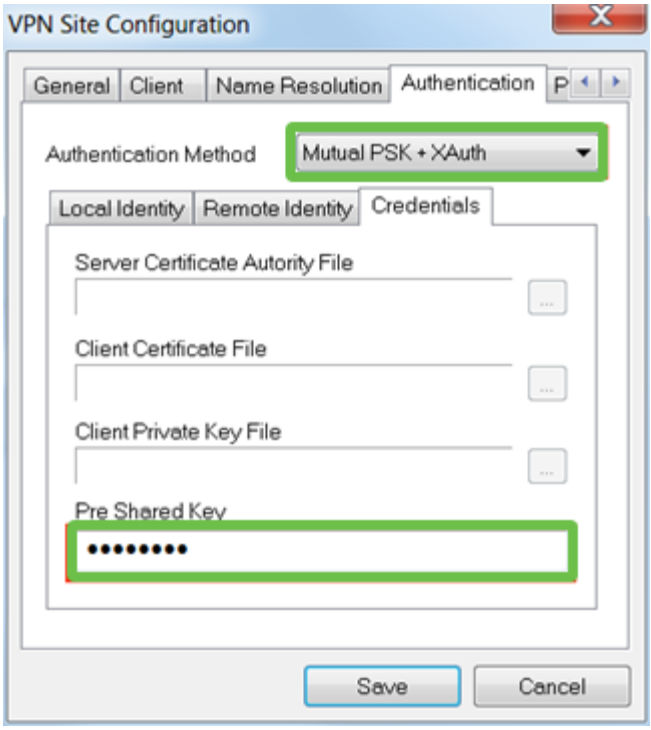
- **IDタイプ**:iSCSIポータルの
- **アドレス文字列**:<blank>
- **検出されたリモートホストアドレスボックスを使**用します。チェックボックスをオンにします。



ステップ7

[**Authentication**] > [**Credentials**]で、次のように設定します。

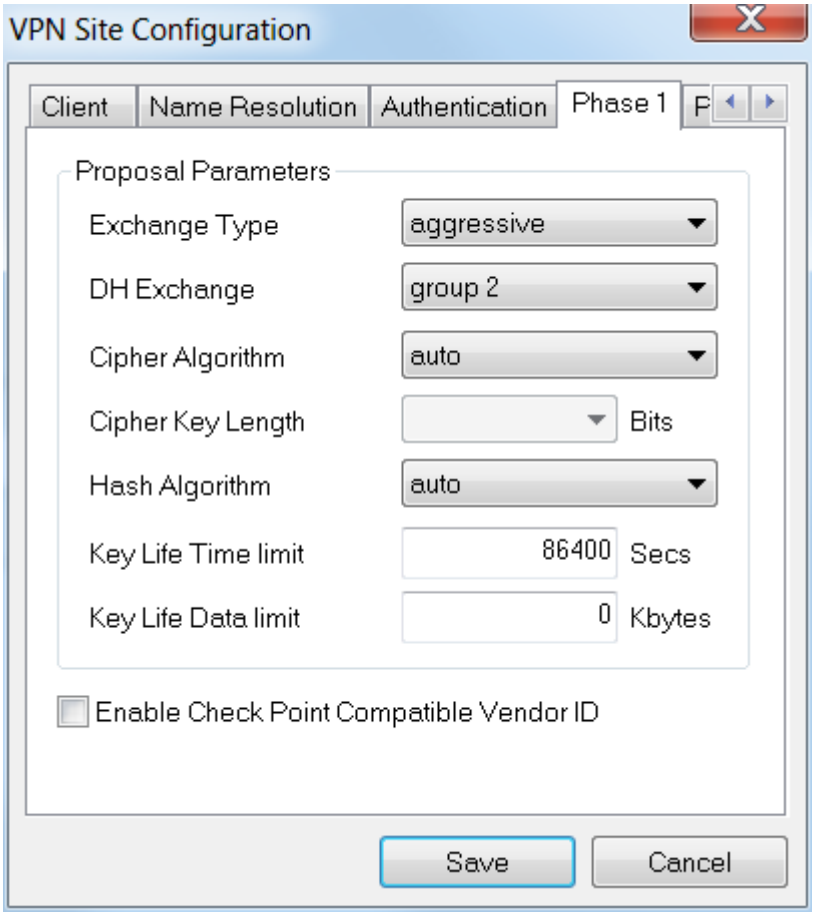
- **Authentication Method**：[相互**PSK + XAuth**]**を選択します**
- **Pre-Shared Key**:RV345Pクライ**アント・ プロ**ファイルに設定されている事前共有キーを入力



手順 8

[Phase 1]タブの場合。この例では、デフォルト設定は保持されています。

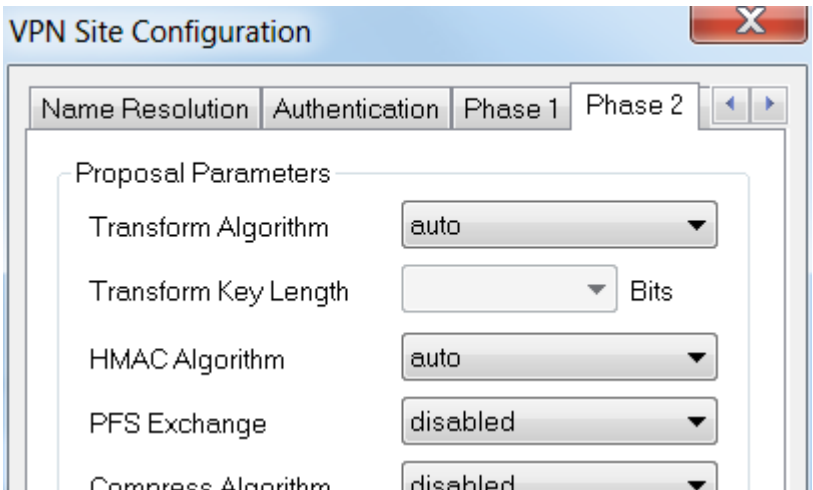
- **交換タイプ：アグレッシブル**
- **DH交換：**グループ2
- **暗号アルゴリズム：**自動
- **ハッシュアルゴリズム：**自動



手順 9

この例では、[Phase 2]タブのデフォルトは同じままになっています。

- **変換アルゴリズム：**自動
- **HMACアルゴリズム：**自動
- **PFS交換：**無効
- **圧縮アルゴリズム：**無効

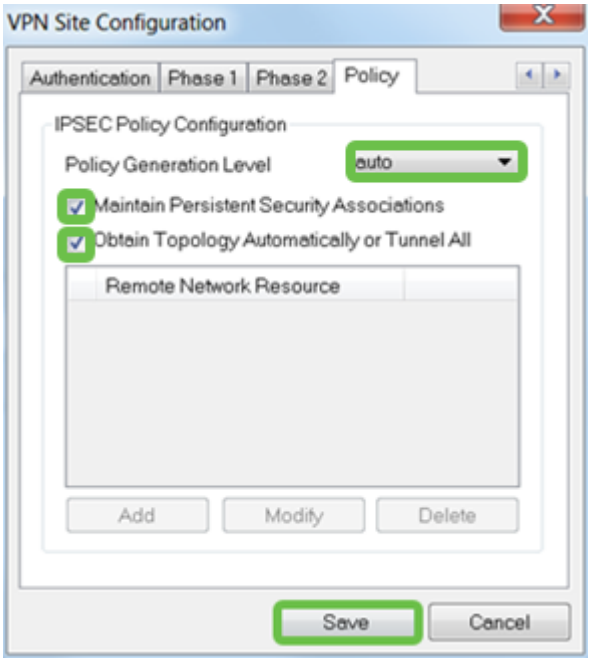


手順 10

[ポリシー]タブの例では、次の設定を使用しました。

- **ポリシー生成レベル**：自動
- **永続的なセキュリティアソシエーションの管理**：オン
- Obtain Topology AutomaticallyまたはTunnel All:オン

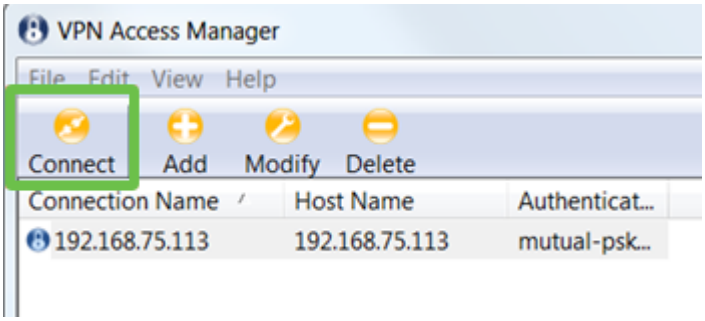
RV345Pで**Split-Tunneling**を設定したため、ここで設定する必要はありません。



終了したら、[保存]をクリックします。

手順 11

これで、接続をテストする準備ができました。*VPN* Access Managerで、*接続プロファイル*を強調表示し、[**Connect**]ボタンをクリックします。

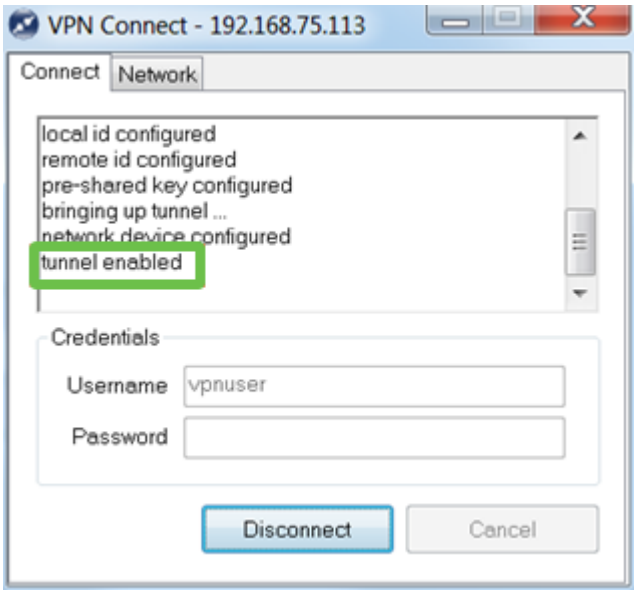


ステップ 12

表示される[**VPN Connect**]ウィンドウで、RV345Pで作成した**ユーザアカウント**のクレデンシャルを使用して**ユーザ名**と**パスワードを入力します（ステップ13 & 14）。** 終了したら、[接続]をクリックします。

手順 13

トンネルが接続されていることを確認します。トンネルが有効になっている**はずです**。



この設定では、Shrew Softを例として使用しました。Shrew Softはシスコ製品ではないため、テクニカルサポートが必要な場合は、このサードパーティに連絡してください。

その他のVPNオプション

VPNを使用する他のオプションがいくつかあります。詳細については、次のリンクをクリックしてください。

- GreenBow VPN Clientを使用したRV34xシリーズルータへの接続
- RV34xシリーズルータでのテレワーカーVPNクライアントの設定
- Rv34xシリーズルータでのポイントツーポイントトンネリングプロトコル(PPTP)サーバの設定
- RV34xシリーズルータでのインターネットプロトコルセキュリティ(IPsec)プロファイル

の設定
- RV34xルータでのL2TP WANの設定
- RV34xでのサイト間VPNの設定

RV345Pルータの補足設定

VLANの設定（オプション）

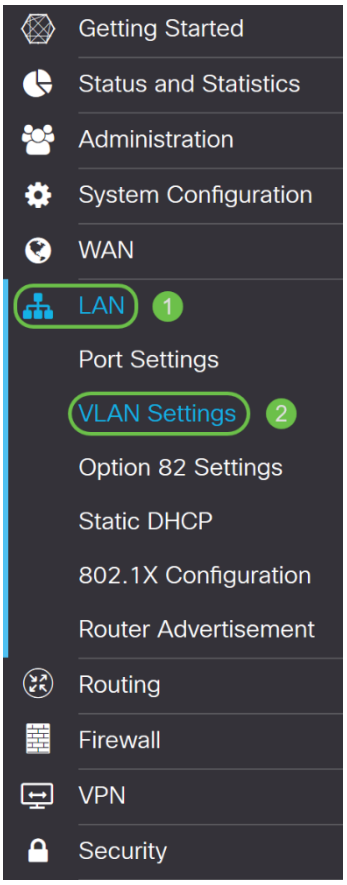
仮想ローカルエリアネットワーク(VLAN)を使用すると、ローカルエリアネットワーク(LAN)を論理的に異なるブロードキャストドメインにセグメント化できます。機密データがネットワーク上でブロードキャストされるシナリオでは、特定のVLANにブロードキャストを指定することでセキュリティを強化するためにVLANを作成できます。また、VLANを使用して、ブロードキャストやマルチキャストを不要な宛先に送信する必要性を減らし、パフォーマンスを向上させることもできます。VLANは作成できますが、VLANが手動または動的に少なくとも1つのポートに接続されるまで、これは影響しません。ポートは常に1つ以上のVLANに属している必要があります。

その他のガイダンスについては、『VLANのベストプラクティスとセキュリティのヒント』を参照してください。

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。

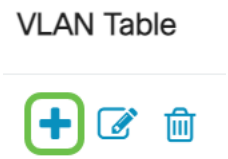
手順 1

[LAN] > [VLAN Settings]に移動します。



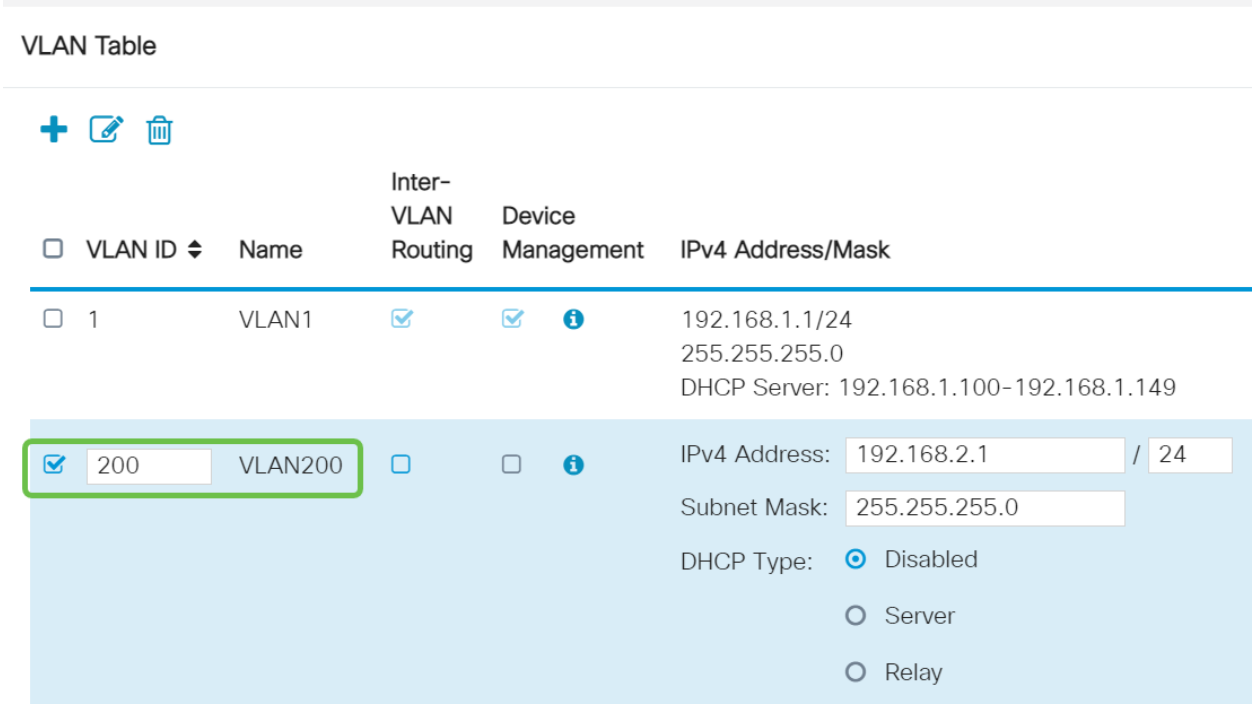
手順 2

新しいVLANを作**成するに**は、追加アイコンをクリックします。



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。



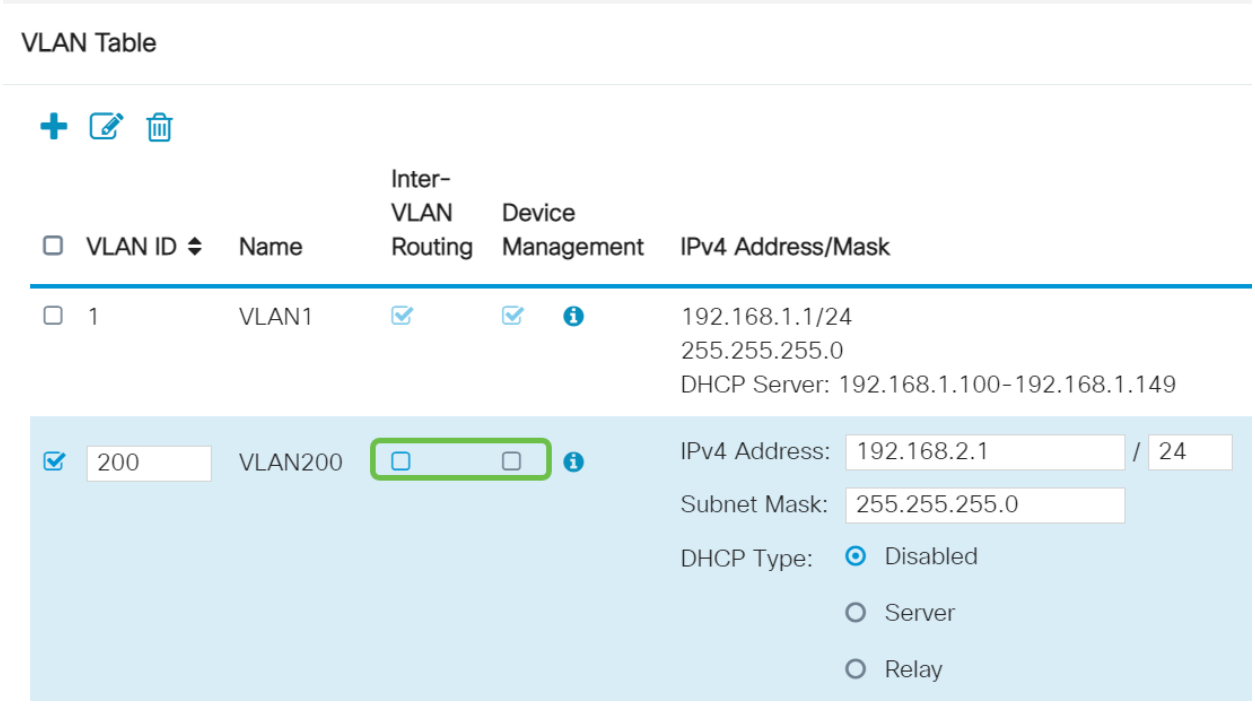
手順 4

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。

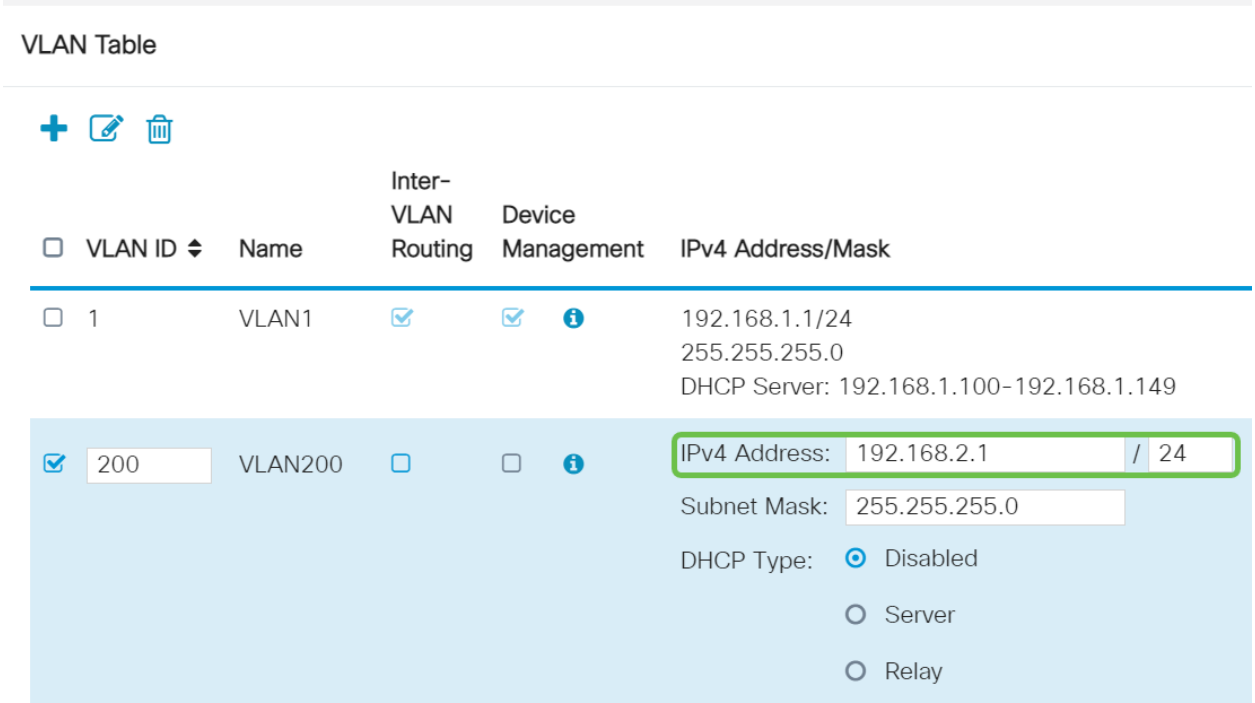
Device Managementは、ブラウザを使用してVLANからRV345PのWeb UIにログインし、RV345Pを管理できるソフトウェアです。これは、ゲストネットワークでも無効にする必要があります。

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

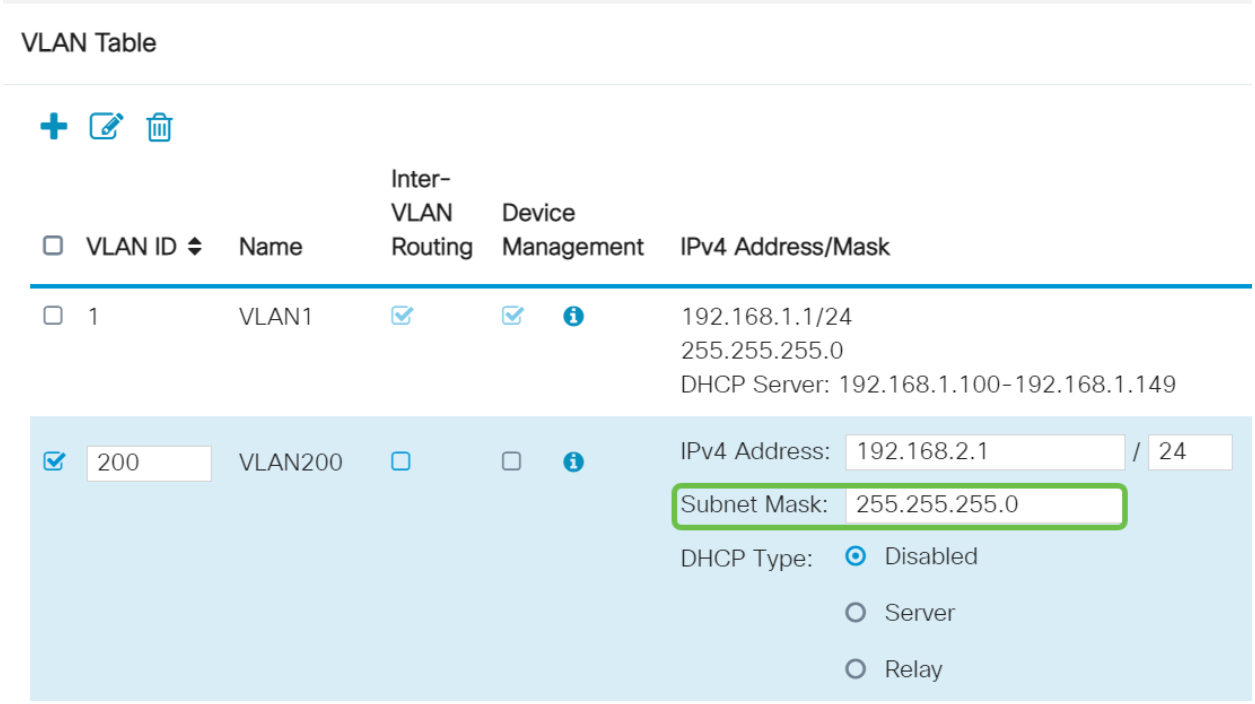
プライベートIPv4アドレスが[IPアドレス]フィールドに自*動的に入力*されます。これを調整するには、次を選択します。この例では、サブネットに192.168.2.100 ~ 192.168.2.149のIPアドレスがDHCPで使用可能です。192.168.2.1 ~ 192.168.2.99および192.168.2.150 ~ 192.168.2.254は、スタティックIPアドレスに使用できます。



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。**



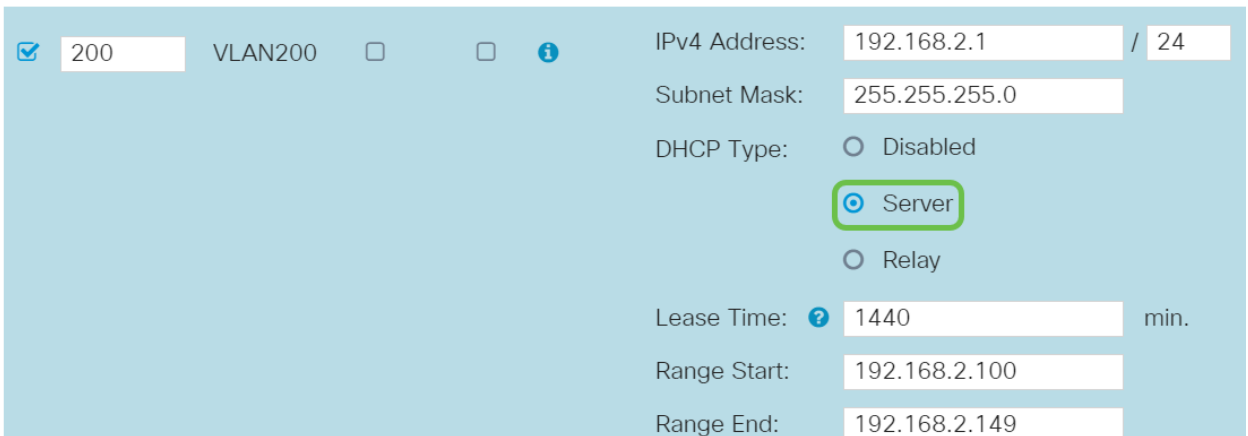
ステップ7

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。

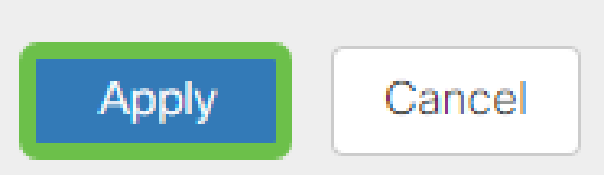
Server : これは最もよく使用されるオプションです。

- [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（オプション）

RV345P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。トランク上で必要としない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には、[Untagged]というラベルを付ける必要があります。
- 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:

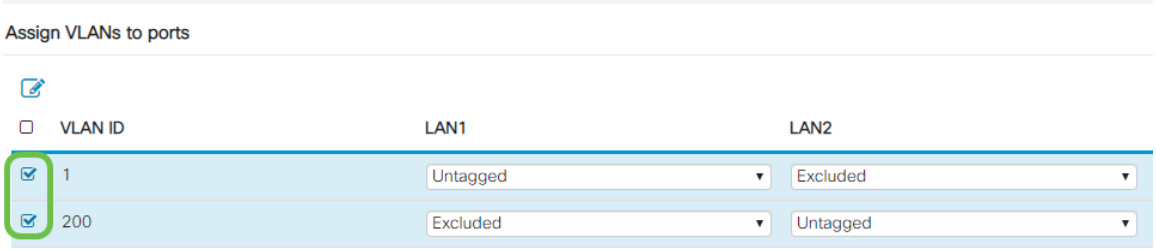
- トランクポートと見なされます。
- いずれかのVLANに[Untagged]というラベルを付けることができます。
- トランクポートの一部である残りのVLANには、[Tagged]というラベルを付ける必要があります。
- トランクポートの一部ではないVLANには、そのポートに対して[Excluded]というラベルを付ける必要があります。

この例では、トランクはありません。

手順 1

編集する*VLAN ID*を選択します。

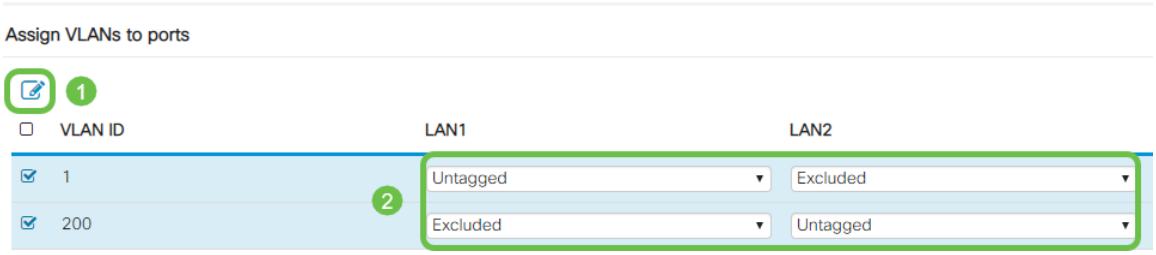
この例では、VLAN 1と*VLAN* 200を選択しています。



手順 2

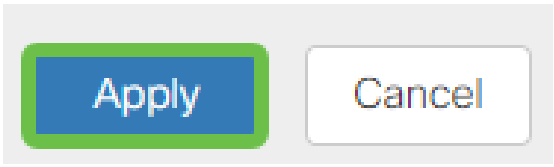
VLANをLANポートに割り当て、[Edit]をクリックし、それぞれの設定を[*Tagged*]、[*Untagged*]、または[*Excluded*]に指定します。

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 3

[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、RV345P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を作成します。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。

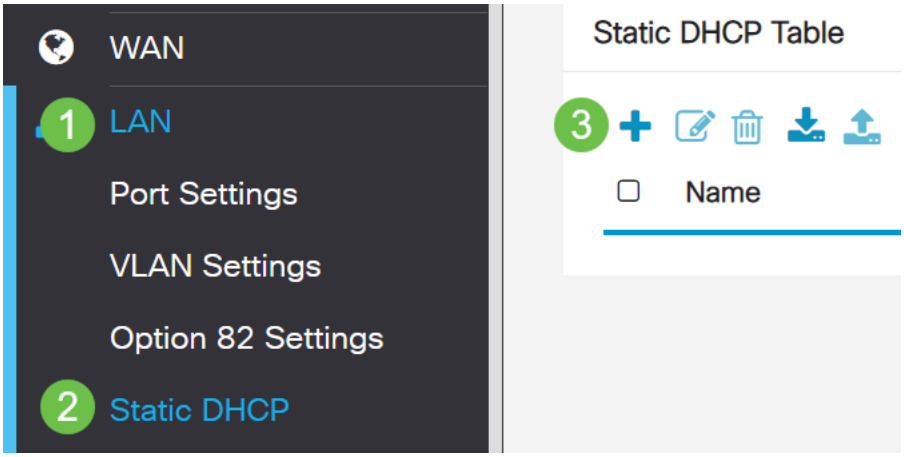
スタティックIPの追加（オプション）

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動できます。

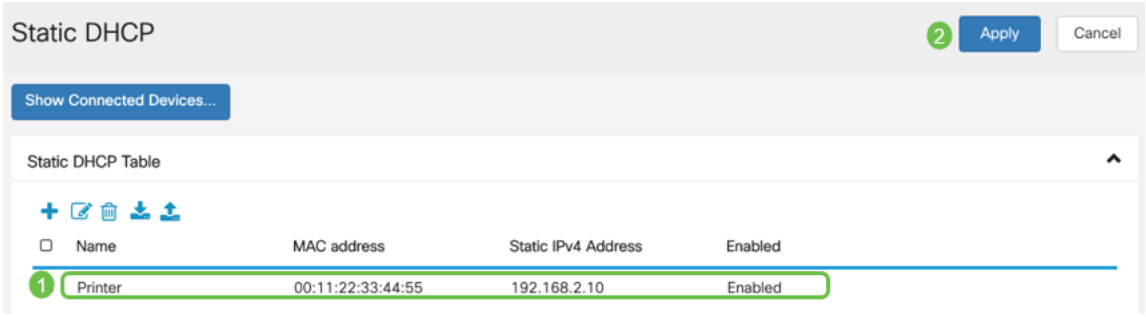
手順 1

[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。



証明書の管理（オプション）

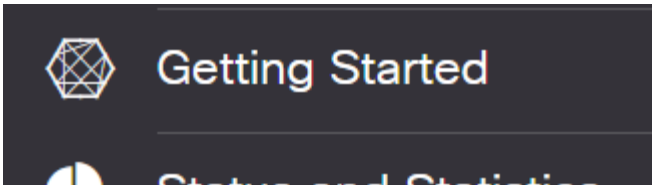
デジタル証明書は、証明書の名前付きサブジェクトによって公開キーの所有権を証明します。これにより、証明書利用者は、認証された公開キーに対応する秘密キーによる署名やアサーションに依存できます。ルータは、自己署名証明書、つまりネットワーク管理者によって作成された証明書を生成できます。また、認証局(CA)に要求を送信して、デジタルID証明書を申請することもできます。サードパーティアプリケーションから正当な証明書を取得することが重要です。

認証局(CA)が認証に使用されます。証明書は、任意の数のサードパーティサイトから購入できます。これは、あなたのサイトが安全であることを証明する公式の方法です。基本的に、CAは正当なビジネスであり、信頼できることを検証する信頼できるソースです。必要に応じて、最小限のコストで証明書を発行します。CAによってチェックアウトされ、情報を確認すると、証明書が発行されます。この証明書は、コンピュータ上のファイルとしてダウンロードできます。その後、ルータ（またはVPNサーバ）に移動し、そこにアップロードできます。

CSR/証明書の生成

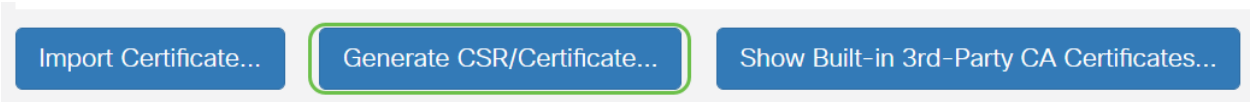
手順 1

ルータのWebベースのユーティリティにログインし、**[Administration] > [Certificate]を選択します。**



手順 2

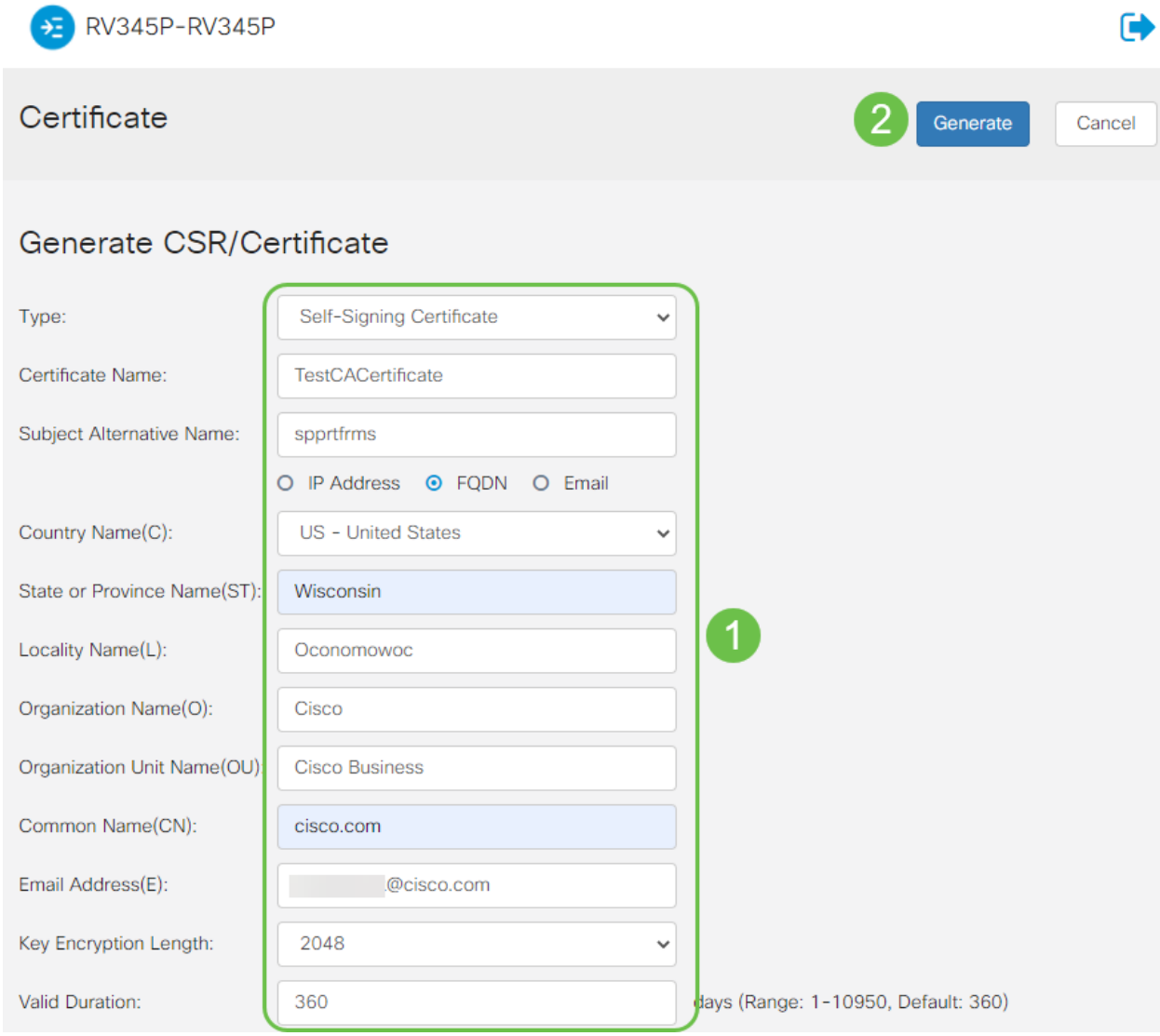
[**Generate CSR/Certificate**]をクリックします。[Generate CSR/Certificate]ページが表示されます。



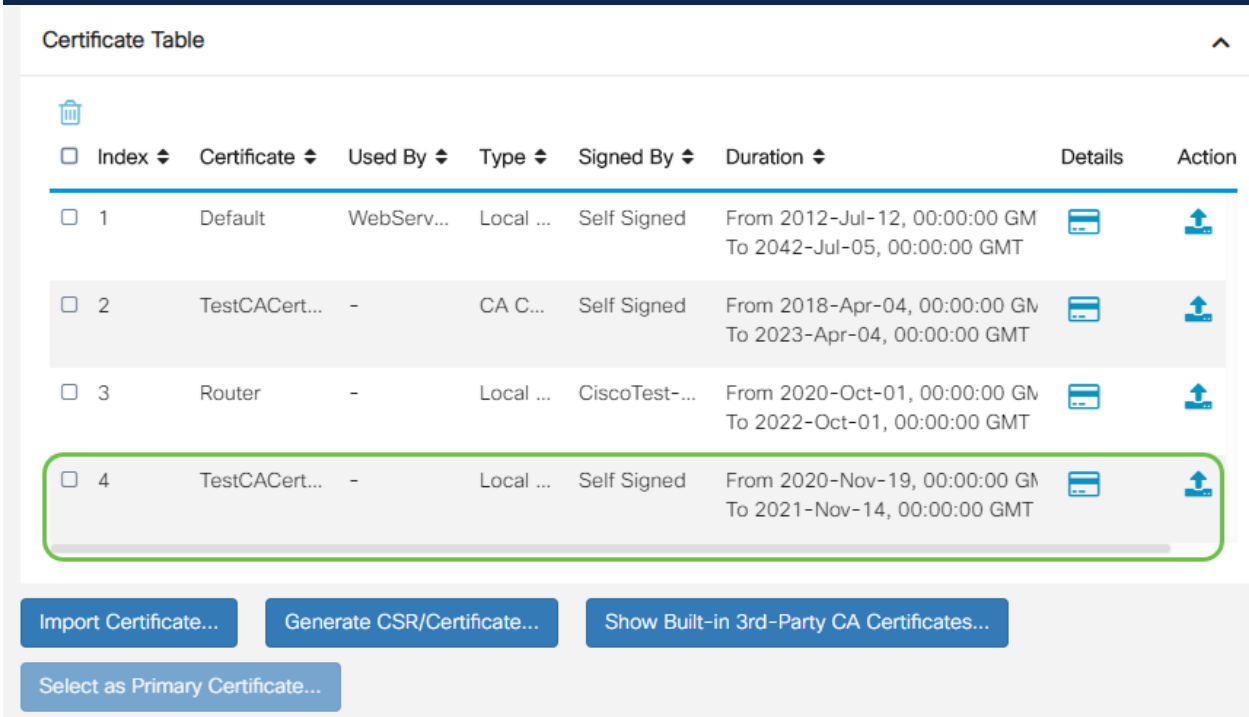
手順 3

次の項目を入力します。

- 適切な証明書タイプを選択します
  - 自己署名証明書：これは、独自の作成者によって署名されたSecure Socket Layer(SSL)証明書です。この証明書は、攻撃者によって秘密キーが侵害された場合に取り消すことができないため、信頼できません。
  - 認定署名要求(CSR)：これは、デジタルID証明書を申請するために認証局に送信される公開キーインフラストラクチャ(PKI)です。秘密キーは秘密にされるため、自己署名よりも安全です。
- [Certificate Name]フィールドに証明書の名前を入力して、要求を識別します。このフィールドは空白にしたり、スペースや特殊文字を含めることはできません。
- （オプション）[Subject Alternative Name]領域で、オプションボタンをクリックします。次のオプションがあります。
  - [IP Address]：インターネットプロトコル(IP)アドレスを入力します
  - [FQDN]：完全修飾ドメイン名(FQDN)を入力します
  - [電子メール]：電子メールアドレスを入力します
- [Subject Alternative Name]フィールドにFQDNを入力します。
- [国名(Country Name)]ドロップダウンリストから、組織が登録されている国名を選択します。
- 組織が所在する都道府県、地域、または地域の名前または省略形を[都道府県(ST)]フィールドに入力します。
- 組織が登録されている地域または市区町村の名前を[Locality Name]フィールドに入力します。
- 会社が法的に登録されている名前を入力します。小規模企業または個人事業主として登録する場合は、[組織名(Organization Name)]フィールドに証明書要求者の名前を入力します。特殊文字は使用できません。
- 「組織単位名」(Organization Unit Name)フィールドに名前を入力して、組織内の部門間で区別します。
- [共通名(Common Name)]フィールドに名前を入力します。この名前は、証明書を使用するWebサイトの完全修飾ドメイン名である必要があります。
- 証明書を生成する個人の電子メールアドレスを入力します。
- [Key Encryption Length]ドロップダウンリストから、キーの長さを選択します。オプションは512、1024、および2048です。キーの長さが長いほど、証明書の安全性が高くなります。
- [有効期間]フィールドに、証明書が有効になる日数を入力します。デフォルト値は 360 です。
- [Generate] をクリックします。



生成された証明書が証明書テーブルに表示されます。

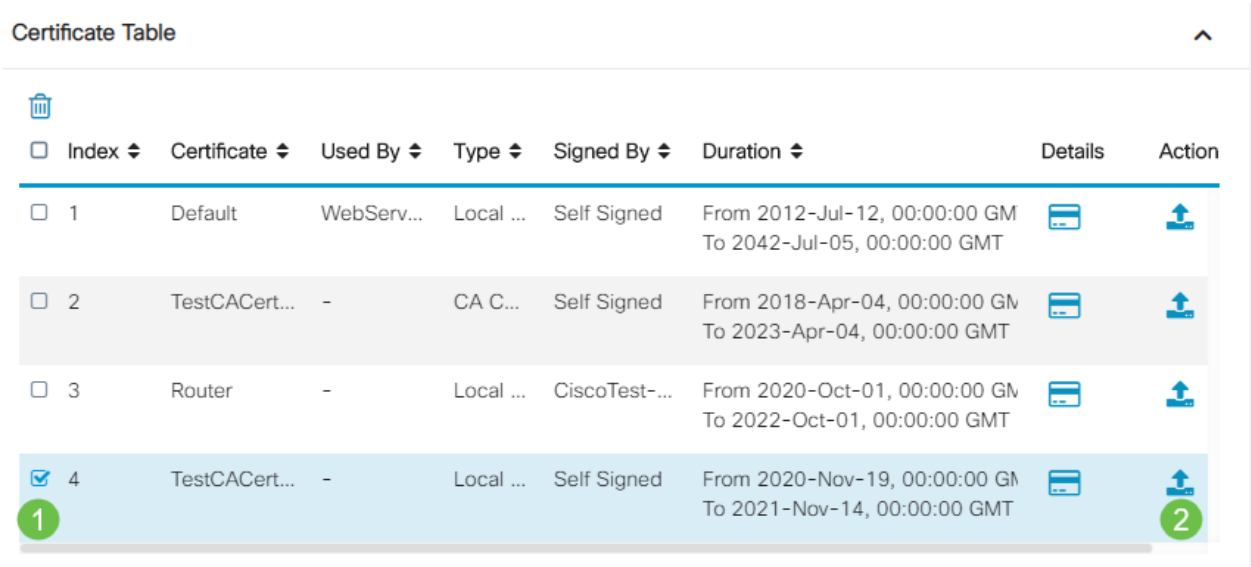


これで、RV345Pルータに証明書が正常に作成されたはずです。

証明書のエクスポート

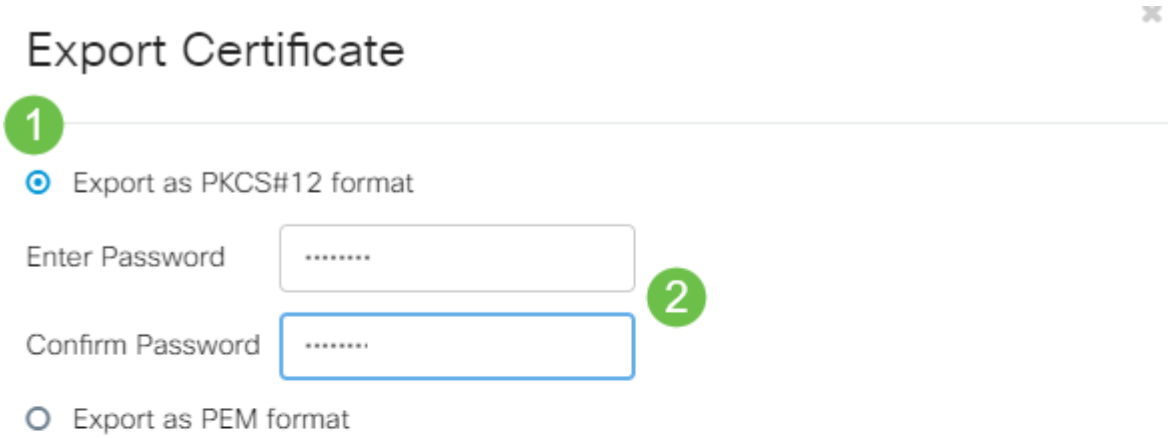
手順 1

証明書テーブルで、エクスポートする証明書のチェックボックスをオンにし、エクスポートアイコンをクリックします。



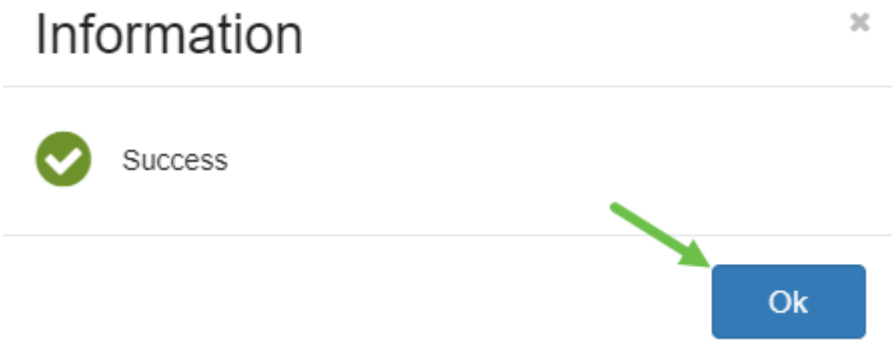
手順 2

- 証明書をエクスポートする形式をクリックします。次のオプションがあります。
  - PKCS #12：公開鍵暗号規格(PKCS)#12は、.p12拡張子に含まれるエクスポートされた証明書です。ファイルを暗号化して、エクスポート、インポート、および削除するときにファイルを保護するには、パスワードが必要です。
  - PEM:Privacy Enhanced Mail(PEM)は、メモ帳などの簡単なテキストエディタを使用して簡単に読み取り可能なデータに変換できるように、Webサーバでよく使用されます。
- PEMを選択した場合は、[Export]をクリックします。
- エクスポートするファイルを保護するためのパスワードを[Enter Password]フィールドに入力します。
- [Confirm Password]フィールドにパスワードを再入力します。
- [Select Destination]エリアでは、PCが選択されており、現在利用可能な唯一のオプションです。
- [Export] をクリックします。



手順 3

ダウンロードの成功を示すメッセージが[Download]ボタンの下に表示されます。ファイルのダウンロードがブラウザで開始されます。[OK] をクリックします。

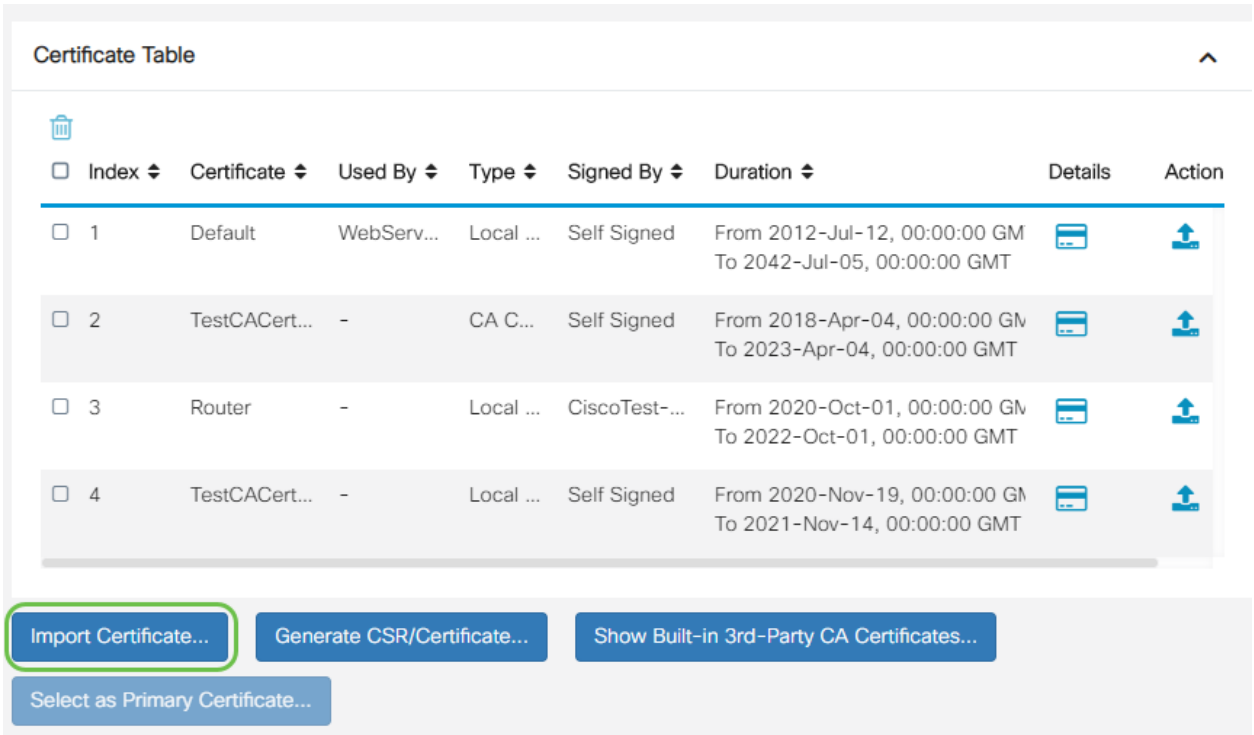


これで、RV345Pシリーズルータで証明書が正常にエクスポートされたはずです。

証明書のインポート

手順 1

[Import Certificate...]をクリックします。.

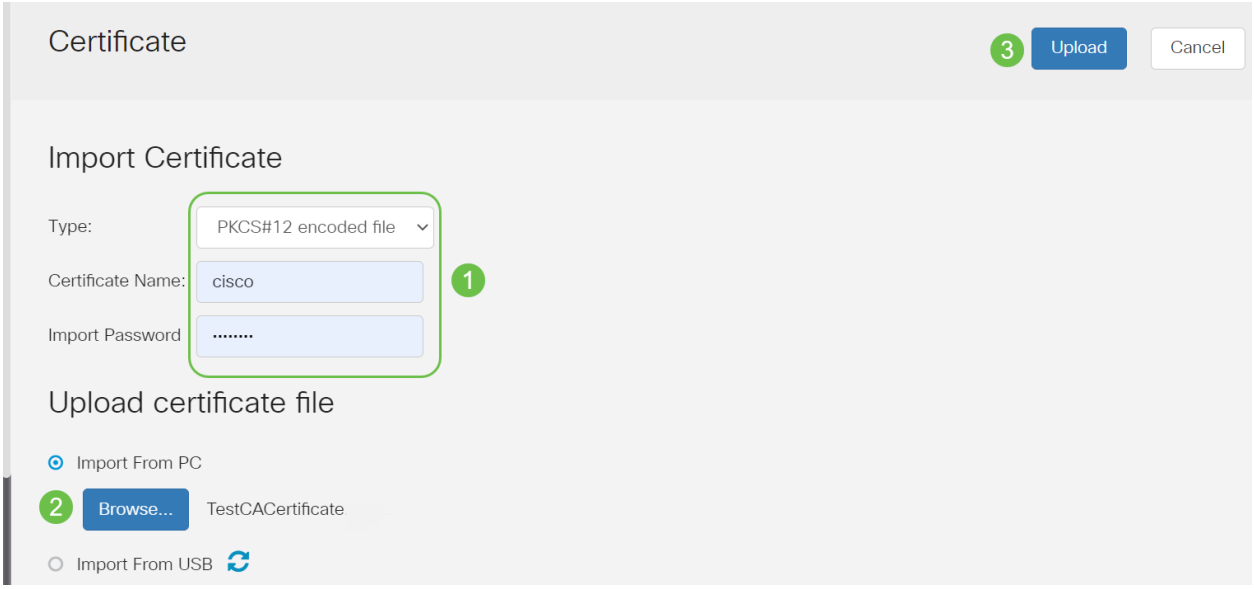


手順 2

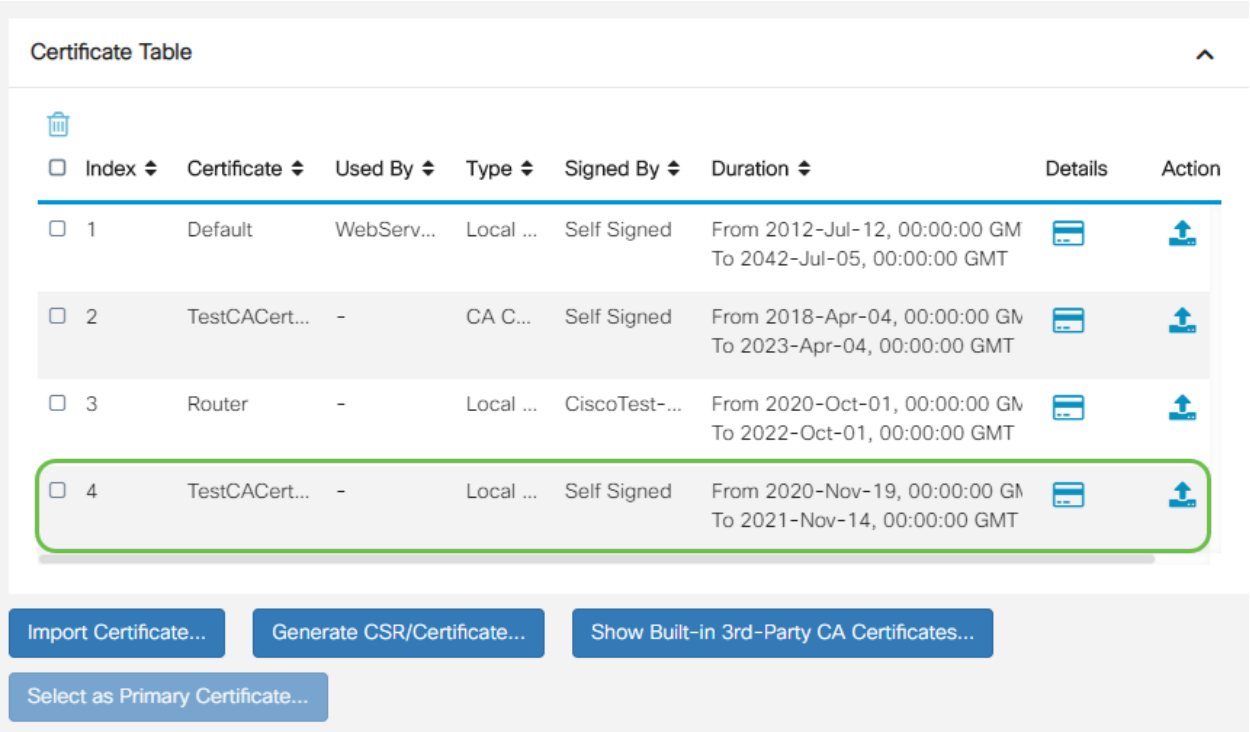
- ドロップダウンリストから、インポートする証明書のタイプを選択します。次のオプションがあります。
  - ローカル証明書：ルータで生成された証明書。
  - CA証明書：証明書に含まれる情報が正確であることを確認した、信頼できるサードパーティ認証局によって認証された証明書。
  - PKCS #12 Encodedファイル：公開鍵暗号規格(PKCS)#12は、サーバ証明書を保存する形式です。

- [Certificate Name]フィールドに証明書の名前を入力します。
- PKCS #12を選択した場合は、[Import Password]フィールドにファイルのパスワードを入力します。それ以外の場合は、ステップ 3 に進みます。
- 証明書をインポートするソースをクリックします。次のオプションがあります。
    - PCからのインポート
    - USBからのインポート

- ルータがUSBドライブを検出しない場合、[Import from USB]オプションはグレー表示されます。
- [USBからインポート]を選択し、USBがルータで認識されない場合は、[更新]をクリックします。
- [Choose File]ボタンをクリックし、適切なファイルを選択します。
- [Upload] をクリックします。



成功すると、自動的にメインの[Certificate]ページに移動します。証明書テーブルに、最近インポートされた証明書が入力されます。



これで、RV345Pルータに証明書が正常にインポートされたはずです。

ドングルとRV345Pシリーズルータを使用したモバイルネットワークの設定（オプション）

ドングルとRV345Pルータを使用して、バックアップモバイルネットワークを設定する必要があるかもしれません。この場合は、「ドングルとRV34xシリーズルータを使用したモバイルネットワークの設定」を読む必要があります。

これで、RV345Pルータの設定は完了です。次に、Cisco Business Wireless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RV345PのPoEポートにイーサネットケーブルを接続します。RV345P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。*この問題に関しては、「RV345xルータのリブートと工場出荷時のデフォルト設定にリセットする方法」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。

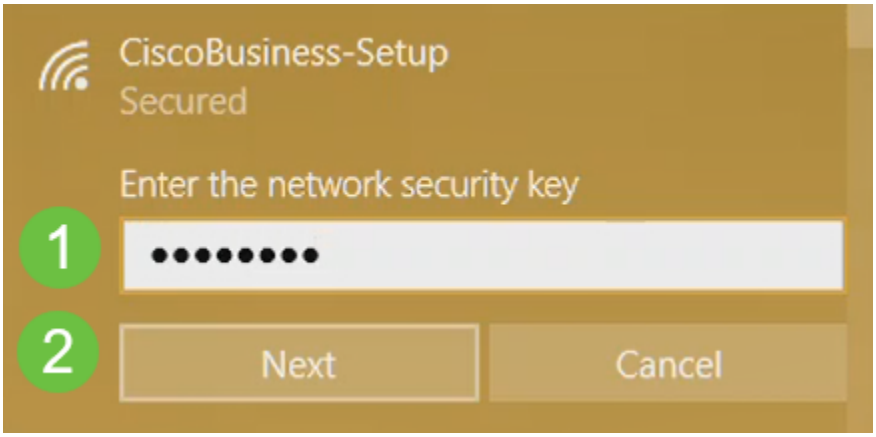
手順 1

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。*

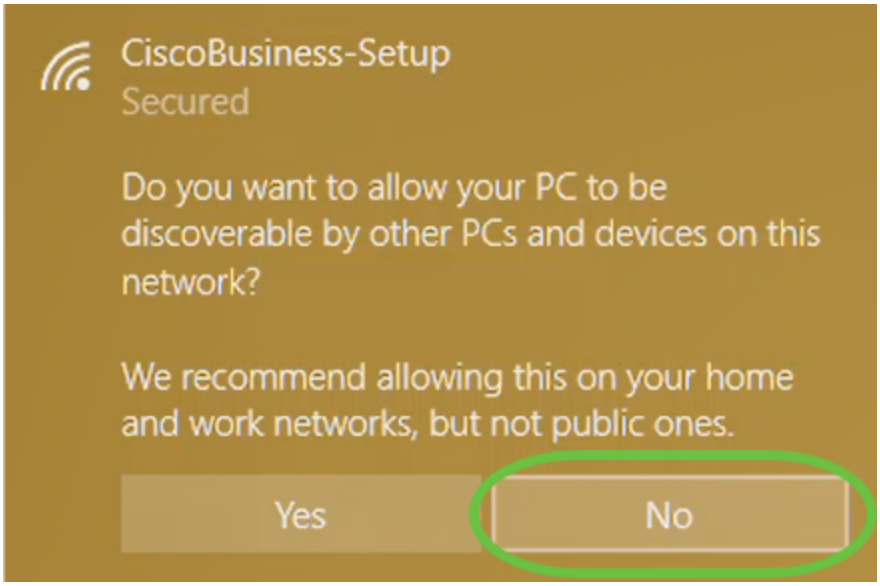
手順 2

パスフレーズcisco123を入力し、[Next]をクリックします。



手順 3

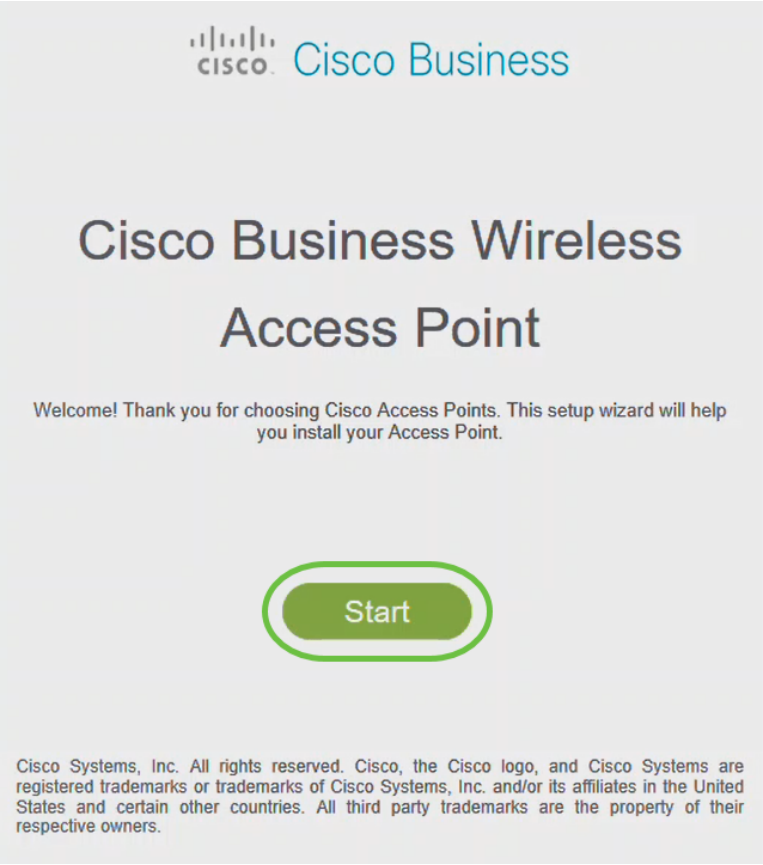
次の画面が表示されます。一度に設定できるデバイスは1つだけなので、[いいえ]をクリックします。



CiscoBusiness-Setup SSIDに接続できるデバイスは*1つだけ*です。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。

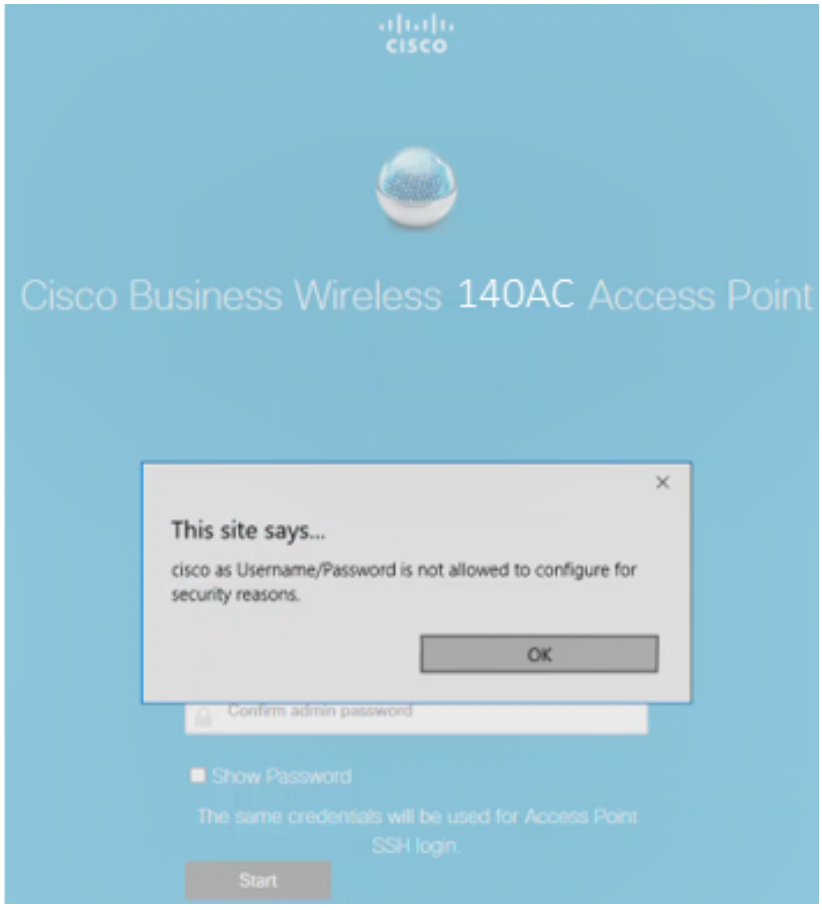
手順 5

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。

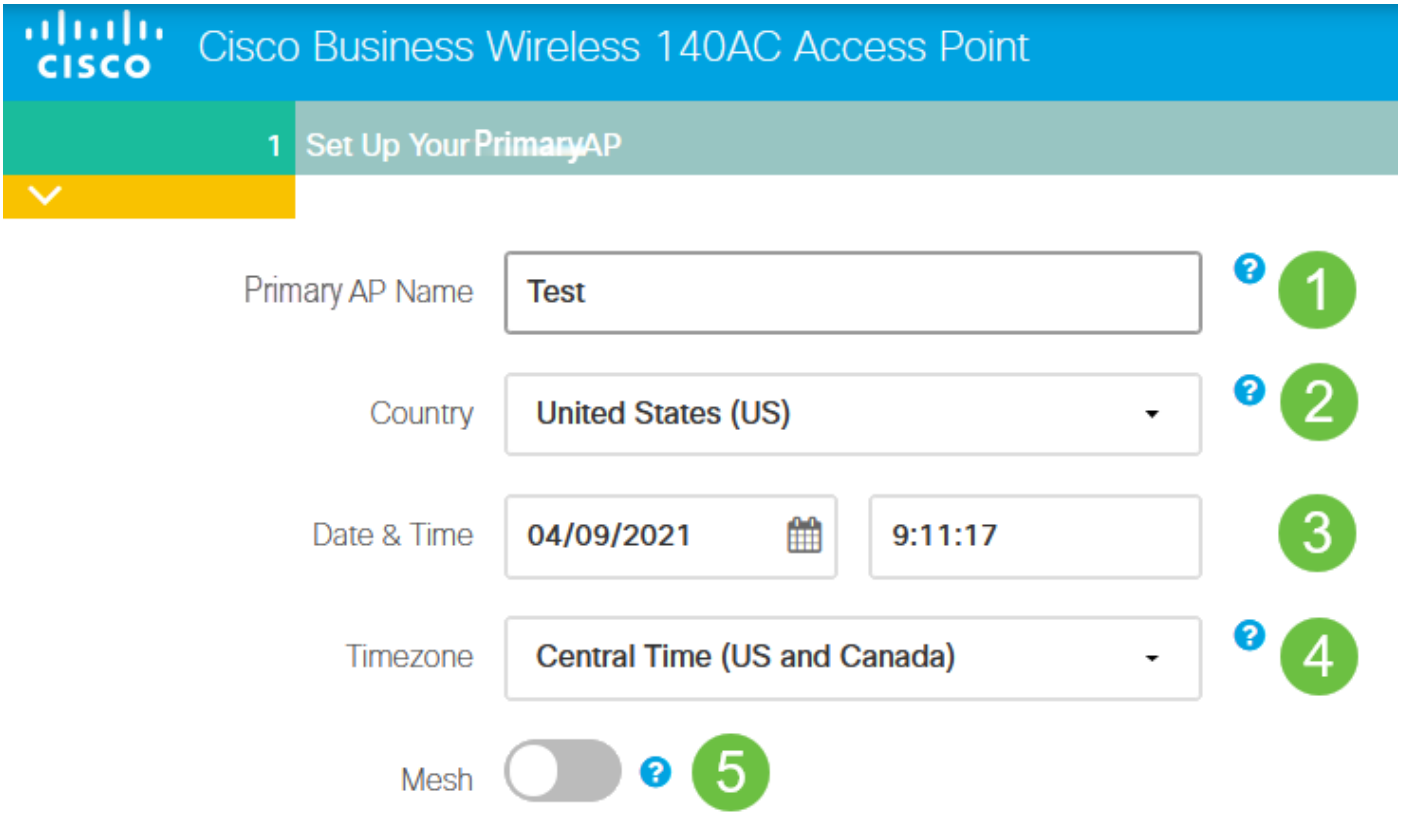


手順 6

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



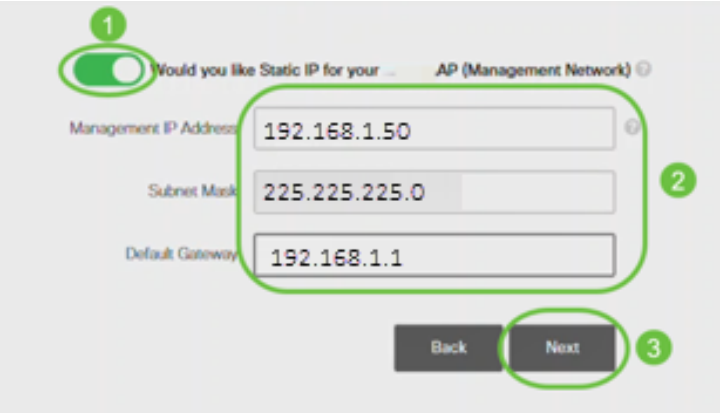
メッシュネットワークを作成する場合にのみ、メッシュを有効にする必要があります。デフォルトでは、無効になっています。

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。



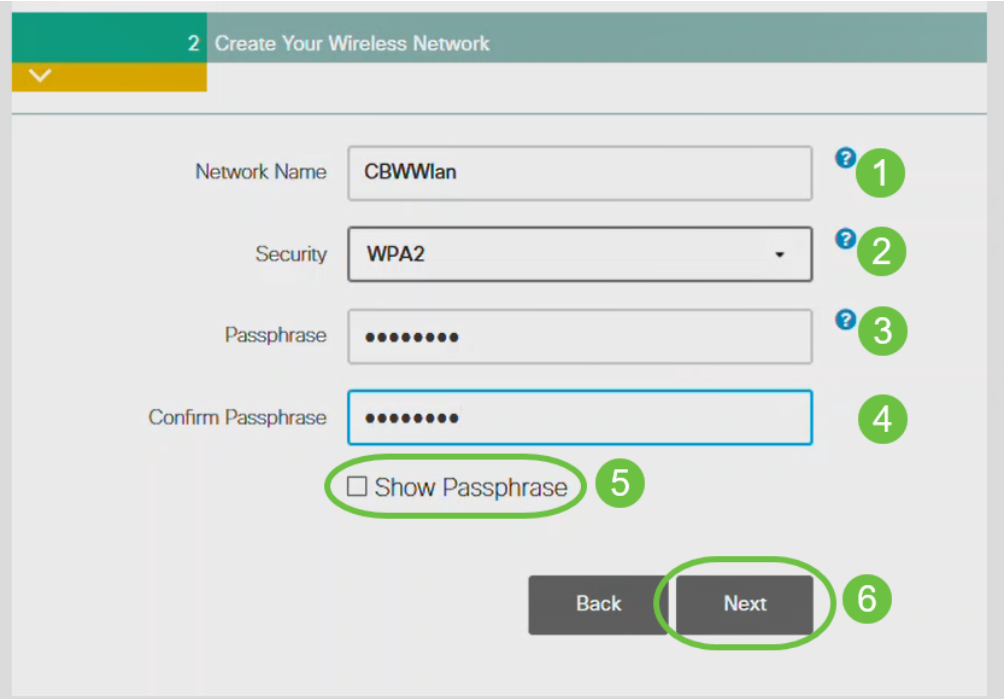
デフォルトでは、このオプションは無効になっています。

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。

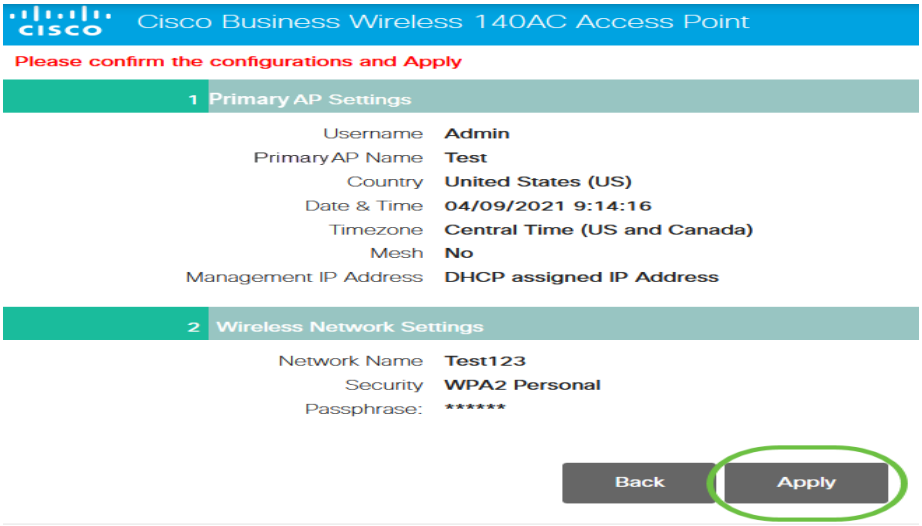
[next] をクリックします。



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。

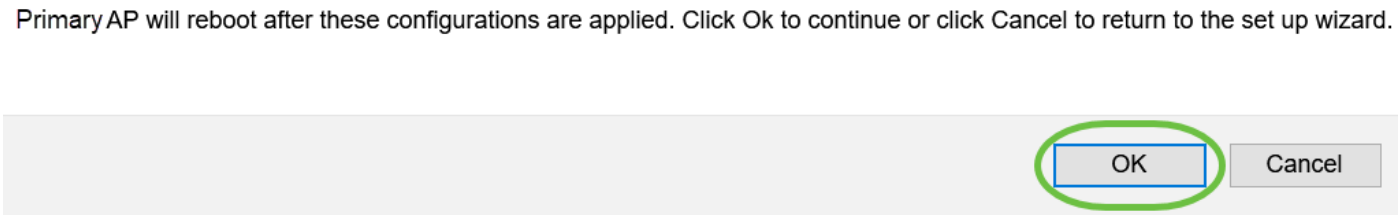
手順 9

設定を確認し、[適用]をクリックします。

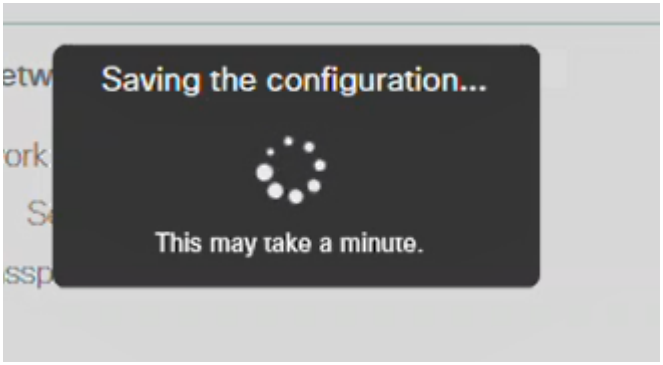


手順 10

[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。

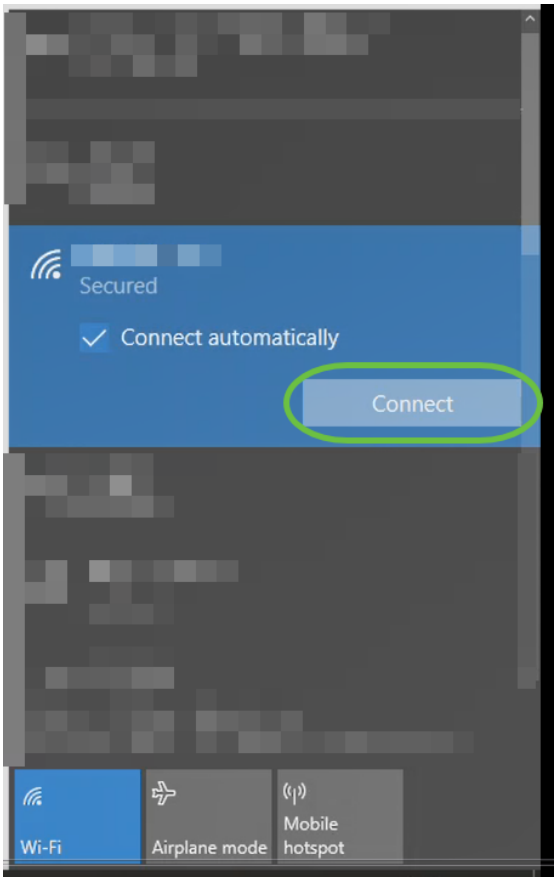


リブート中、アクセスポイントのLEDは複数のカラーパターンを通過します。LEDがグリーンに点滅している場合は、次の手順に進みます。LEDが赤い点滅パターンを超えない場合は、ネットワークにDHCPサーバがないことを示します。APがDHCPサーバを備えたスイッチまたはルータに接続されていることを確認します。

手順 11

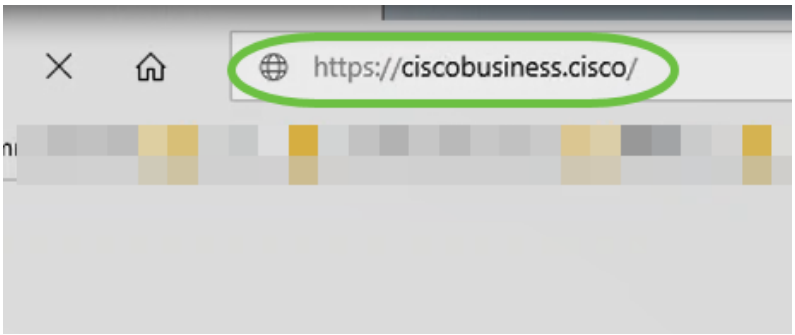
PCのワイヤレスオプションに移動し、設定したネットワークを選択します。[Connect] をクリックします。

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。



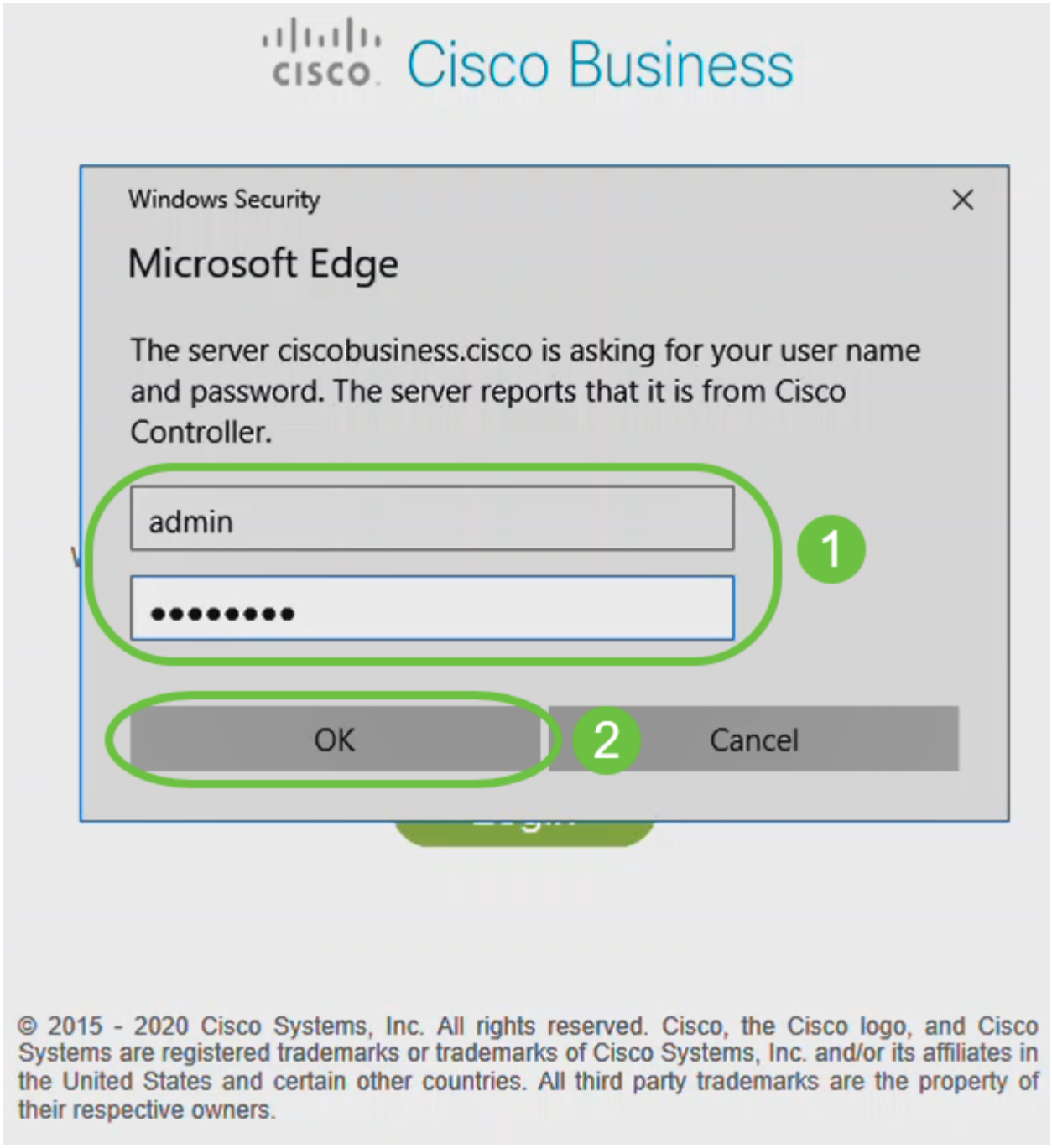
この手順では、httpではなく *https*を入力する ことを確認してください。

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

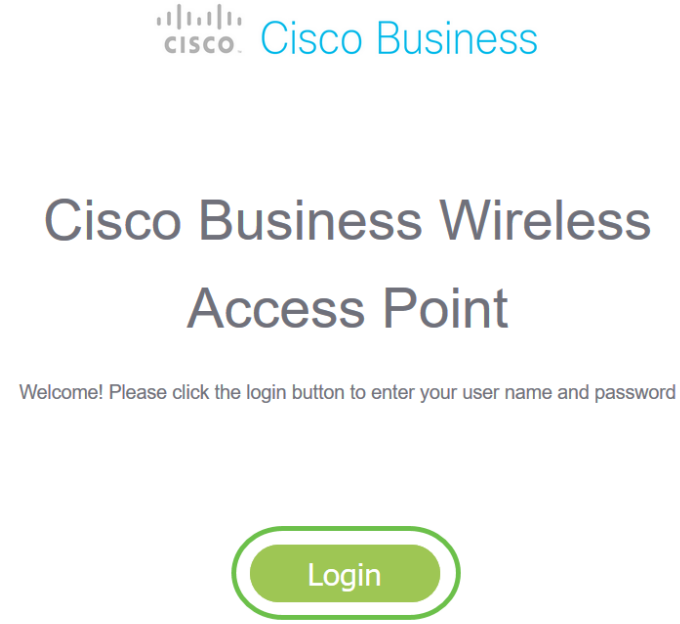
2つのメッシュエクステンダを、選択した位置の壁に差し込みます。各メッシュエクステンダのMACアドレスを書き留めます。

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。

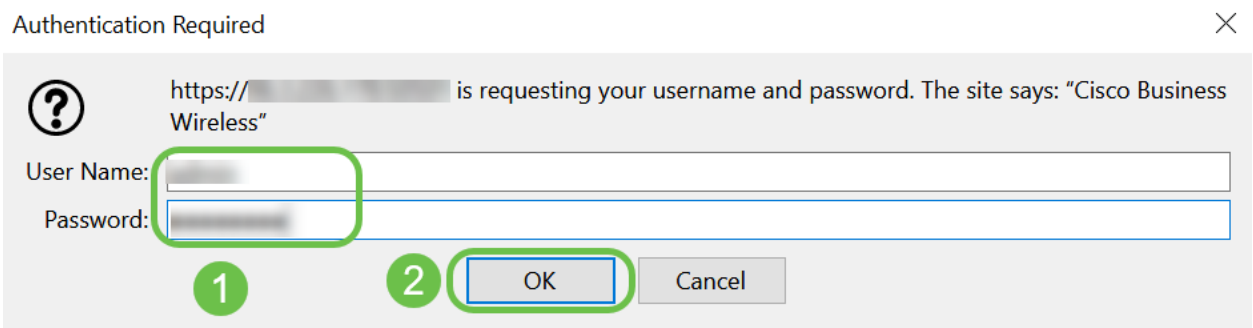
手順 3

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。



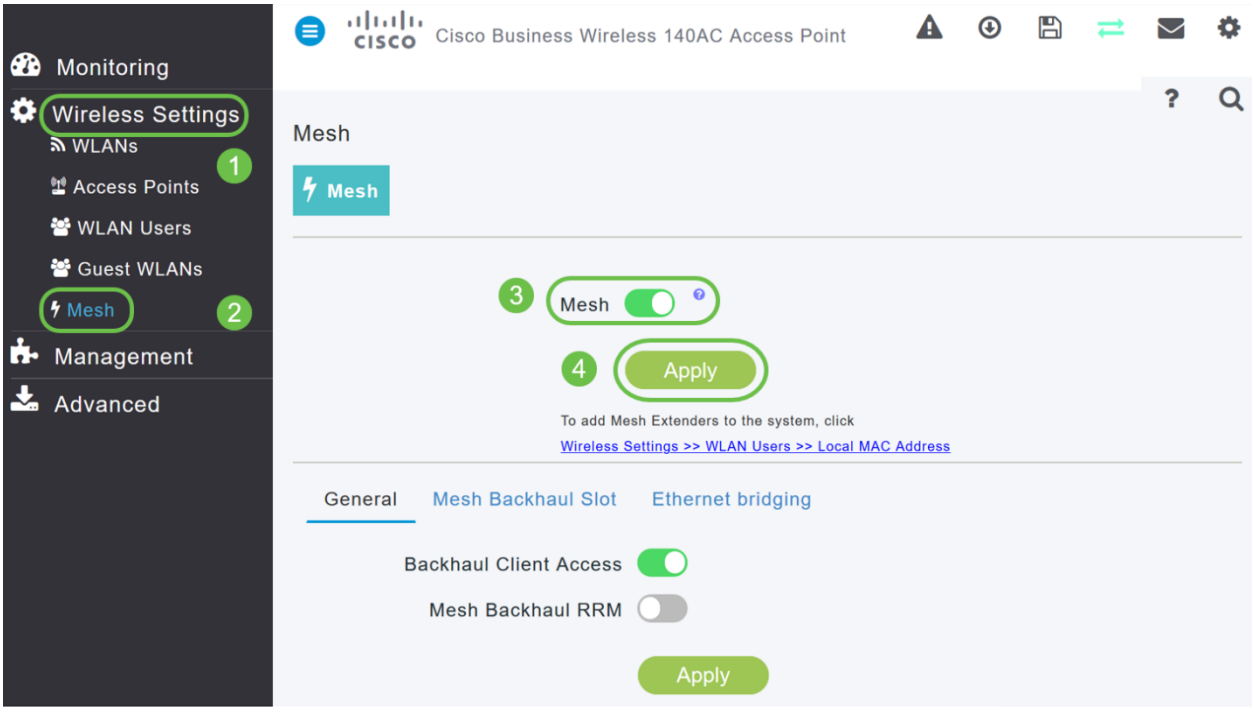
手順 4

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。

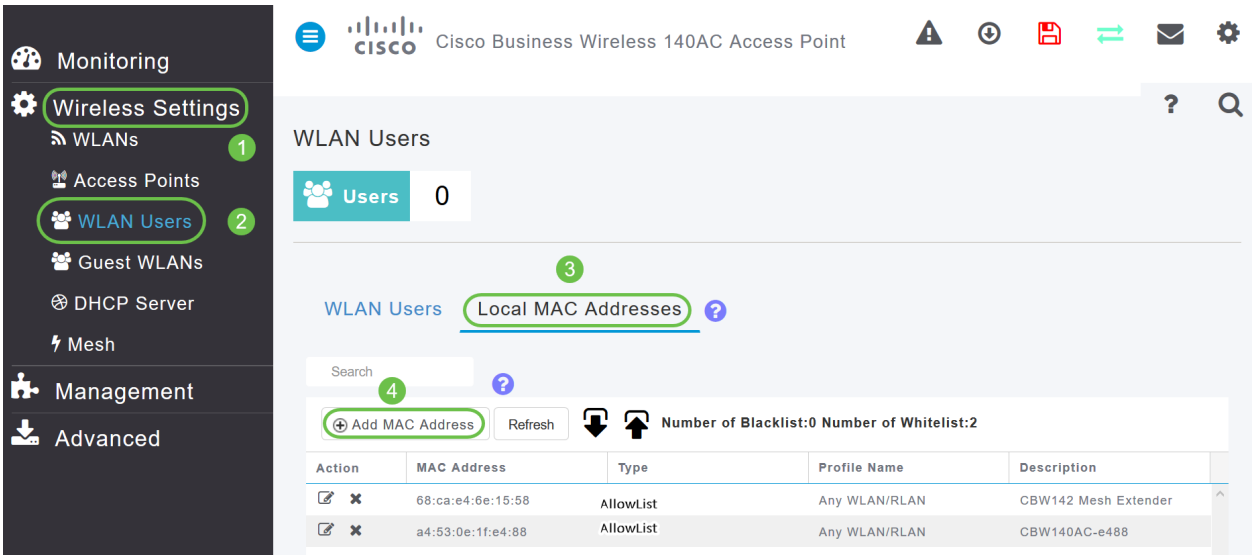


手順 6

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。

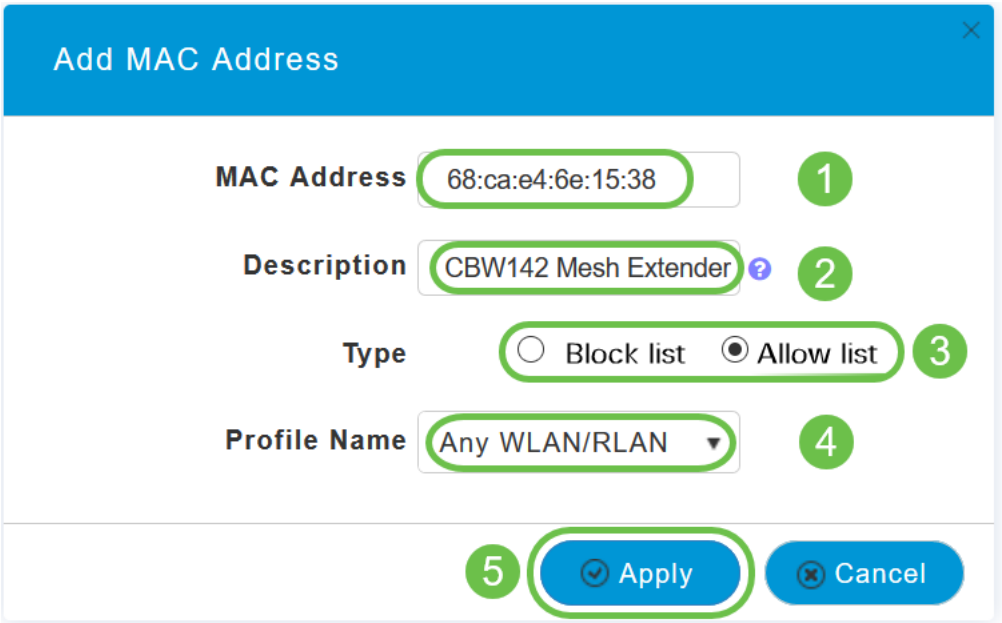
ステップ7

[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。

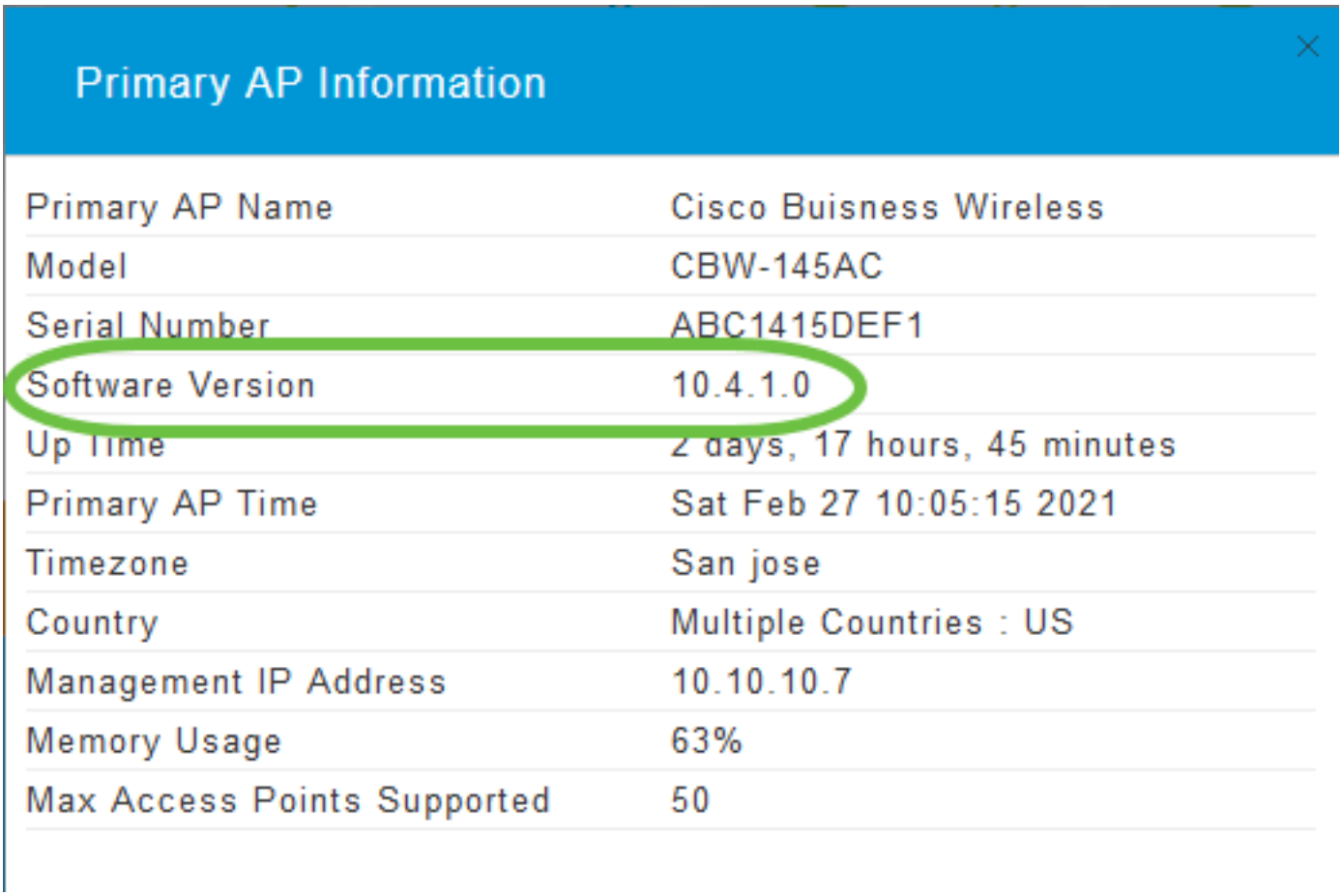
Web UIを使用したソフトウェアの確認と更新

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。

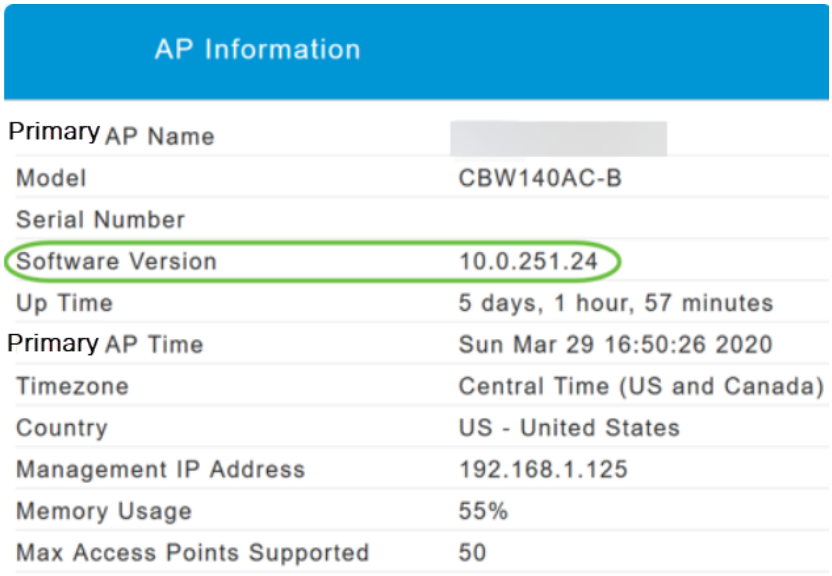
手順 1

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。

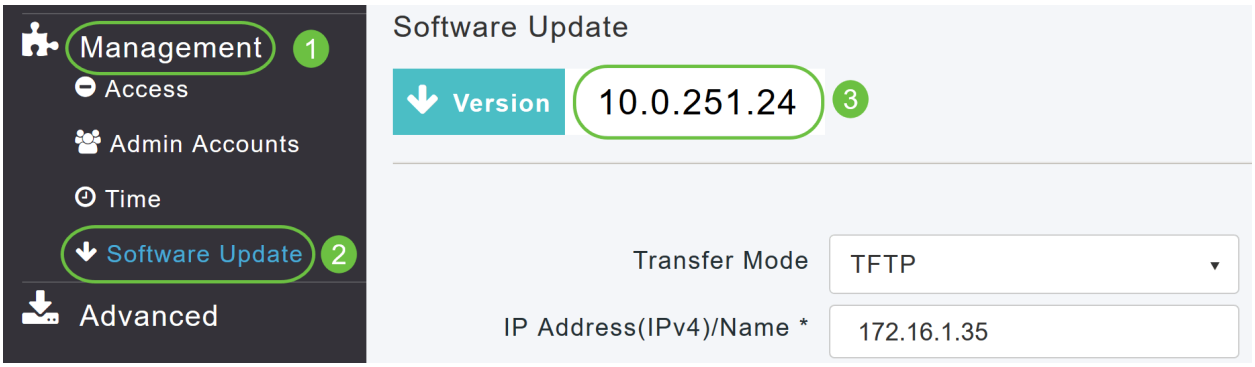


ソフトウェアの最新バージョンを実行している場合は、「WLANの作成」セクションに移動できます。

手順 3

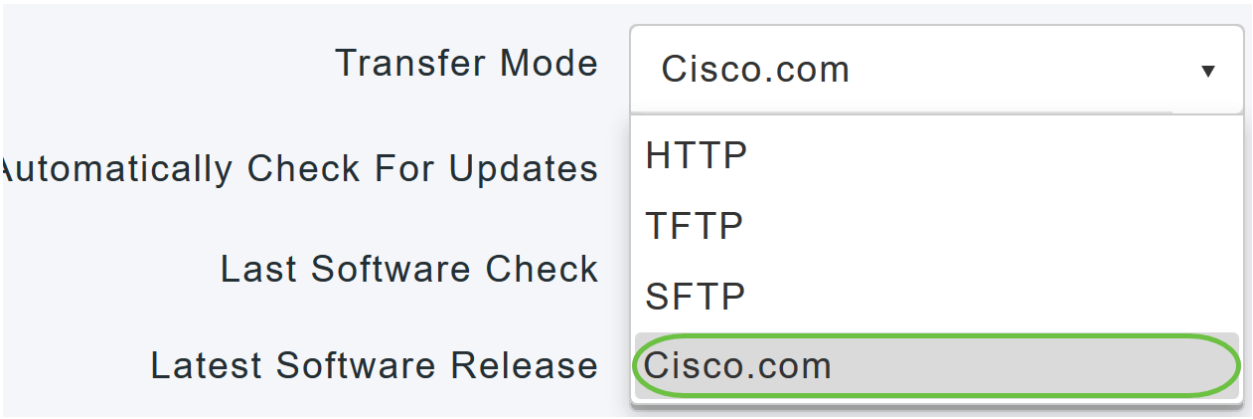
メニューから**[Management] > [Software Update]**を選択します。

[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。



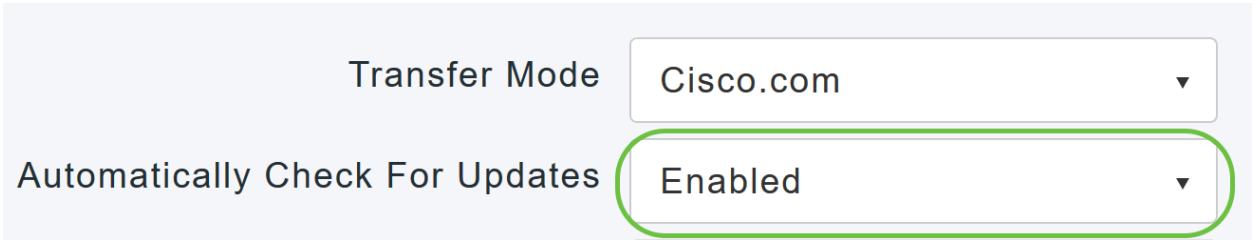
CBW APソフトウェアを更新できます。プライマリAPの現在の設定は削除されません。

[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。**



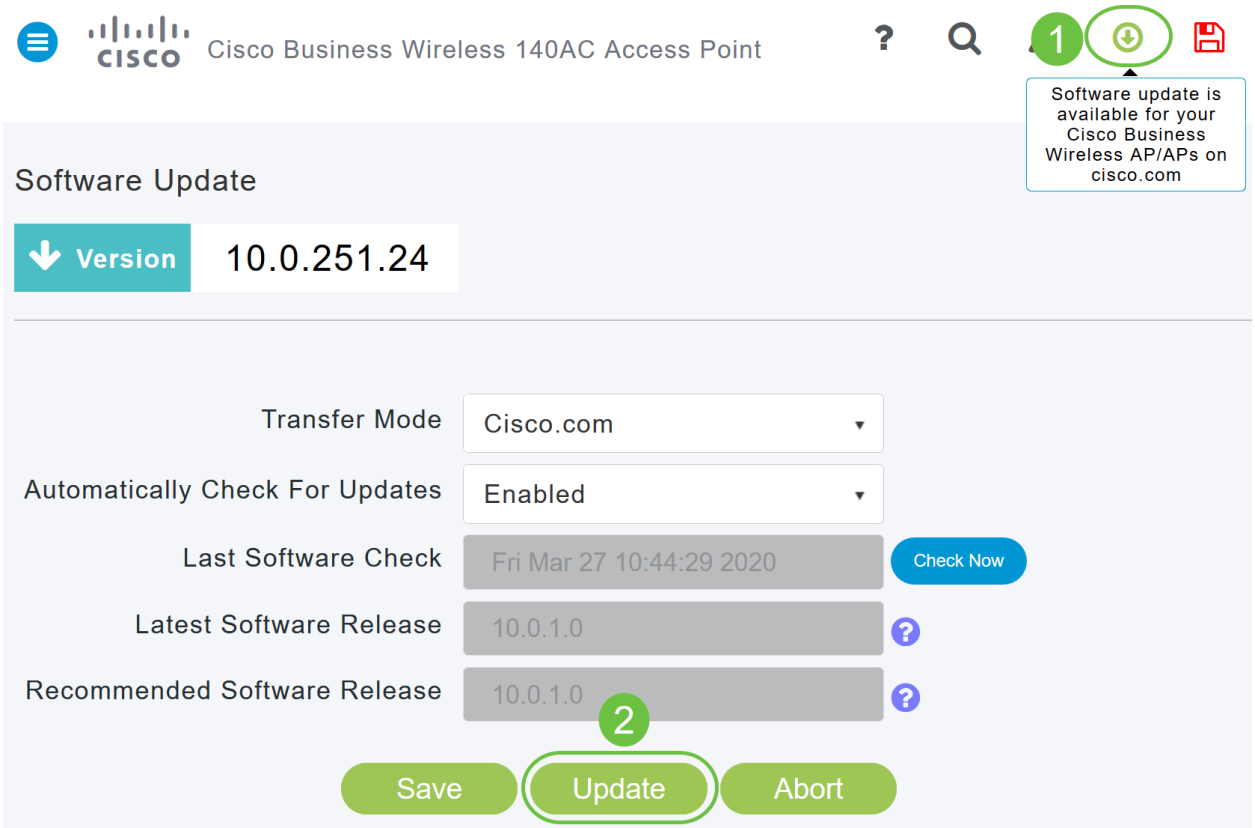
手順 4

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。



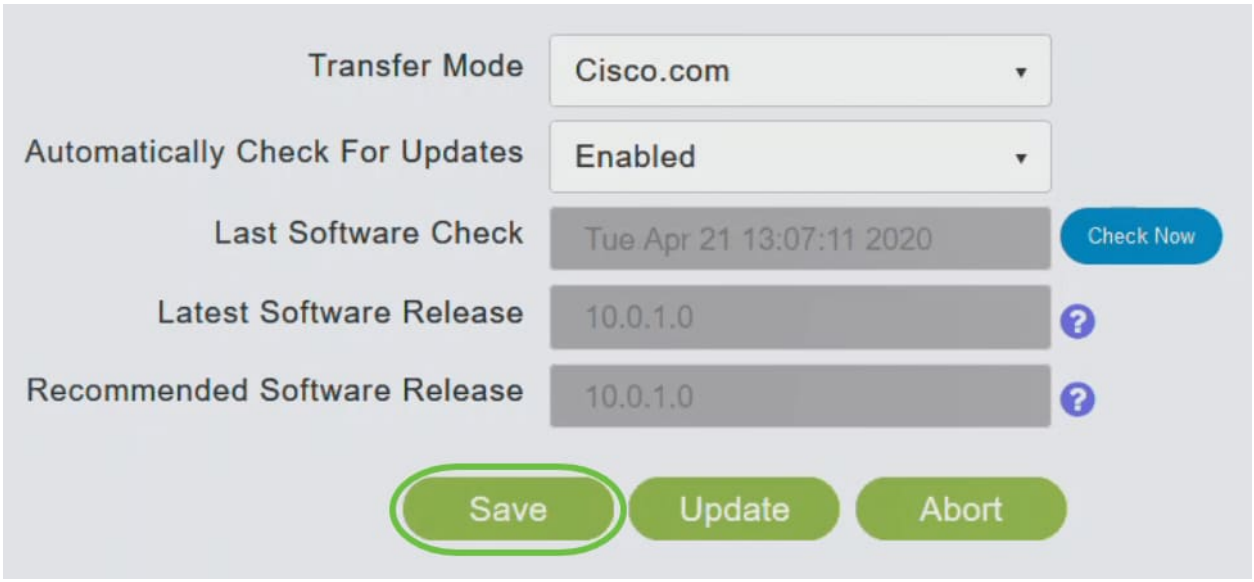
ソフトウェアチェックが完了し、Cisco.comで最新または推奨のソフトウェアアップデートが利用可能な場合は、次の手順を実行します。

- 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。

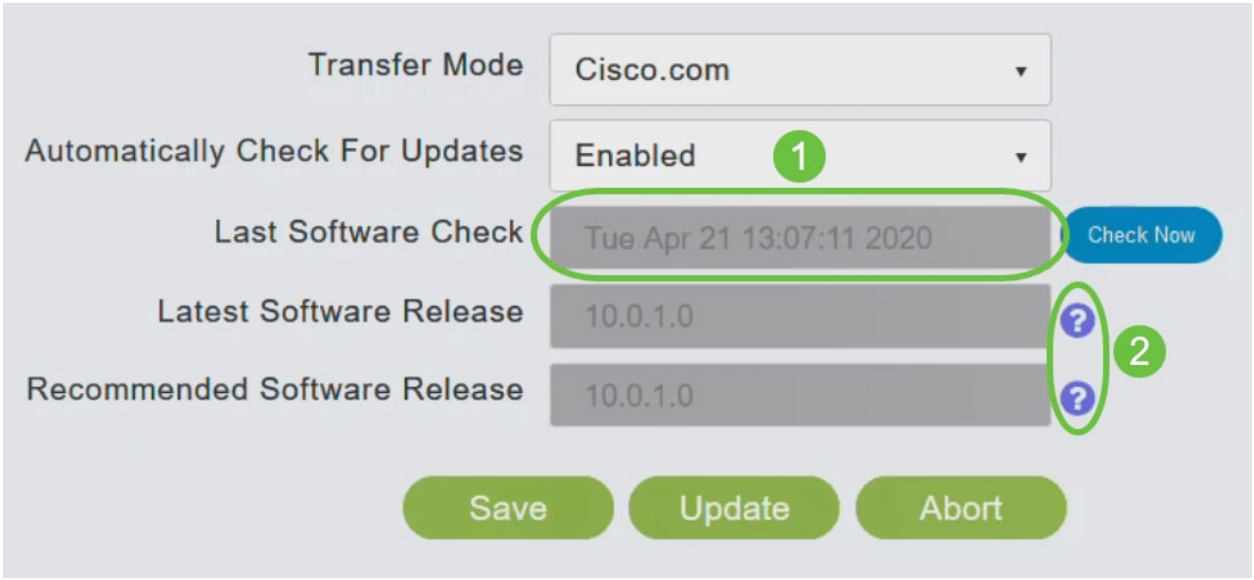


手順 5

[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。

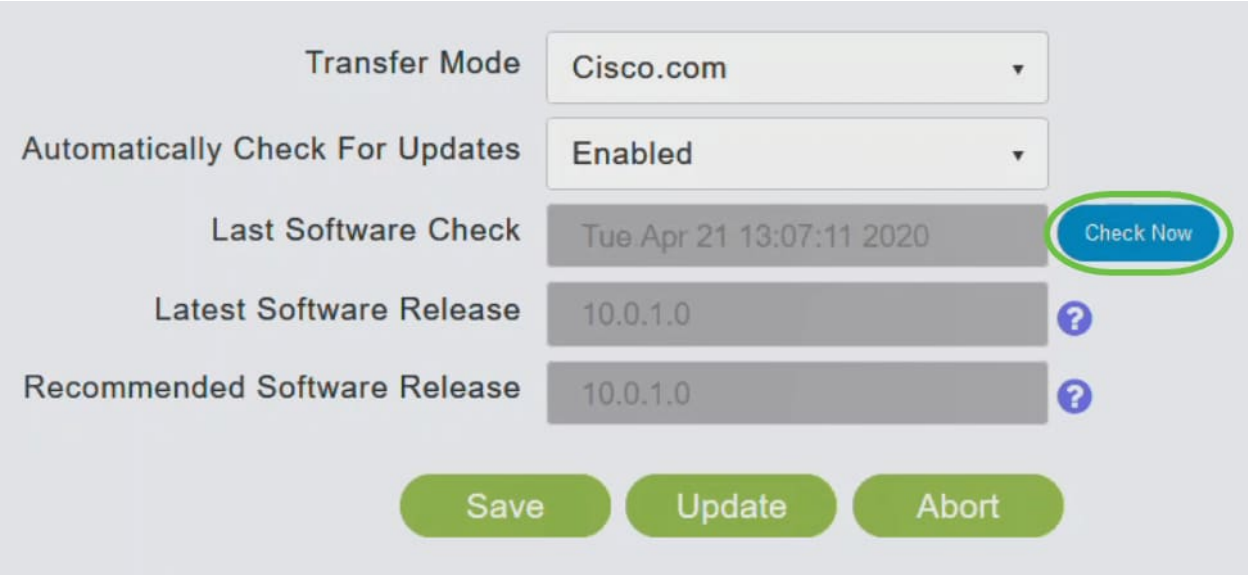


[最後のソフトウェアチェック]フィールドには、最後の自動または手動ソフトウェアチェックのタイムスタンプが表示されます。表示されたリリースの注記は、横にある疑問符アイコンをクリックすると表示できます。



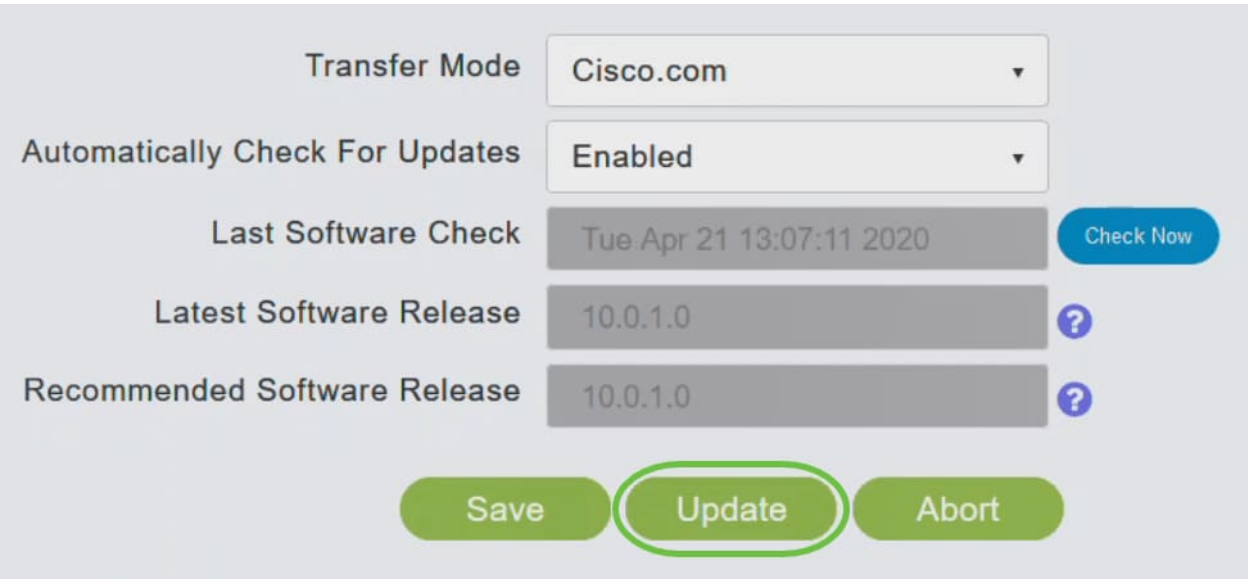
手順 6

[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

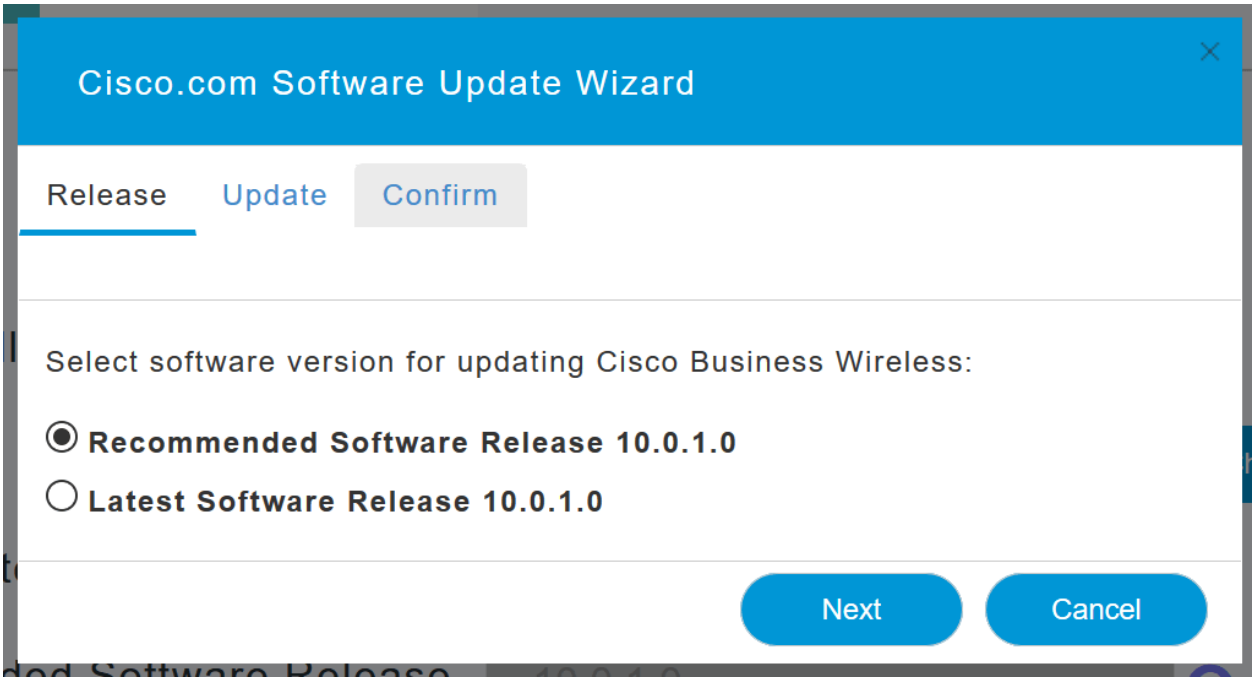
ソフトウェアの更新を続行するには、[更新]をクリックします。



[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。

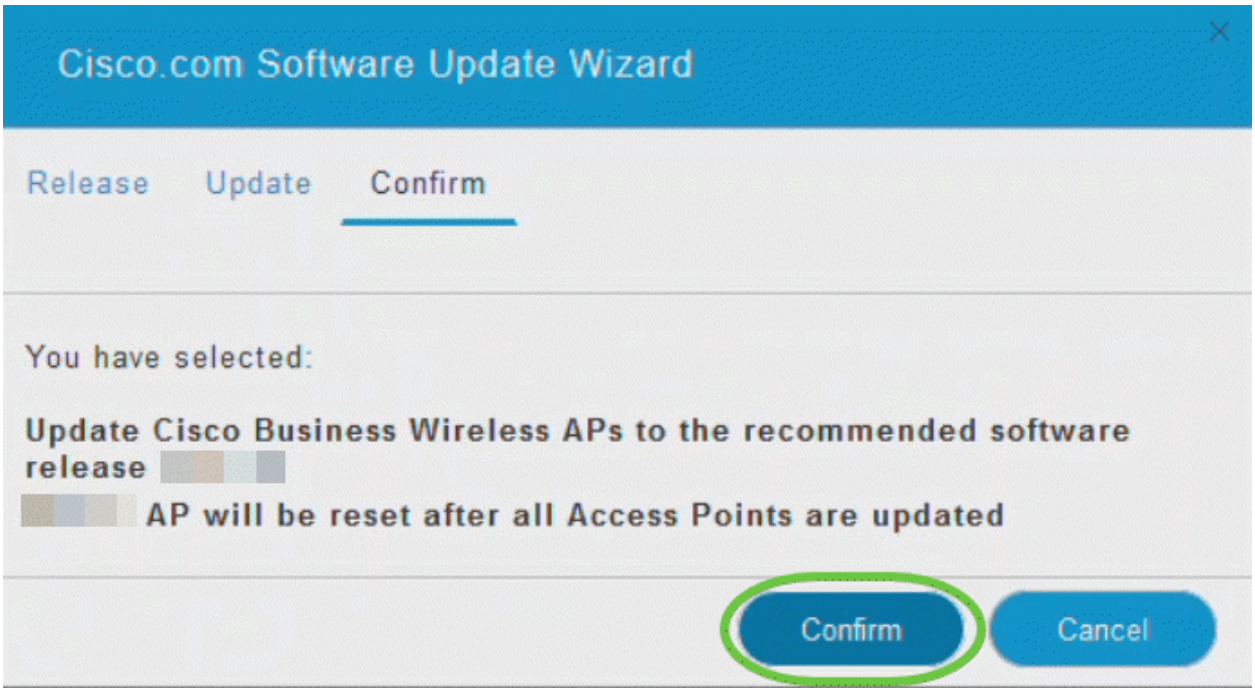
- [リリース(Release)]タブ：推奨ソフトウェアリリースまたは最新ソフトウェアリリースのどちらにアップデートするかを指定します。
- [Update]タブ：APをいつリセットするかを指定します。すぐに実行するか、後でスケジュールするかを選択できます。イメージのプレダウンロードが完了した後にプライマリAPが自動的にリブートするように設定するには、[Auto Restart]チェックボックスをオンにします。
- [Confirm]タブ：選択内容を確認します。

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。

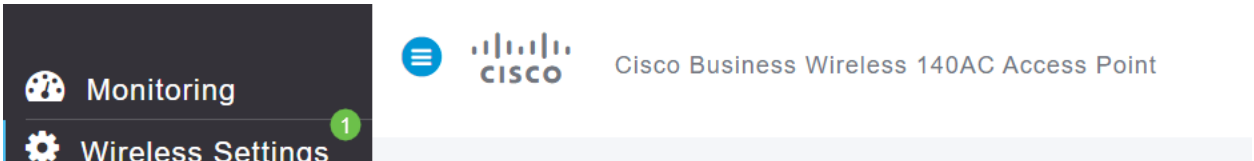


Web UIでのWLANの作成

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

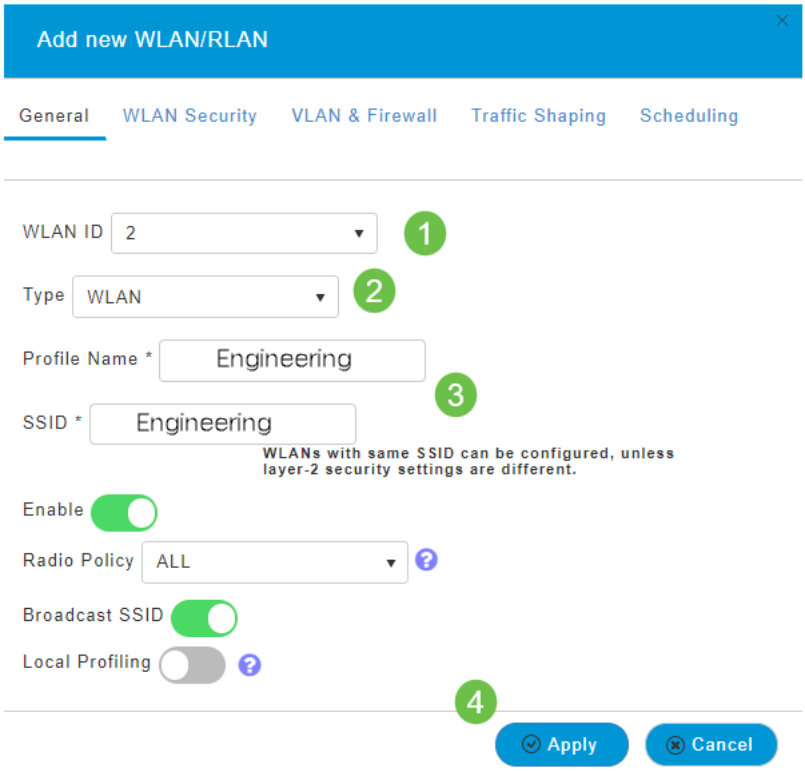
[全般]タブで、次の情報を入力します。

- [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。

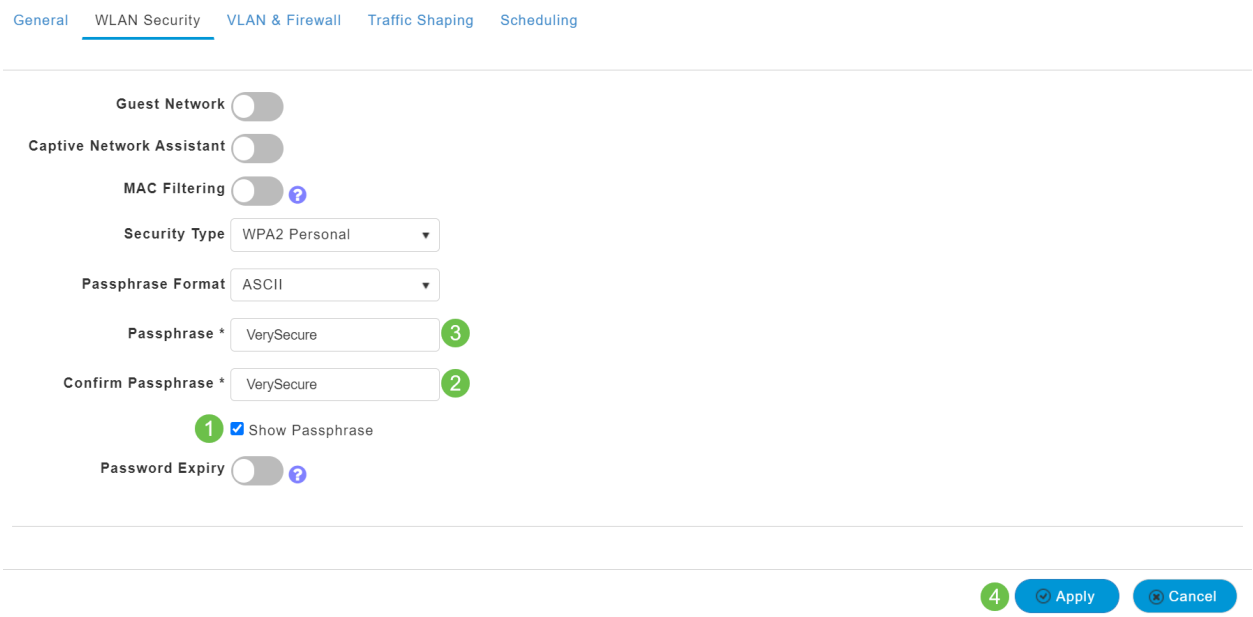
WPA2 Personalは、PSK認証を使用してネットワークを保護するために使用される方法です。PSKは、プライマリAP、WLANセキュリティポリシー、およびクライアントの両方で個別に設定されます。WPA2 Personalは、ネットワーク上の認証サーバに依存しません。

- 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。

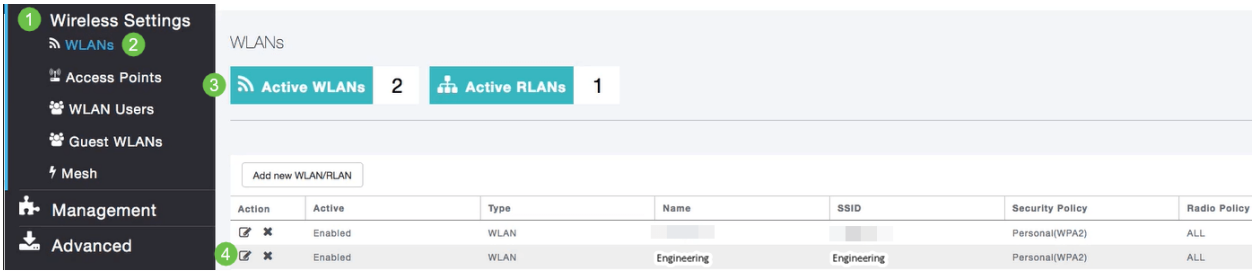


手順 4

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）

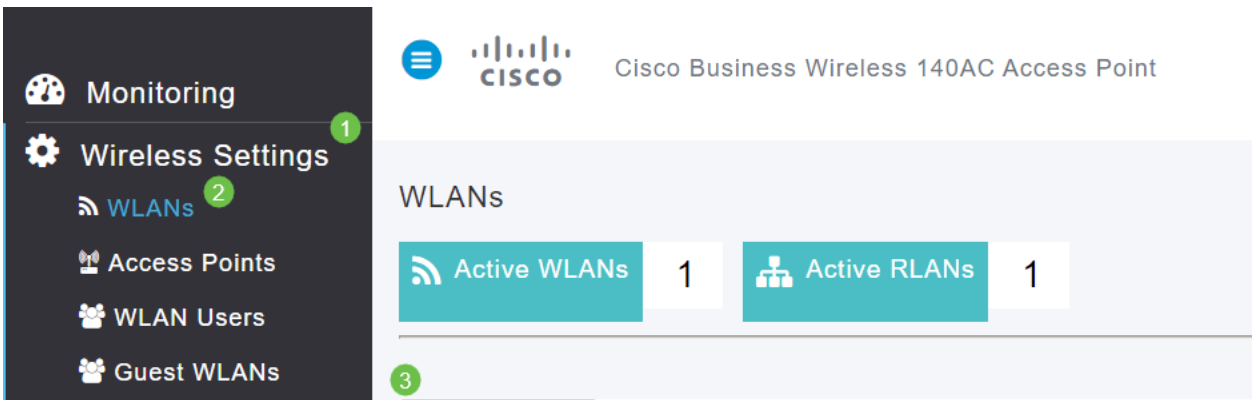
ゲストWLANは、Cisco Business Wirelessネットワークへのゲストアクセスを提供します。

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

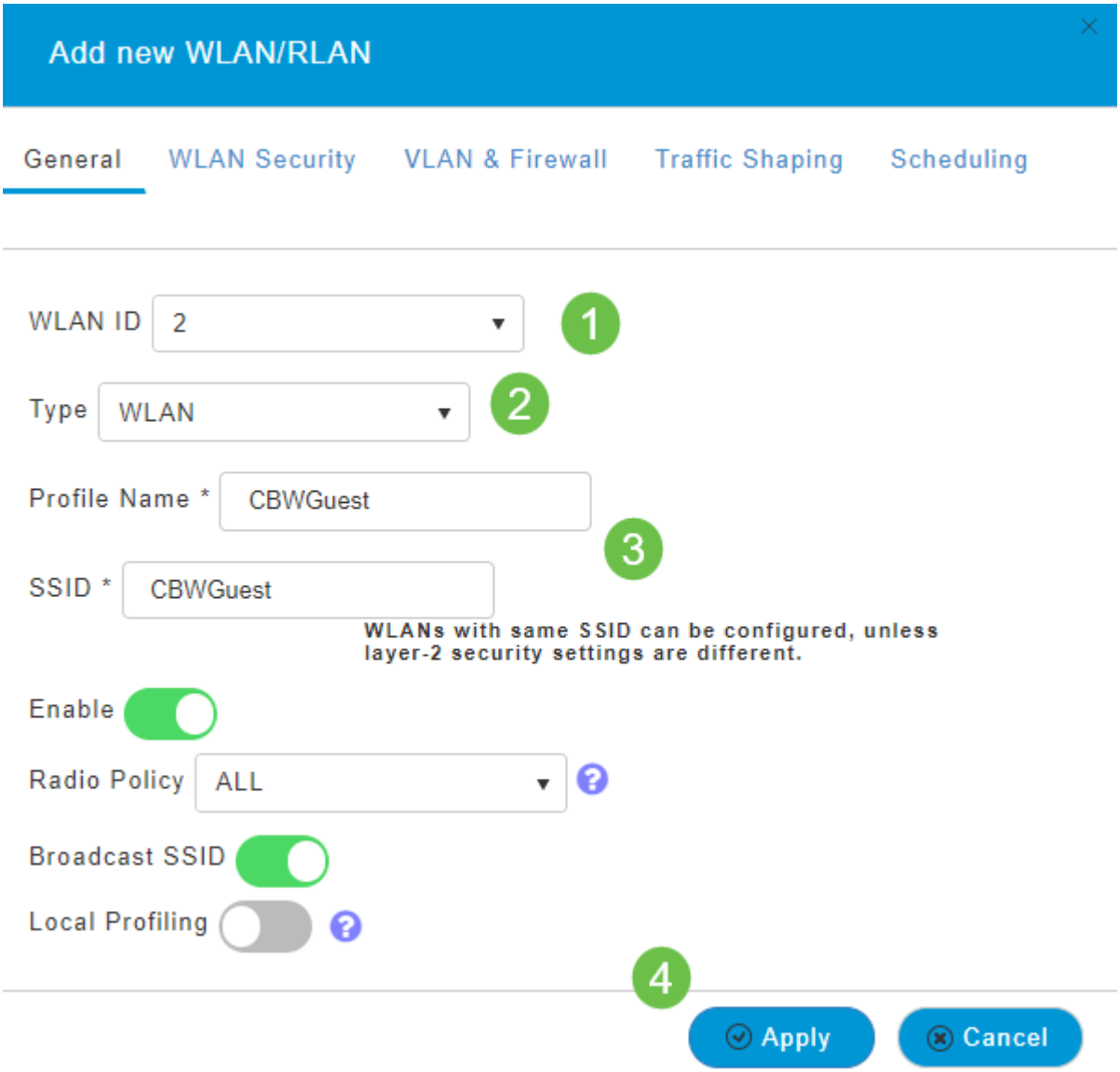
[全般]タブで、次の情報を入力します。

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。

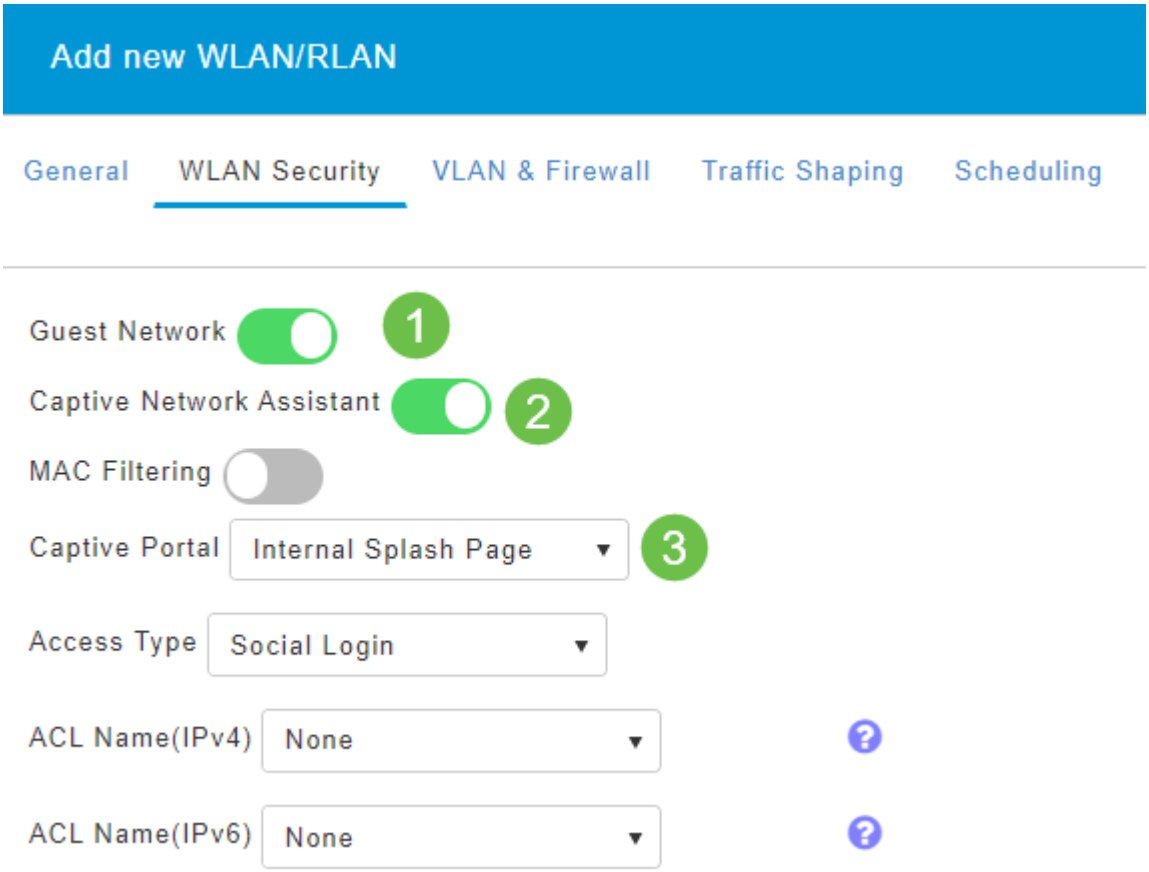


手順 4

[*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。

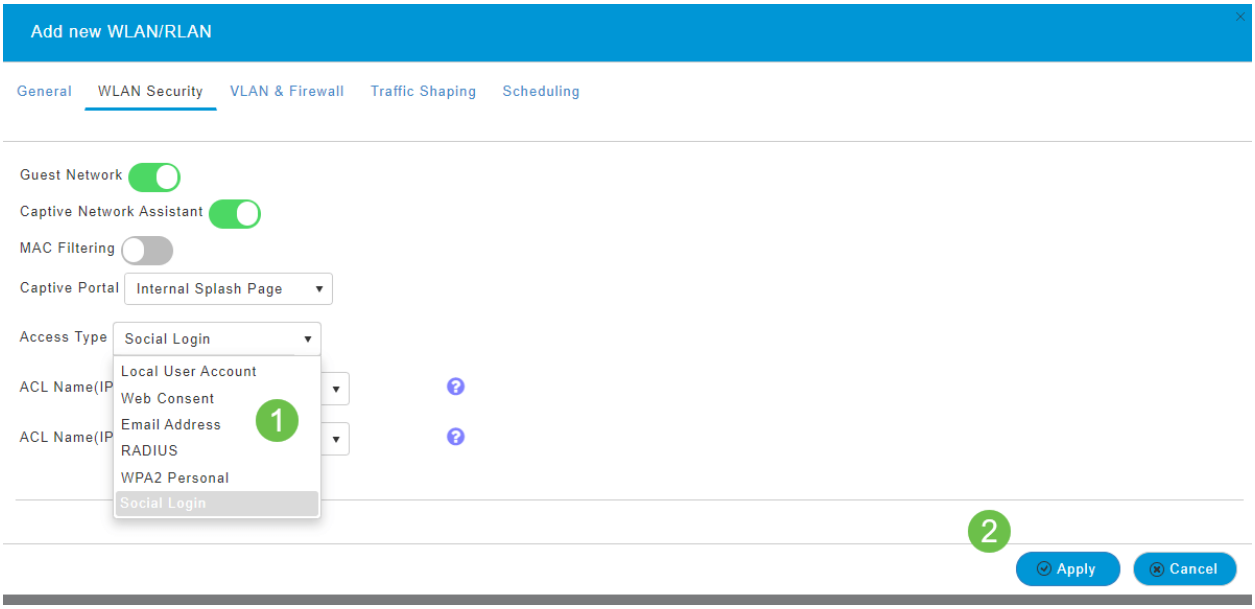
アクセスタイプのその他の*オプション*は*次*のとおりです。

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）

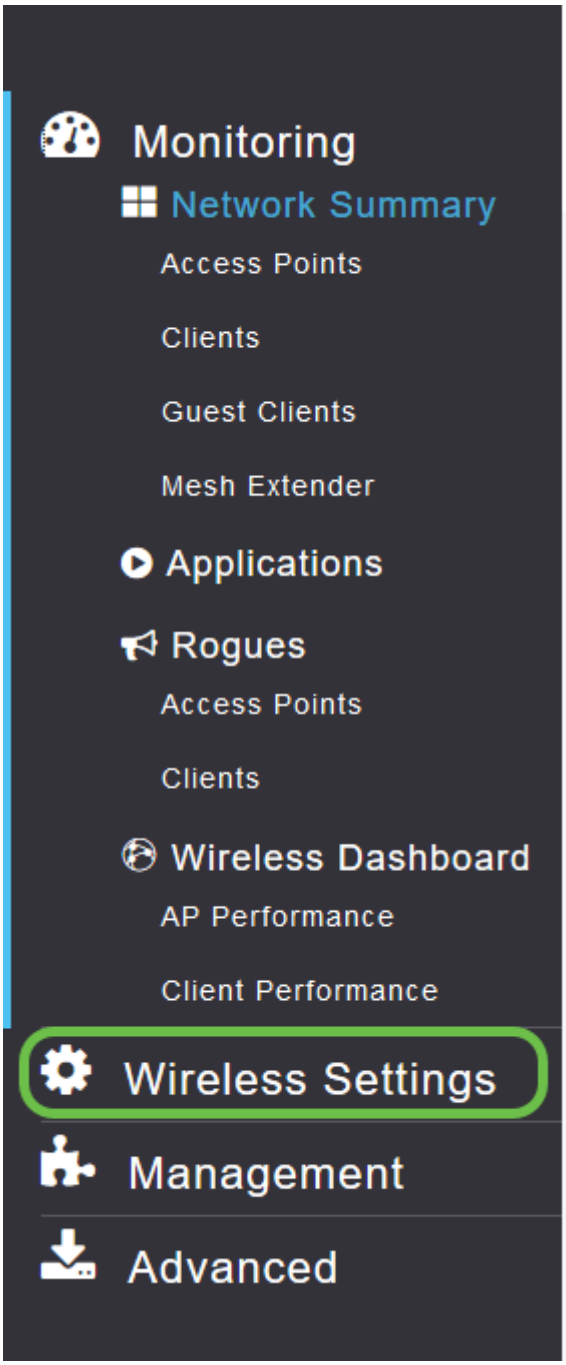
プロファイリングは、組織ポリシーを有効にする機能のサブセットです。トラフィックタイプを照合し、優先順位を付けることができます。ルールと同様に、トラフィックのランク付けやドロップの方法を決定します。Cisco Business Mesh Wirelessシステムには、クライアントとアプリケーションのプロファイリング機能があります。ユーザとしてネットワークにアクセスする行為は、まず多くの情報交換から始まります。その情報の中には、トラフィックの種類があります。ポリシーはトラフィックフローを中断し、フローチャートのようにパスを誘導します。その他のポリシー機能には、ゲストアクセス、アクセスコントロールリ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

手順 1

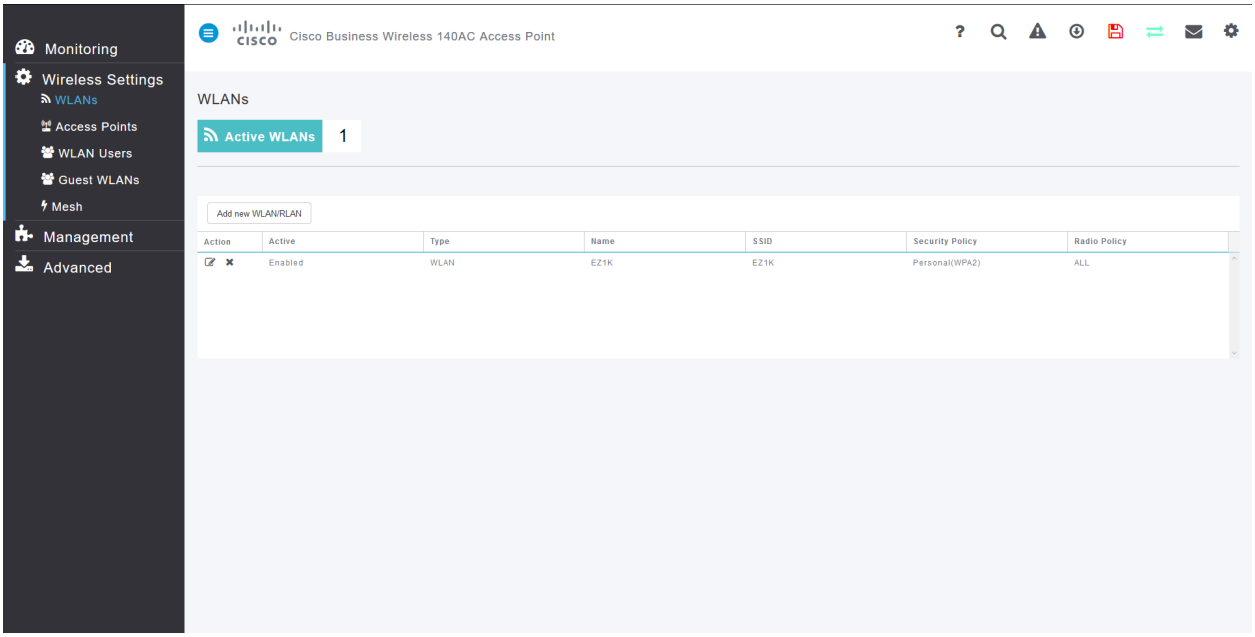
左側のメニューバーが表示されていない場合は、画面の左側にあるメニューに移動します。

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**。

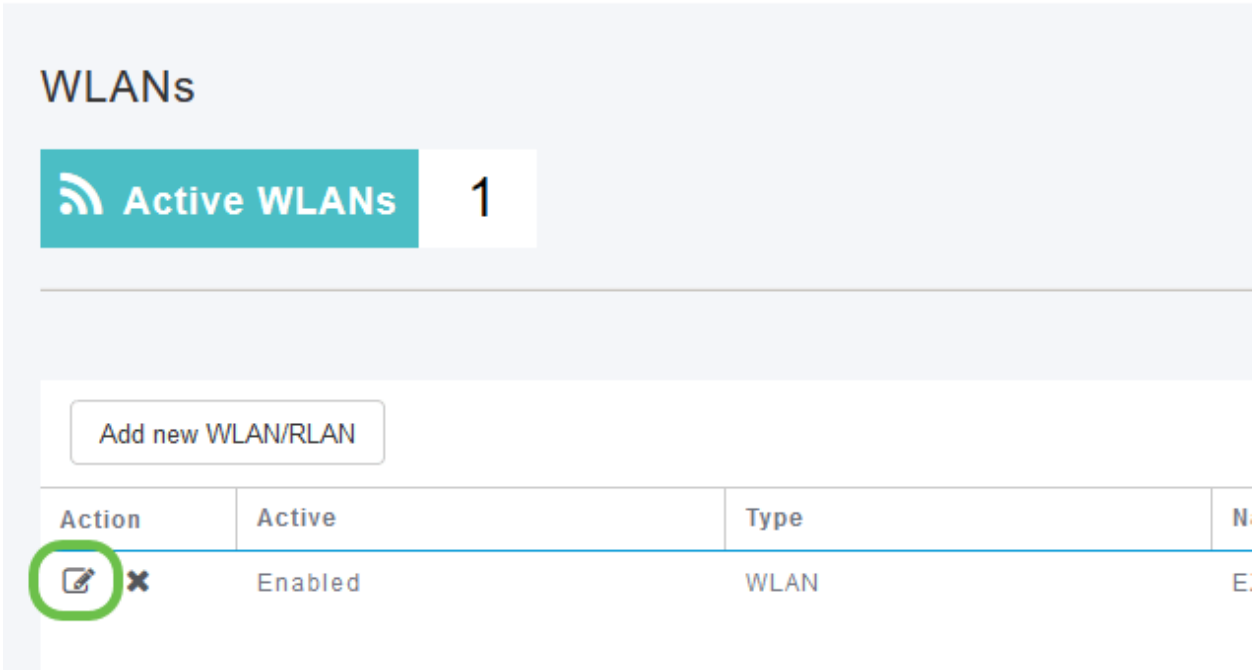


次の図は、[ワイヤレス設定(Wireless Settings)]リンクをクリックしたときに表示されるものと似ています。

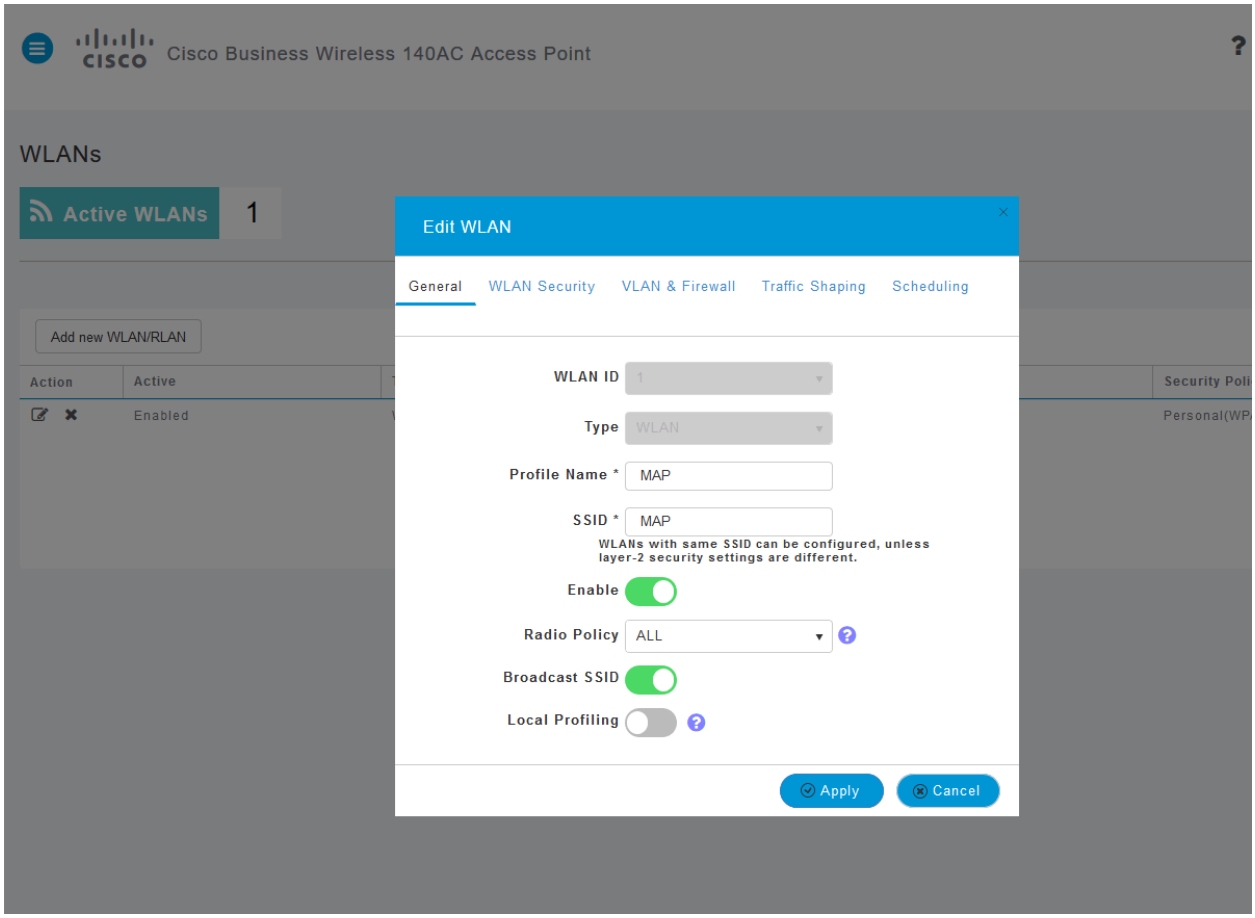


手順 3

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。

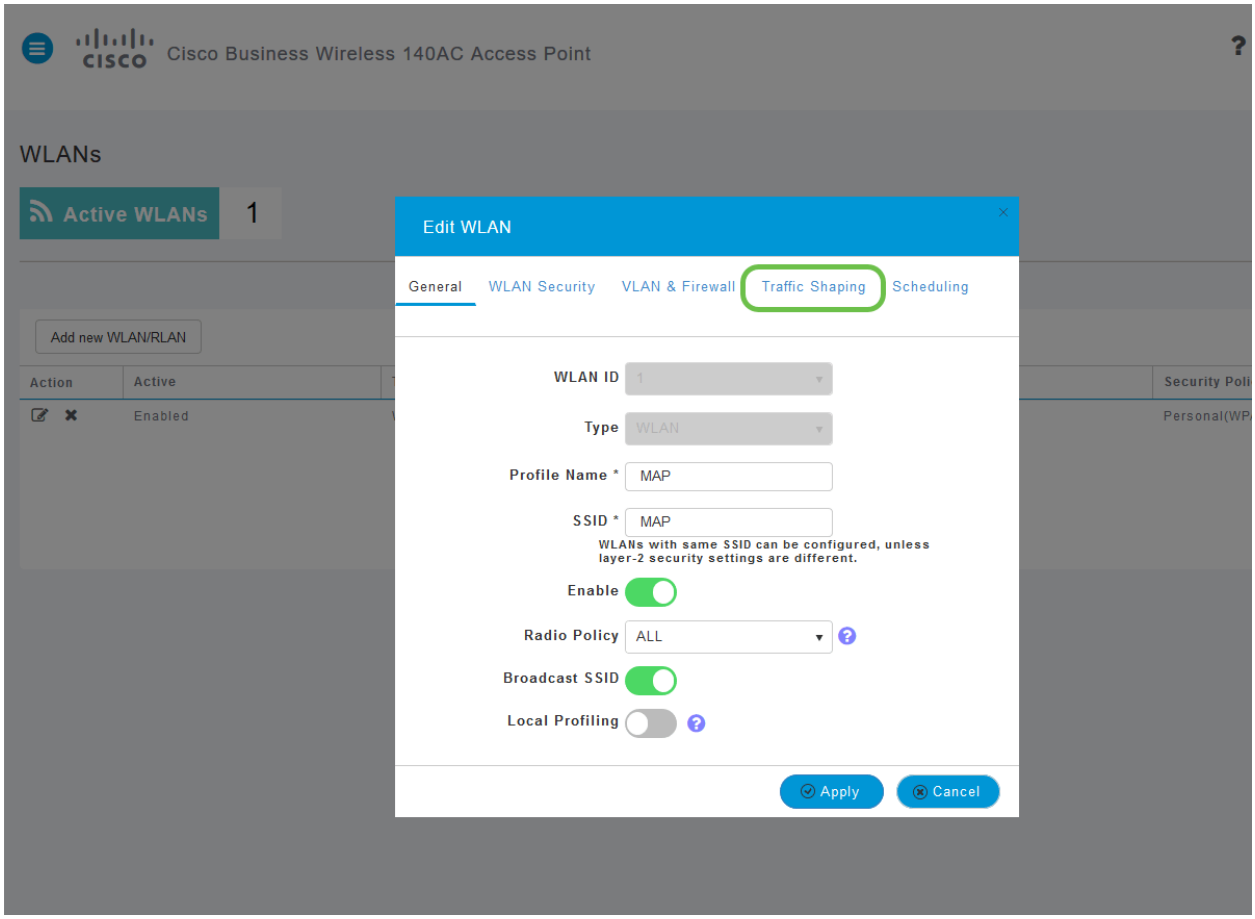


WLANを最近追加したので、[*Edit WLAN*]ページが次のように表示されます。

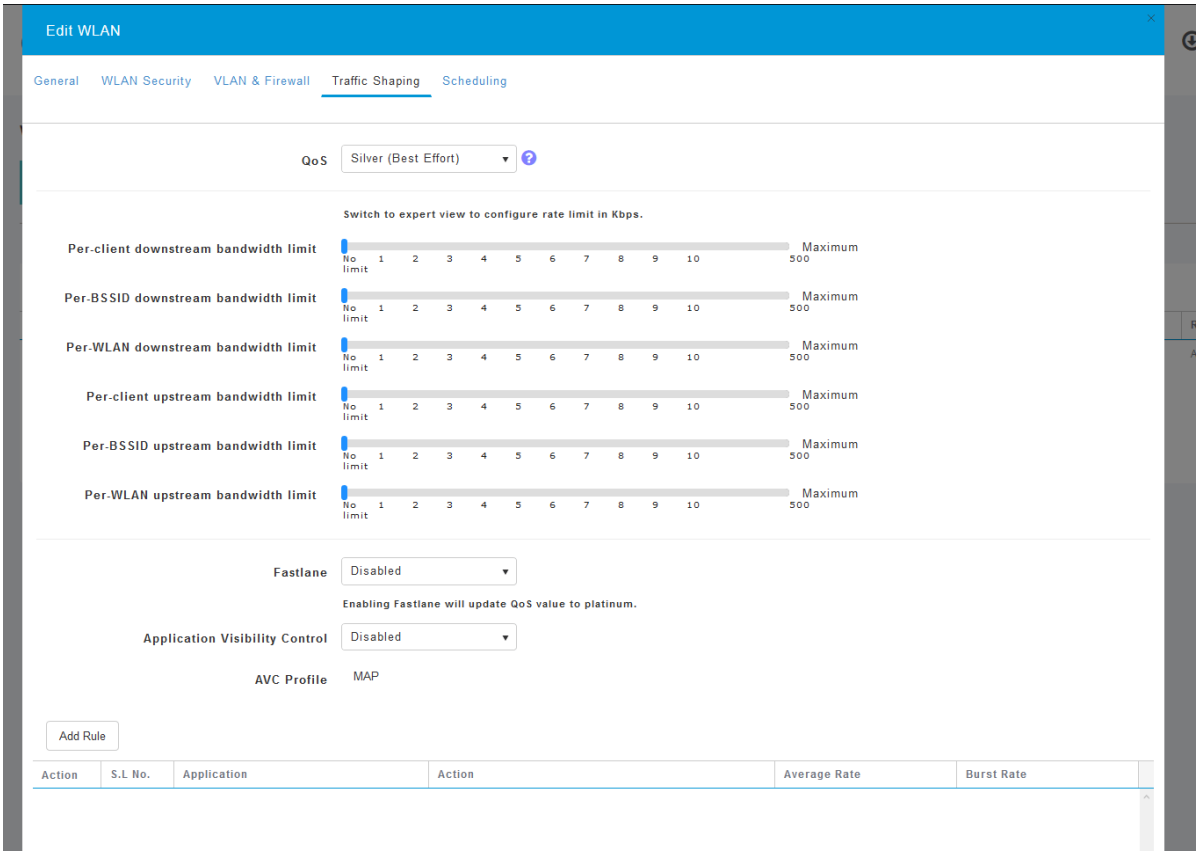


手順 4

[Traffic Shaping]タブをクリックして移動します。

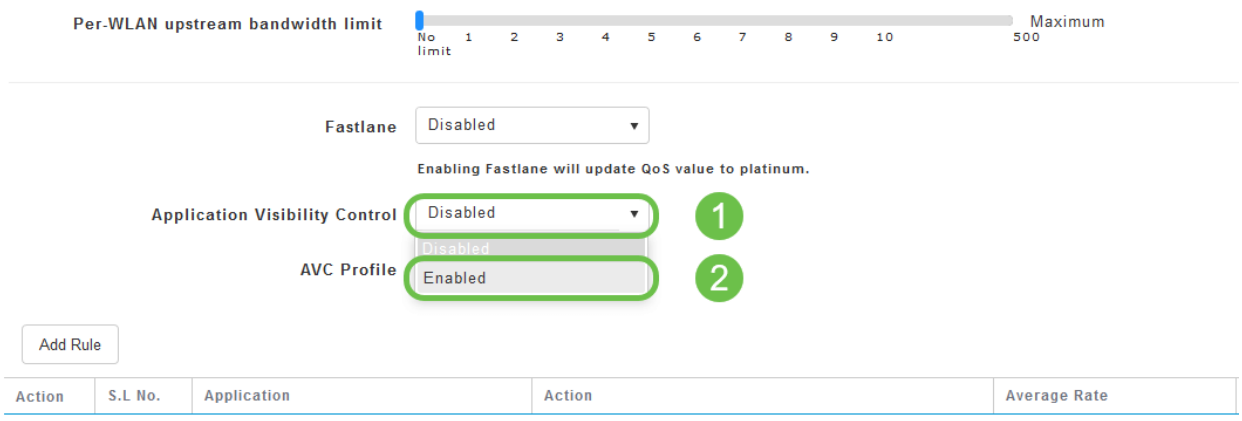


画面は次のように表示されます。



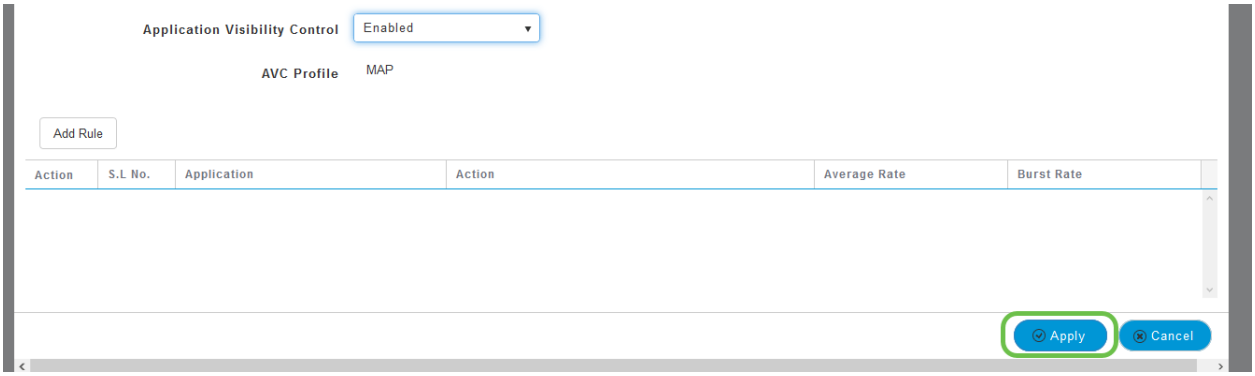
手順 5

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

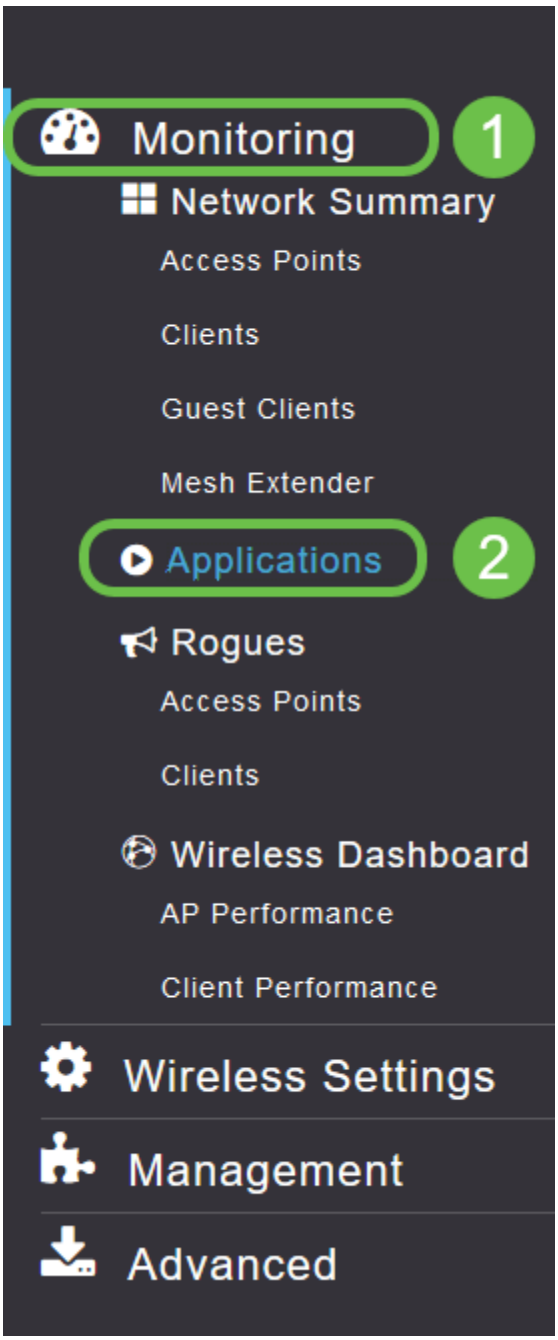
[適用]ボタンを**クリック**します。



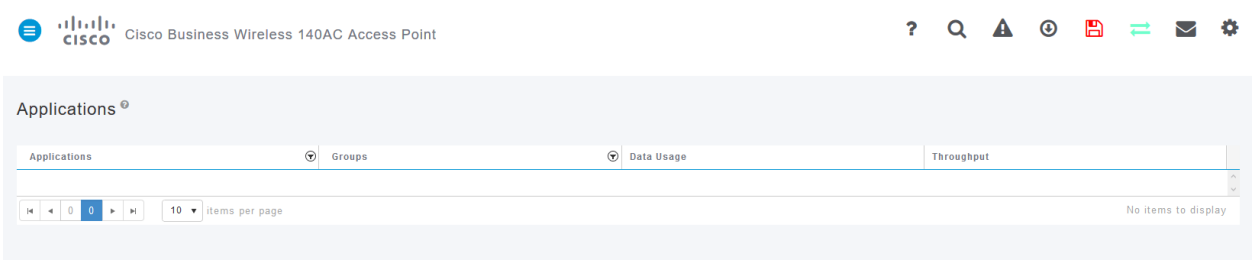
この設定を有効にする必要があります。有効にしない場合、機能は機能しません。

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

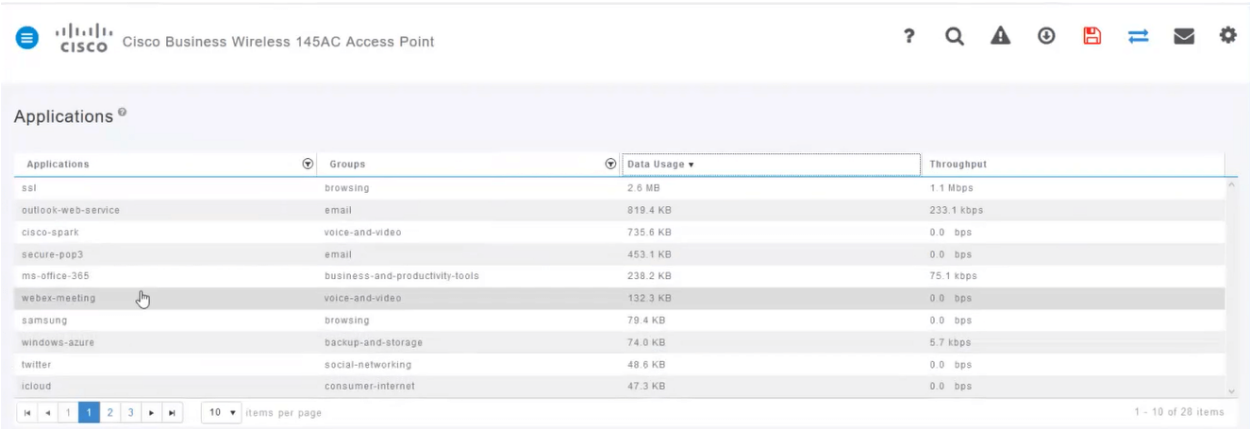
タブをクリックすると、最大から最小に並べ替えることができます。これにより、ネ

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

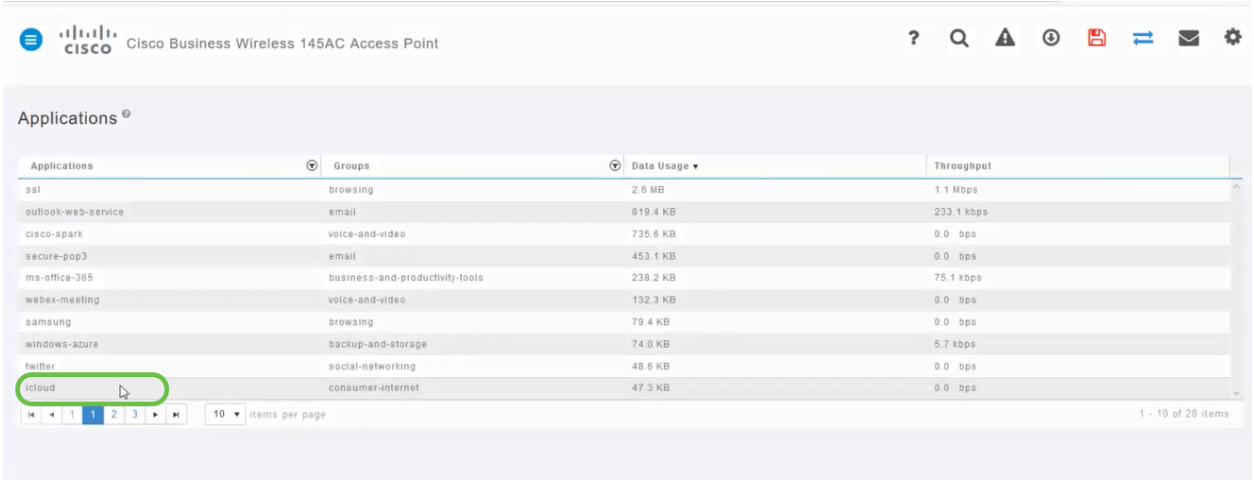
次に、ページを入力したときの表示例を示します。



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。

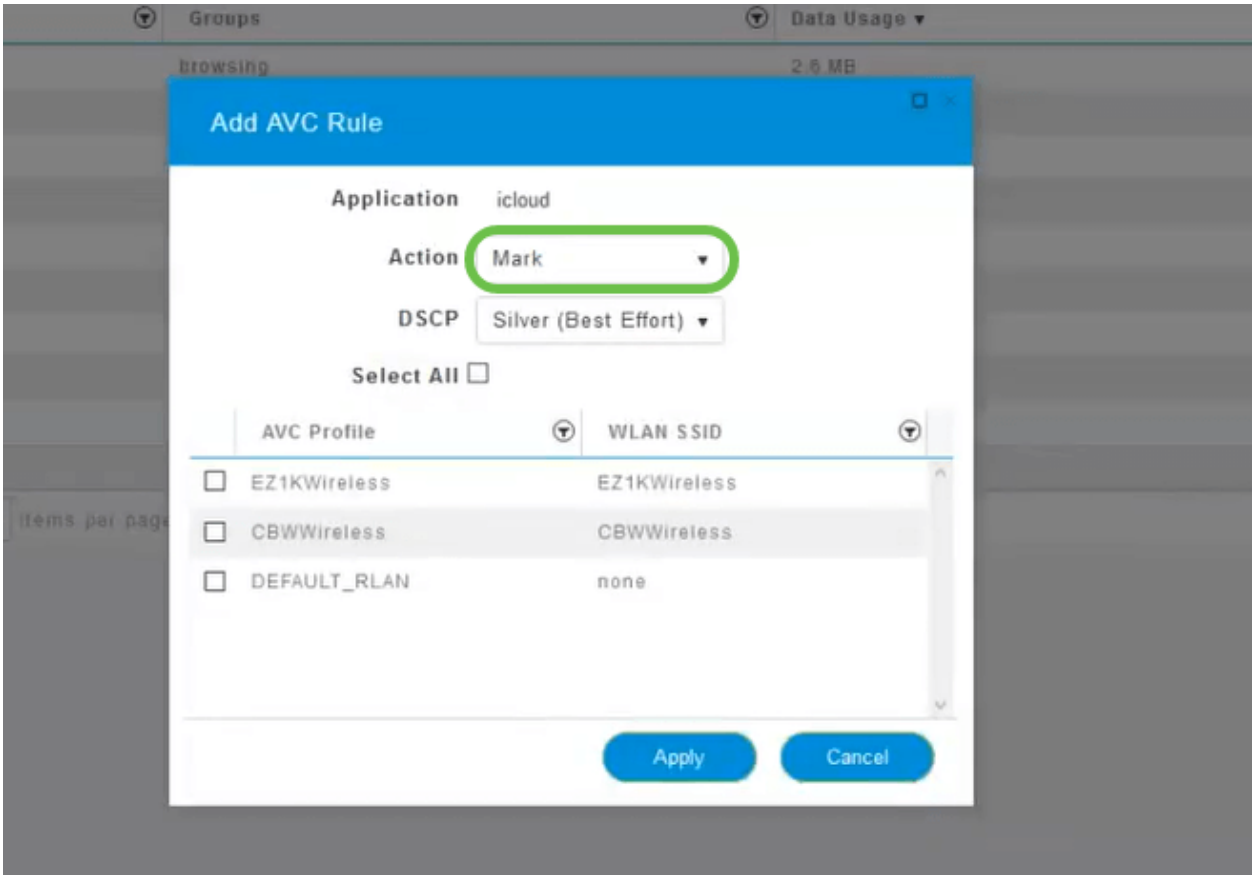
手順 8

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。



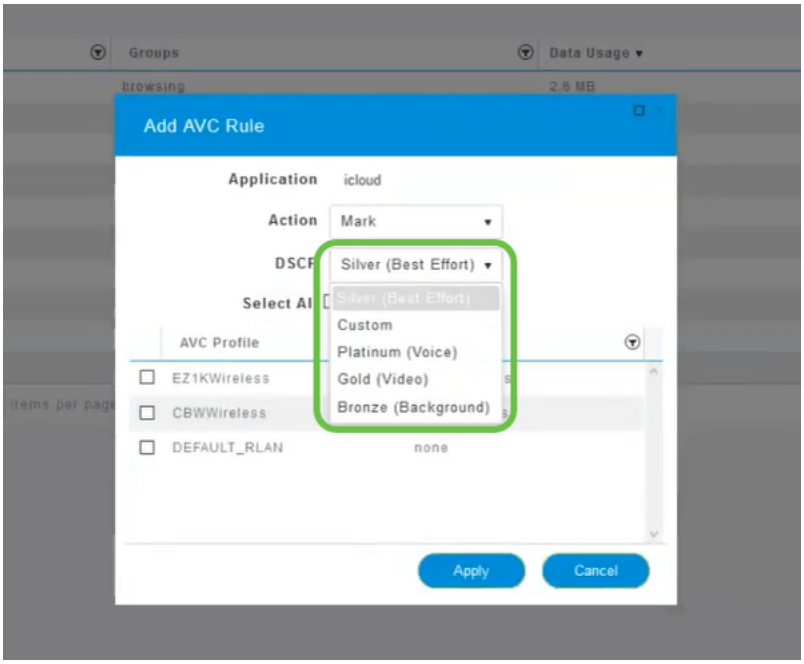
この例では、このオプションは*Mark*のままにしておきます。

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。



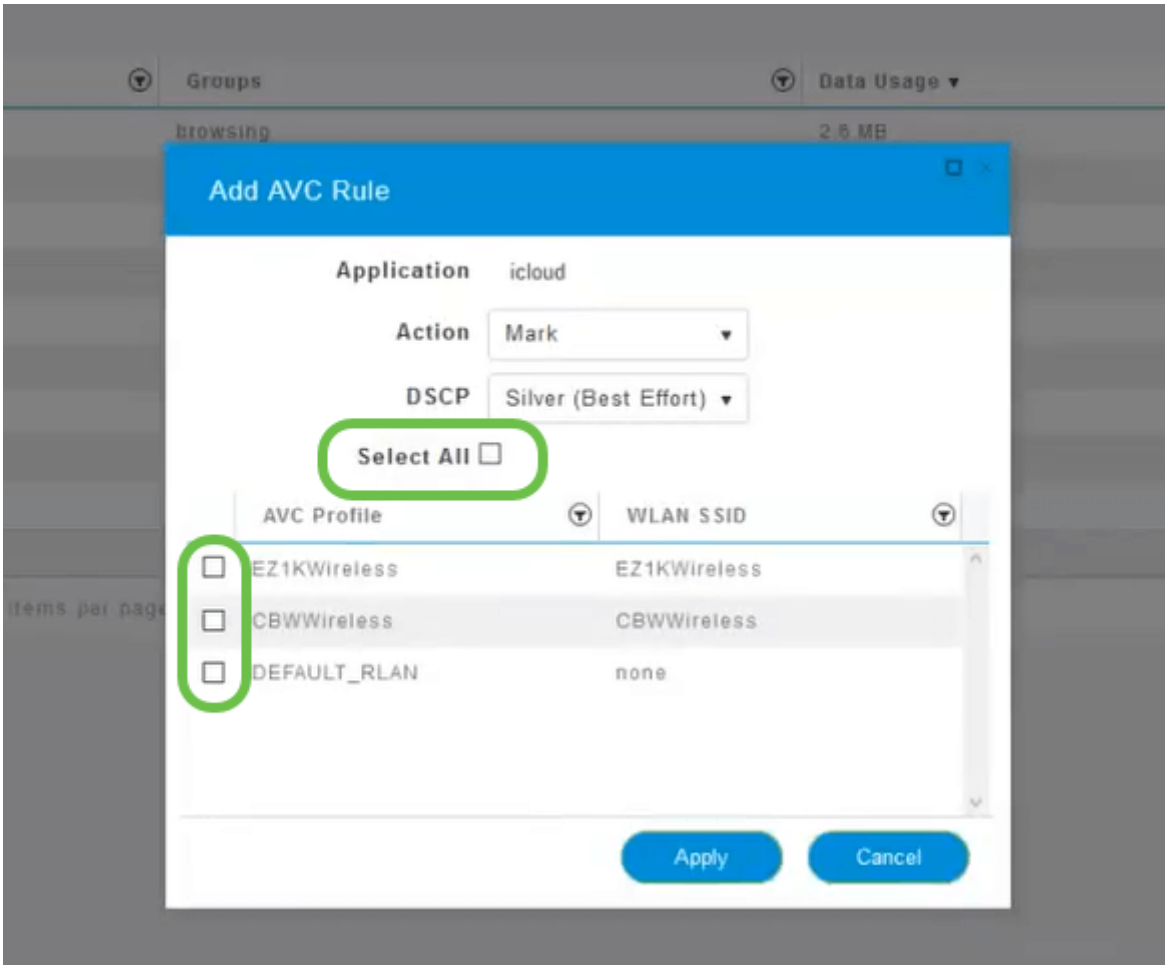
マーキングするトラフィックのDSCPオプションを次に示します。これらのオプションは、編集しているトラフィックタイプで使用できるリソース数が少なくなり、リソース数が増えます。

- 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。

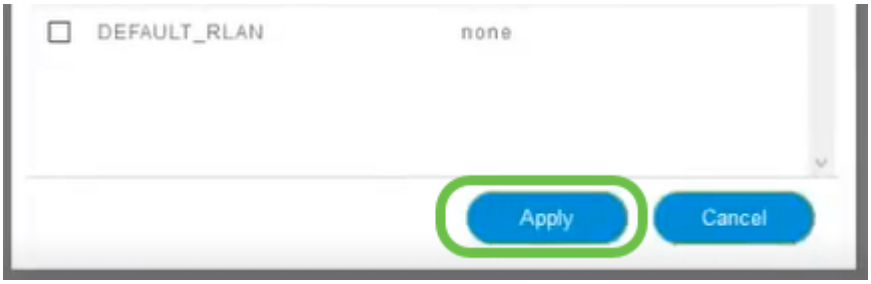
手順 11

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

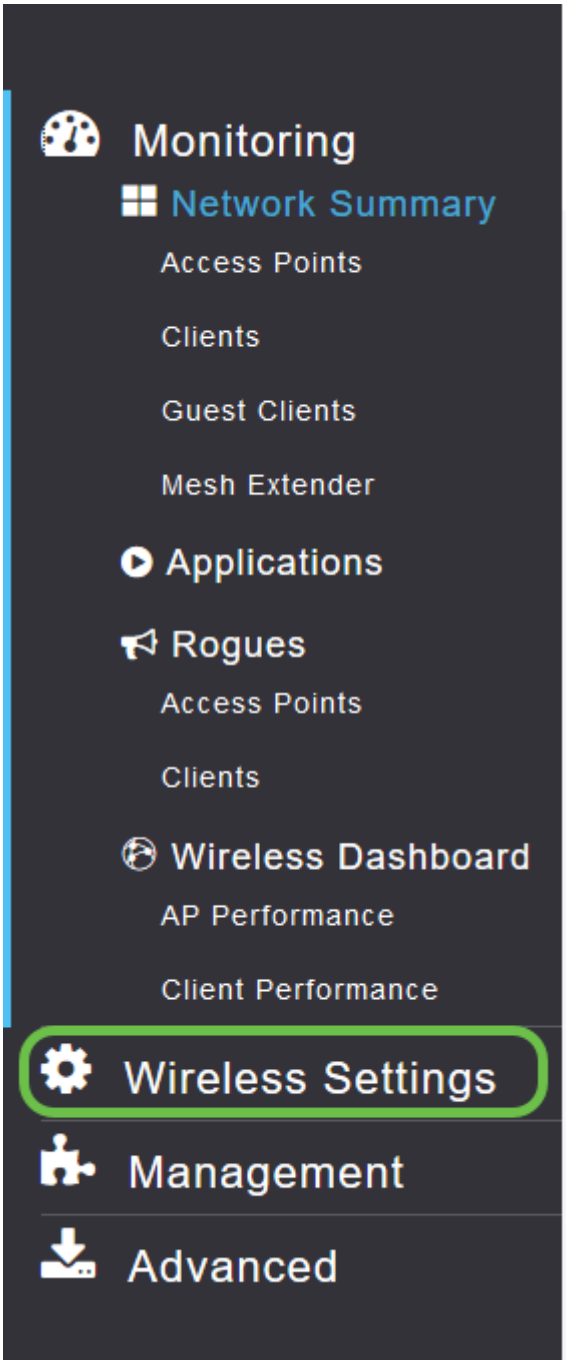
これらのクライアントに関する統計情報には、使用されるデータ量とスループットが含まれます。

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。

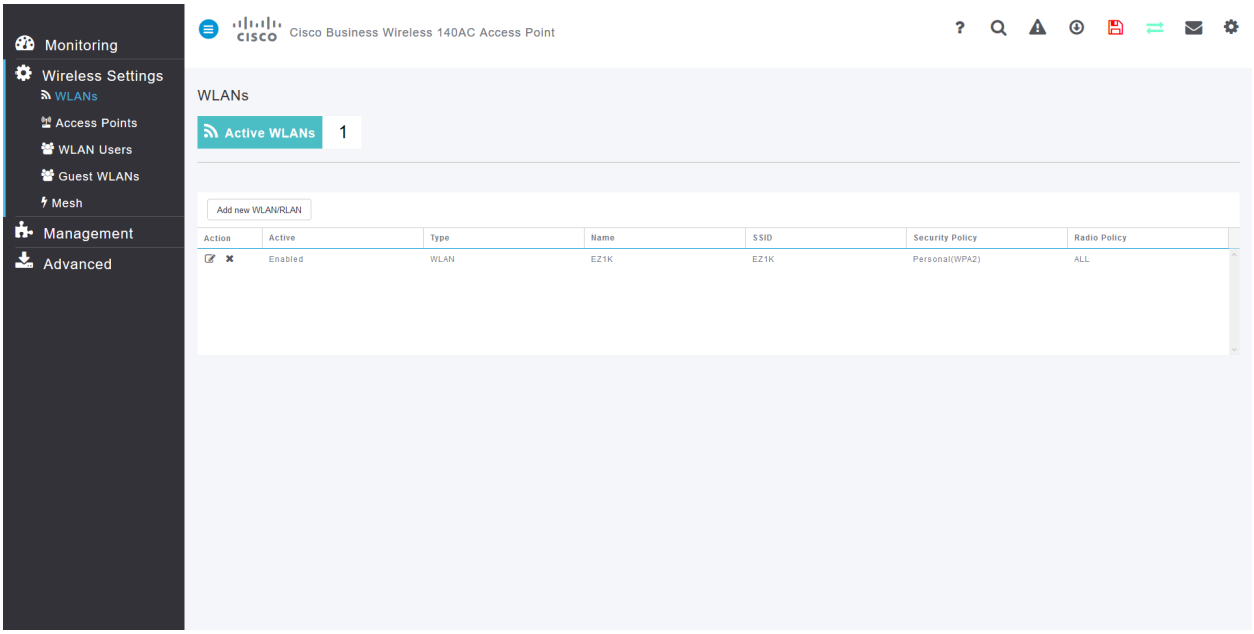
有効にすると、ネットワークのクライアントの詳細がWeb UIの[Monitoring]セクションに表示されます。

手順 1

[ワイヤレス設**定]をクリックします。**

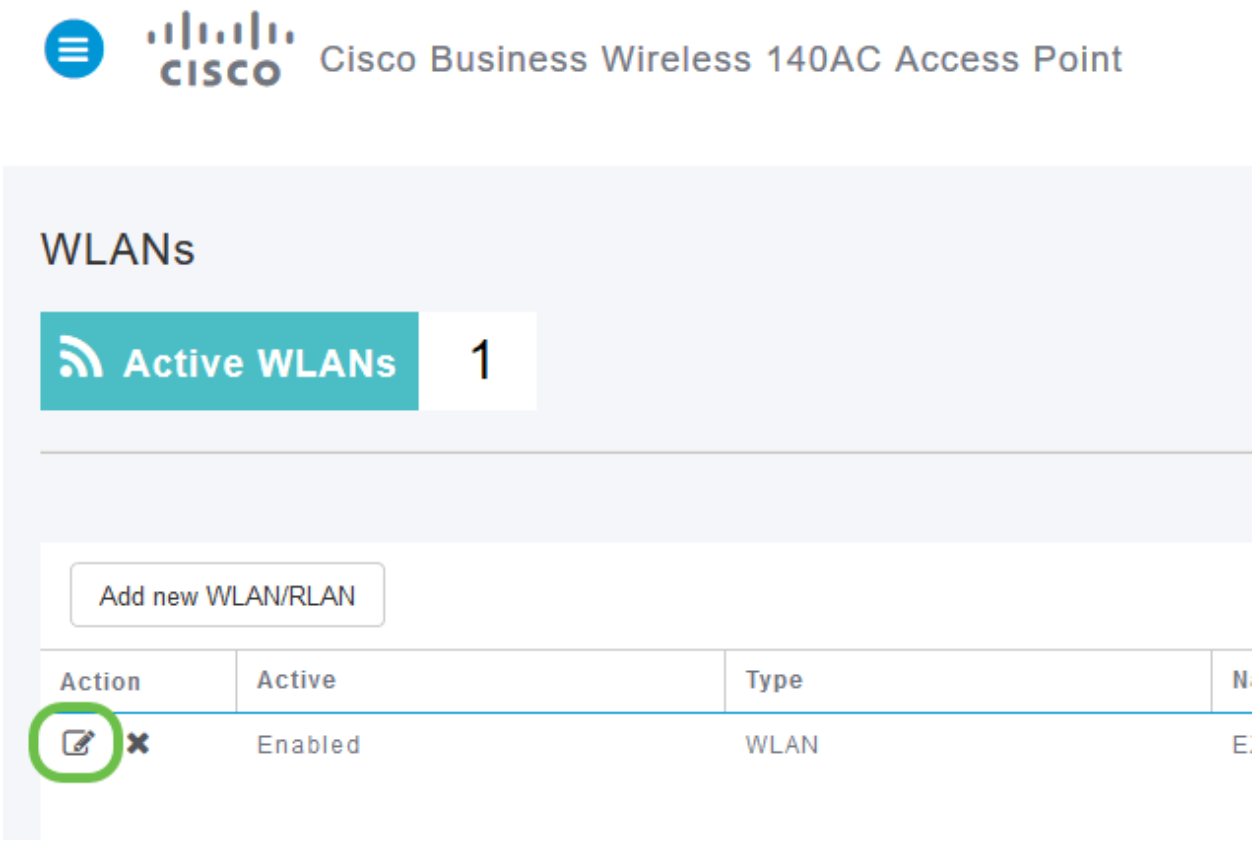


以下は、[ワイヤレス設定(Wireless Settings)]リンクをクリックしたときに表示される内容と似ています。



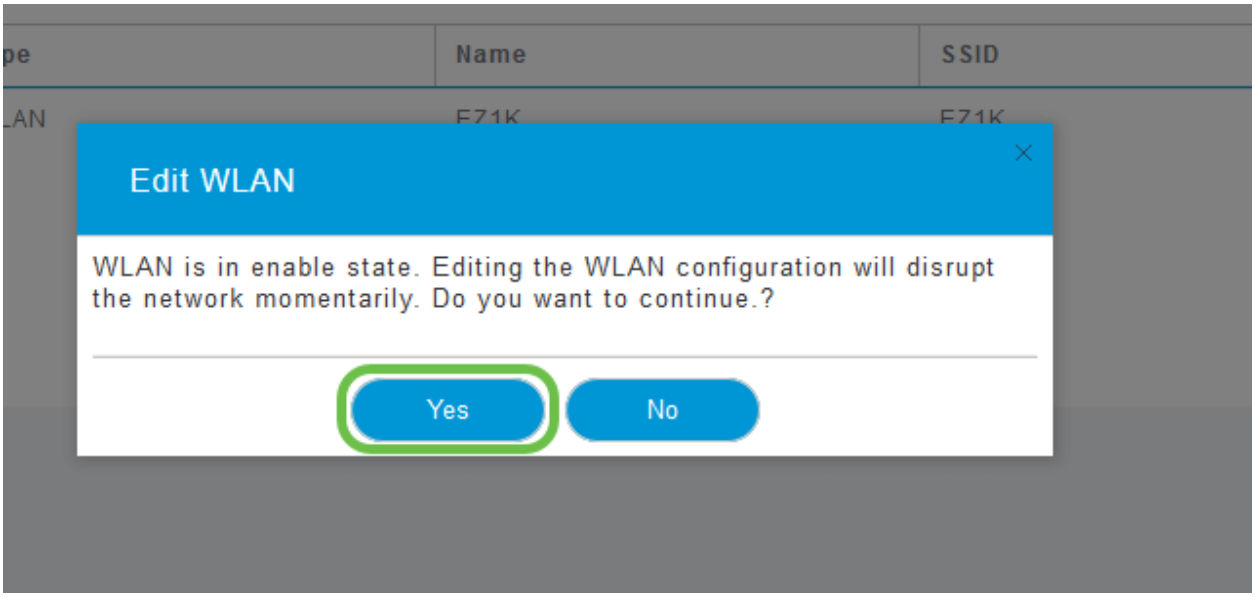
手順 2

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。

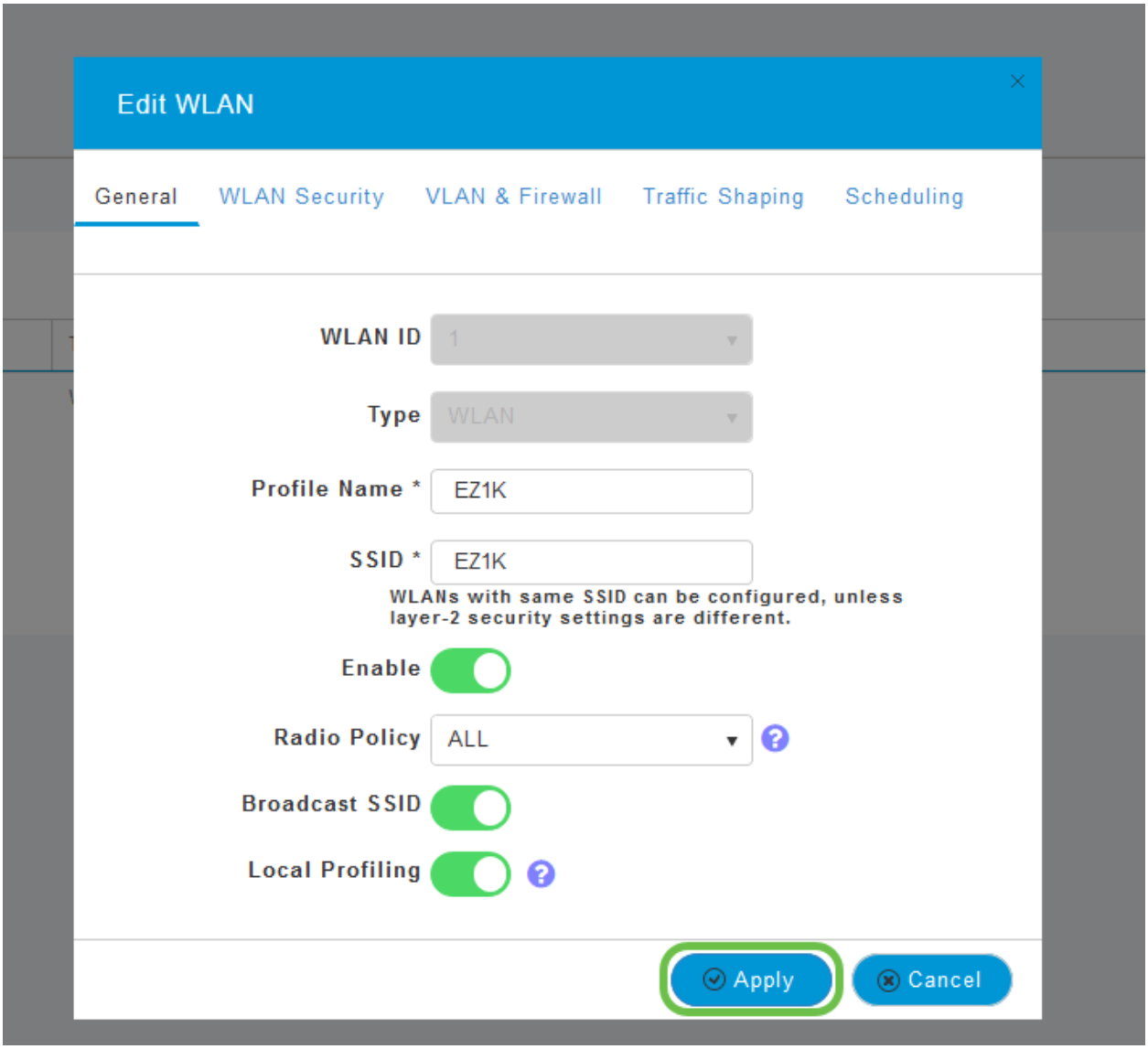


手順 4

[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。

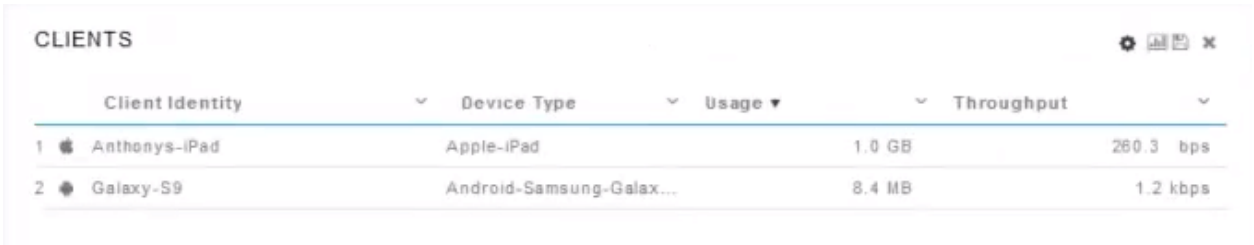
手順 5

[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 RV345P 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