ネットワーク全体の構成：モバイルアプリケーションを使用したRV345PおよびCisco Business Wireless

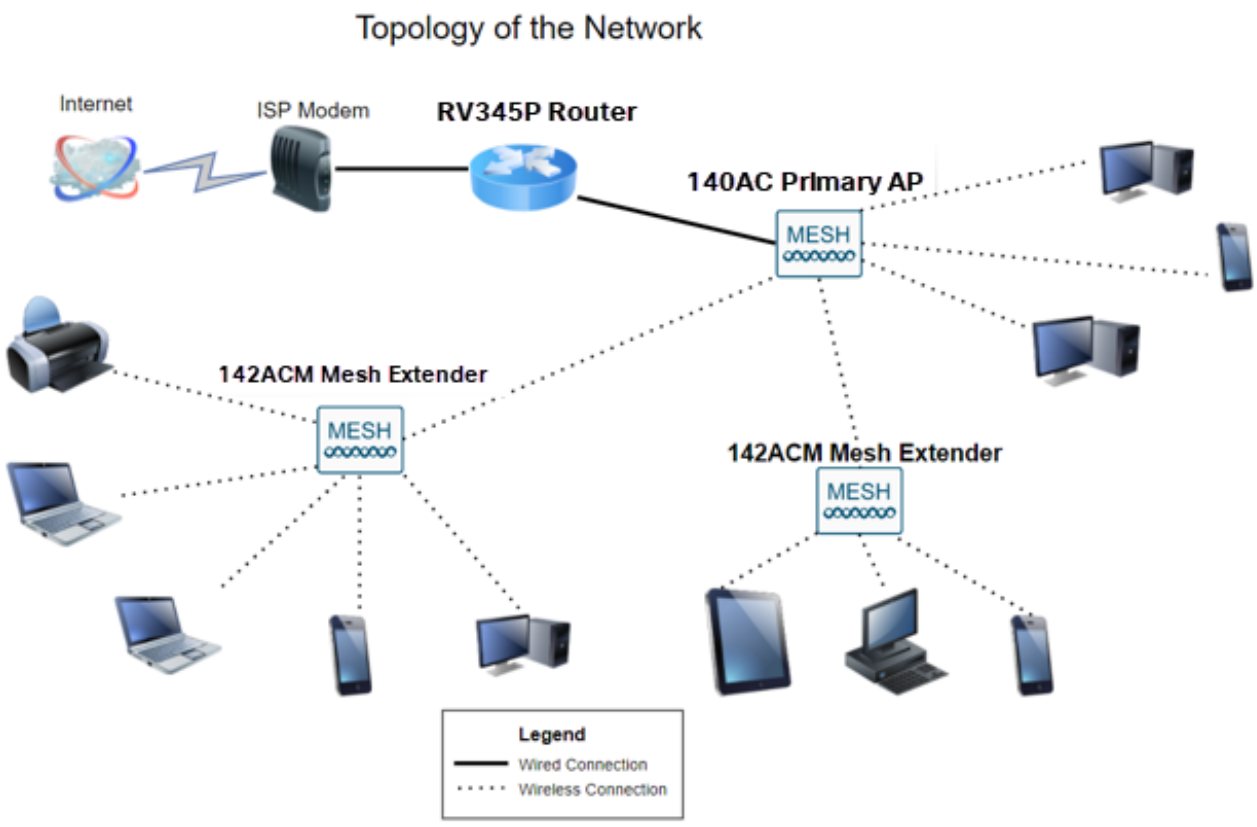
目的

このガイドでは、RV345Pルータ、CBW140ACアクセスポイント、および2台の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、メッシュワイヤレスネットワークの簡単なセットアップに推奨されるモバイルアプリケーションを使用します。すべての構成でWebユーザーインターフェイス(UI)を使用する場合は、をクリックしてWeb UIを使用する記事にジャンプします。

目次

トポロジ



はじめに

すべての調査が完了し、シスコの機器を購入できたことは非常にエ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)を備えているため、スイッチの代わりにCBW140ACを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、そのトラフィックをログに記録するか、トラフィックをブロックしてログに記録するか、または単にトラフィックをブロック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。この機能ではロギングは行われません。
3. AnyConnectは、シスコが提供するSecure Sockets Layer(SSL)Virtual Private Network(VPN)です。VPNを使用すると、リモートユーザとサイトは、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により、会社の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ます。これについては、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の一部に慣れていない場合、またはメッシュネットワーキングの詳細が必要な場合は、次の記事を参照してください。

- シスコビジネス：新しい用語の用語集
- Cisco Businessワイヤレスメッシュネットワーキングへようこそ
- Cisco Business Wireless Networkに関するFAQ

適用可能なデバイス | [Software Version]

- 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ます。
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、ルータが組み込ま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さなければならないことがあります。
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、この作業は簡単ではありません。

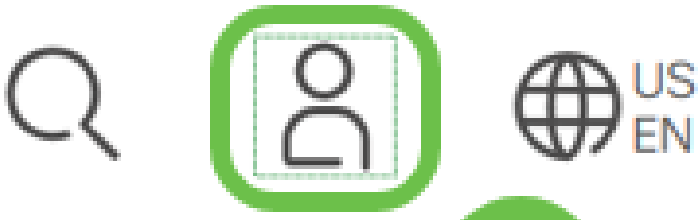
Cisco.comアカウントの取得

シスコ機器を所有したら、Cisco.comアカウントを取得する必要があります。このアカウントは、Cisco Connection Online Identification(CCO ID)と呼ばれることもあります。勘定は無料だ。

すでにアカウントをお持ちの場合は、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にアクセスします。personアイコンをクリックし、次にCreate an accountをクリックします。



1

Have an account?

- Personalized content
- Your products and support

Log In

Forgot your user ID and/or password?

Manage account

My Cisco

Need an account?

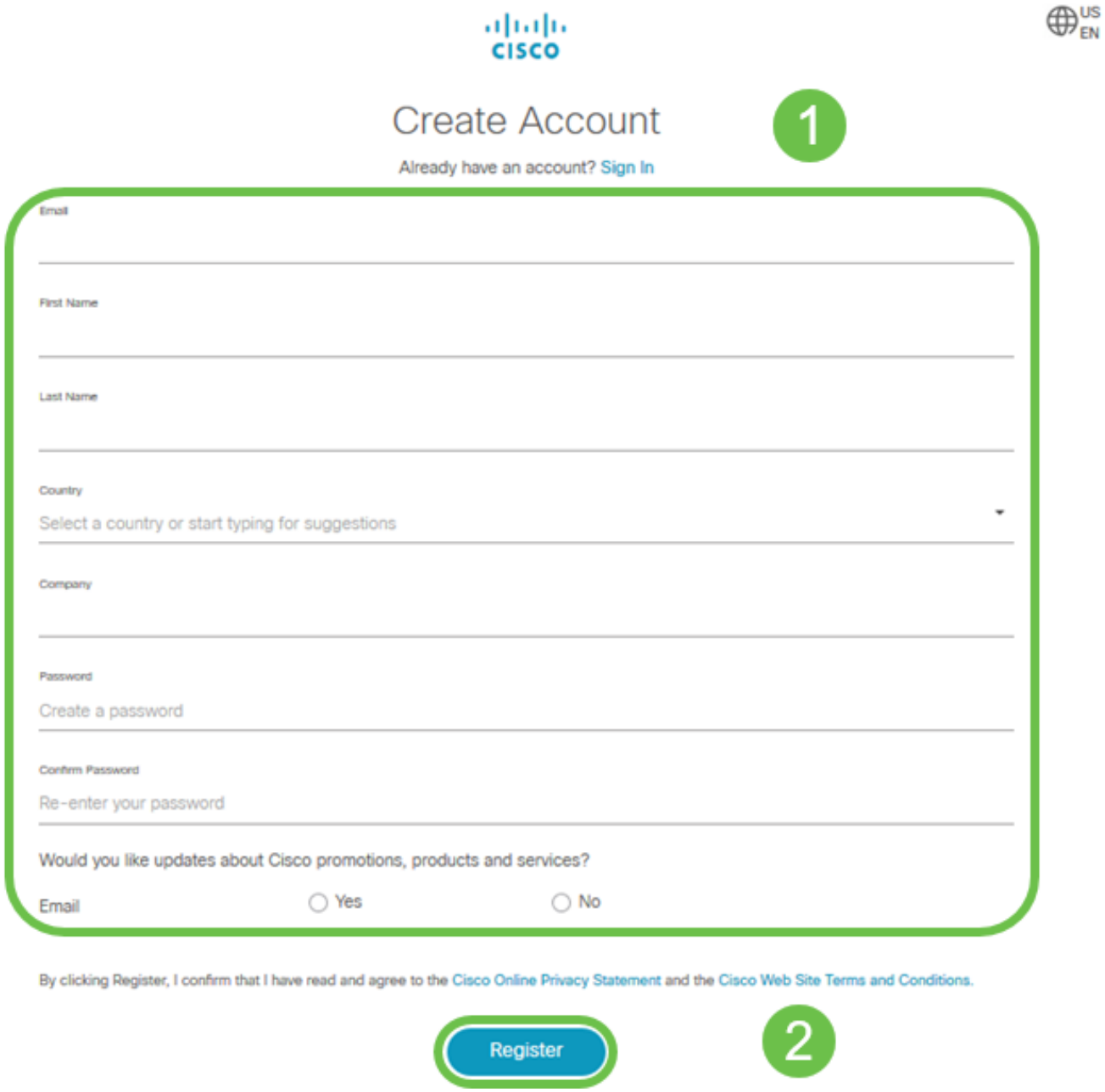
Create an account

2

Help

手順 2

アカウントの作成に必要な詳細情報を入力し、Register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、クリックしてCisco.com Account Registration Helpページにジャンプします。

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。コンピュータが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るようにする。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。スタティック設定とダイナミック設定の両方

をルーティングテーブルにリストして、パケットを特定の宛先に取得できます。

RV345Pには、多くの小規模企業向け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やインターネットサービスプロバイダー(ISP)によっては、これらの設定の一部を変更する必要があります。要件についてISPに問い合わせた後、Webユーザインターフェイス(UI)を使用して変更を加えることができます。

準備はできていますか。さあ、始めましょう。

設定済みRV345P

手順 1

イーサネットケーブルを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。初期設定を行うには、端末がRV345Pと同じ有線サブネットワークに存在している必要があります。

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ドングルで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、まだ電源に接続しないでください。

手順 3

モデムの電源が切れ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、ケーブルモデムまたは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。これにより、RV345Pの電源がオンになります。モデムの電源も入るように、モデムのプラグを差し込みます。電源アダプタが正しく接続され、RV345Pの起動が完了すると、前面パネルの電源ライトが緑色に点灯します。

ルータのセットアップ

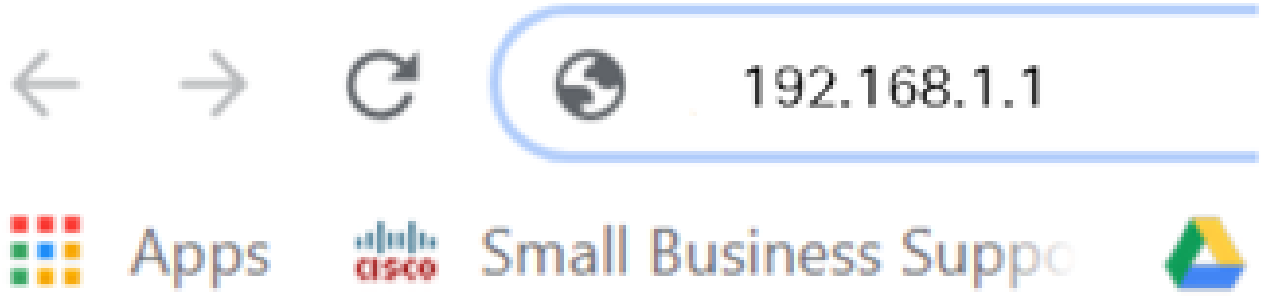
準備作業が完了したので、次は設定を行います。Web UIを起動するには、次の手順に従います。

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は、192.168.1.xの範囲のIPアドレスがPCに割り当てられます。DHCPは、IPアドレス、サブネットマスク、デフォルトゲートウェイ、およびその他の設定をコンピュータに割り当てるプロセスを自動化します。アドレスを取得するには、DHCPプロセスに参加するようにコンピュータを設定する必要があります。これは、コンピュータ上のTCP/IPのプロパティでIPアドレスを自動的に取得することを選択することによって行われます。

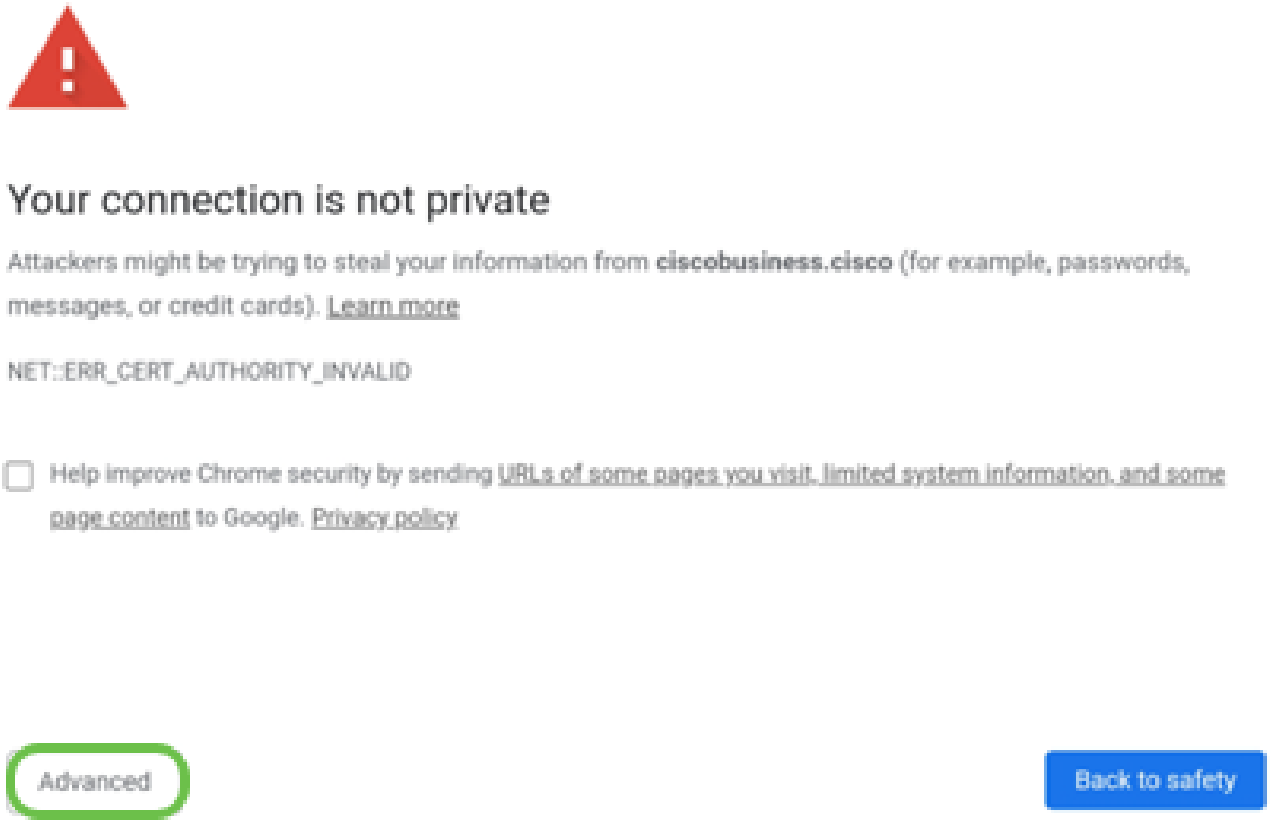
手順 2

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のデフォルトIPアドレス192.168.1.1を入力します。



手順 3

ブラウザから、Webサイトが信頼できないという警告が表示される場合があります。Webサイトに進みます。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」に進んでください。

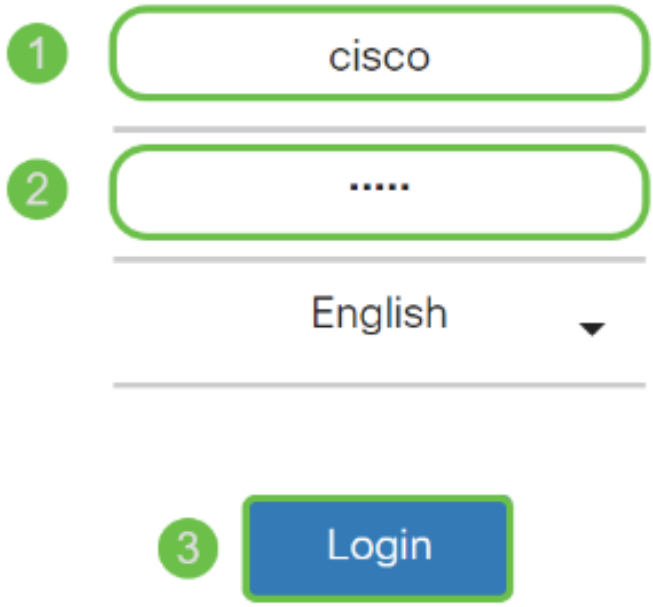


手順 4

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にアクセスする方法をクリックしてください。



手順 5

[Login] をクリックする。Getting Started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くことができます。

接続を確認してルータにログインしたので、この記事の「初期設定」セクションに進みます。

インターネット接続のトラブルシューティング

このドキュメントを読んでいるなら、おそらくインターネットやWeb UIへの接続に問題があります。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では、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) と入力します。要求がタイムアウトすると、ルータと通信できなくなります。

接続が行われていない場合は、このトラブルシューティングの記事を確認できます。

その他の試み：

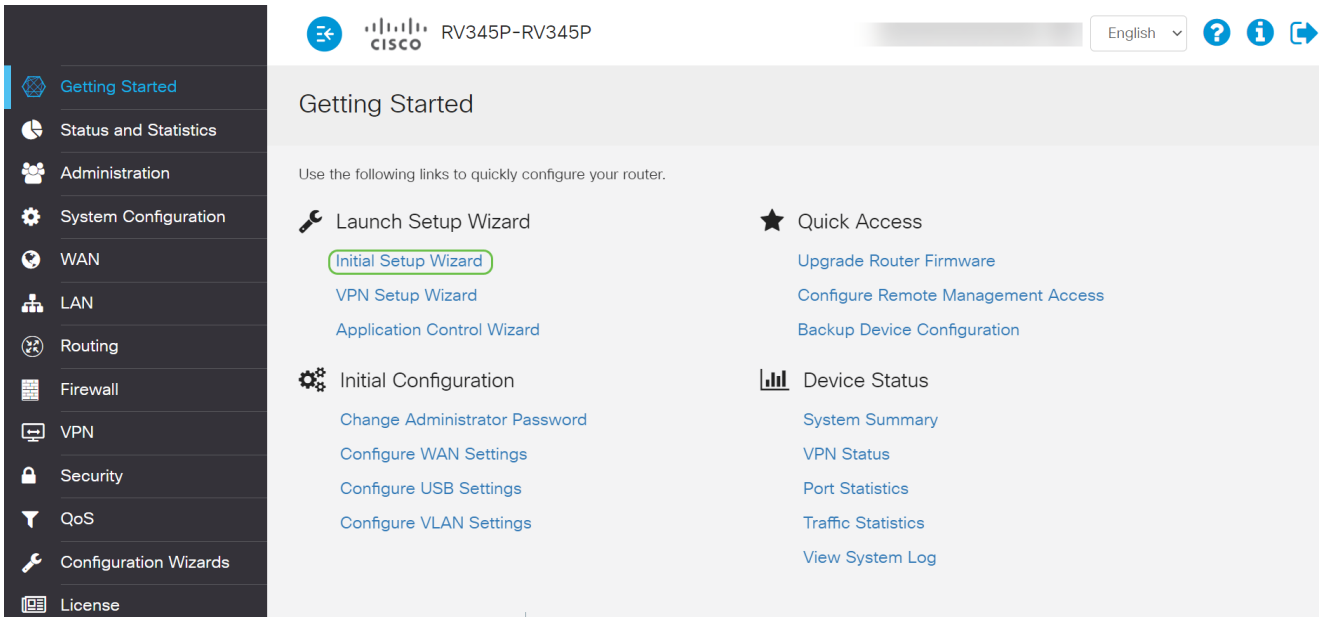
1. Webブラウザが[オフライン作業]に設定されていないことを確認します。
2. イーサネットアダプタのローカルエリアネットワーク接続の設定を確認します。PCはDHCPからIPアドレスを取得する必要があります。または、PCに192.168.1.xの範囲のスタティックIPアドレスを設定し、デフォルトゲートウェイを192.168.1.1（RV345PのデフォルトIPアドレス）に設定することもできます。接続するには、RV345Pのネットワーク設定を変更する必要があります。 Windows 10を使用している場合は、Windows 10の指示を確認してネットワーク設定を変更してください。
3. IPアドレス192.168.1.1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ようにこの競合を解決する必要があります。詳細については、このセクションの最後を参照するか、ここをクリックして直接確認してください。
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。次に、RV345Pの電源をオンにします。これで、WAN IPアドレスを受信します。
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に依頼します。

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。

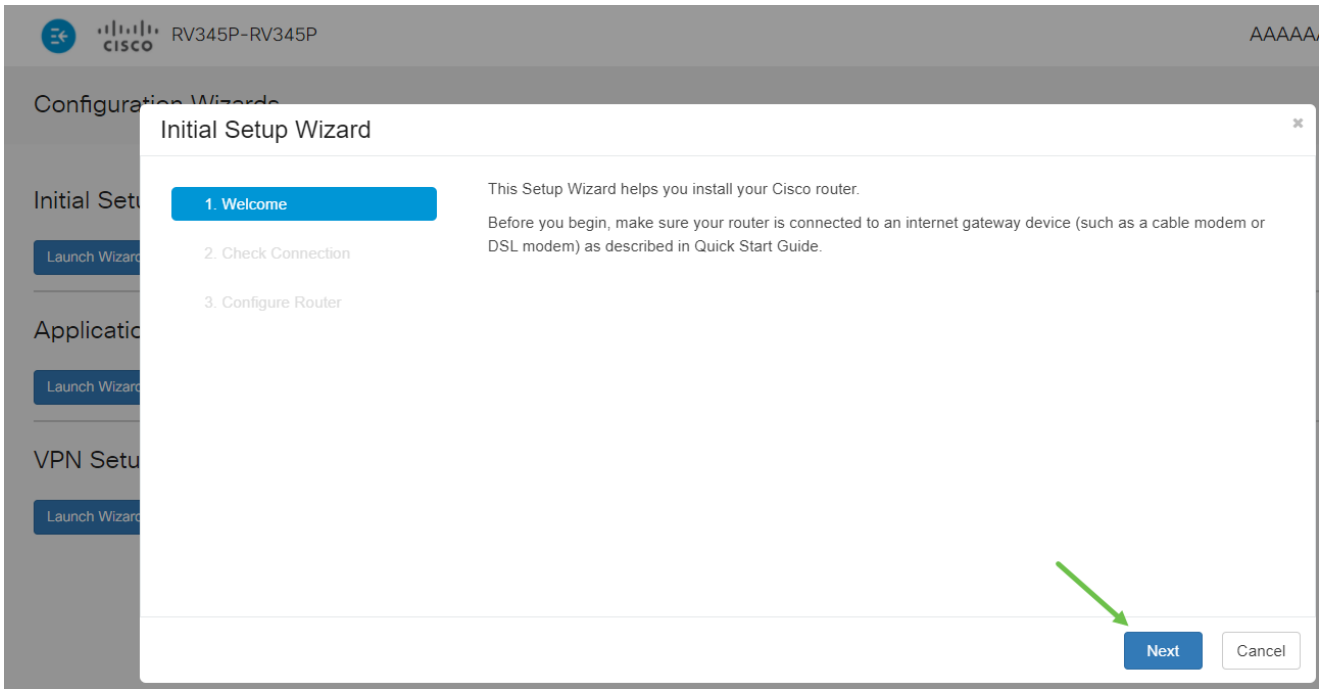
手順 1

Getting StartedページでInitial Setup Wizardをクリックします。



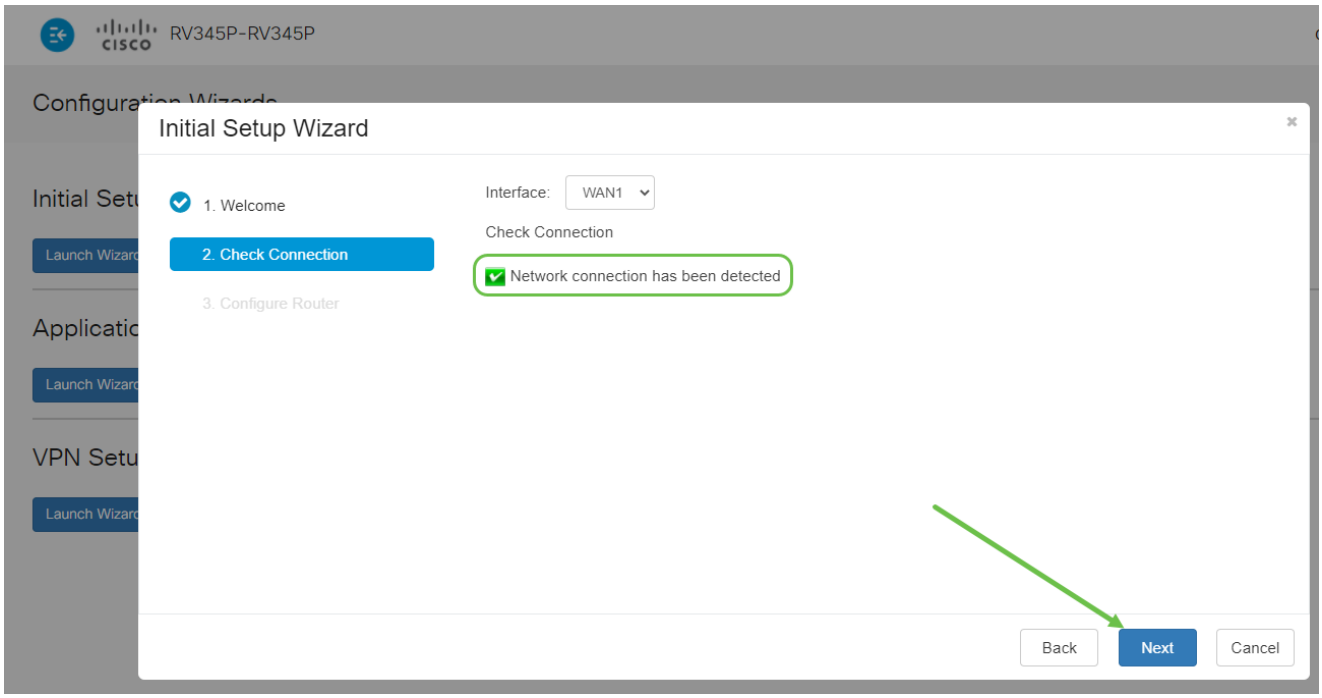
手順 2

この手順で、ケーブルが接続されていることを確認します。これはすでに確認しているので、Nextをクリックします。



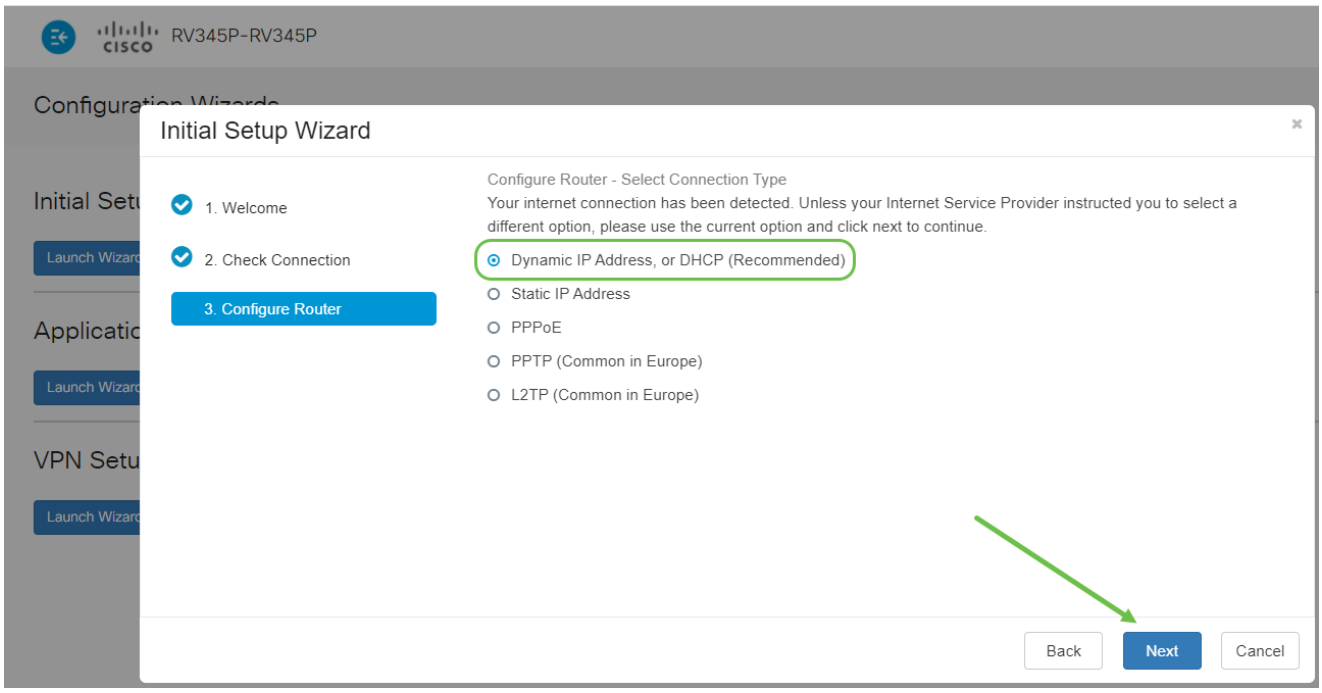
手順 3

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。これはすでに確認しているので、Nextをクリックします。



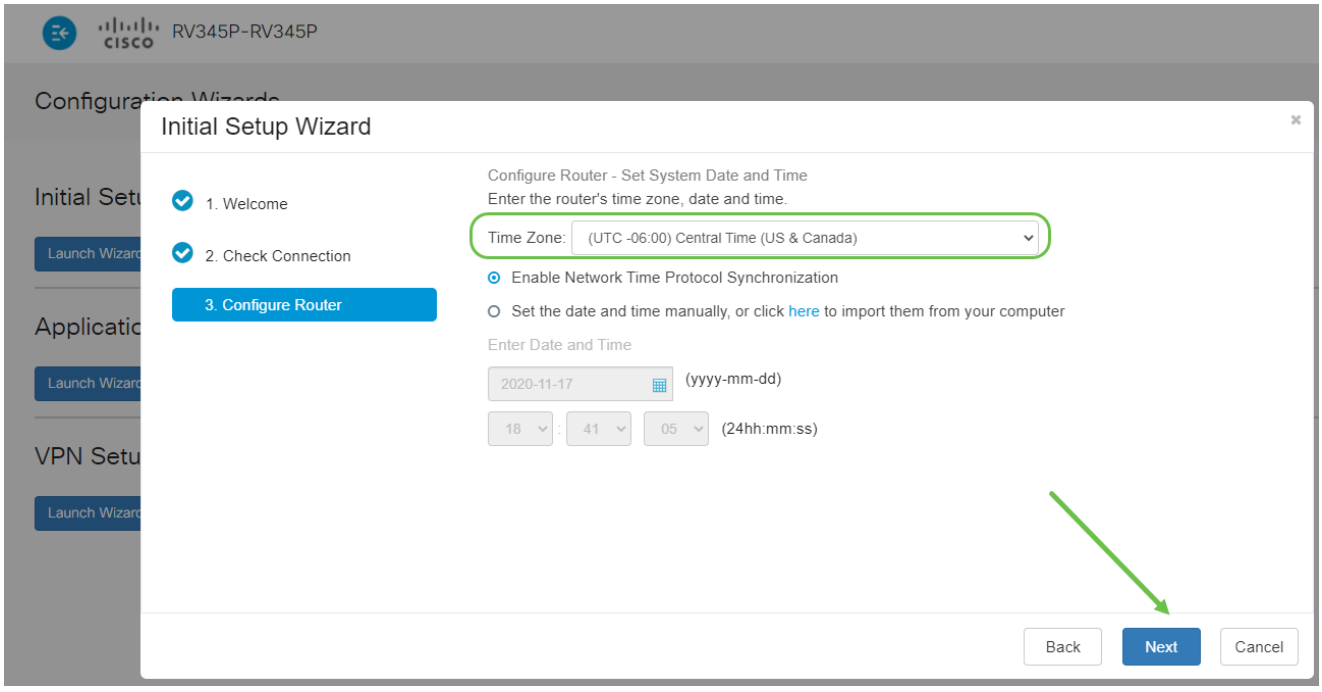
手順 4

次の画面に、ルータにIPアドレスを割り当てるための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。



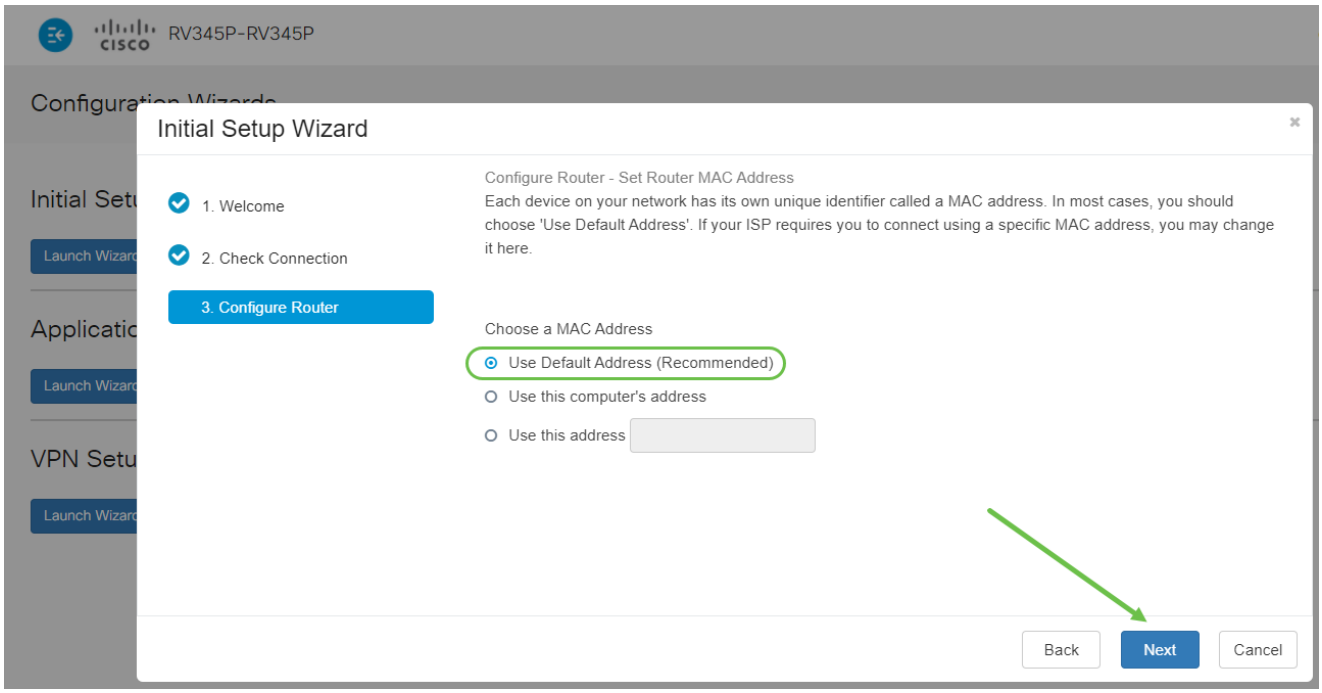
手順 5

ルータの時刻設定を求めるプロンプトが表示されます。ログの確認やイベントのトラブルシューティングを正確に行えるため、これは重要です。Time Zoneを選択し、Nextをクリックします。



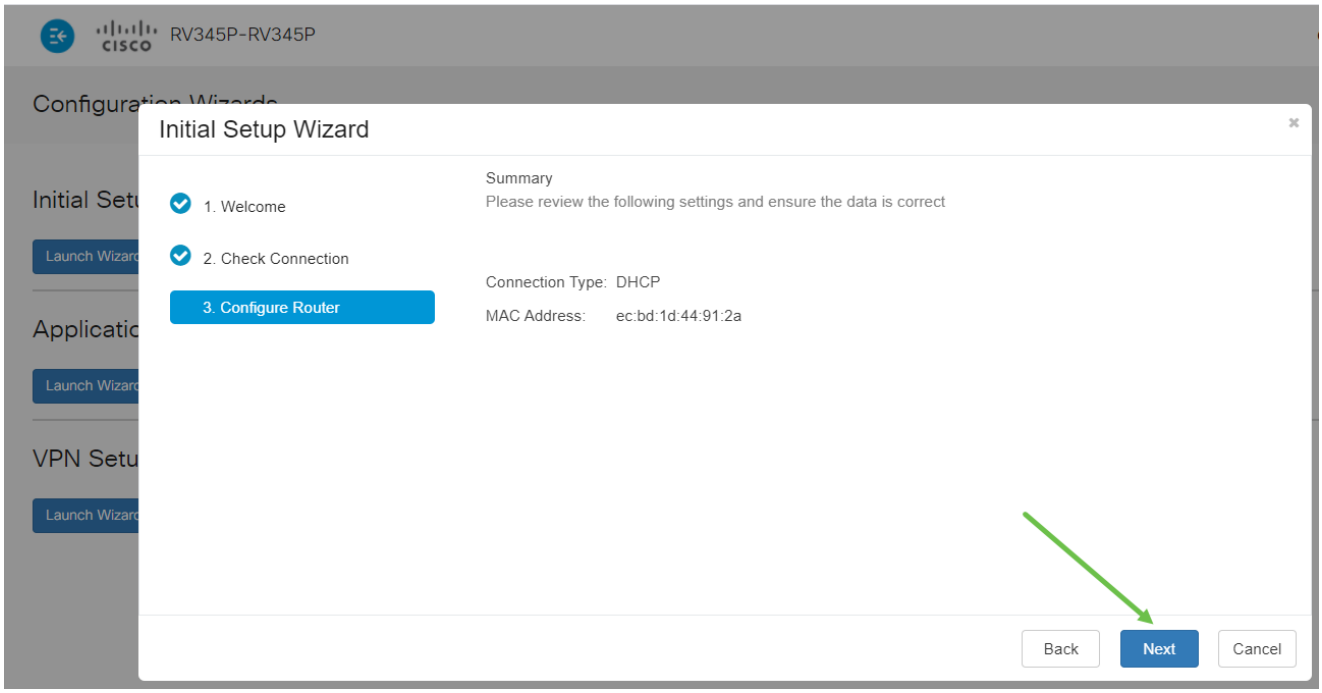
手順 6

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。



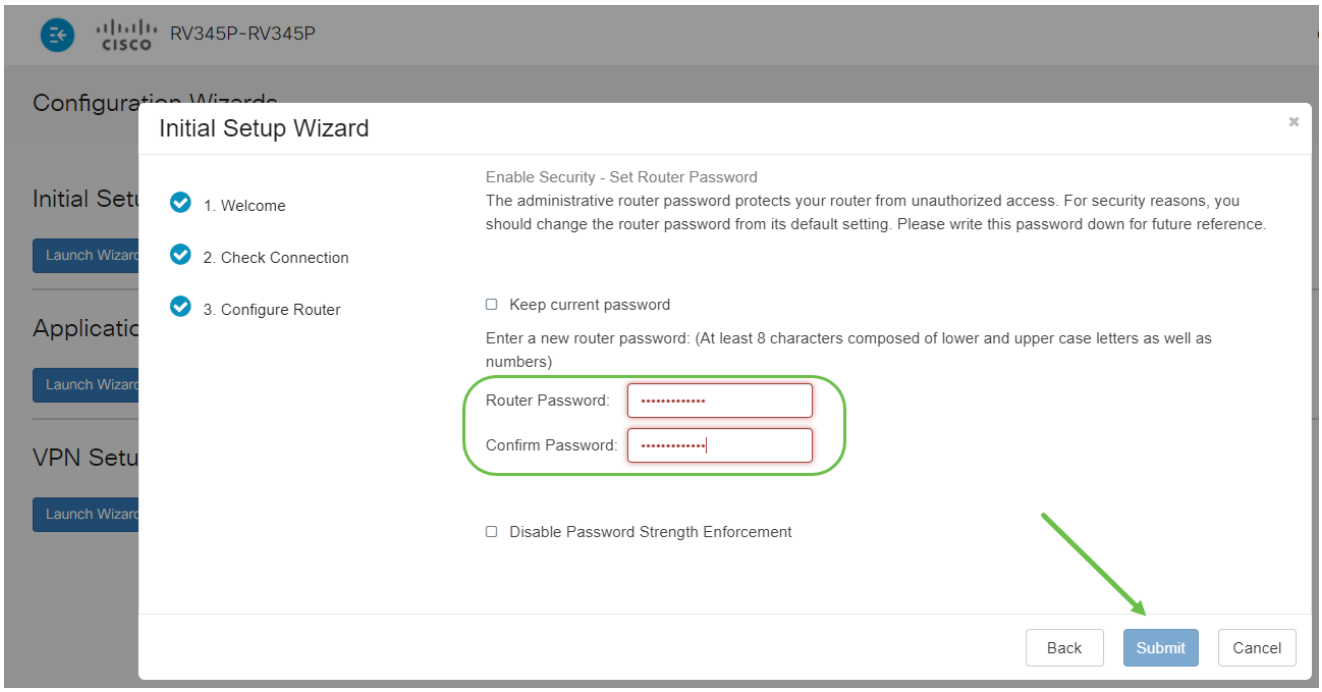
ステップ7

次のページは、選択したオプションの概要です。確認し、問題がなければNext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、少なくとも8文字（大文字と小文字の両方）を含み、数字を含むことです。 強度要件に準拠したパスワードを入力します。[Next] をクリックします。今後のログインのためにパスワードを書き留めておきます。



Disable Password Strength Enforcementを選択することは推奨されません。このオプションを選択すると、123という単純なパスワードを選択できます。これは、悪意のある攻撃者がクラックする1-2-3と同じくらい簡単です。

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設定の設定」を参照してください。

RV345PではPower over Ethernet(PoE)がデフォルトで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ルータでのPower over Ethernet(PoE)設定の構成』を参照してください。

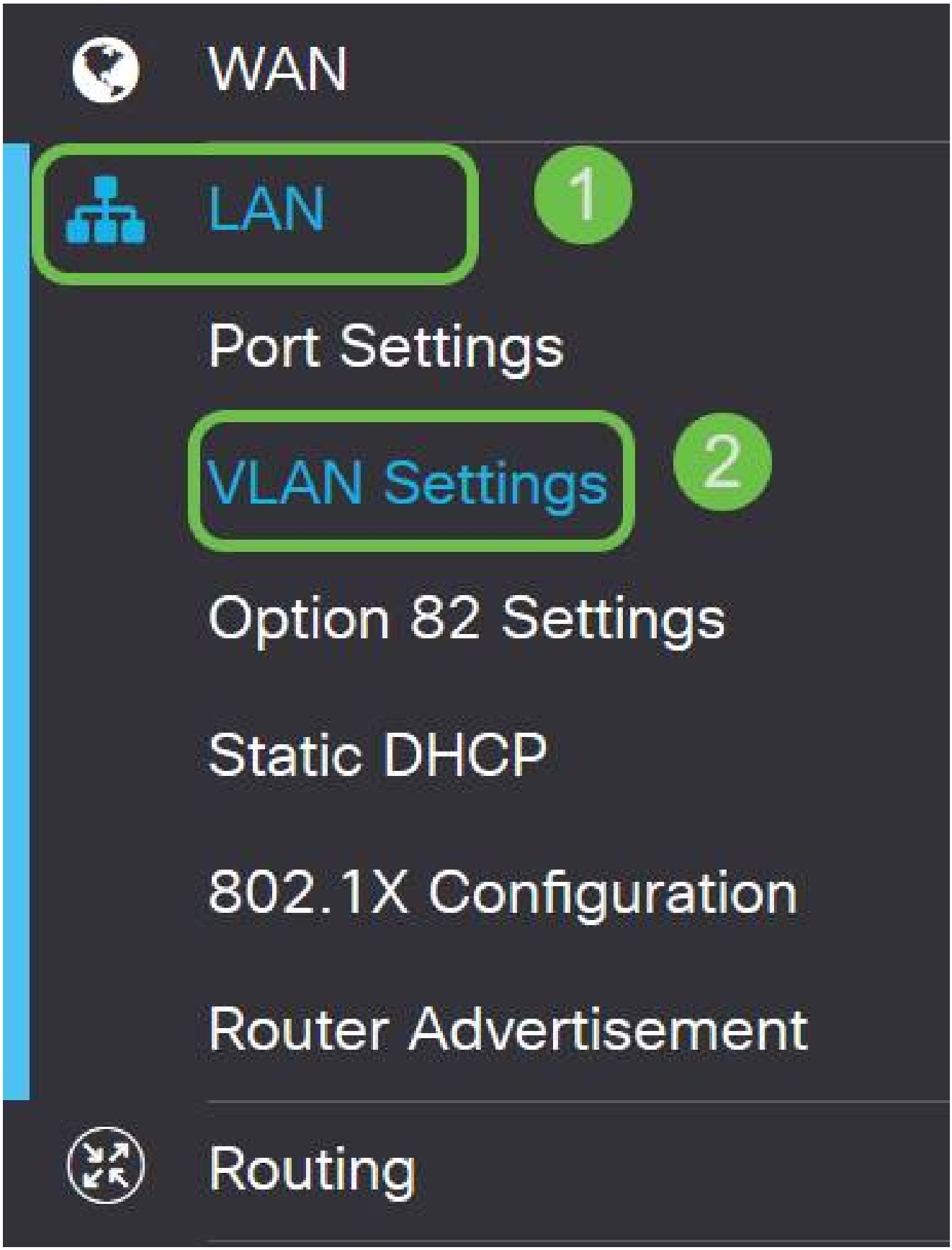
必要に応じてIPアドレスを編集する（オプション）

Initial Setup Wizardが完了したら、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アドレスに既存のネットワーク内の特定のアドレスを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進んでください。

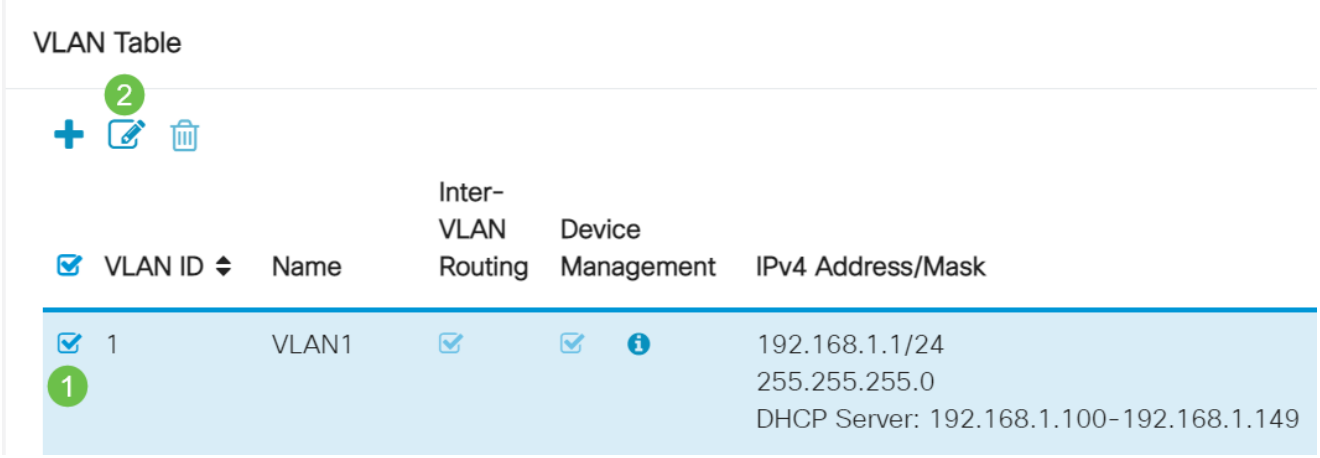
手順 1

左側のメニューで、LAN > VLAN Settingsの順にクリックします。



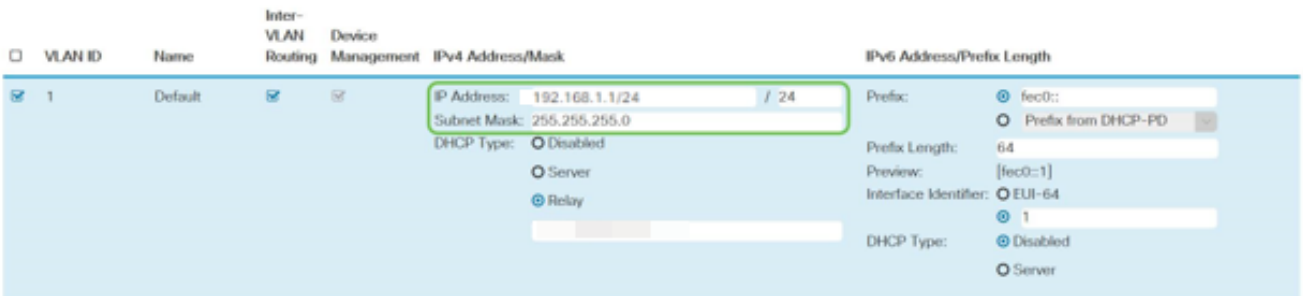
手順 2

ルーティングデバイスが含まれているVLANを選択し、編集アイコンをクリックします。



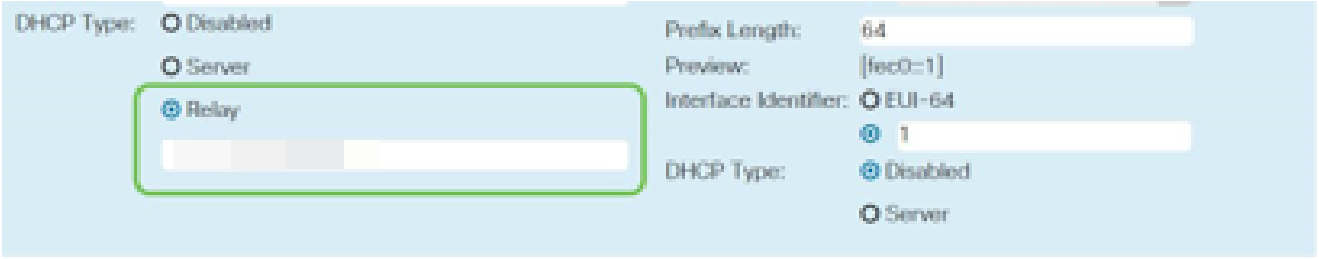
手順 3

目的の固定IPアドレスを入力し、右上隅にあるApplyをクリックします。



手順 4（オプション）

ルータがIPアドレスを割り当てるDHCPサーバ/デバイスではない場合は、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。

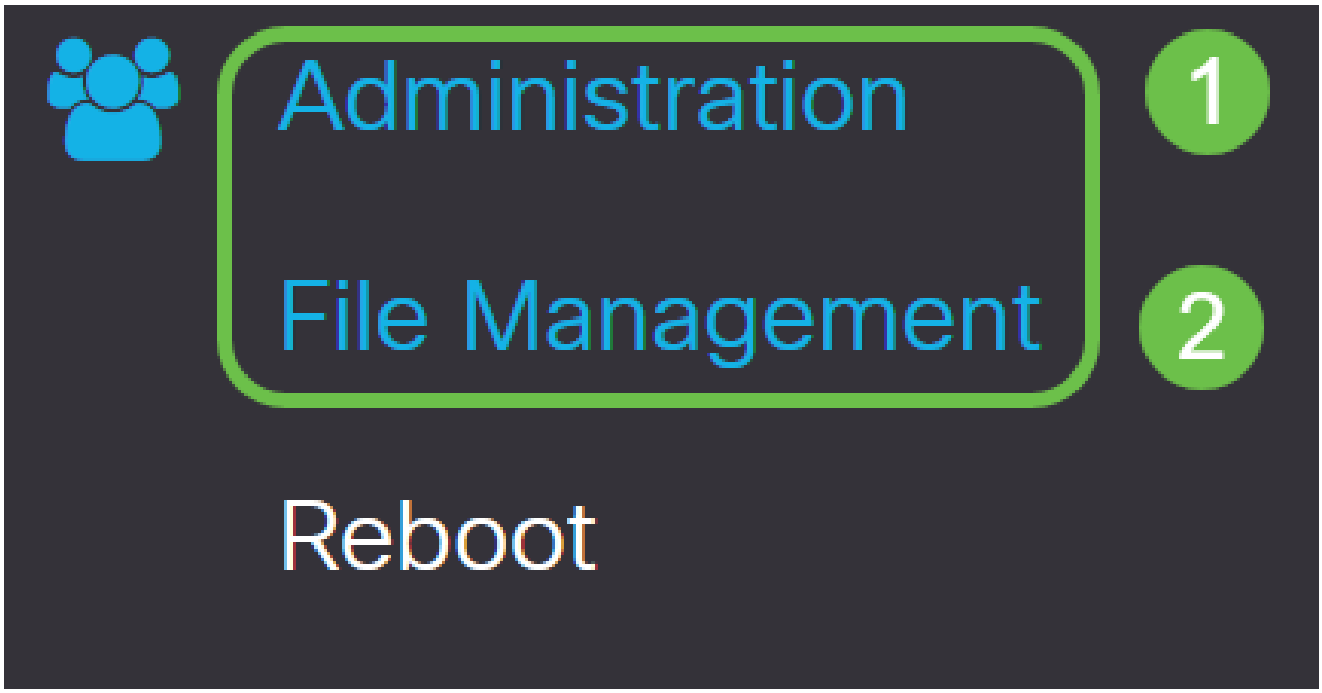


必要に応じてファームウェアをアップグレード

これは重要なステップです。スキップしないでください。

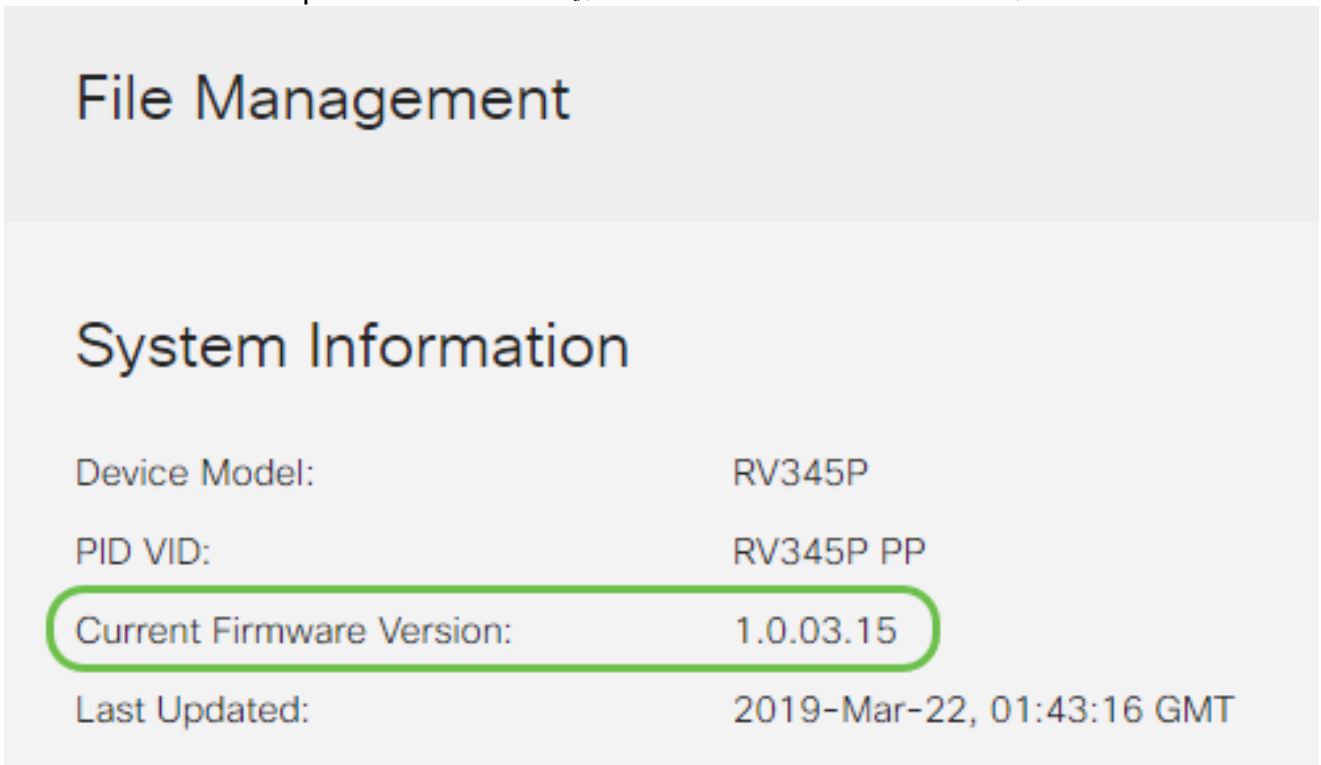
手順 1

Administration > File Managementの順に選択します。



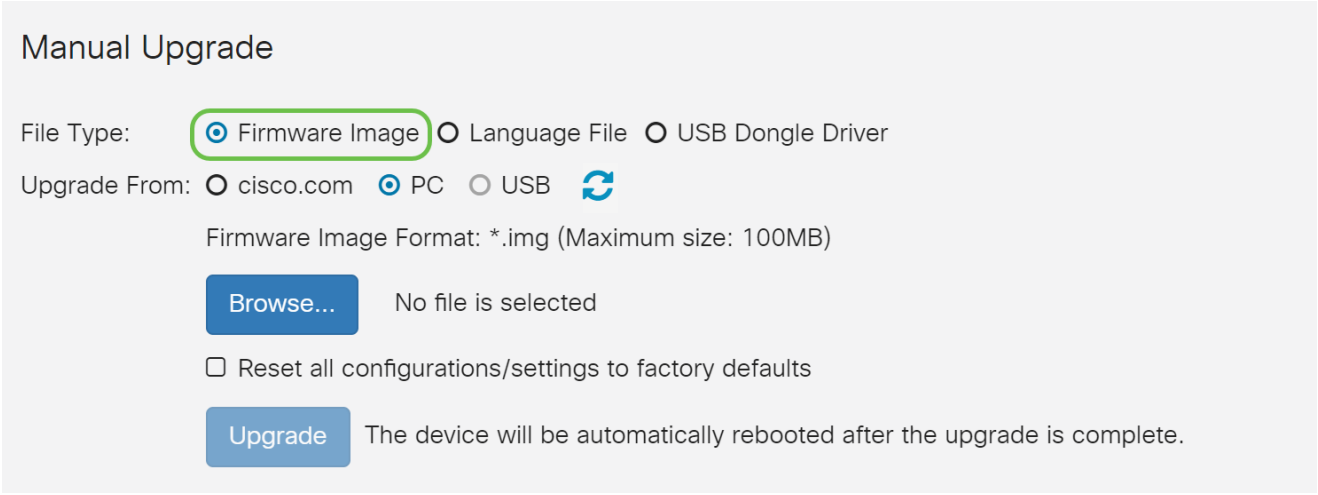
System Information領域では、次のサブエリアで次の項目を説明します。

- Device Model（デバイスモデル）：デバイスのモデルが表示されます。
- PID VID：ルータの製品IDとベンダーID。
- Current Firmware Version（現在のファームウェアバージョン）：デバイスで現在実行されているファームウェア。
- Cisco.comで入手可能な最新バージョン：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をアップデートした日時。



手順 2

Manual Upgradeセクションで、File Typeに対してFirmware Imageオプションボタンをクリックします。



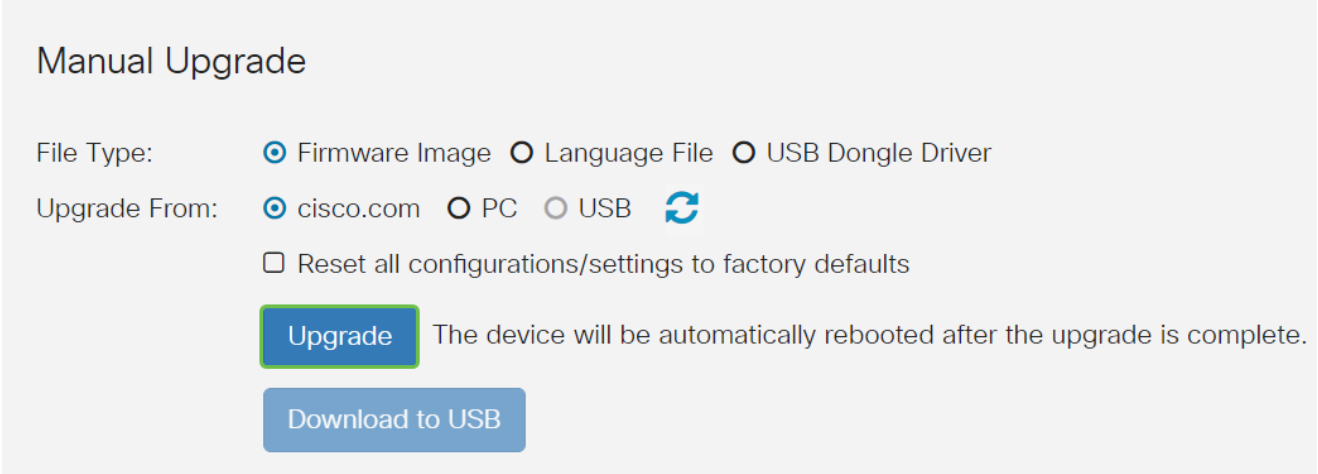
手順 3

Manual Upgrade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。このため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。このプロセスにより、最新のアップグレードファイルがシスコソフトウェアダウンロードWebページから直接インストールされます。

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接続が切断されている場合は、cisco.comからアップグレードできません。これがお客様に関係する場合は、 ここで別のオプションを確認できます。

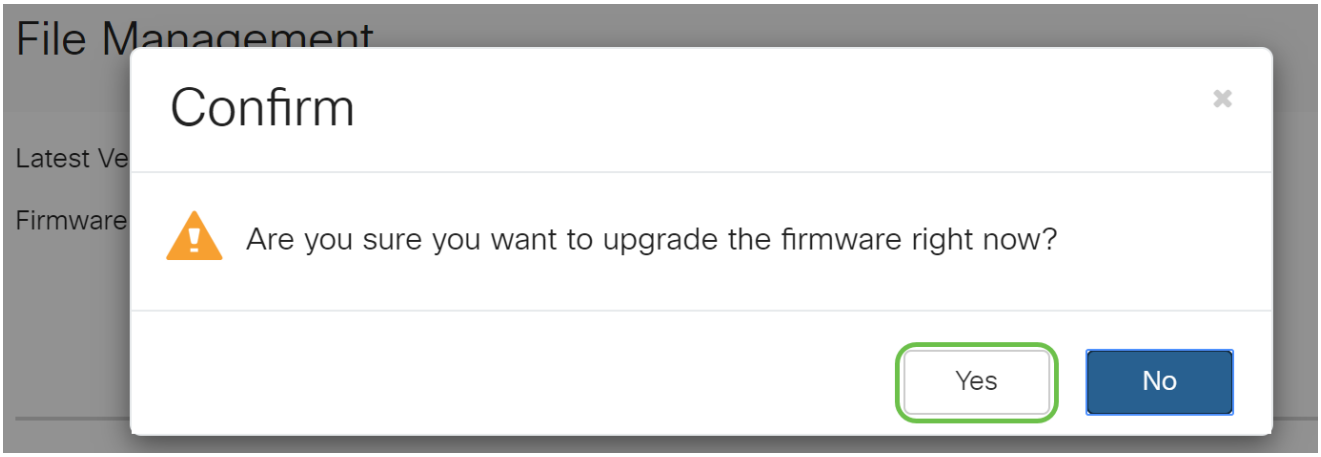
手順 4

[Upgrade] をクリックします。

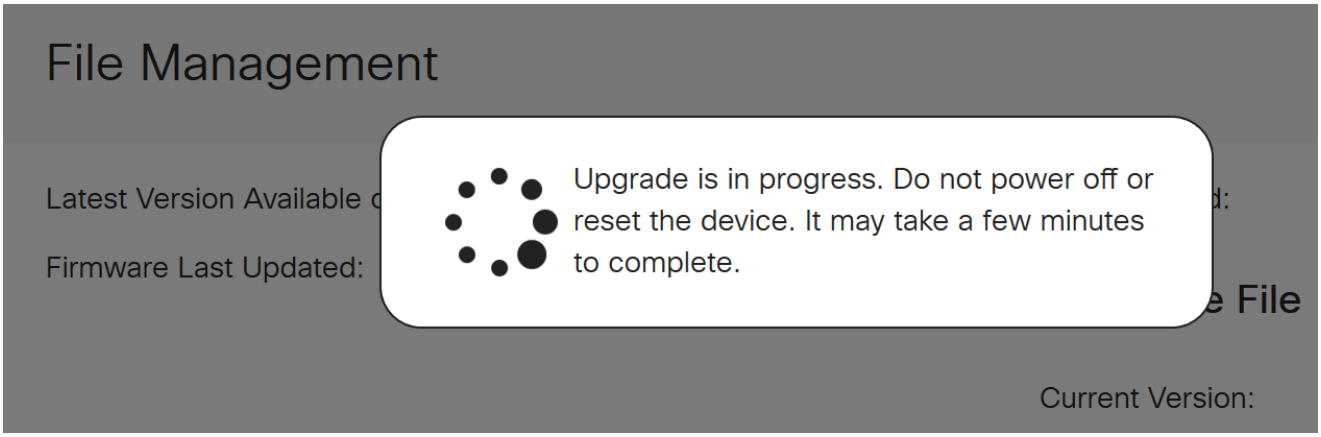


手順 5

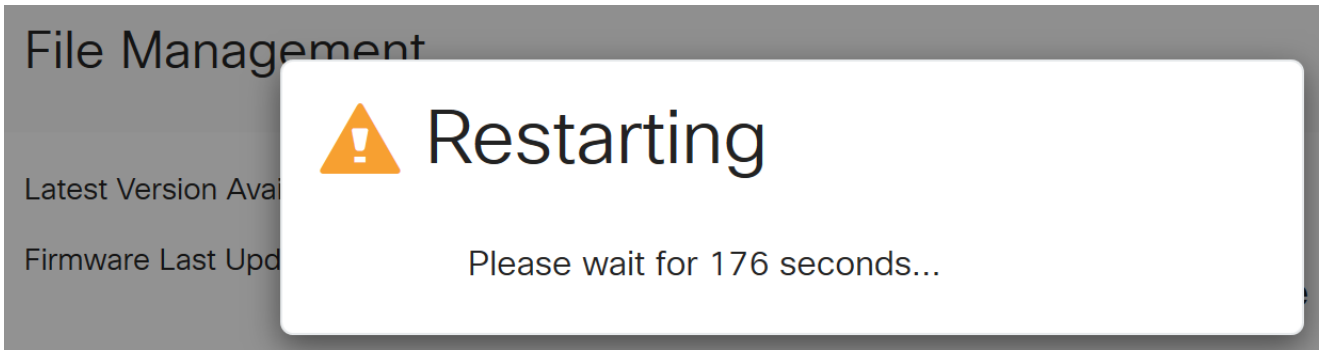
確認ウィンドウでYesをクリックして続行します。



更新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。

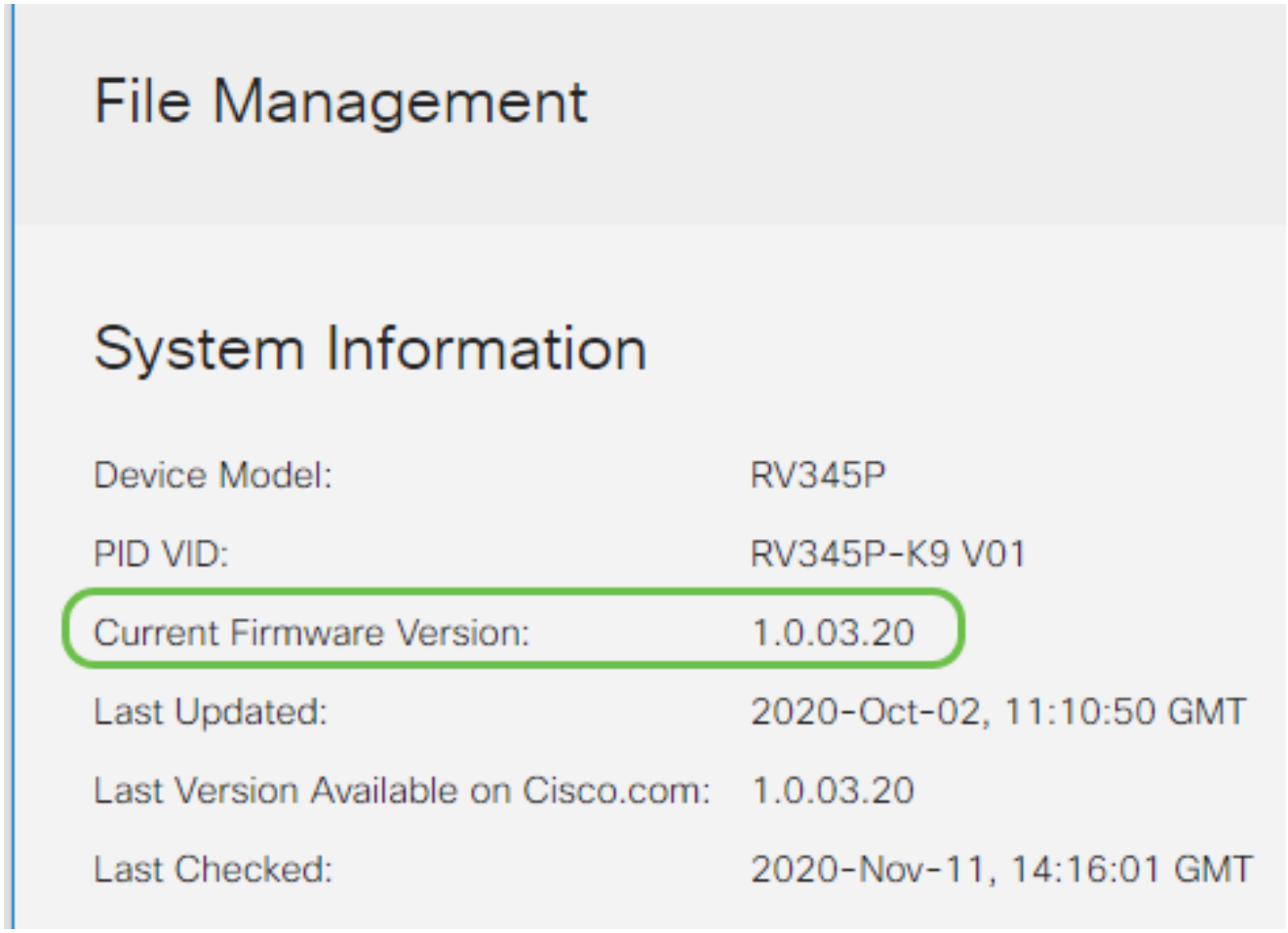


アップグレードが完了すると、通知ウィンドウがポップアップし、プロセスが完了するまでの推定時間をカウントダウンしてルータが再起動することを通知します。この後、ログアウトします。



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ていることを確認し、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るようになります。

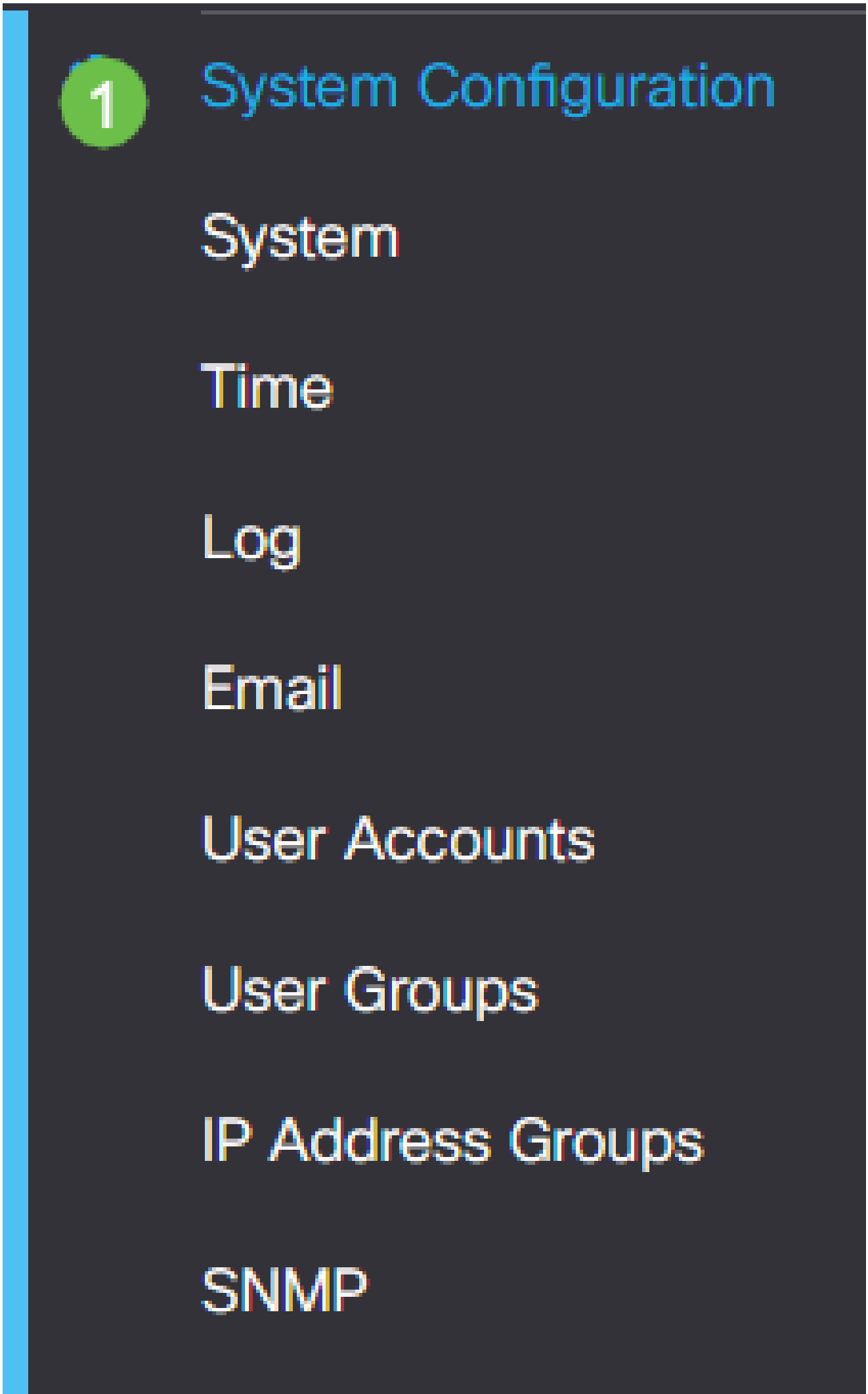


RV345Pシリーズルータでの自動更新の設定

更新は非常に重要であり、あなたは忙しい人なので、これから自動更新を設定することは理にかなっています！

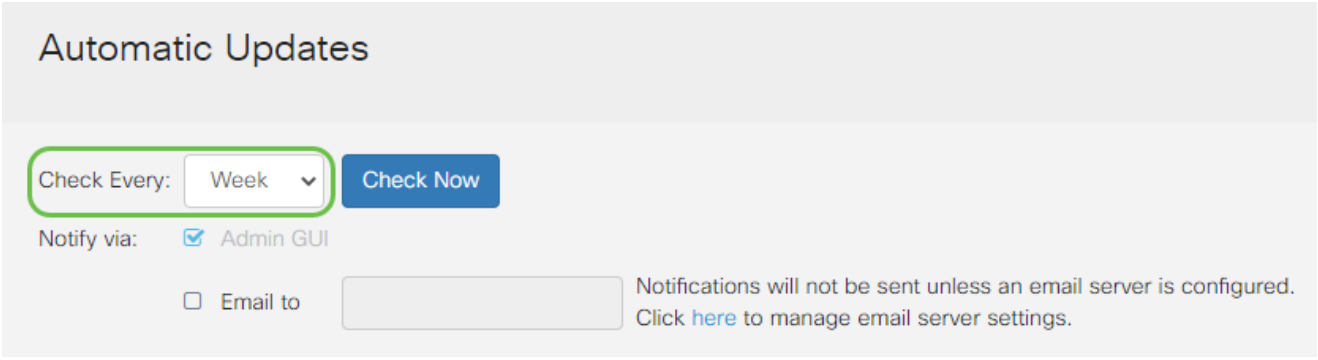
手順 1

Webベースのユーティリティにログインし、System Configuration > Automatic Updatesの順に選択します。


1
System Configuration
System
Time
Log
Email
User Accounts
User Groups
IP Address Groups
SNMP

手順 2

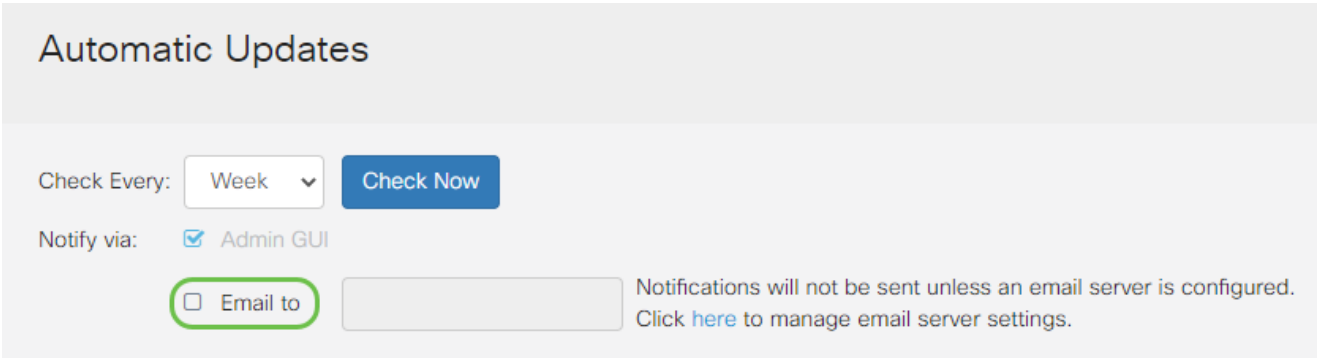
Check Everyドロップダウンリストから、ルータがアップデートをチェックする頻度を選択します。



手順 3

Eメールで更新情報を受信するには、Notify via領域でEmail toチェックボックスにチェックマークを入れます。Admin 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。アップデート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。

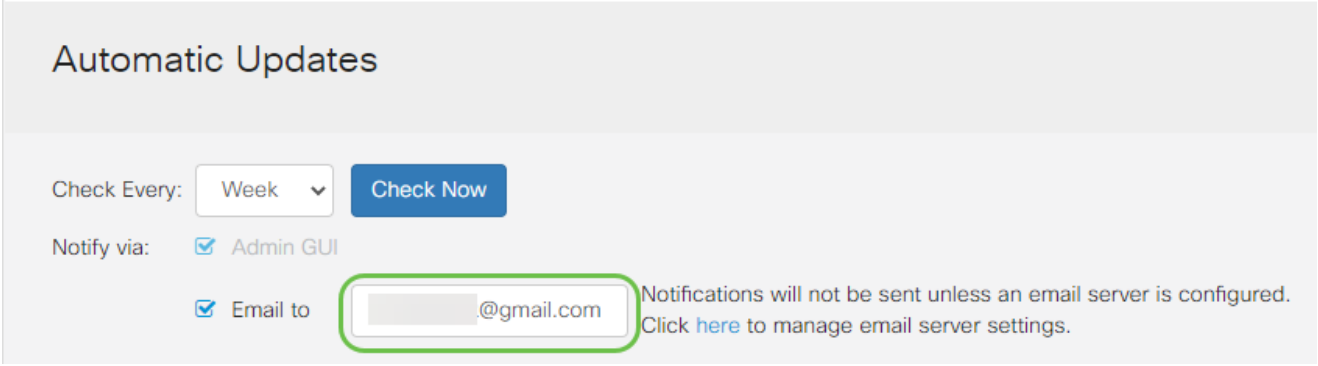
電子メールサーバの設定を設定する方法については、ここをクリックしてください。



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。

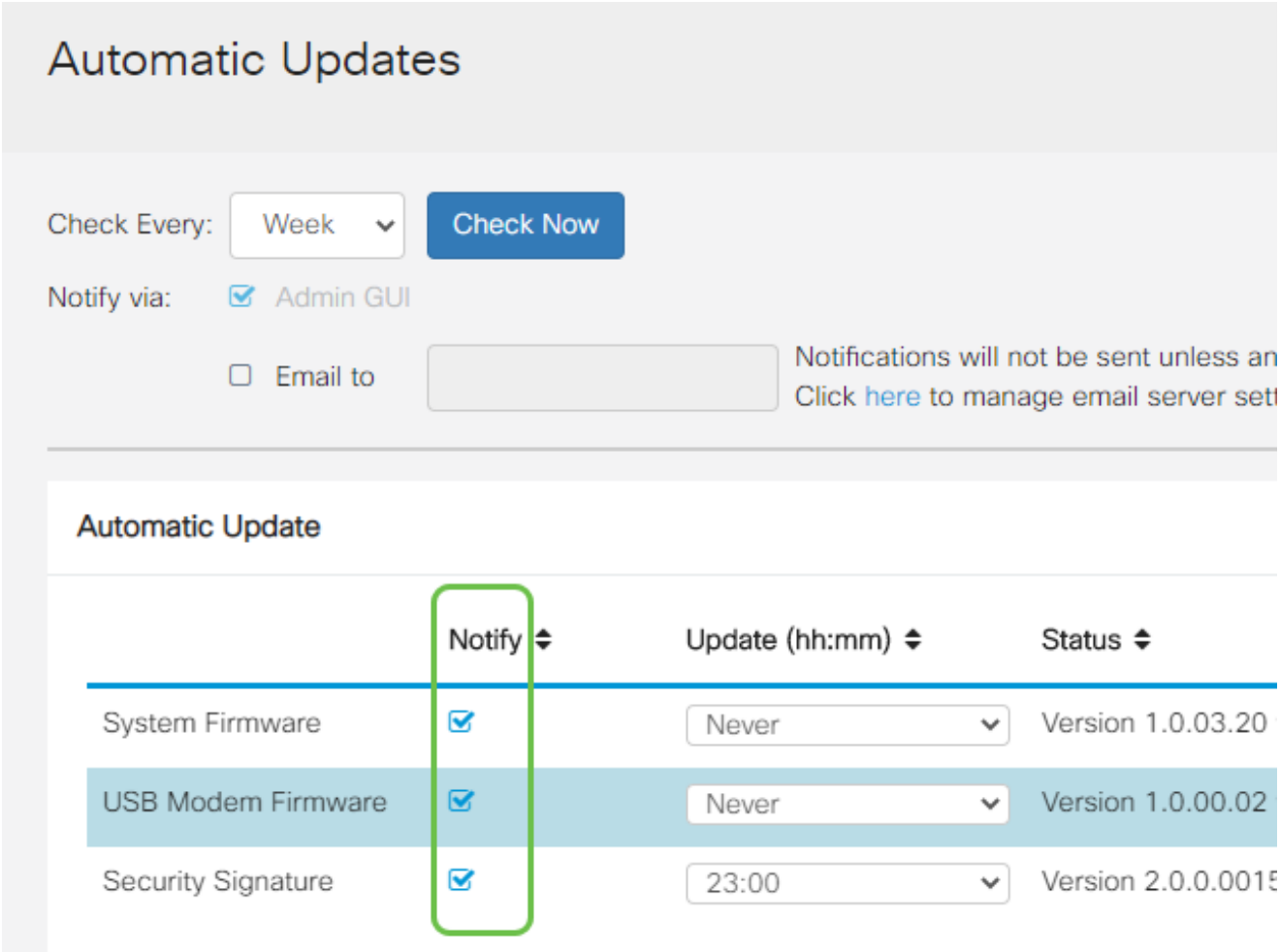
プライバシーを維持するために、個人の電子メールを使用する代わりに、別の電子メールアカウントを使用することを強くお勧めします。



手順 5

Automatically Update領域で、通知を受け取る更新の種類のNotifyチェックボックスにチェックマークを入れます。次のオプションがあります。

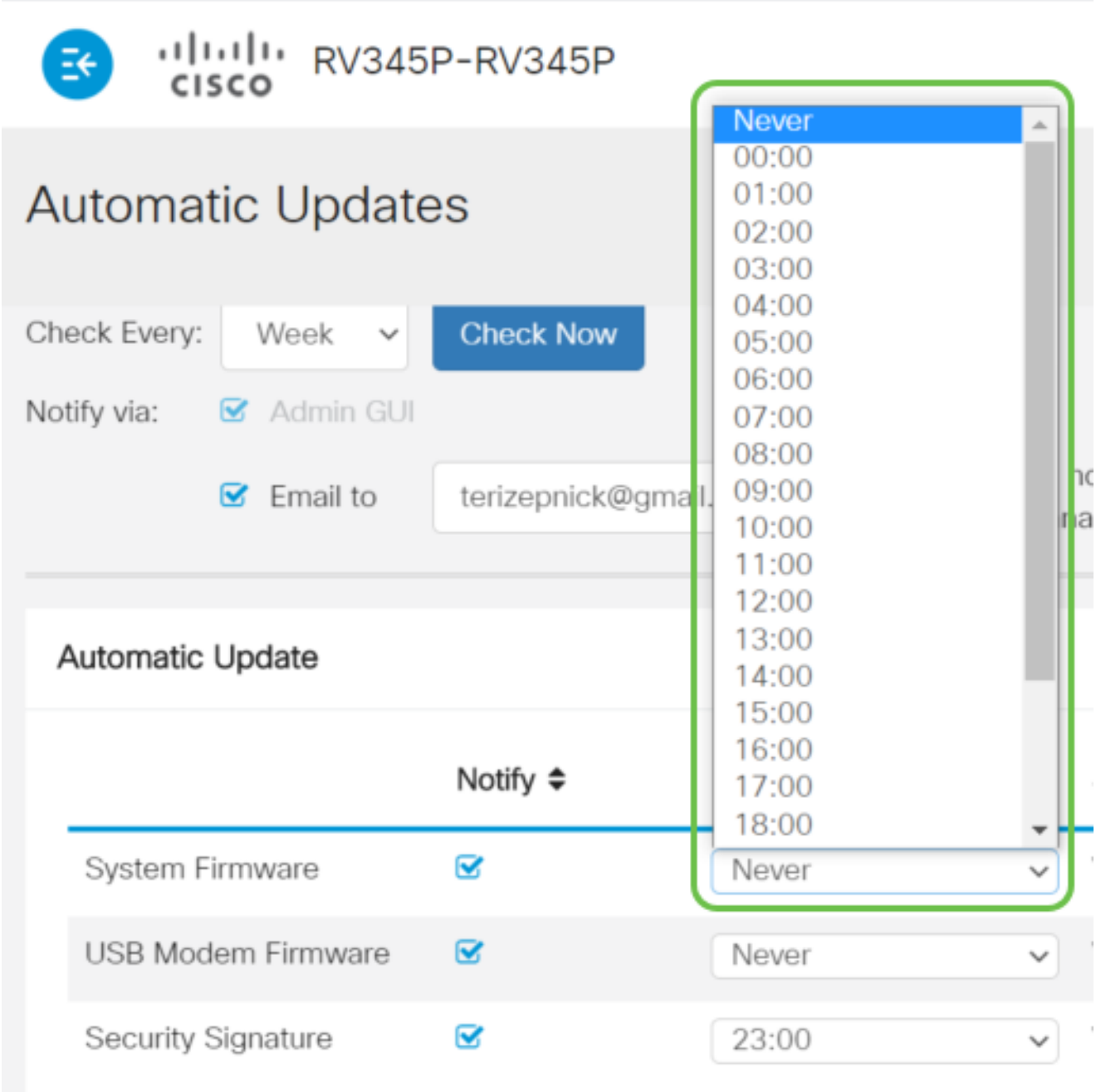
- システムファームウェア：デバイスのメイン制御プログラム。
- USBモデムファームウェア：USBポートの制御プログラムまたはドライバ。
- セキュリティシグニチャ：アプリケーション、デバイスタイプ、オペレーティングシステムなどを識別するアプリケーション制御のシグニチャが含まれます。



手順 6

Automatic Update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。一部

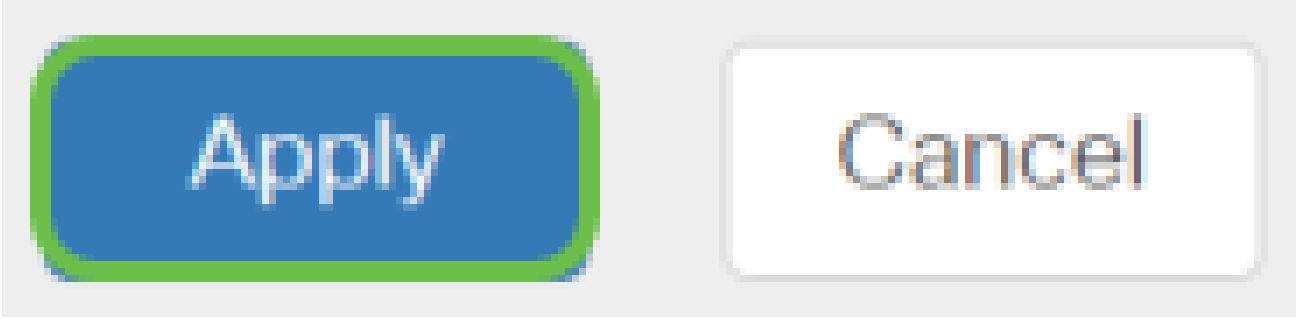
のオプションは、選択した更新プログラムの種類によって異なる場合があります。セキュリティシグニチャは、即時更新を行う唯一のオプションです。都合の悪い時間帯にサービスが中断されないように、オフィスが閉まっている時間を設定することをお勧めします。



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中のバージョンが表示されます。

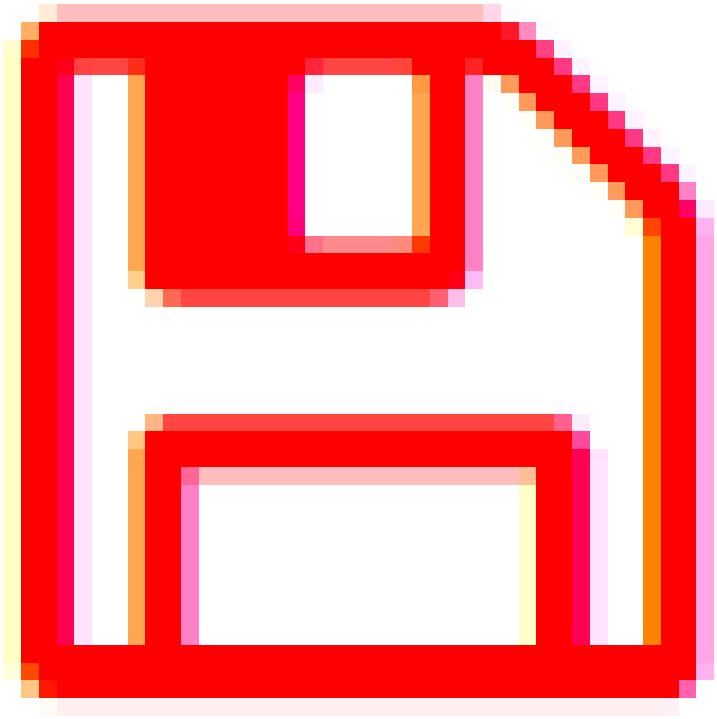
ステップ7

[APPLY] をクリックします。



手順 8

設定を永続的に保存するには、Copy/Save Configurationページに移動するか、ページの上部にあるsaveアイコンをクリックします。



素晴らしい、あなたのルータ上のあなたの基本的な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に保つ必要があります。複雑なパスワードを設定するなどの簡単なオプションがありますが、より安全なネットワークの手順を実行する場合は、セキュリティに関するこのセクションを参照してください。

RVセキュリティライセンス（オプション）

次の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、ログを検査し、幅広い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：アプリケーションをスキャンして、ルータを通過する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、IMAP電子メールの添付ファイルなどのさまざまなプロトコルを検出し、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によっ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、80を超えるカテゴリと4億5,000万以上のドメインが分類されています。
- アプリケーションの識別：インターネットアプリケーションを識別し、ポリシーを割り当てます。500の固有のアプリケーションが自動的に特定されます。
- クライアントの特定：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 Security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。

ライセンス付与されたセキュリティ機能は、90日間無料で試用できます。評価期間後もルータで高度なセキュリティ機能を引き続き使用するには、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 Security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。

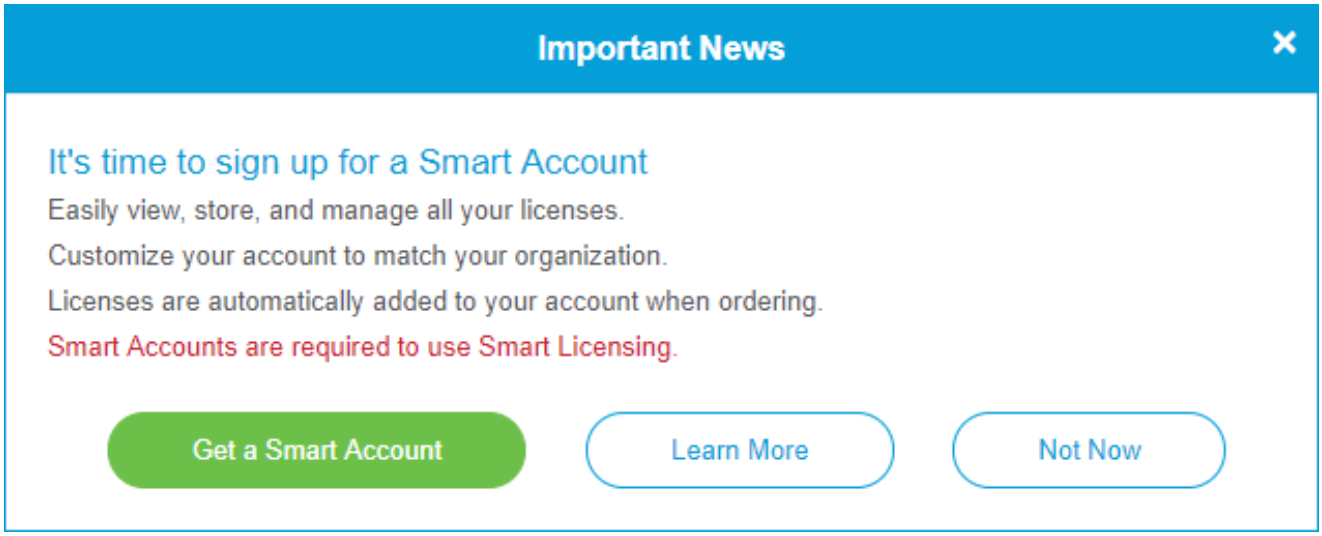
このスマートアカウントのアクティブ化を承認することにより、アカウントの作成、製品およびサービスの利用資格、ライセンス契約、組織の代理としてのアカウントへのユーザーアクセスの管理を行う権限が与えられていることに同意したことになります。シスコのパートナーは、お客様に代わってアカウントの作成を許可することはできません。

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、その時点からの管理はツー

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もの）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ていない場合は、クリックしてスマートアカウント作成ページに移動できます。Cisco.comアカウントの認証情報を使用してログインする必要があります。

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。

他の登録の詳細と一緒にアカウント名を必ずメモしてください。

ヒント：ドメインの入力が必要で、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応じてgmail、yahooなどです。

RV Security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持っていることが非常に重要です。

RV Security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、ここをクリックしてください。

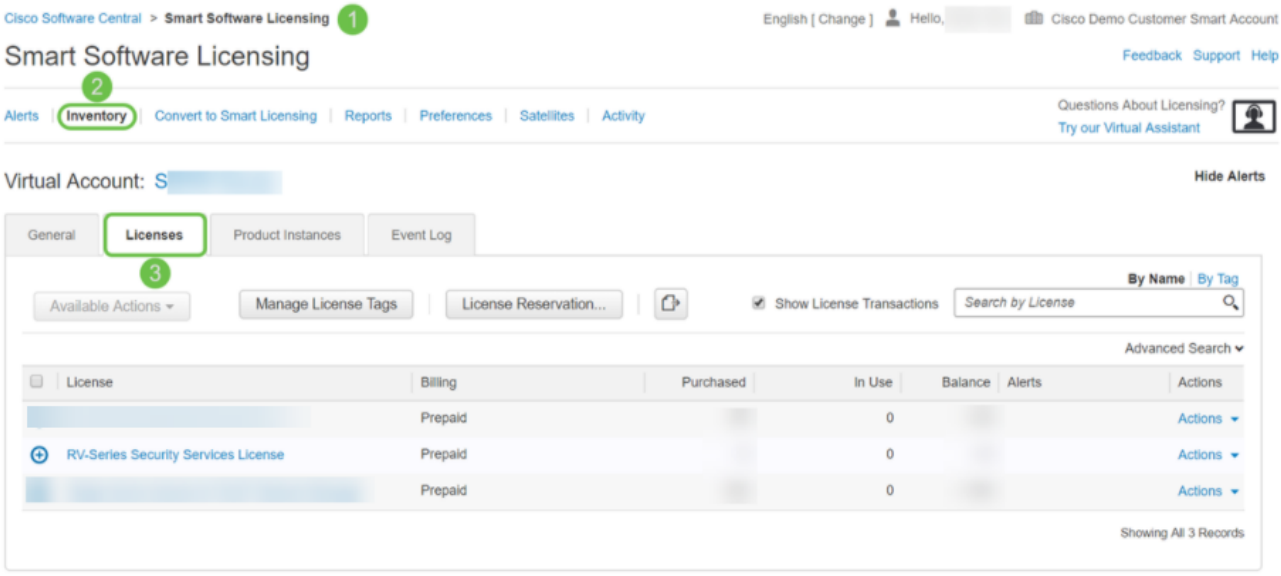
次の表に、ライセンスの製品番号を示します。

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年間：ダイナミックWebフィルタ、アプリケーションの可視性、クライアントの識別と統計情報、ゲートウェイウイルス対策、侵入防御システム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、パートナーがいつ注文を受け入れるか、リセラーがいつアカウントにライセンスをリンクするかによって異なります。通常は24 ~ 48時間です。

ライセンスがスマートアカウントにあることを確認

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。

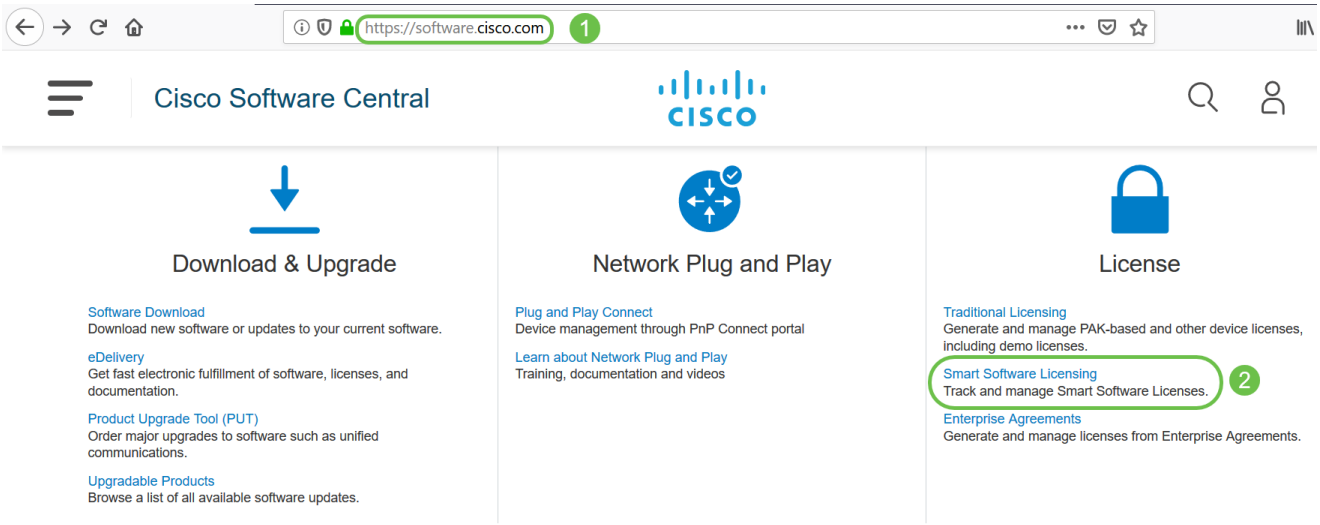


スマートアカウントにライセンスが表示されない場合は、シスコパートナーにお問い合わせください。

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

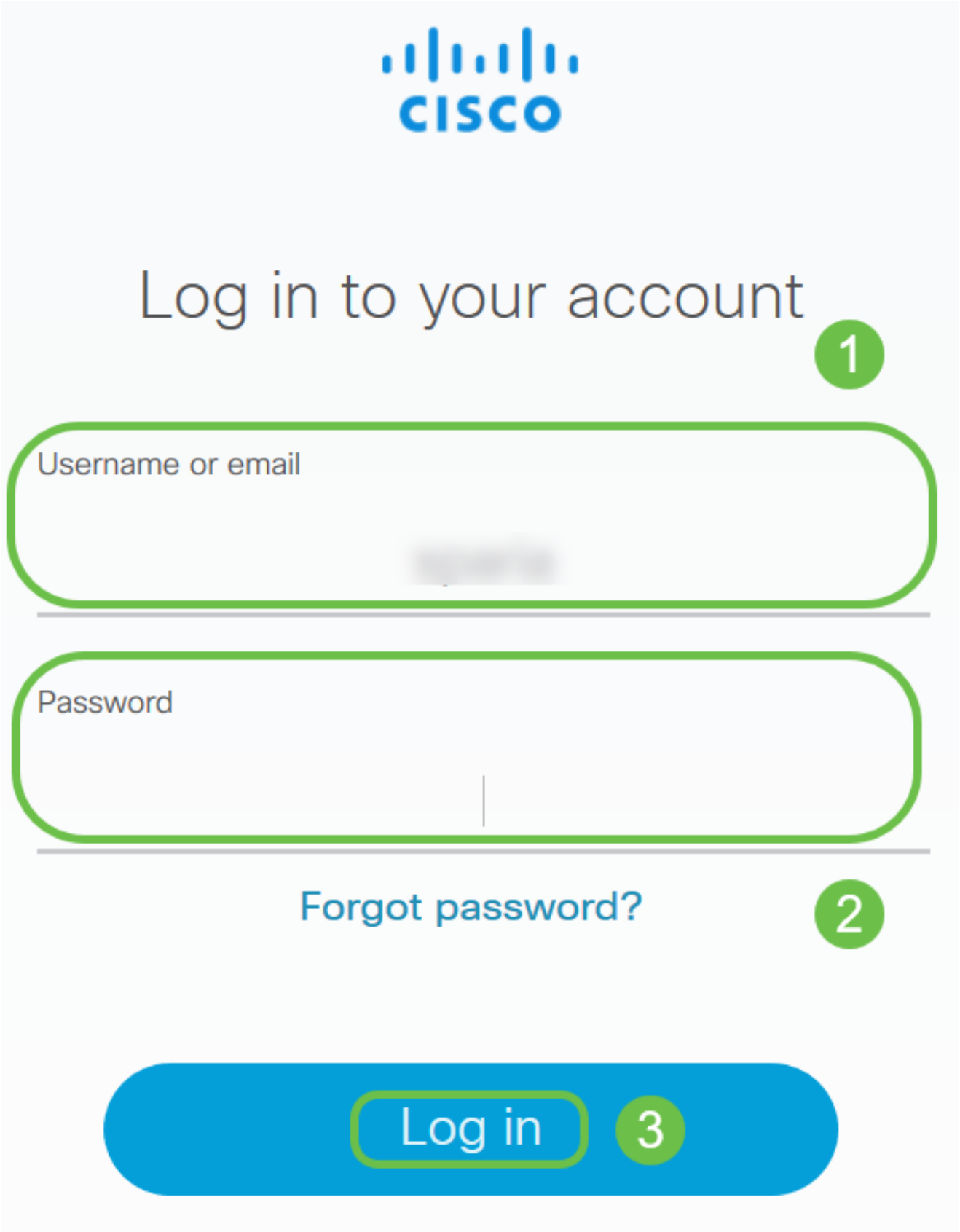
手順 1

Cisco Softwareにアクセスし、Smart Software Licensingに移動します。



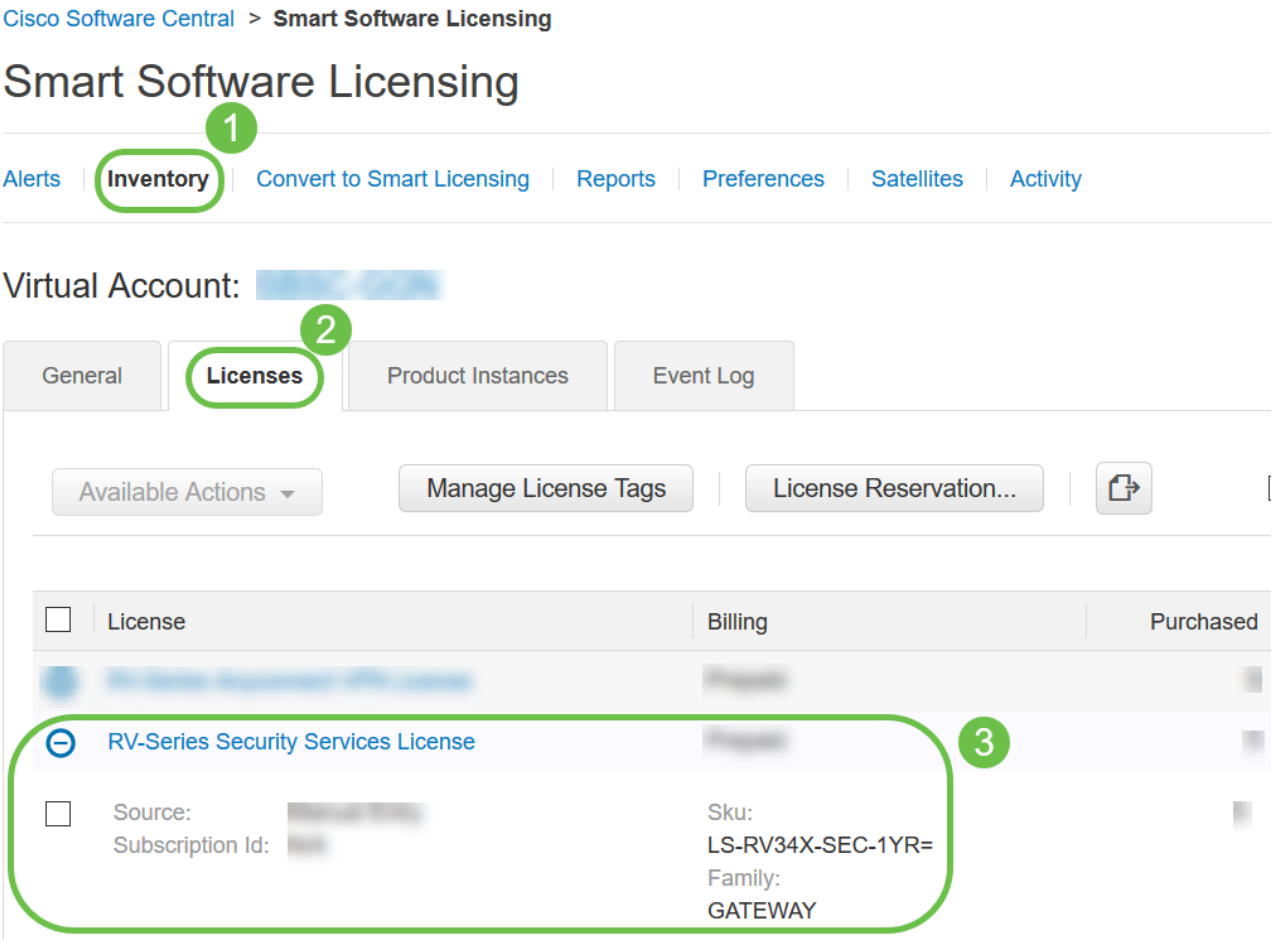
手順 2

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。



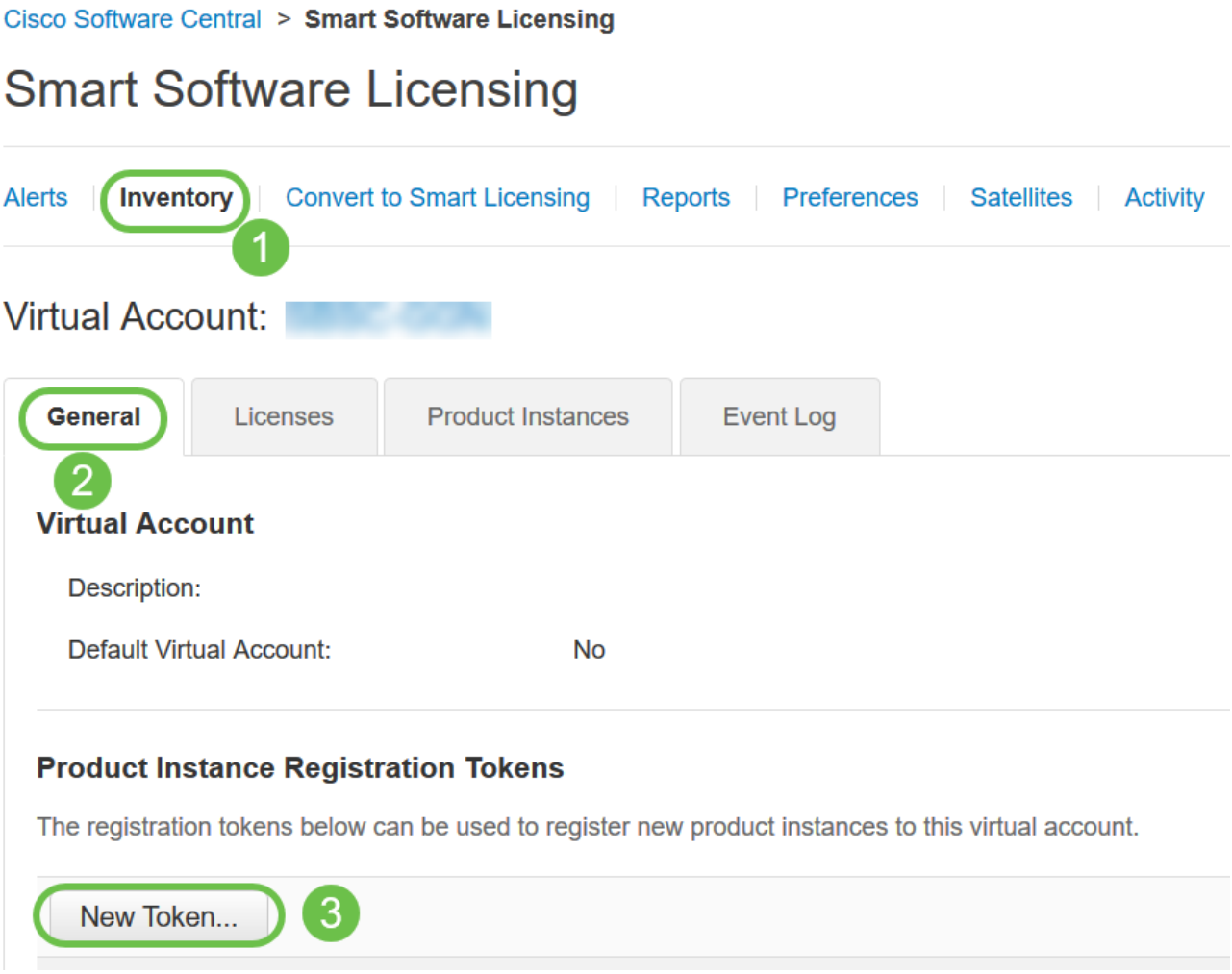
手順 3

Inventory > Licensesの順に移動し、スマートアカウントにRV-Series Security Services Licenseが表示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

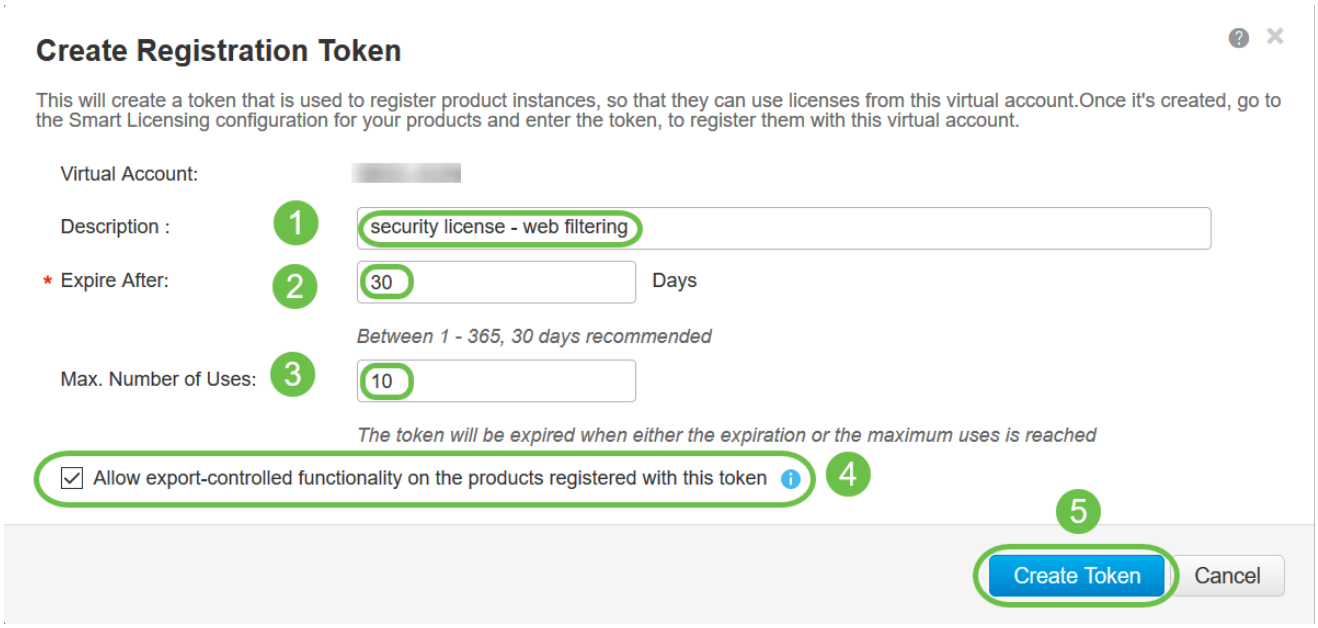
Inventory > Generalの順に移動します。Product Instance Registration TokensでNew Tokenをクリックします。



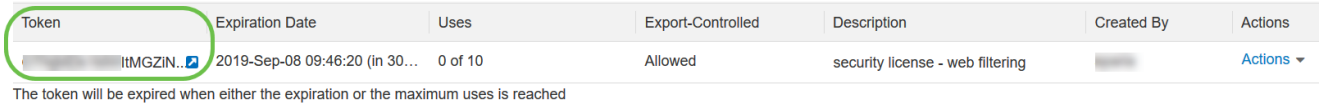
手順 5

Create Registration Tokenウィンドウが表示されます。Virtual Account領域には、登録トークンを作成す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。

- Description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、security license - web filteringと入力します。
- [有効期限]フィールドに、1 ～ 365日の範囲で値を入力します。このフィールドの値は30日を推奨しますが、必要に応じて値を編集できます。
- 最大で「使用回数」フィールド値を入力して、そのトークンを使用する回数を定義します。トークンは、日数または最大使用数に達すると期限切れになります。
- 仮想アカウント内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機能を有効にするには、[このトークンに登録されている製品でエクスポート制御機能を許可する]チェックボックスをオンにします。このトークンでエクスポート制御機能を使用できないようにするには、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、エクスポート制御機能に準拠している場合にのみ使用します。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。チェックボックスをオフにすると、このトークンを使用して登録された製品に対してこれらの機能が制限されます。違反は罰金と行政費用の対象となります。
- Create Tokenをクリックして、トークンを生成します。

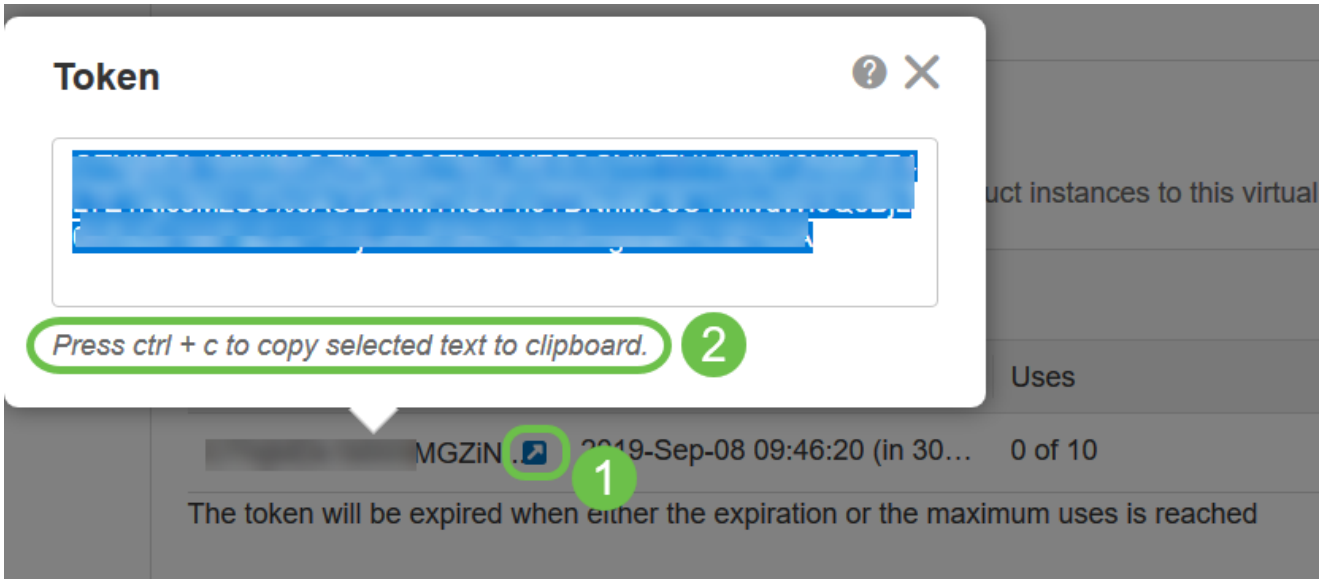


製品インスタンスの登録トークンが正常に生成されました。



手順 6

Token列の矢印アイコンをクリックして、トークンをクリップボードにコピーします。キーボードでctrl+cキーを押します。

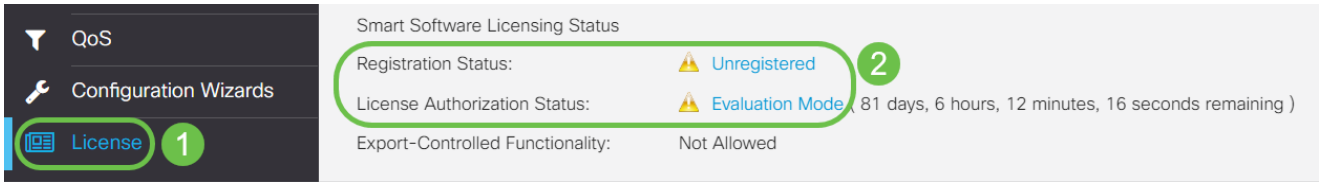


ステップ 7（オプション）

Actionsドロップダウンメニューをクリックし、Copyを選択してトークンをクリップボードにコピーするか、Download...を選択してトークンのコピー元となるテキストファイルのコピーをダウンロードします。

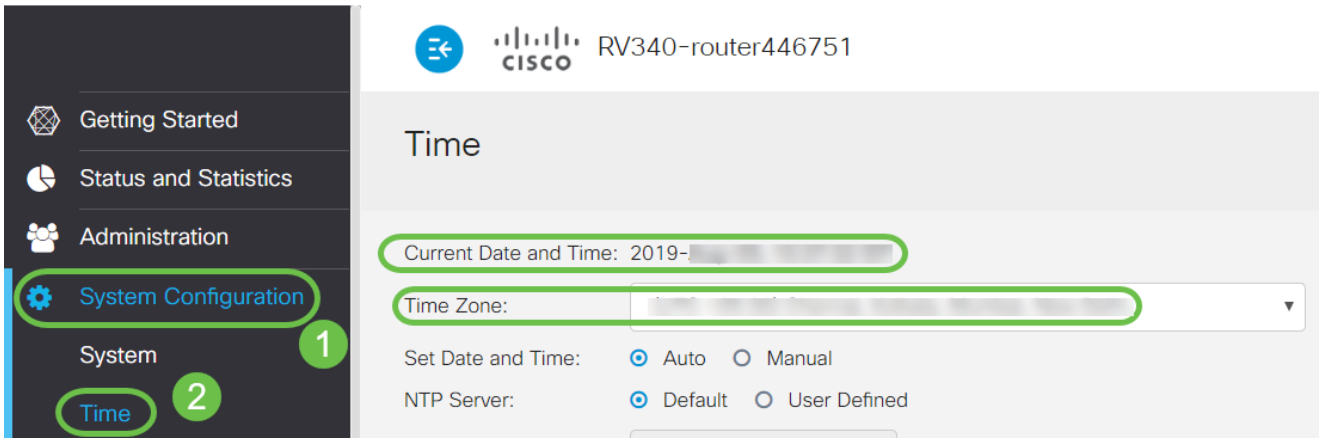
手順 8

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



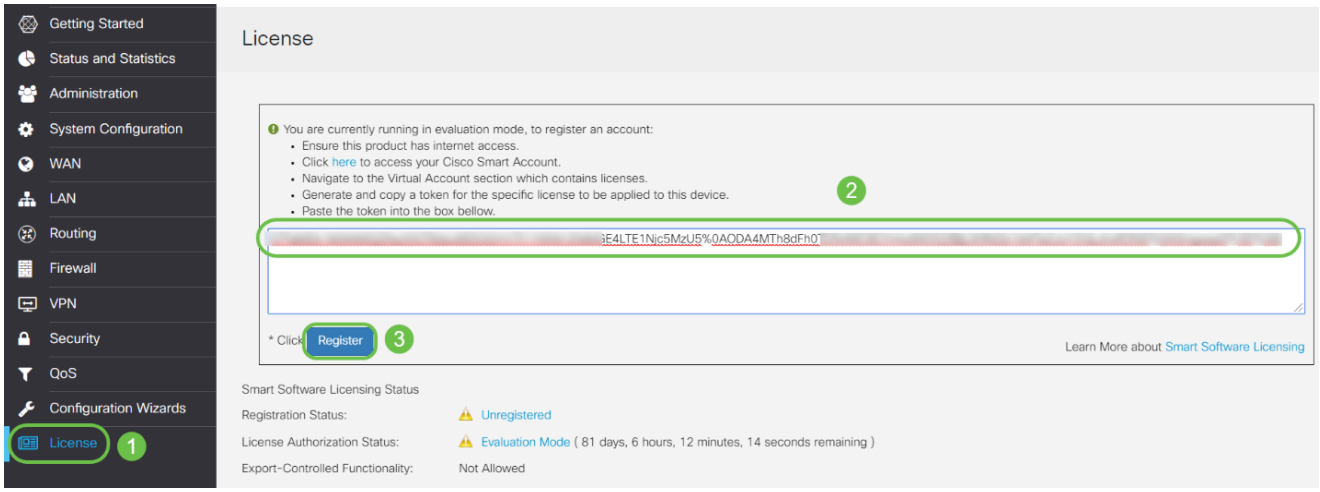
ステップ9

System Configuration > Timeの順に移動し、Current Date and TimeとTime Zoneがタイムゾーンに従って正しく反映されていることを確認します。



手順 10

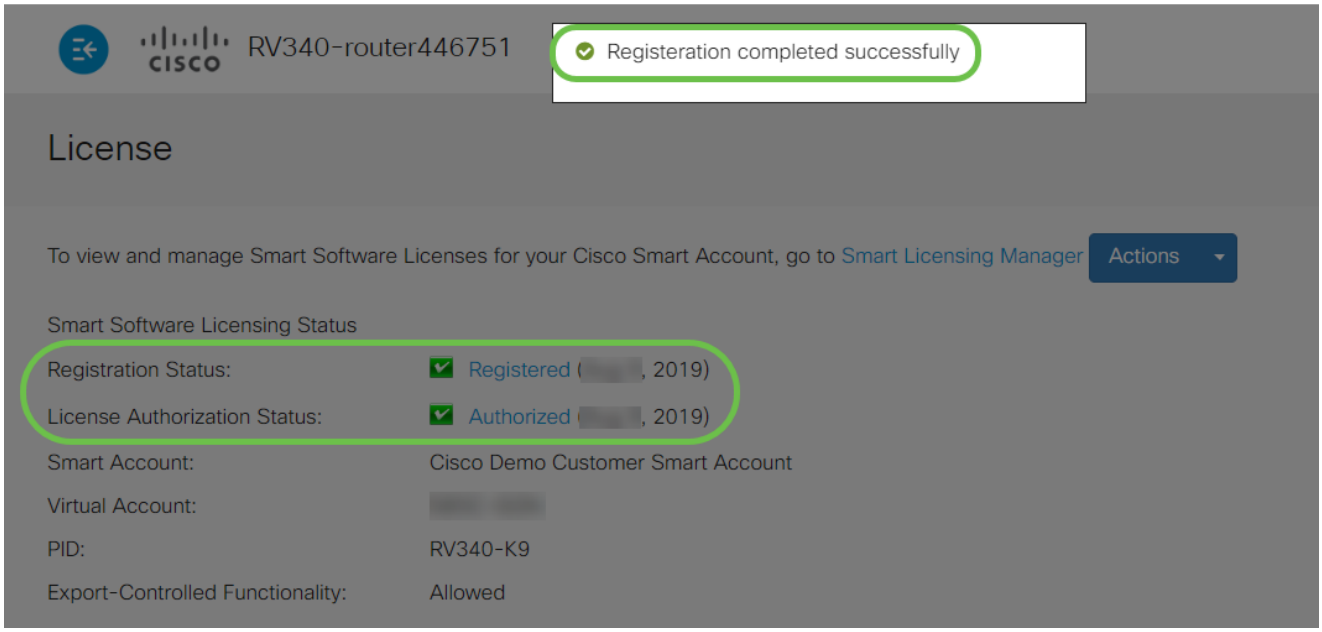
Licenseに移動します。ステップ6でコピーしたトークンをLicenseタブの下のテキストボックスに貼り付けます。このとき、キーボードでctrl + vキーを押します。[Register] をクリックします。



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への接続を試みるため、ページを離れないでください。

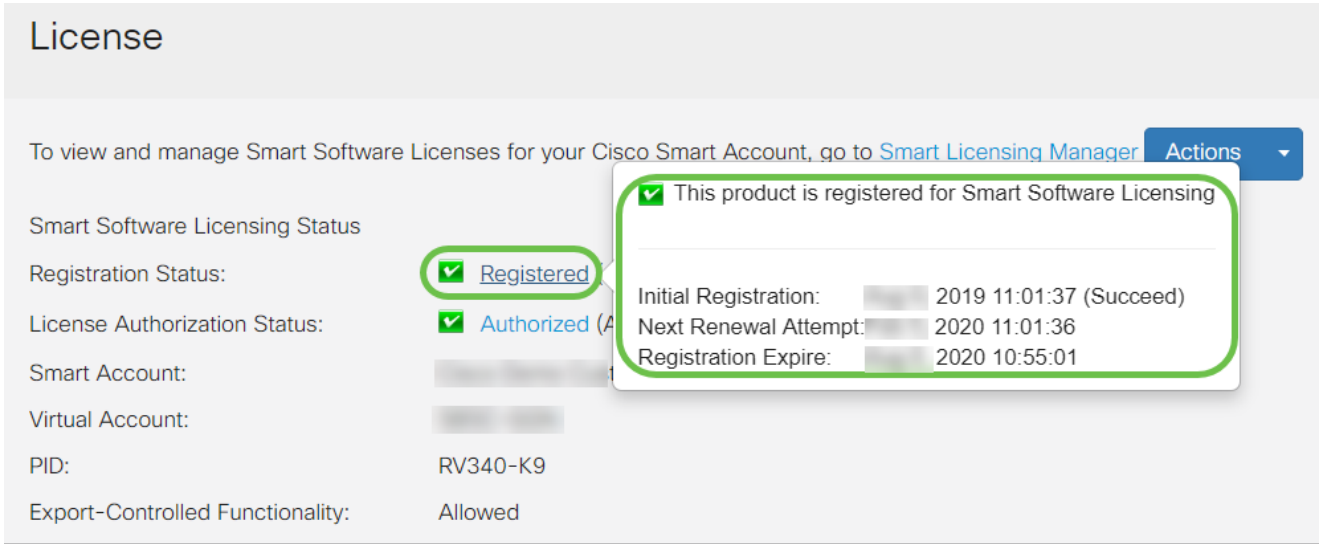
手順 11

これで、RV345Pシリーズルータがスマートライセンスに正常に登録され、認証されました。「Registration completed successfully」という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と表示されていることを確認できます。



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、ポインタを登録ステータスに合わせます。次の情報を含むダイアログメッセージが表示されます。

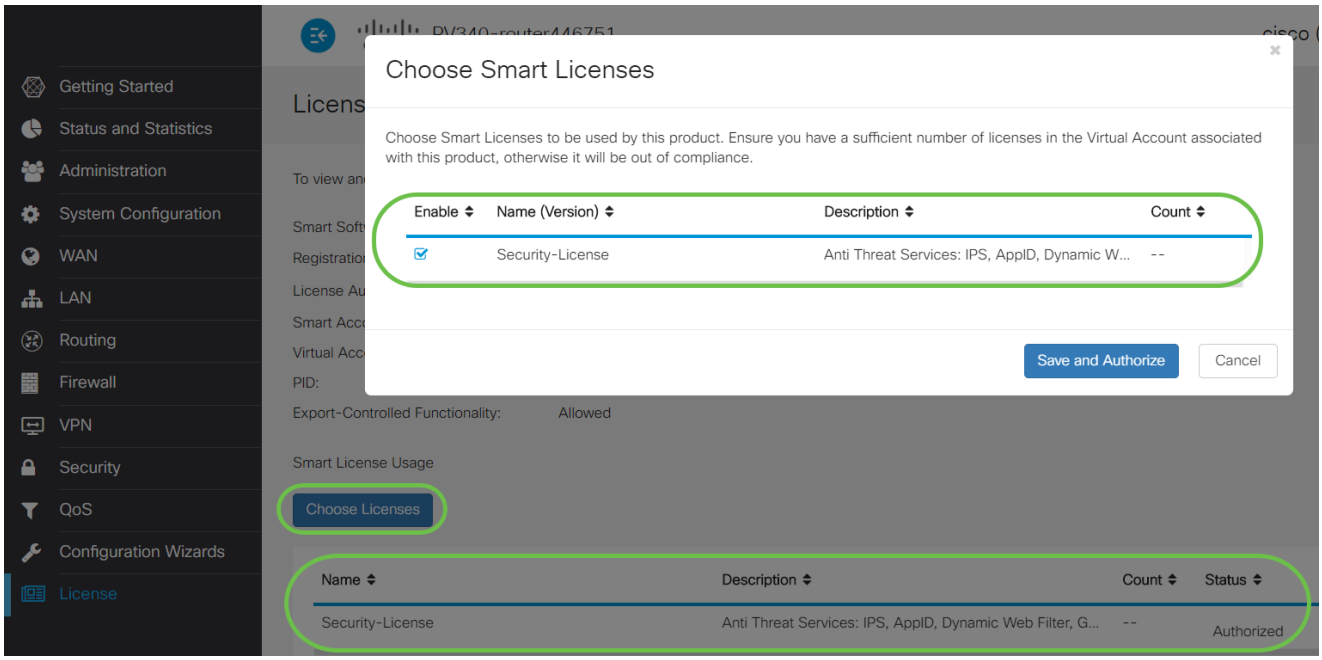


- Initial Registration：このエリアには、ライセンスが登録された日付と時刻が表示されます。
- Next Renewal Attempt：このエリアは、ルータがライセンスの更新を試行する日時を示します。
- Registration Expire：このエリアには、登録の有効期限が切れる日時が表示されます。

手順 13

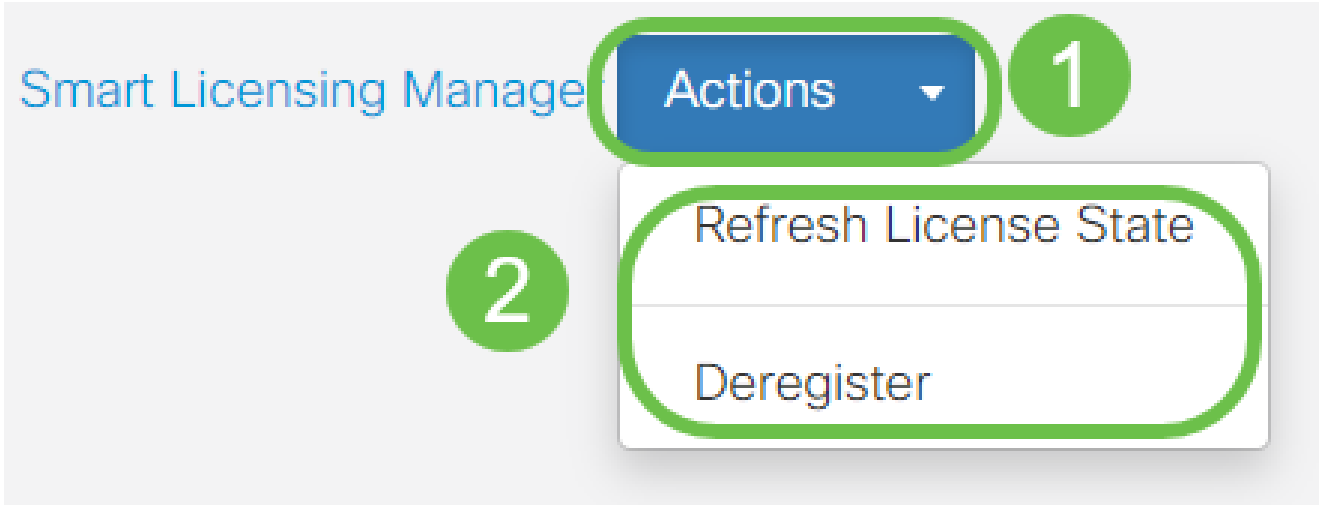
Licenseページで、Security-LicenseのステータスがAuthorizedになっていることを確認します。Choose Licenseボタンをクリックして、Security-Licenseが有効になっていることを確認することもできます。

この手順で問題が発生した場合は、ルータのリブートが必要になる場合があります。



手順 14（オプション）

ライセンスの状態を更新するか、ルータからライセンスを登録解除するには、Smart Licensing Managerの[アクション]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。



ルータのライセンスを取得したので、次のセクションの手順を実行する必要があります。

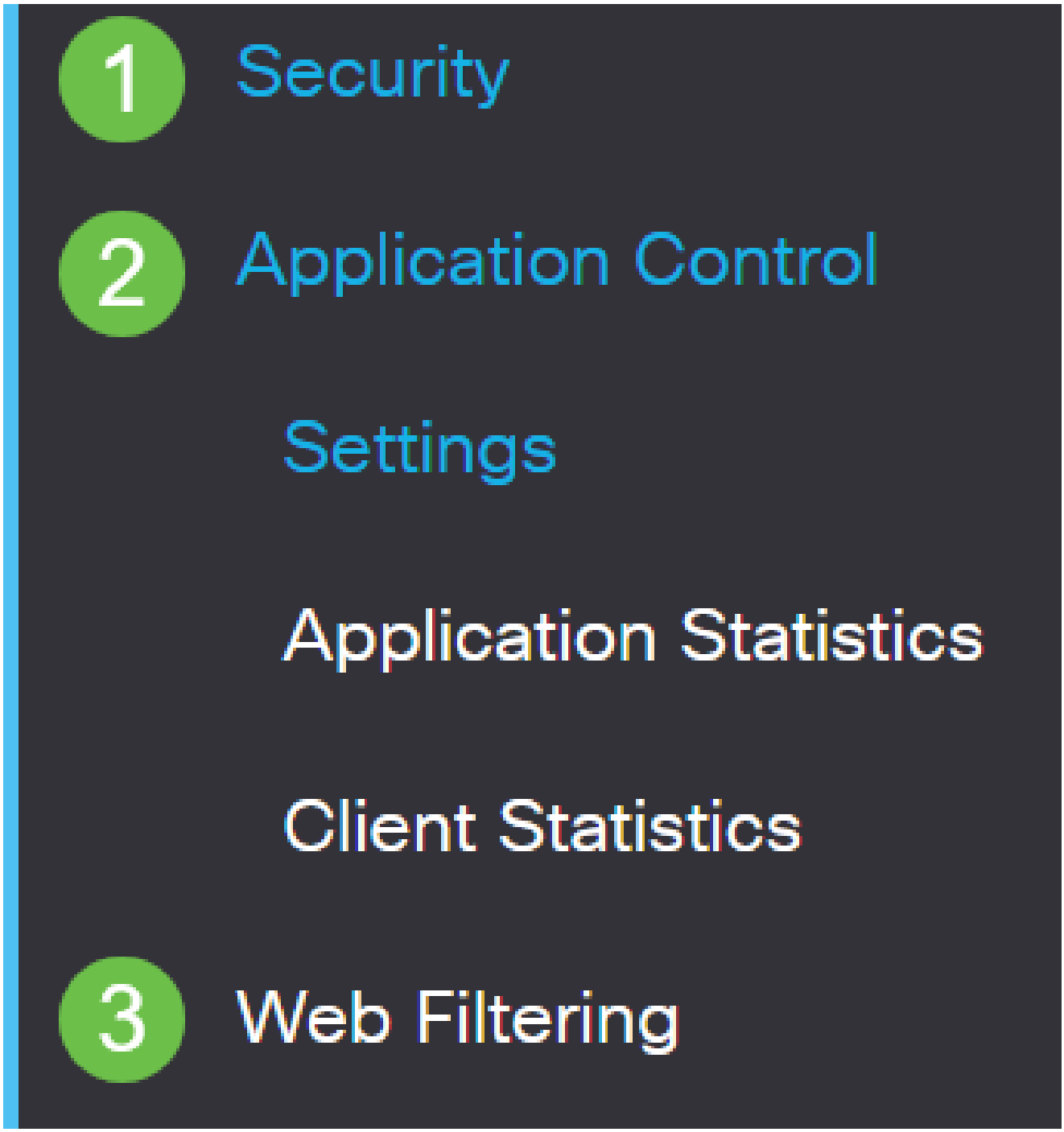
RV345Pルータでのwebフィルタリング

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

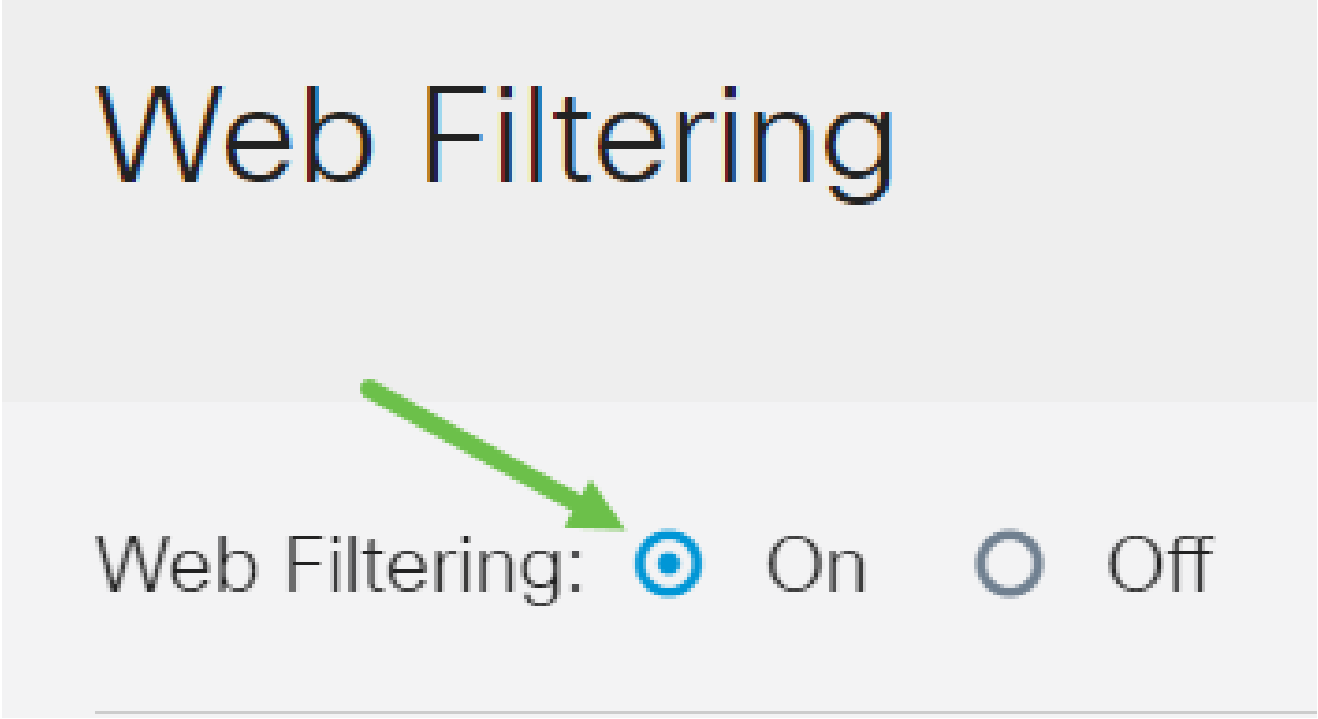
Webベースのユーティリティにログインし、Security > Application Control > Web

Filteringの順に選択します。



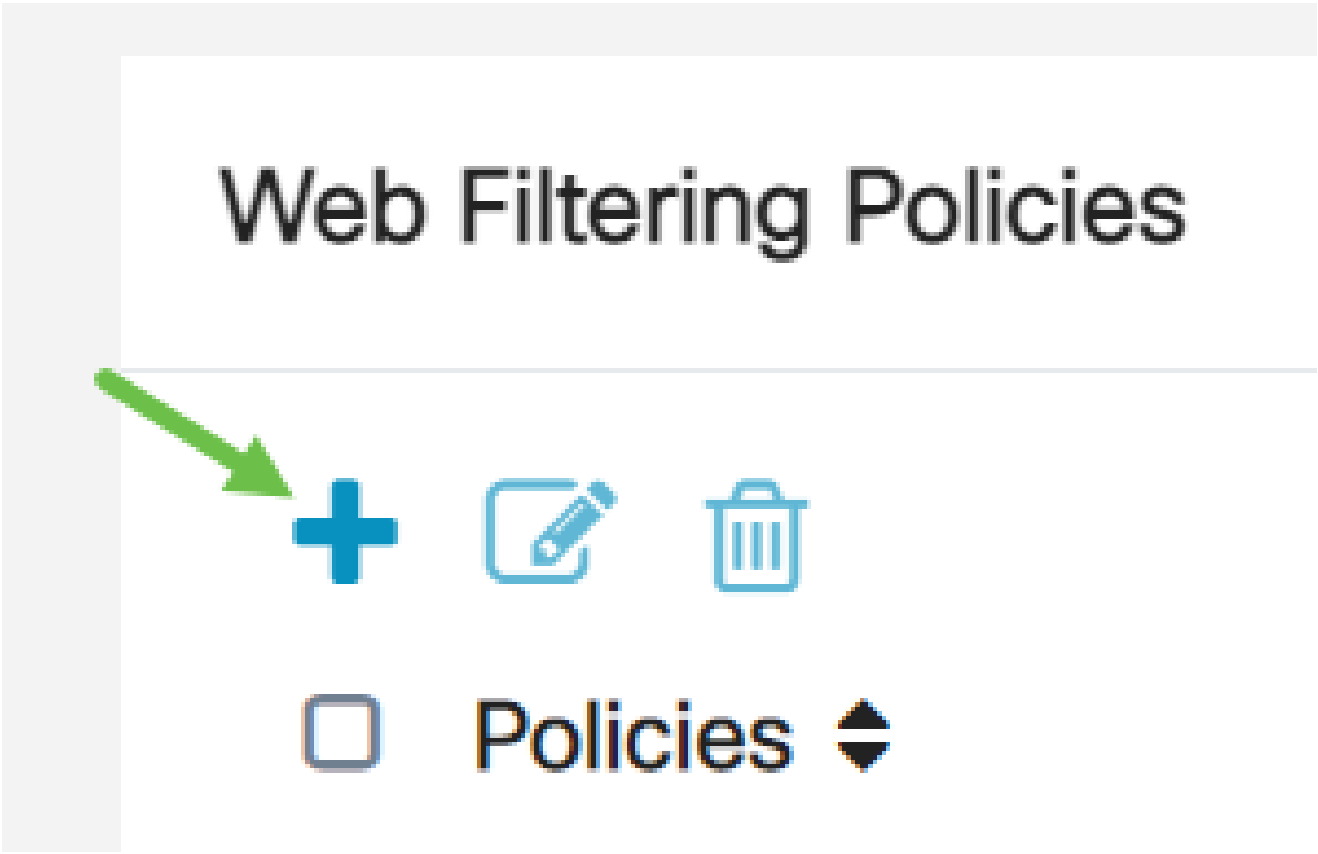
手順 2

Onオプションボタンを選択します。



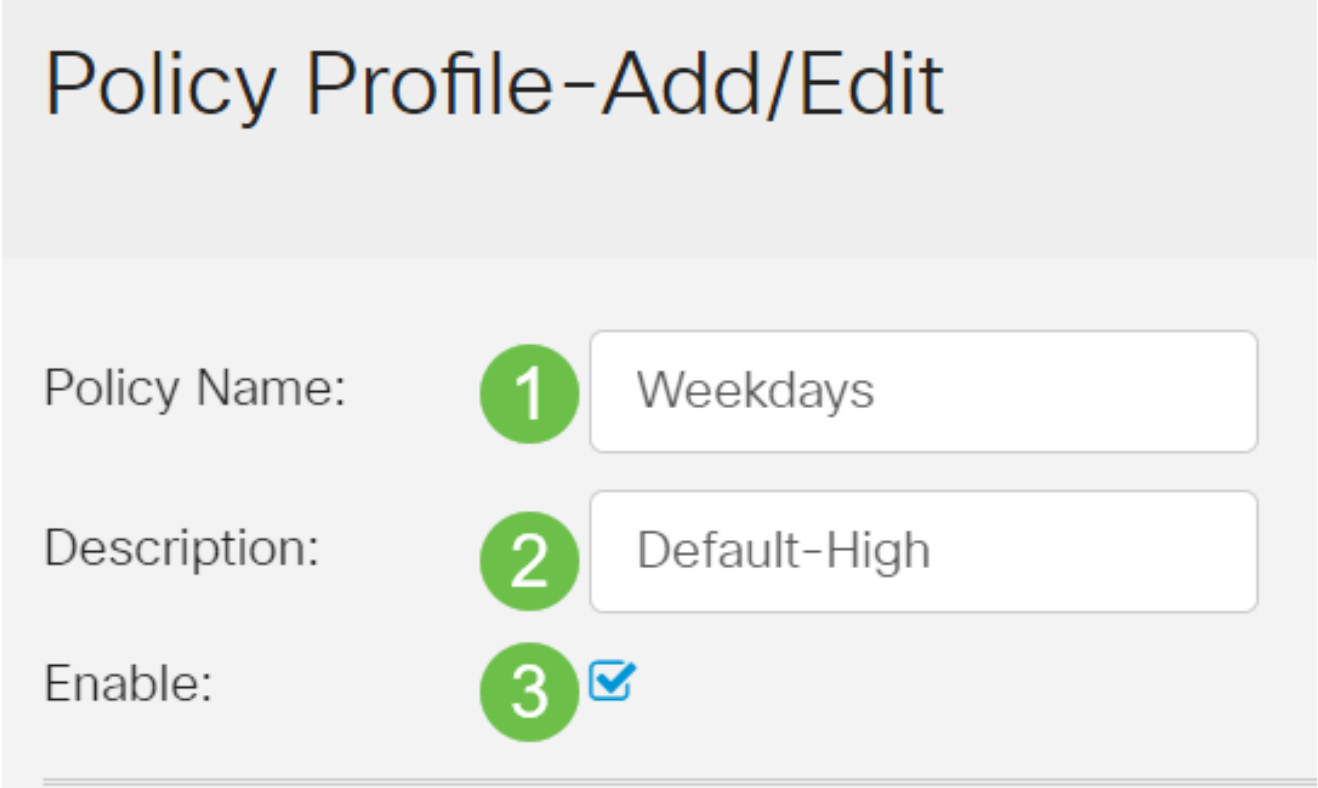
手順 3

addアイコンをクリックします。



手順 4

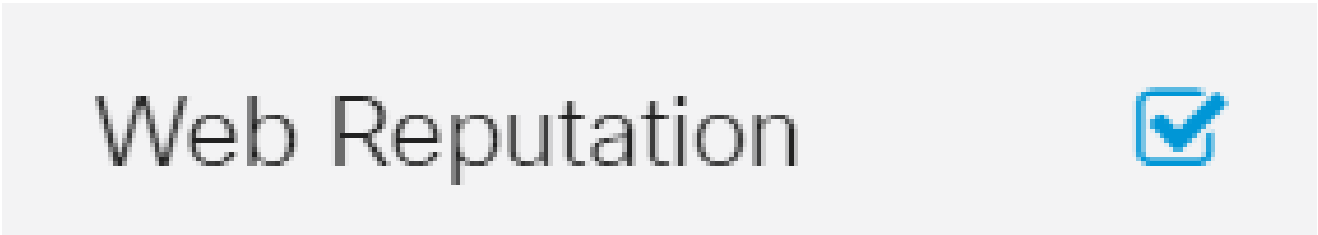
Policy Name、Description、およびEnableチェックボックスにチェックマークを付けます。



ルータでコンテンツフィルタリングが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をクリックして、設定を続行します。

手順 5

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するには、Web Reputationチェックボックスをオンにします。



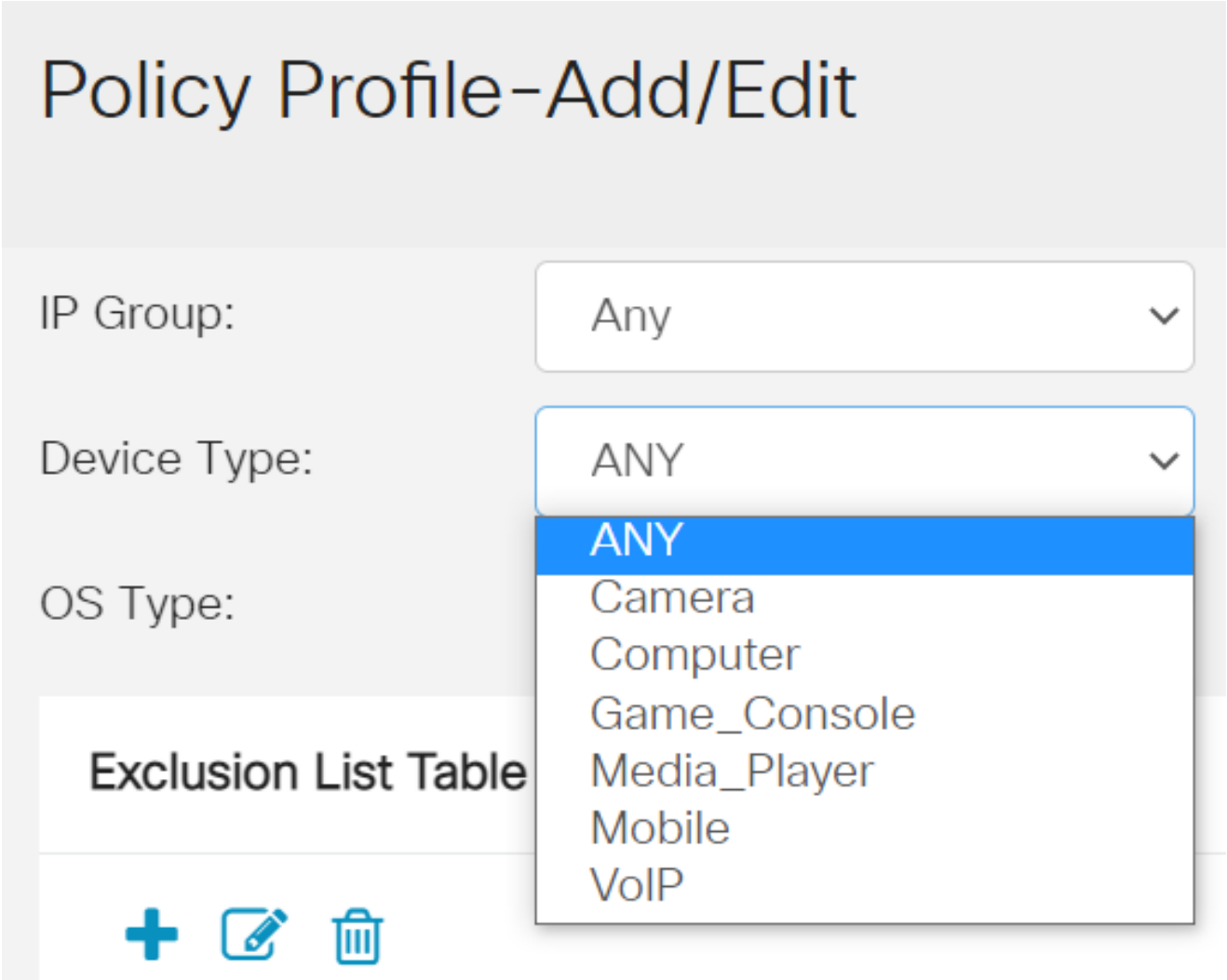
コンテンツは、Webレピュテーションインデックスに基づいて、WebサイトまたはURLの悪評に従ってフィルタリングされます。スコアが40を下回ると、Webサイトはブロックされます。Webレピュテーションテクノロジーの詳細については、 ここをクリックしてください。

手順 6

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場合に選択します。
- Camera：カメラ（IPセキュリティカメラなど）にポリシーを適用する場合に選択します。

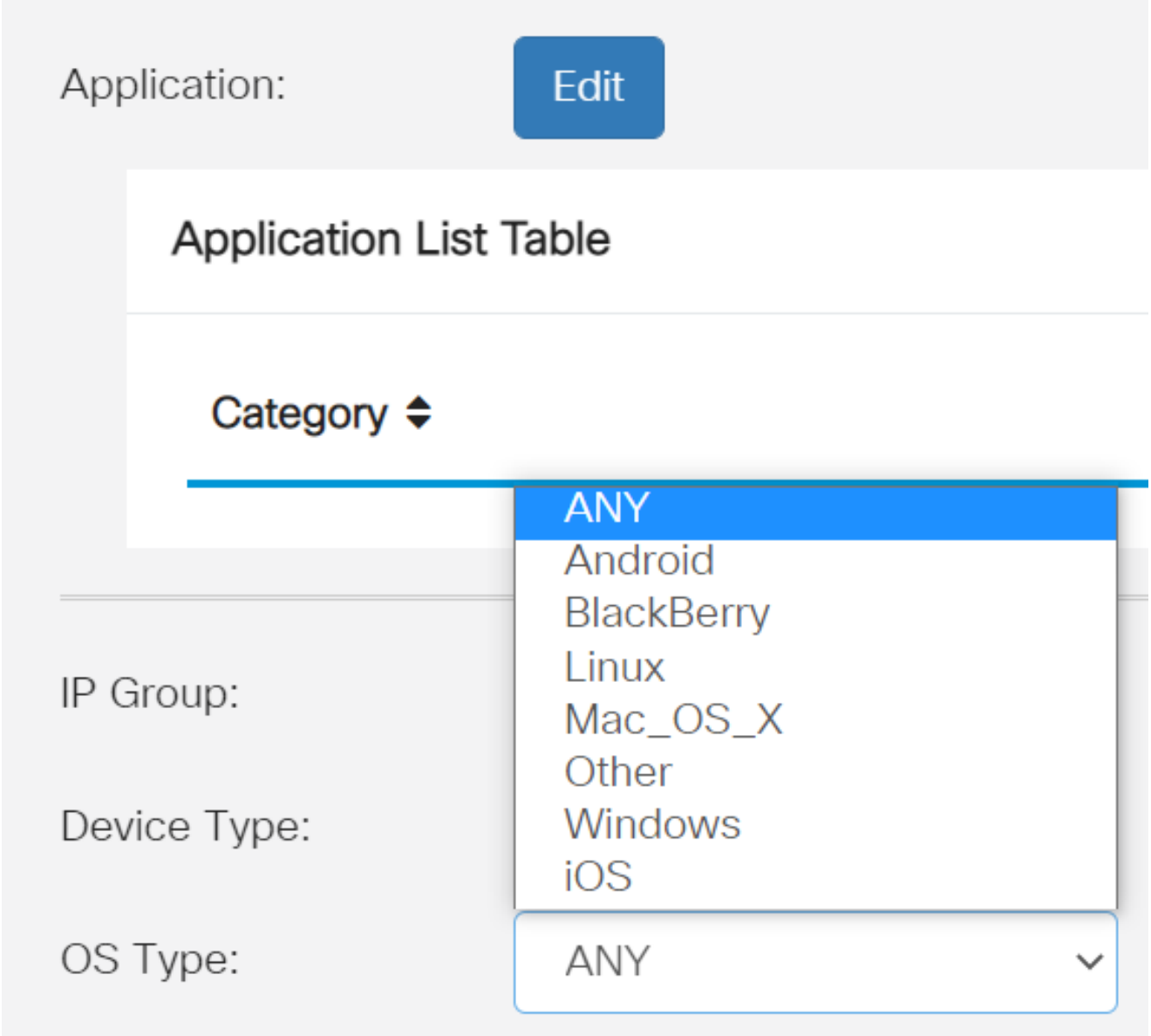
- [コンピューター] – コンピューターにポリシーを適用する場合に選択します。
- Game_Console：ゲームコンソールにポリシーを適用する場合に選択します。
- Media_Player：ポリシーをメディアプレーヤーに適用する場合に選択します。
- Mobile：モバイルデバイスにポリシーを適用する場合に選択します。
- VoIP:Voice over Internet Protocol(VoIP)デバイスにポリシーを適用する場合に選択します。



ステップ7

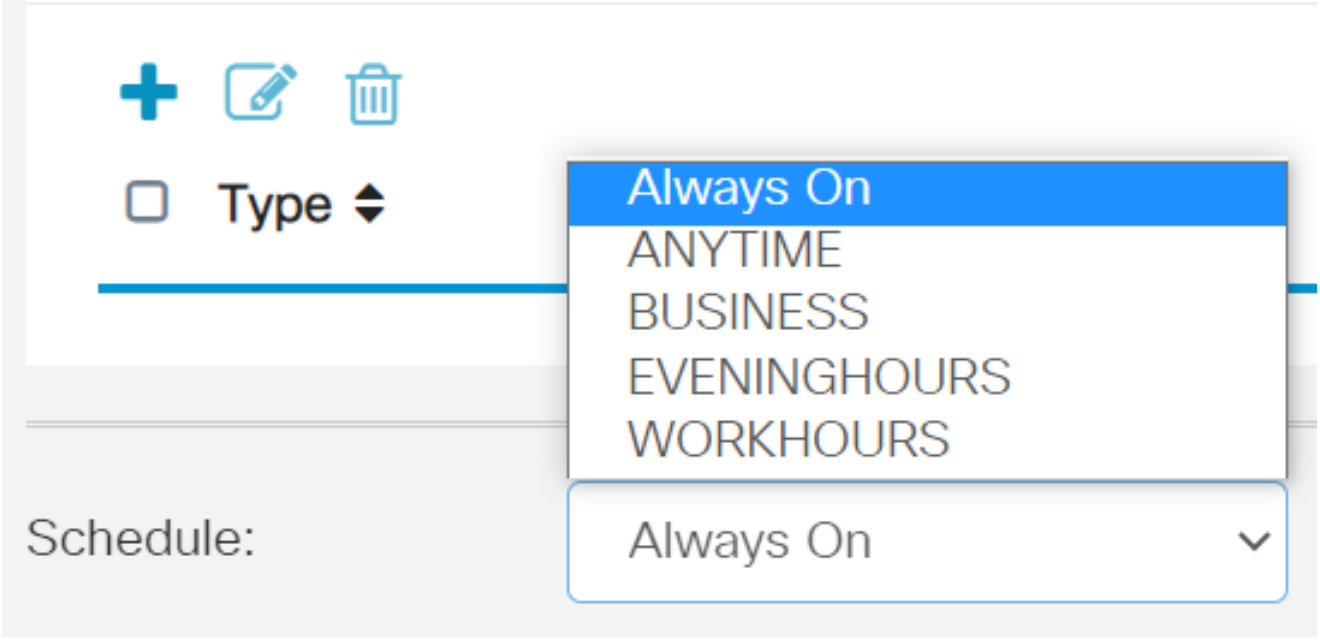
OS Typeドロップダウンリストから、ポリシーを適用するオペレーティングシステム(OS)を選択します。一度に選択できるオプションは1つだけです。次のオプションがあります。

- 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のみ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：ポリシーをLinux OSのみに適用します。
- Mac_OS_X:Mac OSだけにポリシーを適用します。
- 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。



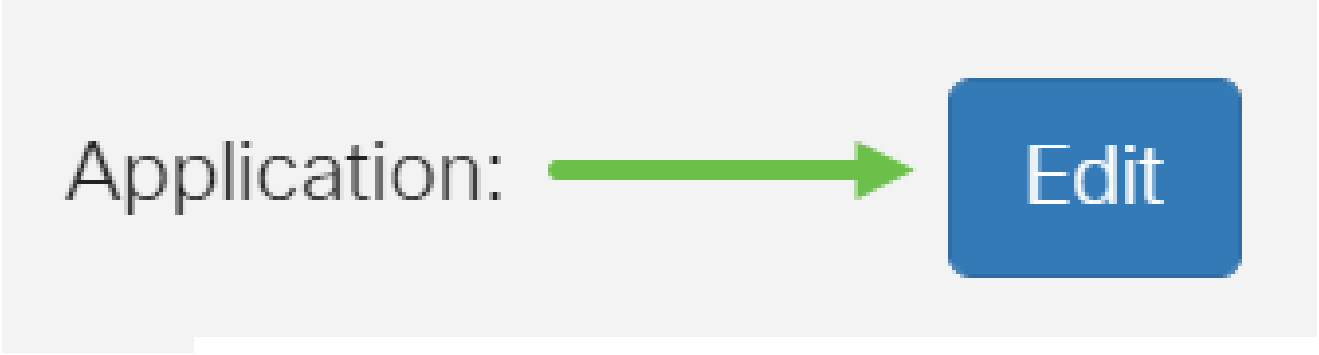
手順 8

Schedule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

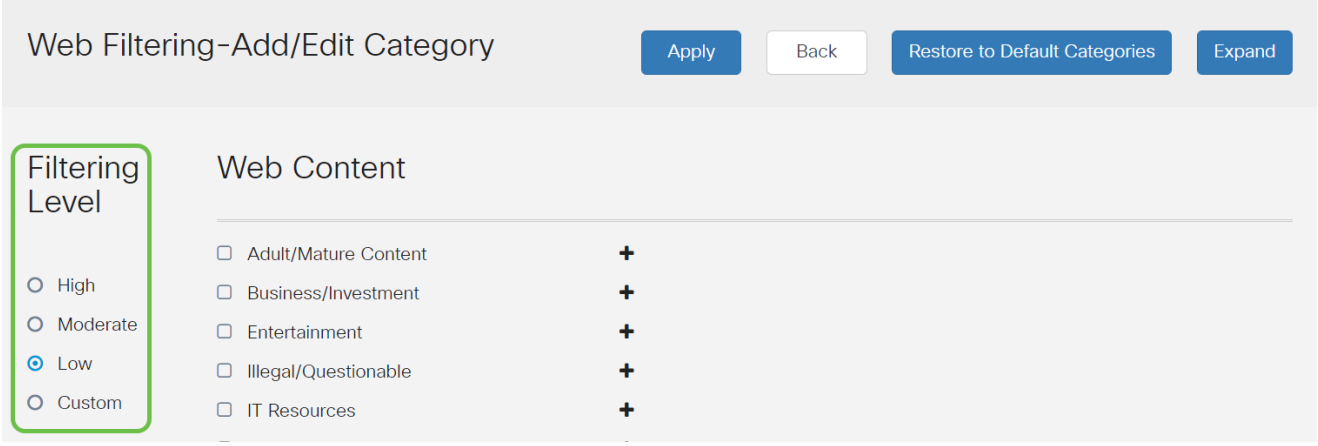
編集アイコンをクリックします。



手順 10

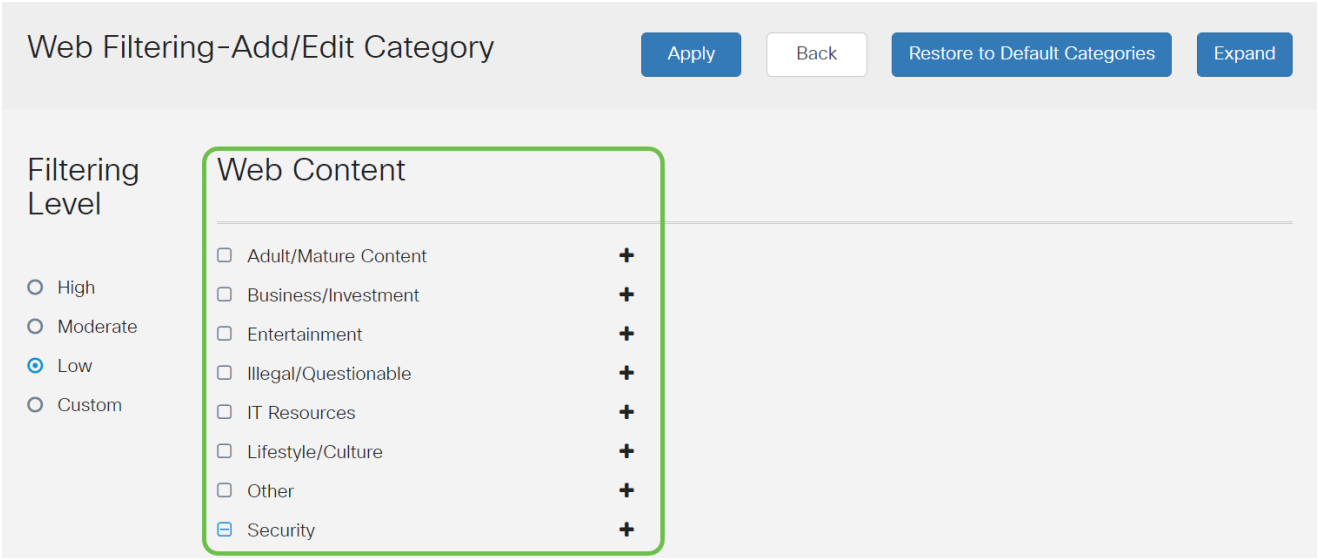
[Filtering Level]列で、オプションボタンをクリックして、ネットワークポリシーに最も適したフィルタリング範囲をすばやく定義します。オプションは、[高]、[中]、[低]、[カスタム]です。以下のフィルタリングレベルのいずれかをクリックすると、有効な各Webコンテンツカテゴリにフィルタリングされた事前定義された特定のサブカテゴリが表示されます。定義済みフィルタは、それ以上変更できず、グレー表示されます。

- Low：これはデフォルトオプションです。このオプションではセキュリティが有効になっています。
- Moderate：成人向け/成人向けコンテンツ、違法/要注意、およびセキュリティがこのオプションで有効になっています。
- 高：成人向け/成人向けコンテンツ、ビジネス向け/投資向けコンテンツ、違法性の疑わしいコンテンツ、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。
- Custom：ユーザ定義のフィルタを許可するデフォルトは設定されていません。



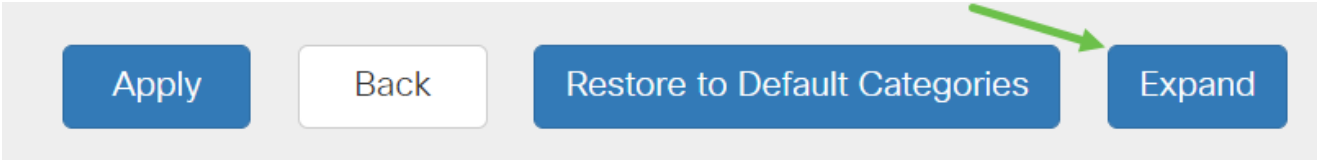
手順 11

フィルタリングする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、プラスアイコンをクリックします。



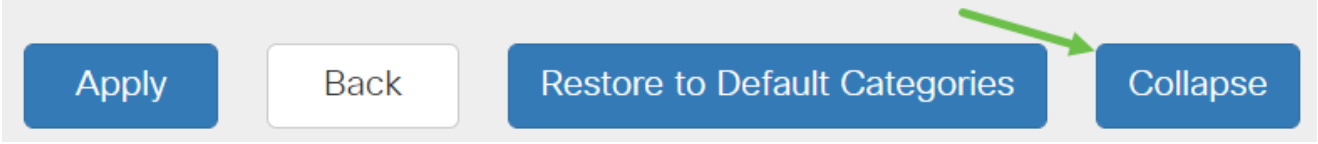
手順 12（オプション）

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



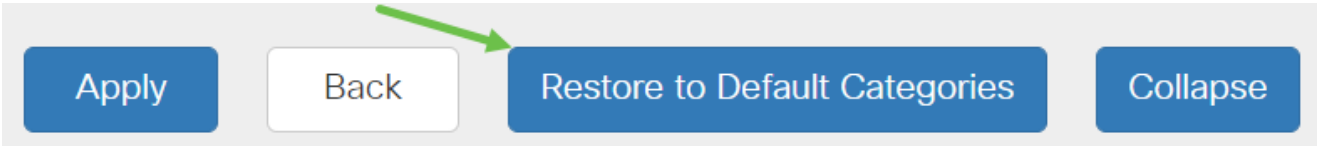
手順 13（オプション）

サブカテゴリと説明を折りたたむには、[折りたたむ]をクリックします。



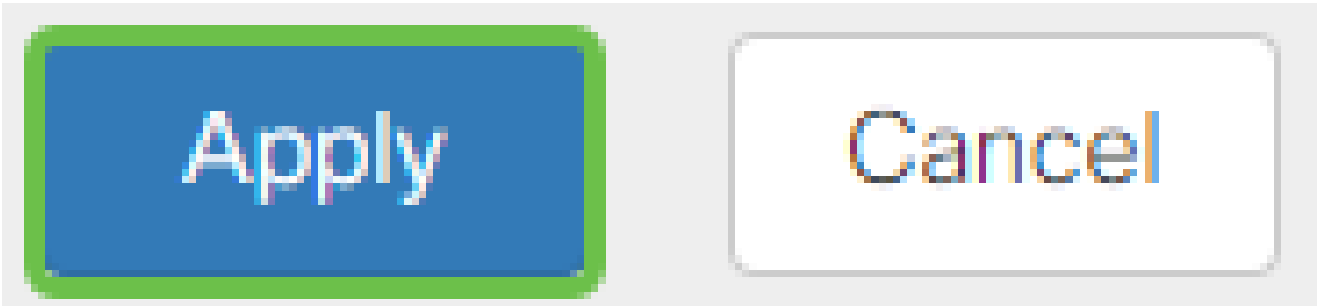
手順 14（オプション）

デフォルトのカテゴリに戻るには、Restore to Default Categoriesをクリックします。



手順 15

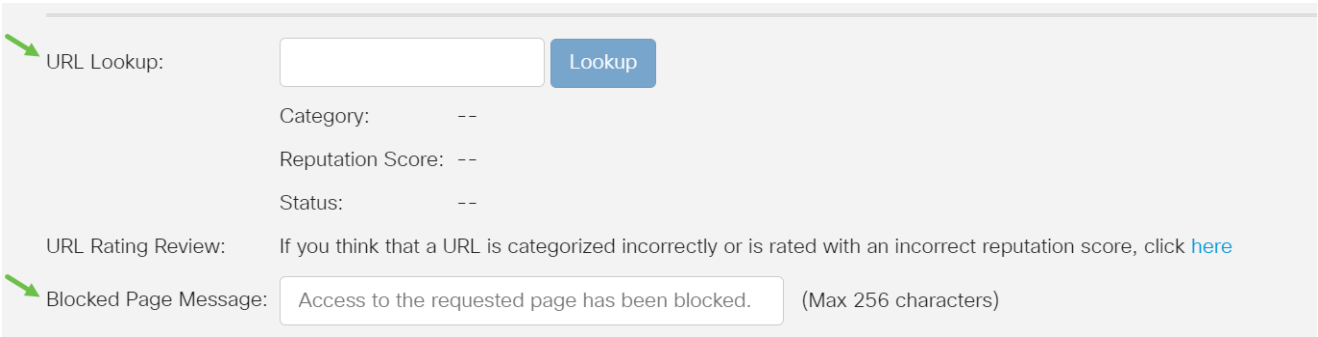
Applyをクリックして設定を保存し、Filterページに戻って設定を続行します。



アプリケーションリストテーブルには、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表示されます。

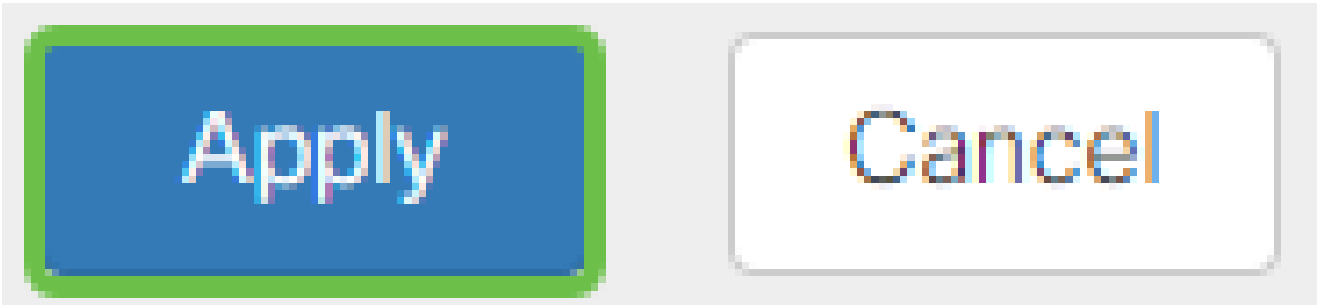
手順 16（オプション）

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。



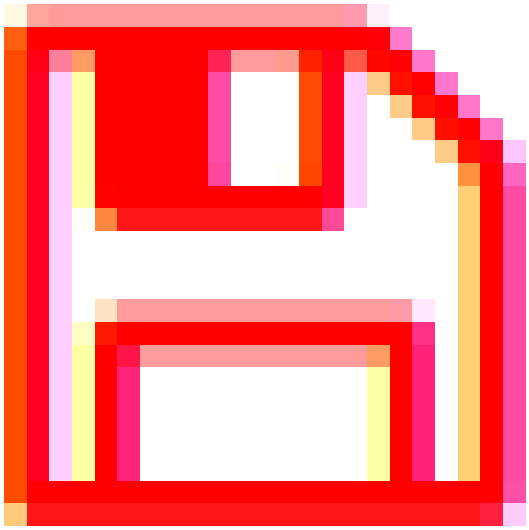
手順 17（オプション）

[APPLY] をクリックします。



手順 18

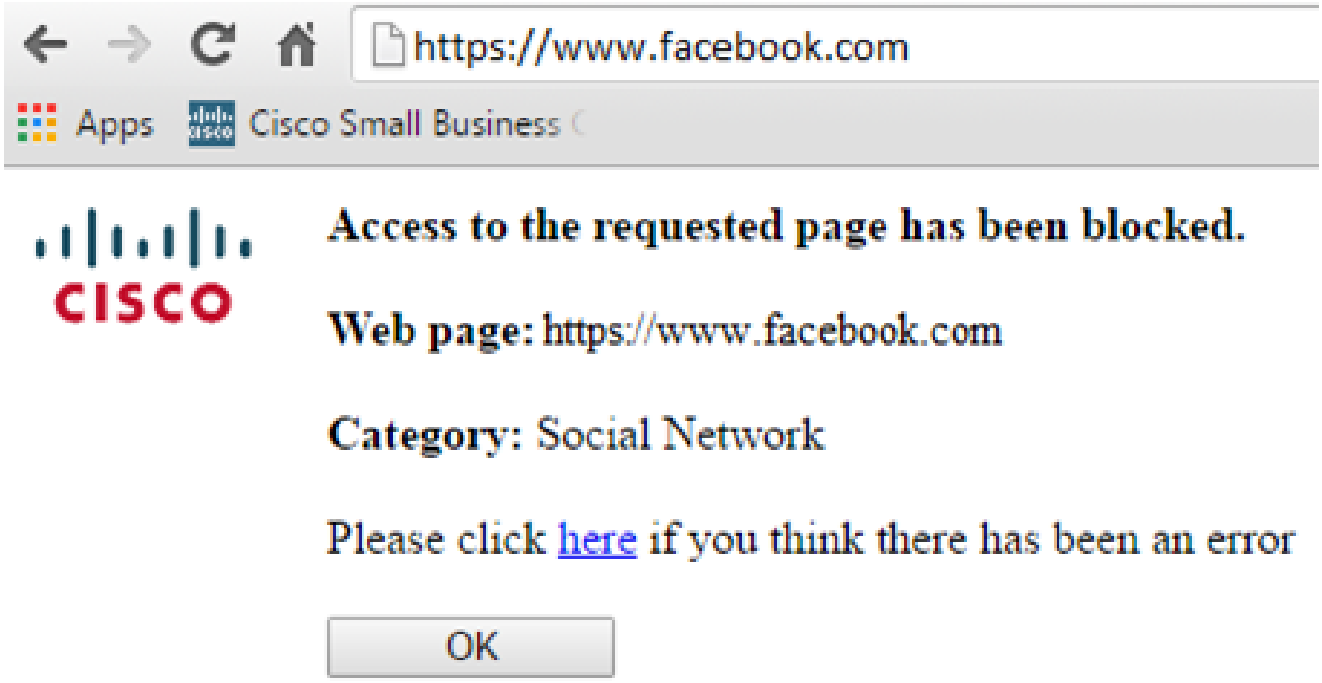
設定を永続的に保存するには、Copy/Save Configurationページに移動するか、ページの上部にあるsaveアイコンをクリックします。



手順 19（オプション）

WebサイトまたはURLがフィルタまたはブロックされた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。ブロックの一覧に表示されているドメイン名、またはブロックまたは拒否するようにフィルタされているドメイン名を入力します。

この例では、www.facebook.comを使用しています。



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 RVセキュリティライセンスを使用しているため、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。十分なセキュリティがある場合は、クリックして次のセクションに進んでください。

（「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ようフォローアップします。
2. お問い合わせください。リセラーに連絡します。

理想的には、あなたはどちらも行う必要はありませんが、この交差点に到着した場合、私たちは幸せです！プロセスをできるだけ迅速に進めるには、上の表に示したクレデンシャルと、次に示すクレデンシャルが必要です。

必要な情報	情報の検索
ライセンス請求書	ライセンスの購入が完了したら、この電子メールを送信する必要があります。
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あります。

必要な情報	情報の検索
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、画面の内容がキャプチャされ、チームと共有できます。スクリーンショットに慣れていない場合は、次の方法を使用できます。

スクリーンショット

トークンを取得した後、またはトラブルシューティングを行う場合は、スクリーンショットを撮って画面の内容をキャプチャ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、オペレーティングシステムに固有のリンクについては、以下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、シスコが提供するシンプルでありながら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。

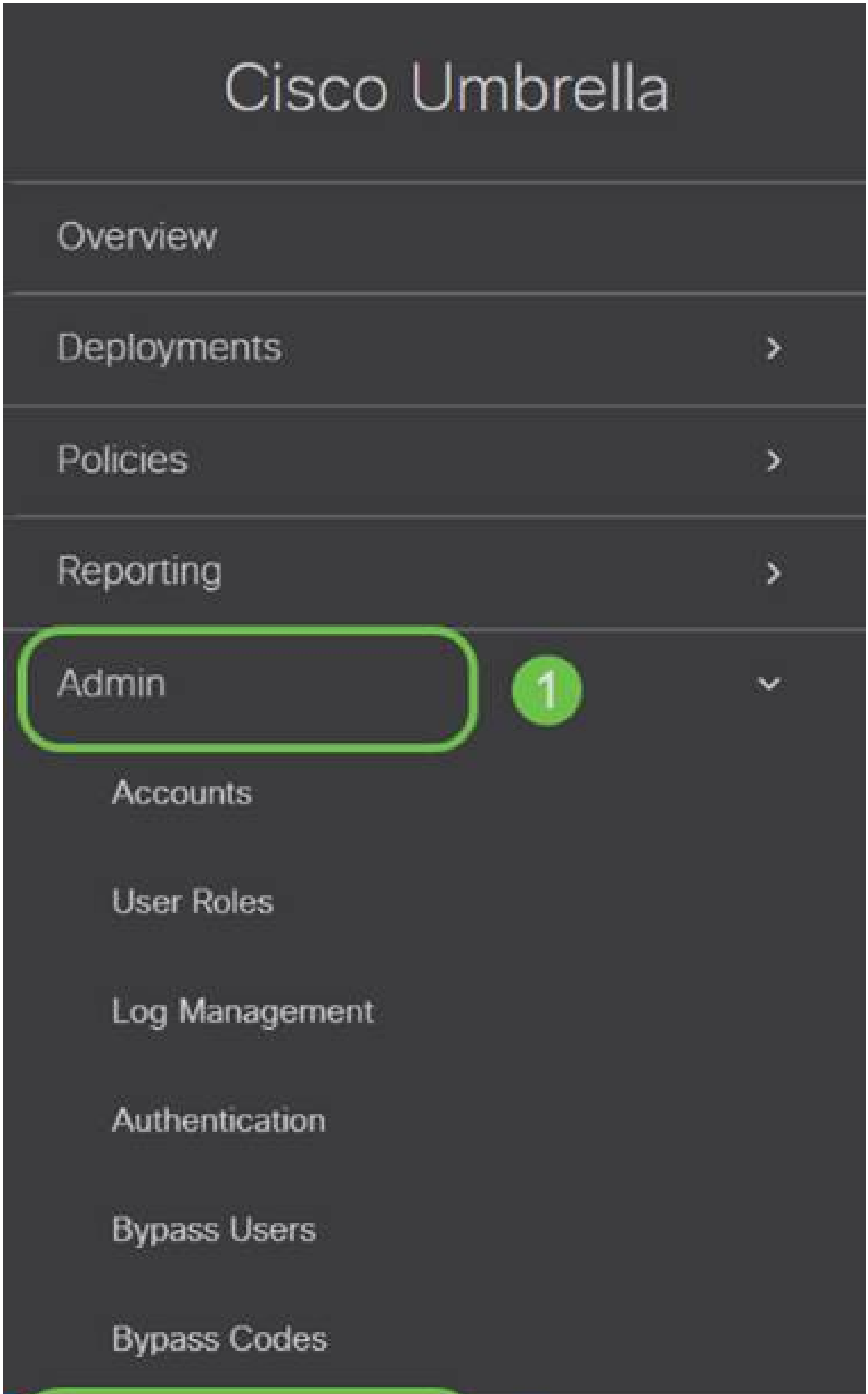
Umbrellaはクラウドで動作し、多くのセキュリティ関連サービスを実行します。新たな脅威からイベント後の調査まで。Umbrellaは、すべてのポートとプロトコルを検出して攻撃を防止します。

UmbrellaはDNSを防御用の主要な手段として使用します。ユーザがブラウザバーにURLを入力してEnterキーを押すと、Umbrellaが転送に参加します。その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の転送はマイクロ秒単位で分析され、遅延はほとんど発生しません。テレメトリデータは、世界中の何十億ものDNS要求を追跡するログと機器を使用します。このデータが世界中に拡散すると、世界中でデータを関連付けることができ、攻撃が始まったときにすばやく対応できます。詳細については、こちらのシスコのプライバシーポリシー(完全なポリシー、要約バージョン)を参照してください。テレメトリデータは、ツールとログから取得されたデータと考えてください。

Cisco Umbrellaにアクセスして、詳細を確認し、アカウントを作成してください。問題が発生した場合は、ここをクリックしてドキュメントを参照し、ここをクリックしてUmbrellaサポートの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、Dashboard画面でAdmin > API Keysの順にクリックします。

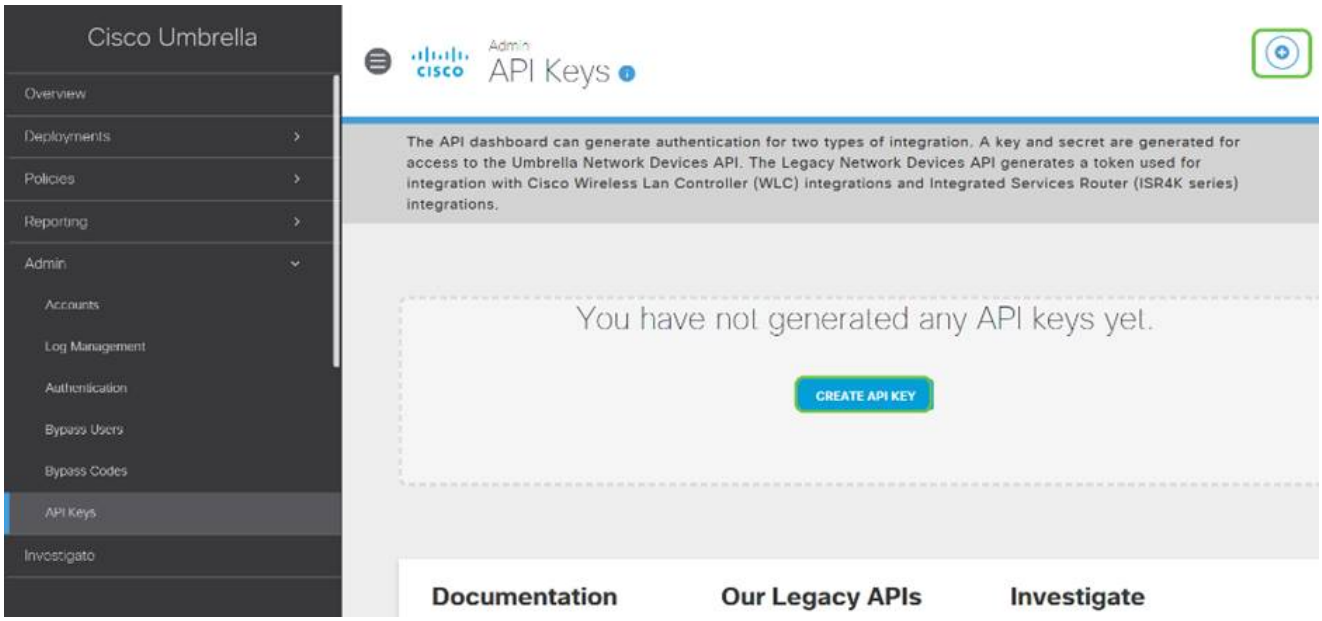

Cisco Umbrella
Overview
Deployments
Policies
Reporting
Admin
1
Accounts
User Roles
Log Management
Authentication
Bypass Users
Bypass Codes

APIキー画面の構造（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ともに下/上にスライドします。
3. トークンウェル：このアカウントで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連するUmbrellaサイトのドキュメントへのリンク。

手順 2

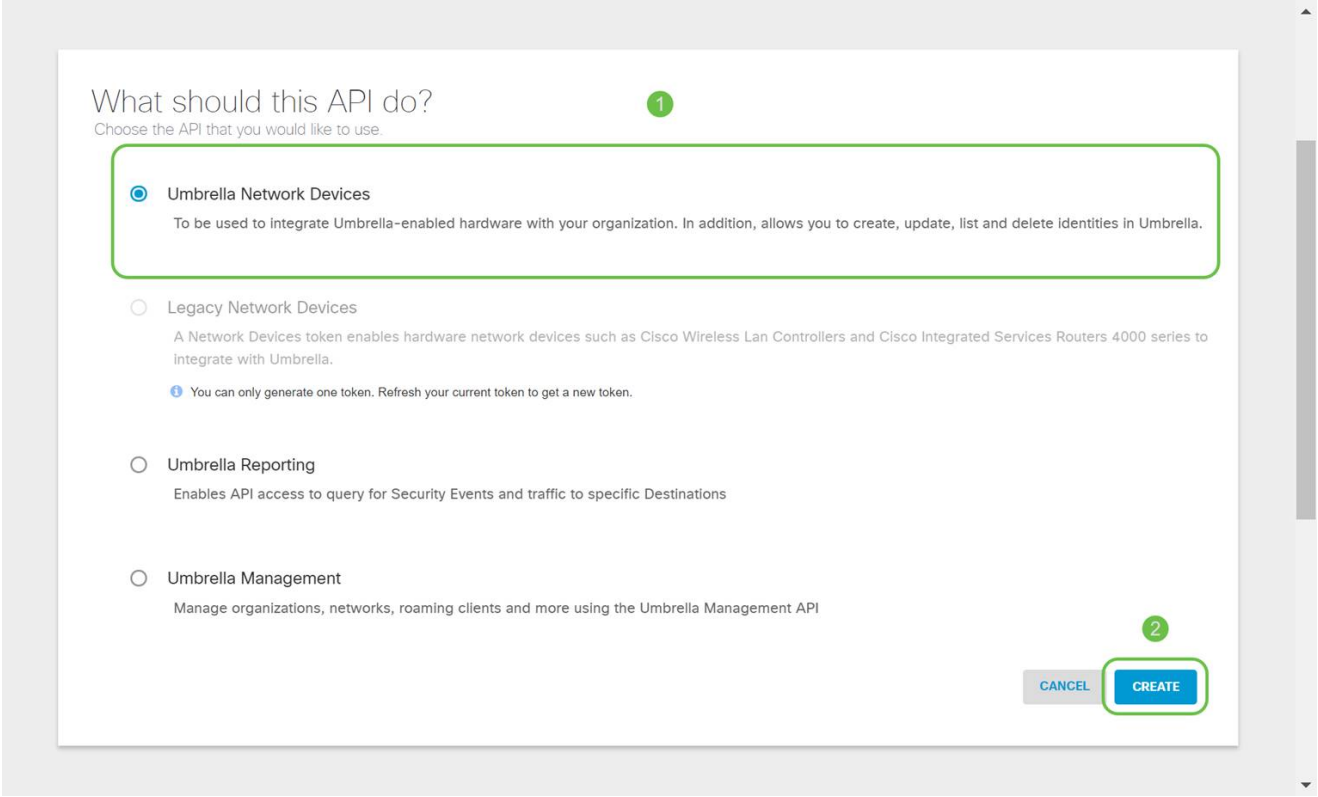
右上隅のAdd API Keyボタンをクリックするか、Create API Keyボタンをクリックします。両方とも同じ機能を果たします。



上のスクリーンショットは、このメニューを初めて開いたときと同じように表示されます。

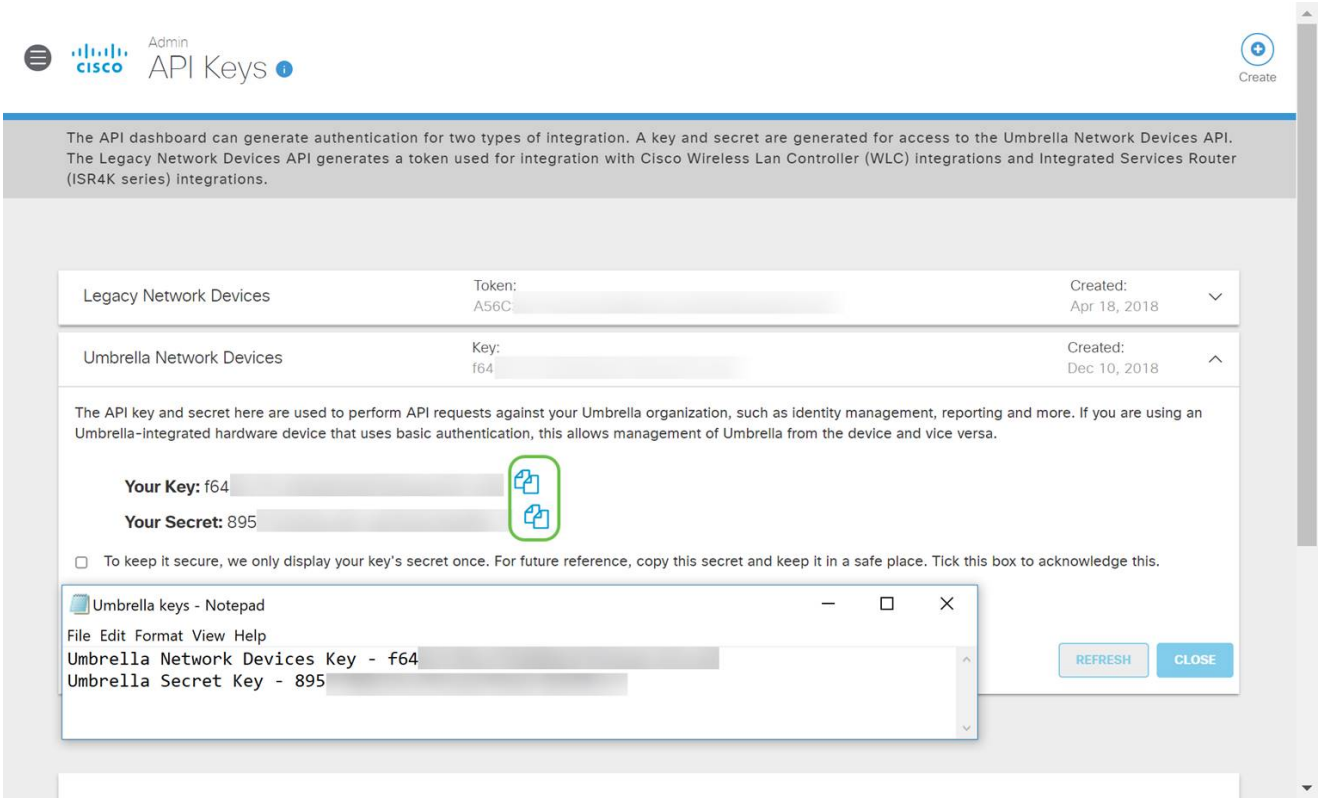
手順 3

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



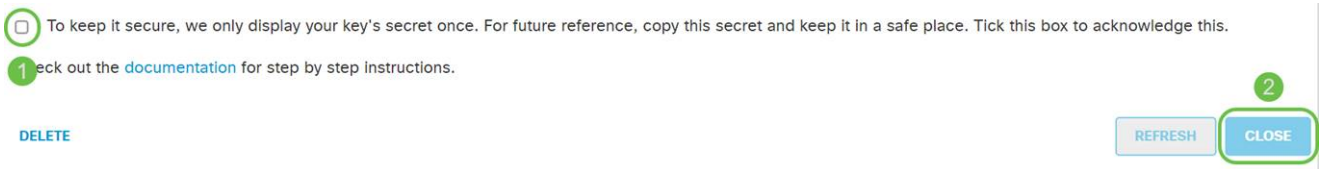
手順 4

メモ帳などのテキストエディタを開き、APIおよび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。ポップアップ通知で、キーがクリップボードにコピーされたことを確認できます。一度に1つずつ、シークレットと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ネットワークデバイスキー」です。その後、後でアクセスしやすい安全な場所にテキストファイルを保存します。



手順 5

鍵と秘密鍵を安全な場所にコピーしたら、Umbrella API画面でチェックボックスをクリックして、秘密鍵の一時的な表示の確認応答が完了したことを確認し、Closeボタンをクリックします。



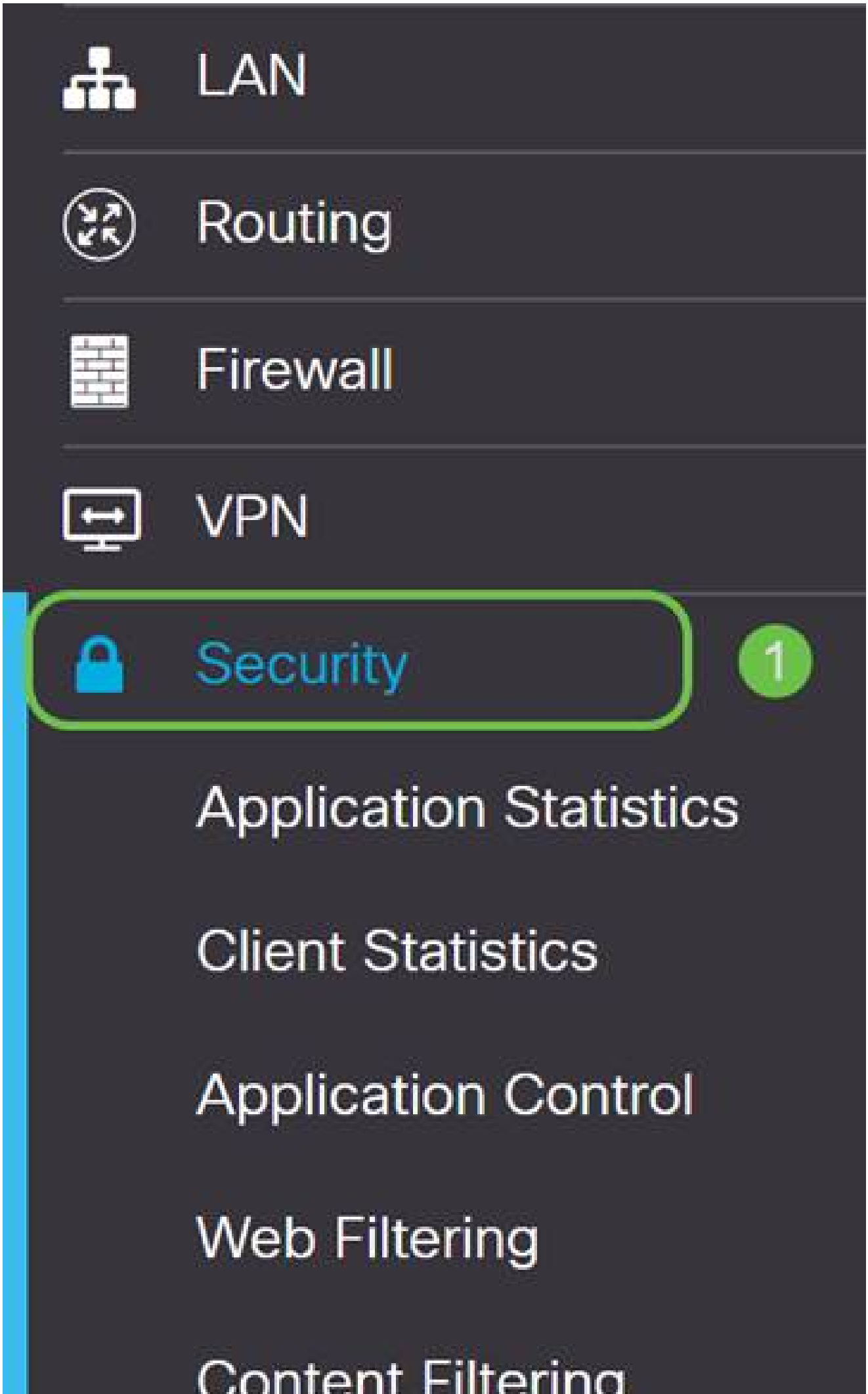
秘密キーを紛失したり、誤って削除したりした場合、このキーを取得するために呼び出す機能やサポート番号はありません。紛失した場合は、キーを削除し、Umbrellaで保護する各デバイスで新しいAPIキーを再認証する必要があります。

RV345PでのUmbrella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。

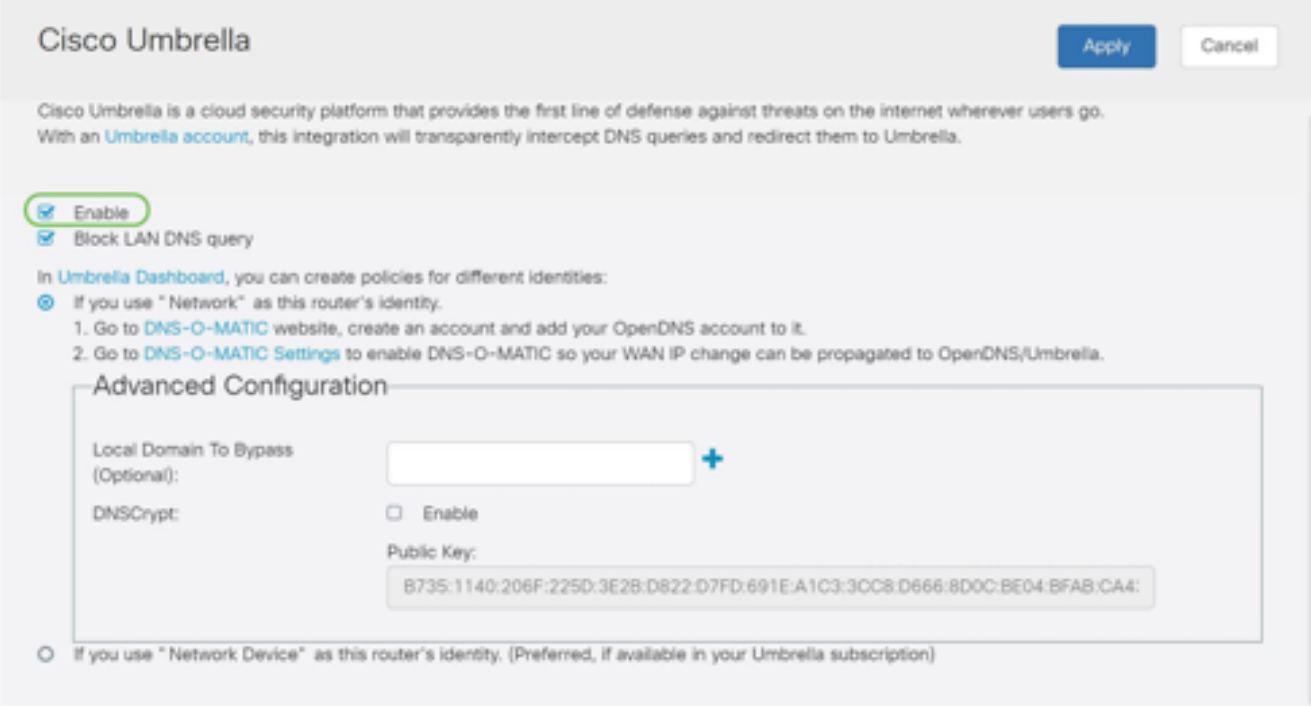
手順 1

RV345Pルータにログインした後、サイドバーメニューでSecurity > Umbrellaの順にクリックします。


LAN
Routing
Firewall
VPN
Security
1
Application Statistics
Client Statistics
Application Control
Web Filtering
Content Filtering

手順 2

Umbrella API画面にはさまざまなオプションがあります。Umbrellaの有効化を開始するには、Enableチェックボックスをクリックします。

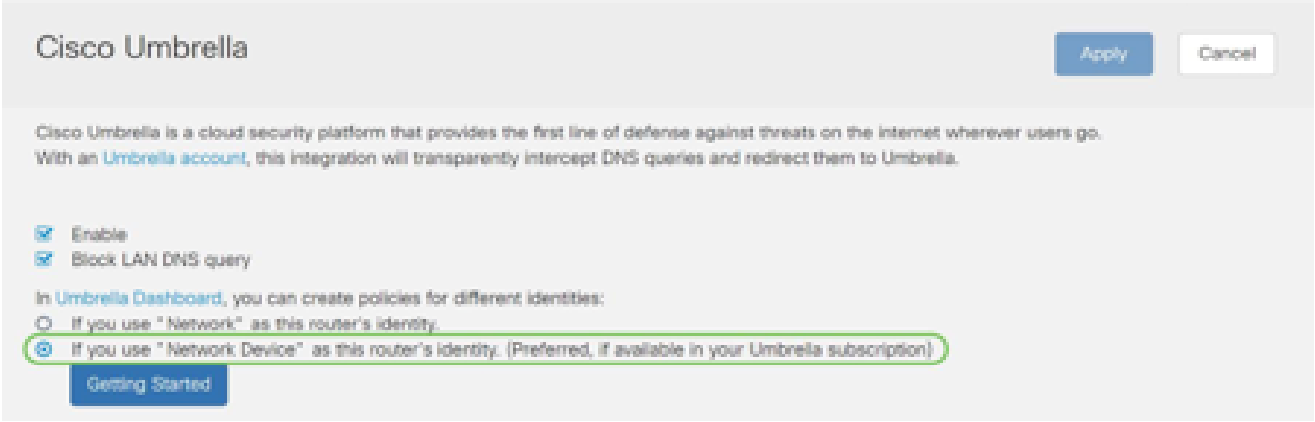


手順 3（オプション）

デフォルトでは、Block LAN DNS Queriesボックスが選択されています。この便利な機能により、ルータ上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。この機能は、すべてのドメイン変換要求を強制的にRV345P経由で転送するため、ほとんどのユーザに適しています。

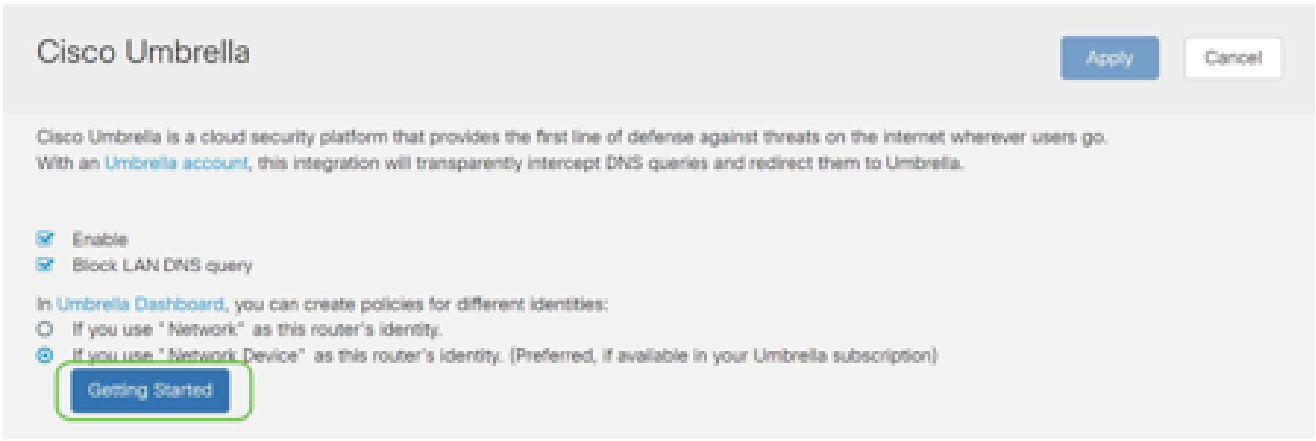
手順 4

次のステップは、2つの異なる方法で実行されます。どちらもネットワークのセットアップに依存します。DynDNSやNoIPなどのサービスを使用する場合は、デフォルトの命名方式である「Network」のままにしておきます。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連動することを確認する必要があります。私たちの目的のために「ネットワークデバイス」に依存しているので、下部のオプションボタンをクリックします。



手順 5

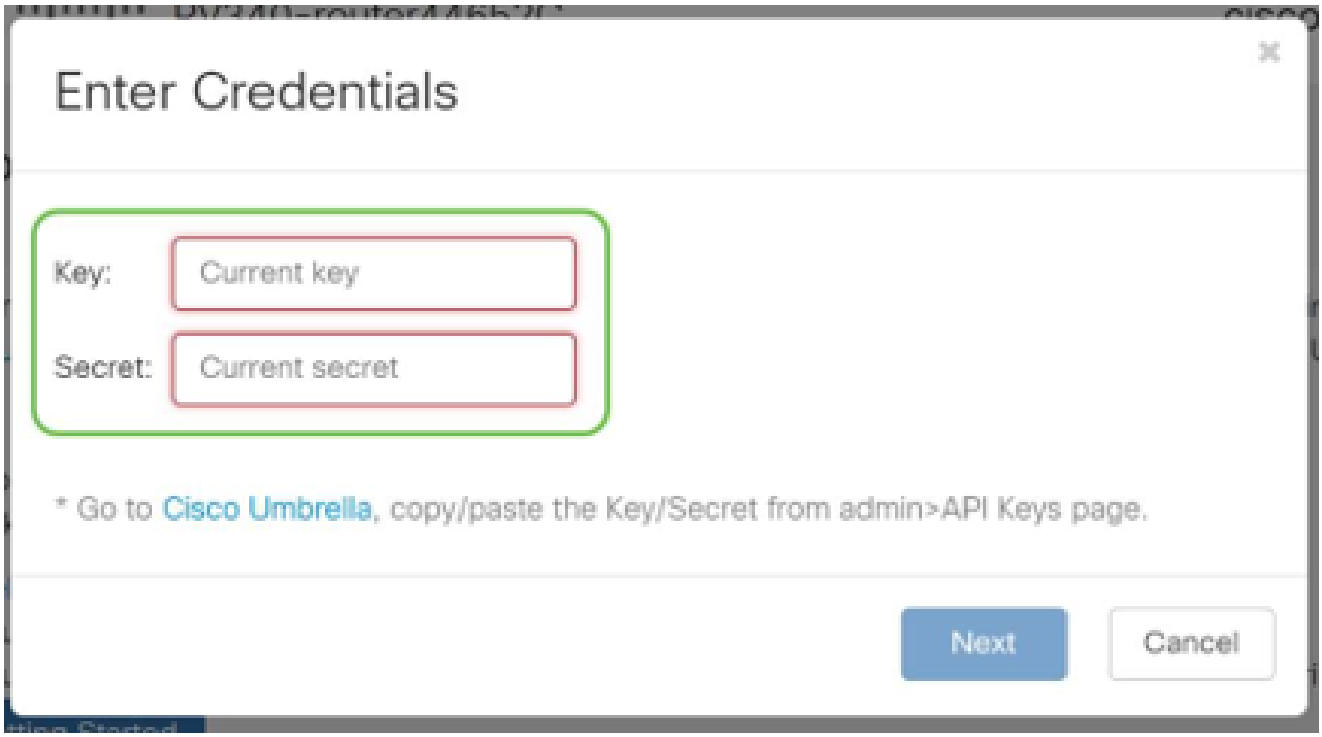
Getting Startedをクリックします。



手順 6

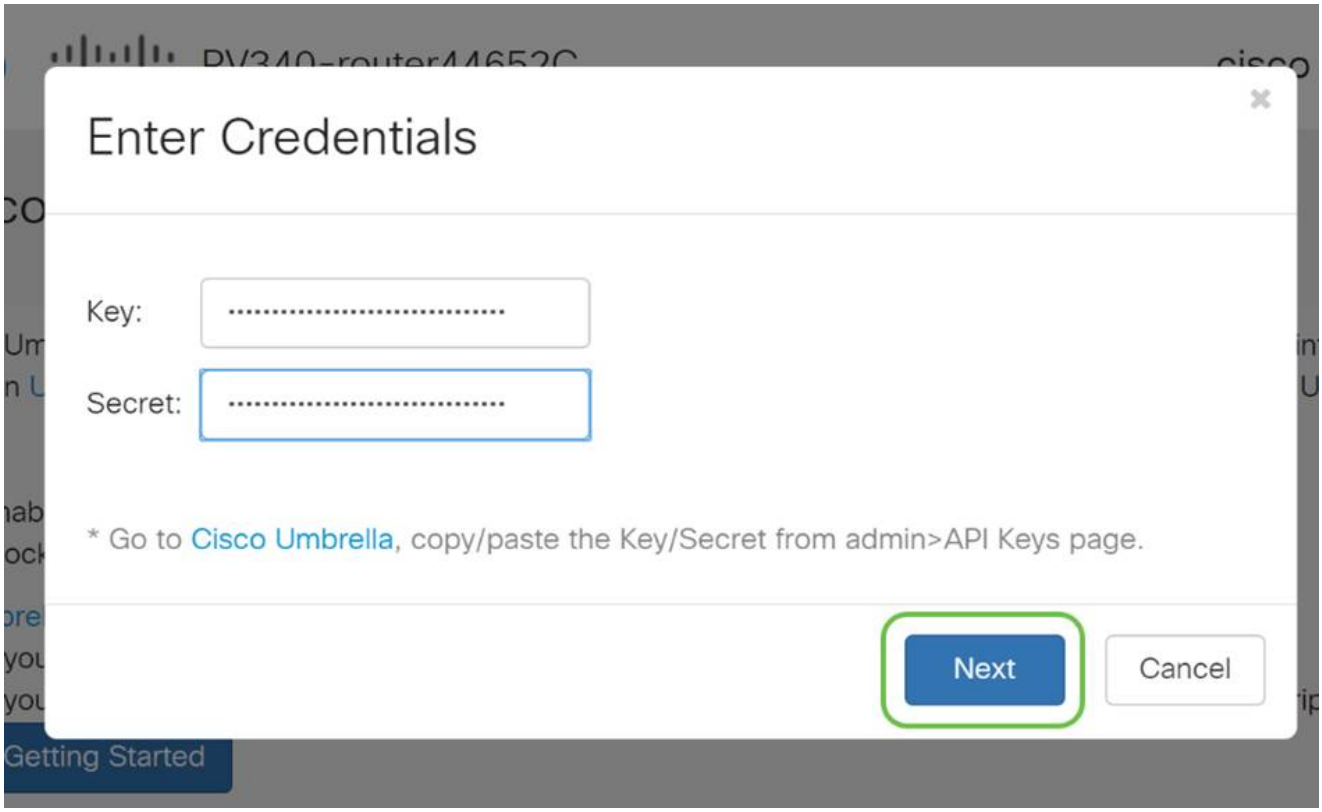
テキストボックスにAPI KeyとSecret Keyを入力します。

重要だと分かるように2回呼び出す！秘密キーを紛失したり、誤って削除したりした場合、このキーを取得するために呼び出す機能やサポート番号はありません。 それを秘密にして安全にしておきなさい。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キーを再認証する必要があります。



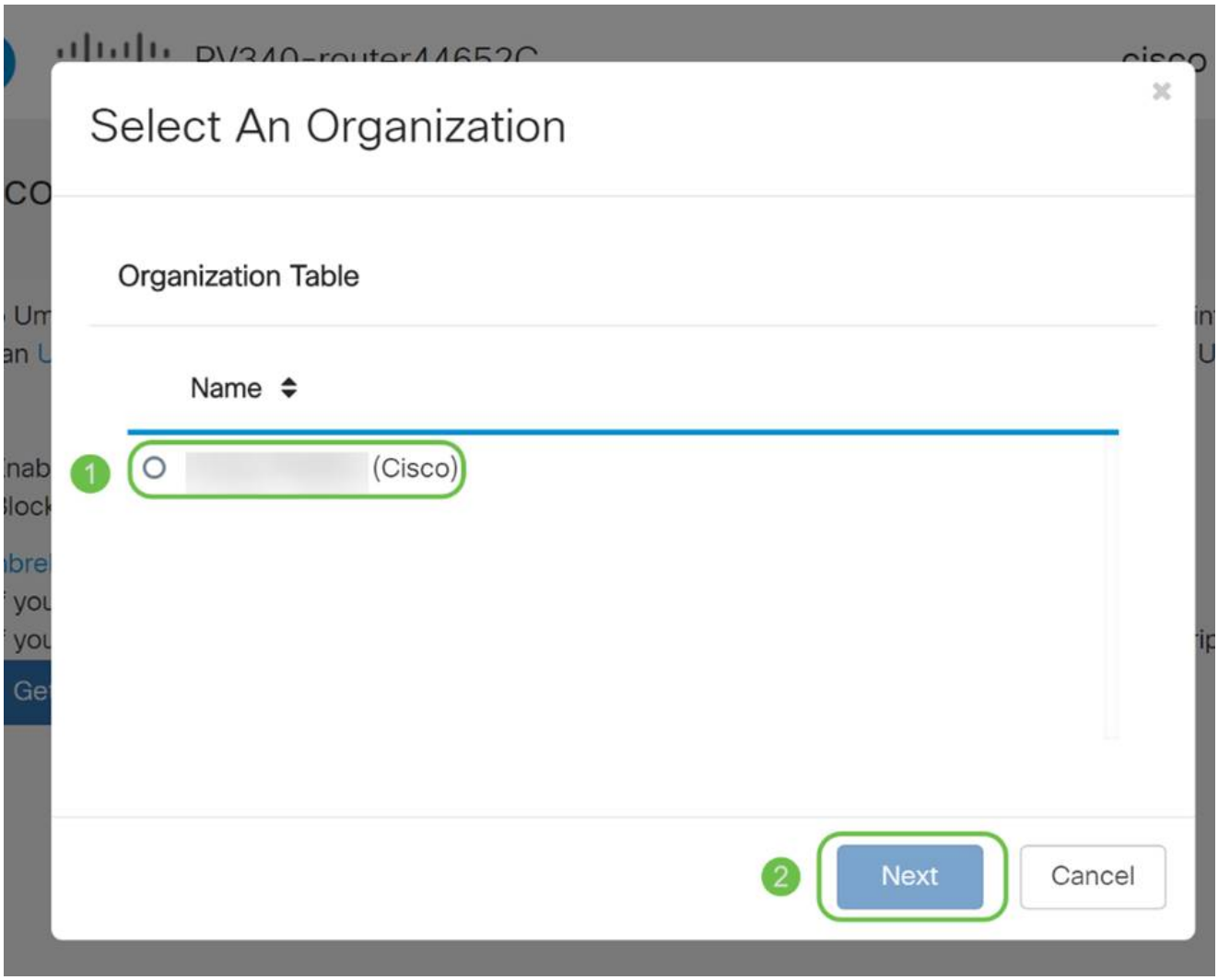
ステップ7

APIと秘密鍵を入力したら、Nextボタンをクリックします。



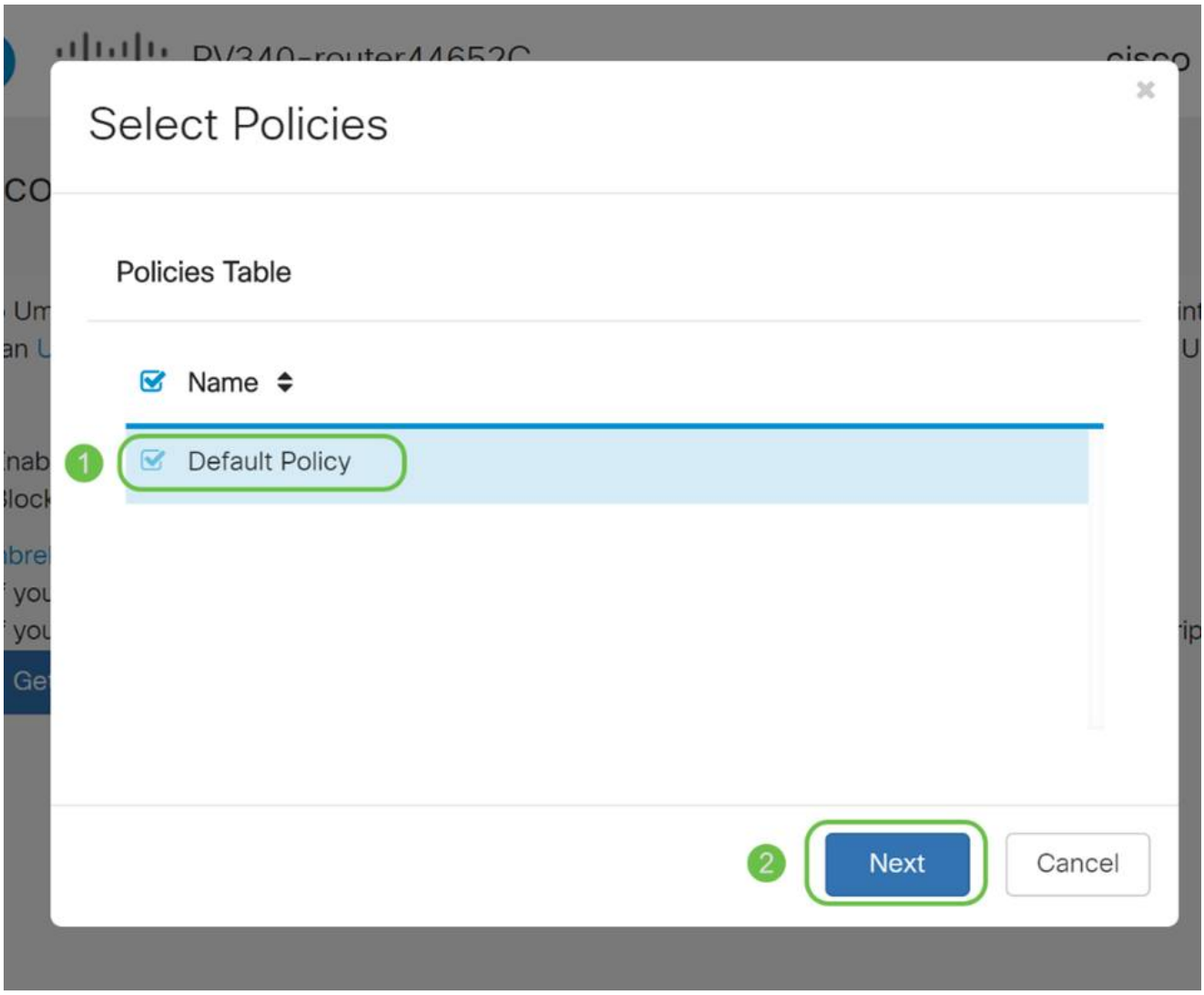
手順 8

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。



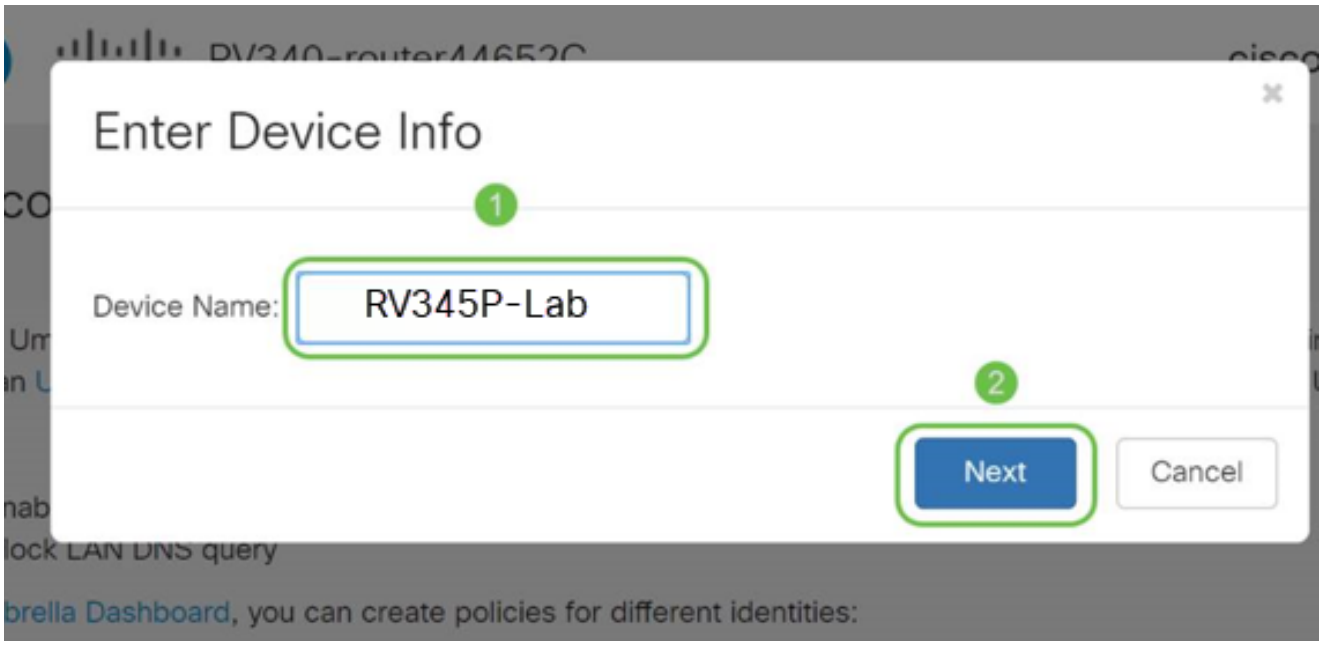
手順 9

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。ほとんどのユーザでは、デフォルトポリシーで十分なカバレッジが提供されます。



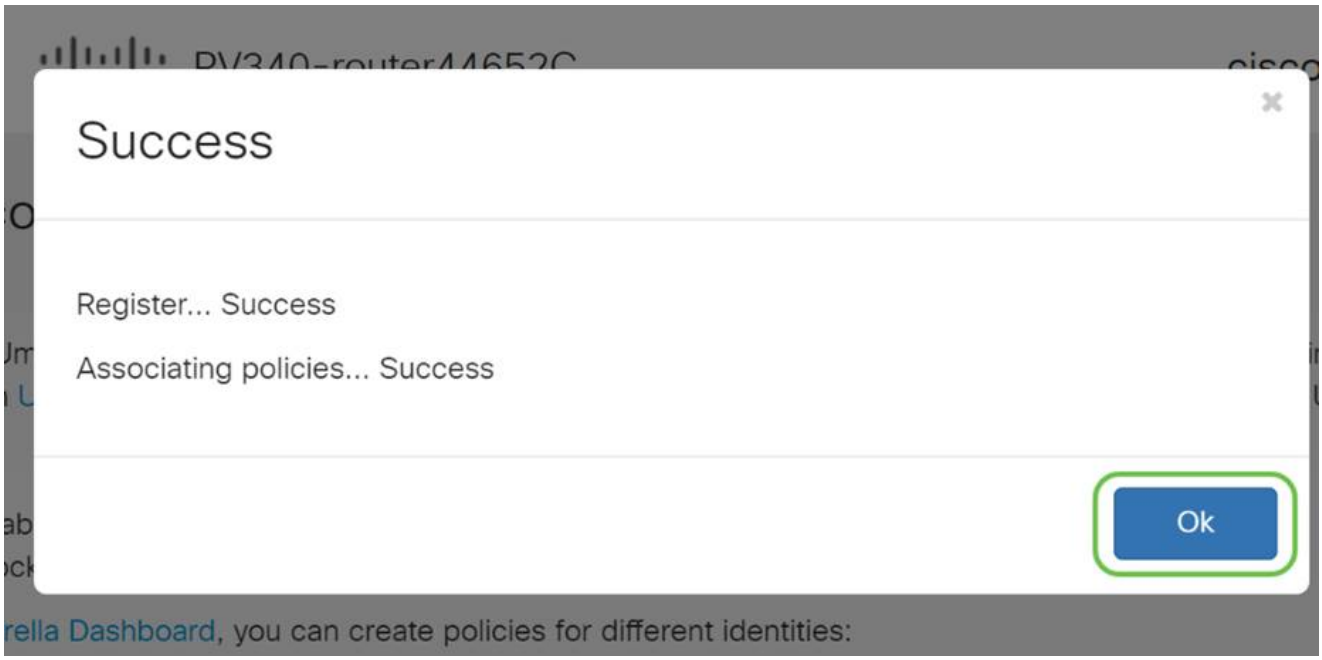
手順 10

デバイスに名前を割り当て、Umbrellaレポートで指定できるようにします。この設定では、名前をRV345P-Labとしています。



手順 11

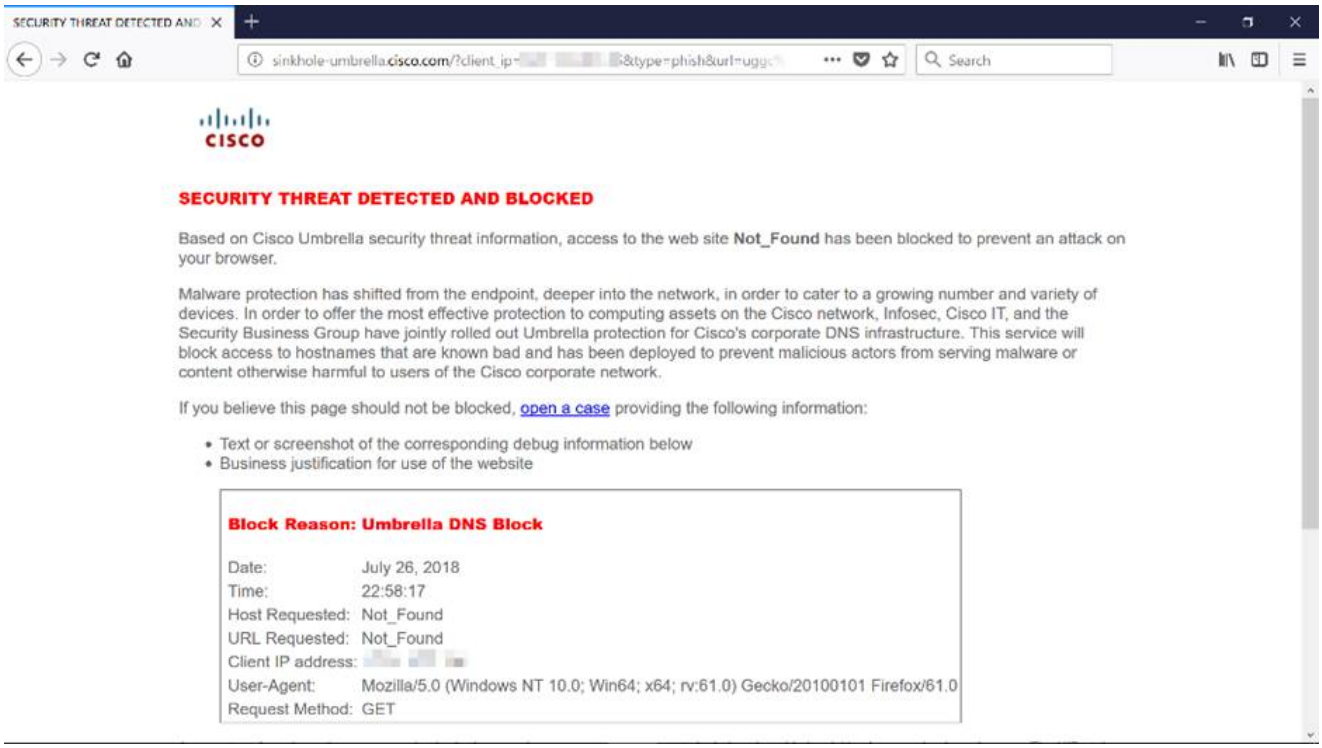
次の画面で選択した設定が検証され、関連付けが正常に完了すると更新が表示されます。[OK] をクリックします。



確認

おめでとうございます。Cisco Umbrellaによって保護されました。それとも君か？実際の例を使って再確認してみましょう。シスコは、ページがロードされるとすぐにこれを判断するための専用Webサイトを作成しました。 ここをクリックするか、ブラウザバーにhttps://InternetBadGuys.comと入力します。

Umbrellaが正しく設定されている場合は、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

誰かがネットワークデバイスからイーサネットケーブルを取り外して接続することで、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。この場合は、許可されたホストのリストを、対応するIPアドレスとMACアドレスを使用してルータに直接接続するように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

仮想プライベートネットワーク(VPN)接続では、インターネットなどのパブリックまたは共有ネットワークを経由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、送信、および受信を行うことができます。ただし、プライベートネットワークとそのリソースを保護するために、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。従業員がオフィスの外にいて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ことは有用で必要であるため、企業オフィスでは主にVPN接続を使用します。

VPNを使用すると、リモートホストが同じローカルネットワーク上に存在するかのように動作できます。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で、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、接続を確立できるかどうかは、VPNルータの設定に完全に依存しています。

どのVPNがニーズに最も適しているかわからない場合は、『Cisco Business VPN Overview and Best Practices』を参照してください。

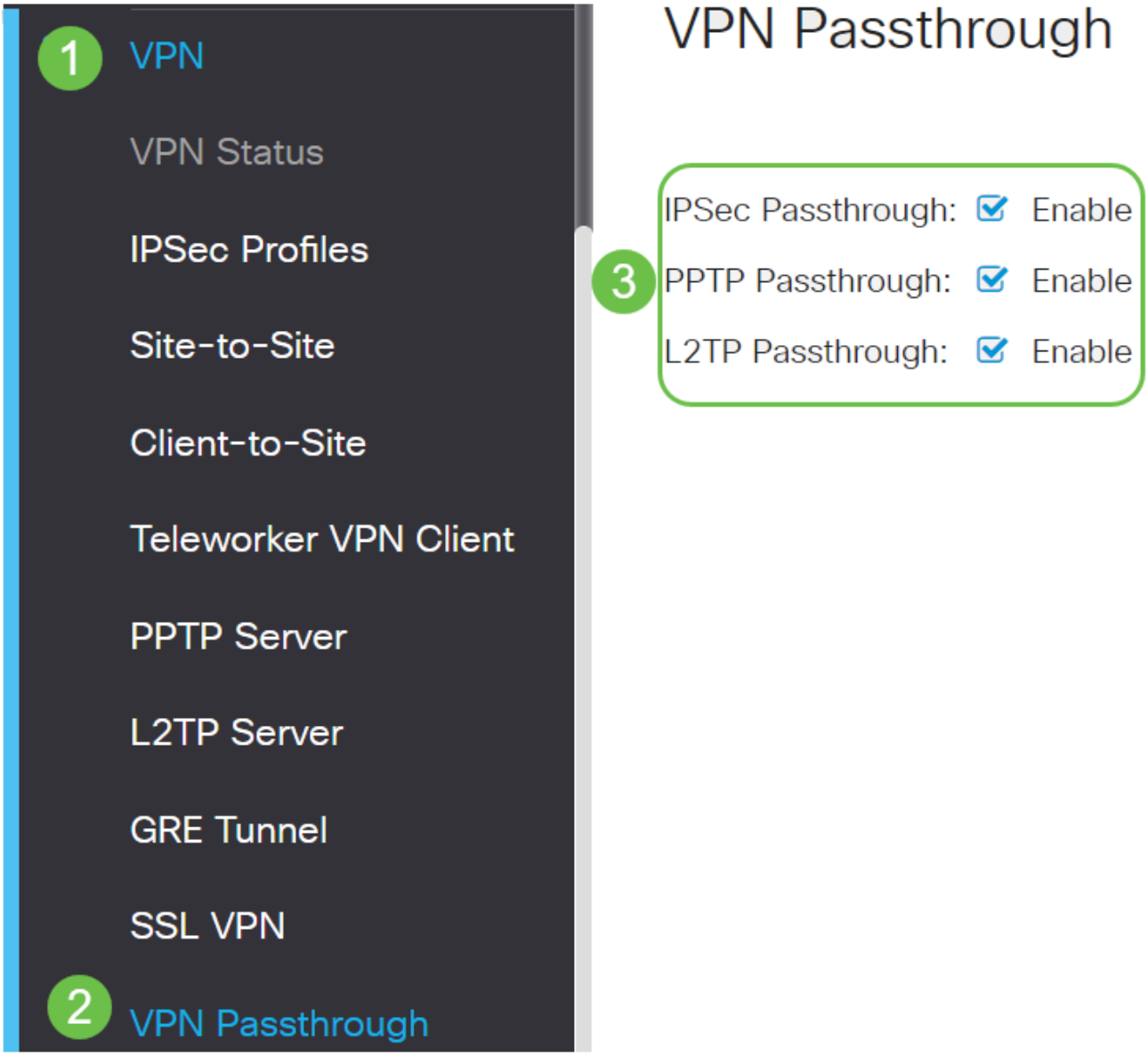
AnyConnect VPNは、このコンフィギュレーションガイドに記載されている唯一のCisco VPNサポート製品です。TheGreenBowやShrew Softなどのシスコ以外のサードパーティ製品はシスコのサポート対象外です。これらはガイダンスの目的でのみ含まれています。上記のサポートが必要な場合は、そのサードパーティに連絡してサポートを受けてください。

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進むことができます。

[VPN パススルー]

通常、同じインターネット接続で複数のクライアントをサポートする場合は、IPアドレスを節約するために、すべてのルータでネットワークアドレス変換(NAT)がサポートされています。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パススルーが開始されます。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て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および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と、リモートVPNゲートウェイへの到達のみを許可します。この機能は、NATをサポートするホームルータによく見られます。

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には、VPN > VPN Passthroughの順に選択します。必要に応じて表示または調整します。



AnyConnect VPN（トンネルモード）

Cisco AnyConnectを使用する利点は次のとおりです。

1. 安全で永続的な接続
2. 永続的なセキュリティおよびポリシーの適用
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デプロイメントシステムから導入可能
4. カスタマイズ可能で翻訳可能
5. 設定が簡単
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します

RV345PでのAnyConnect SSL VPNの設定

手順 1

ルータのWebベースユーティリティにアクセスし、VPN > SSL VPNの順に選択します。

VPN 1

VPN Status

IPSec Profiles

Site-to-Site

Client-to-Site

Teleworker VPN Client

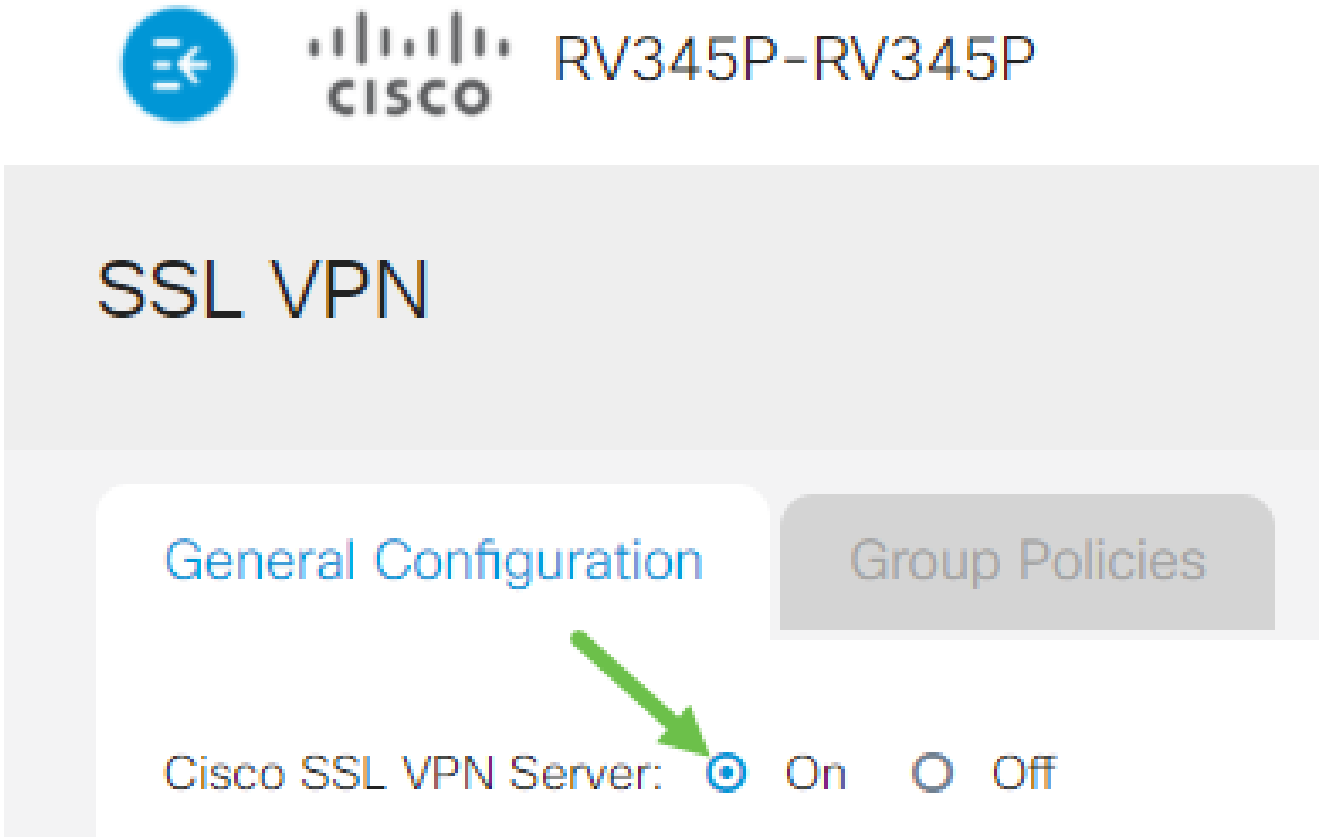
PPTP Server

L2TP Server

GRE Tunnel

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

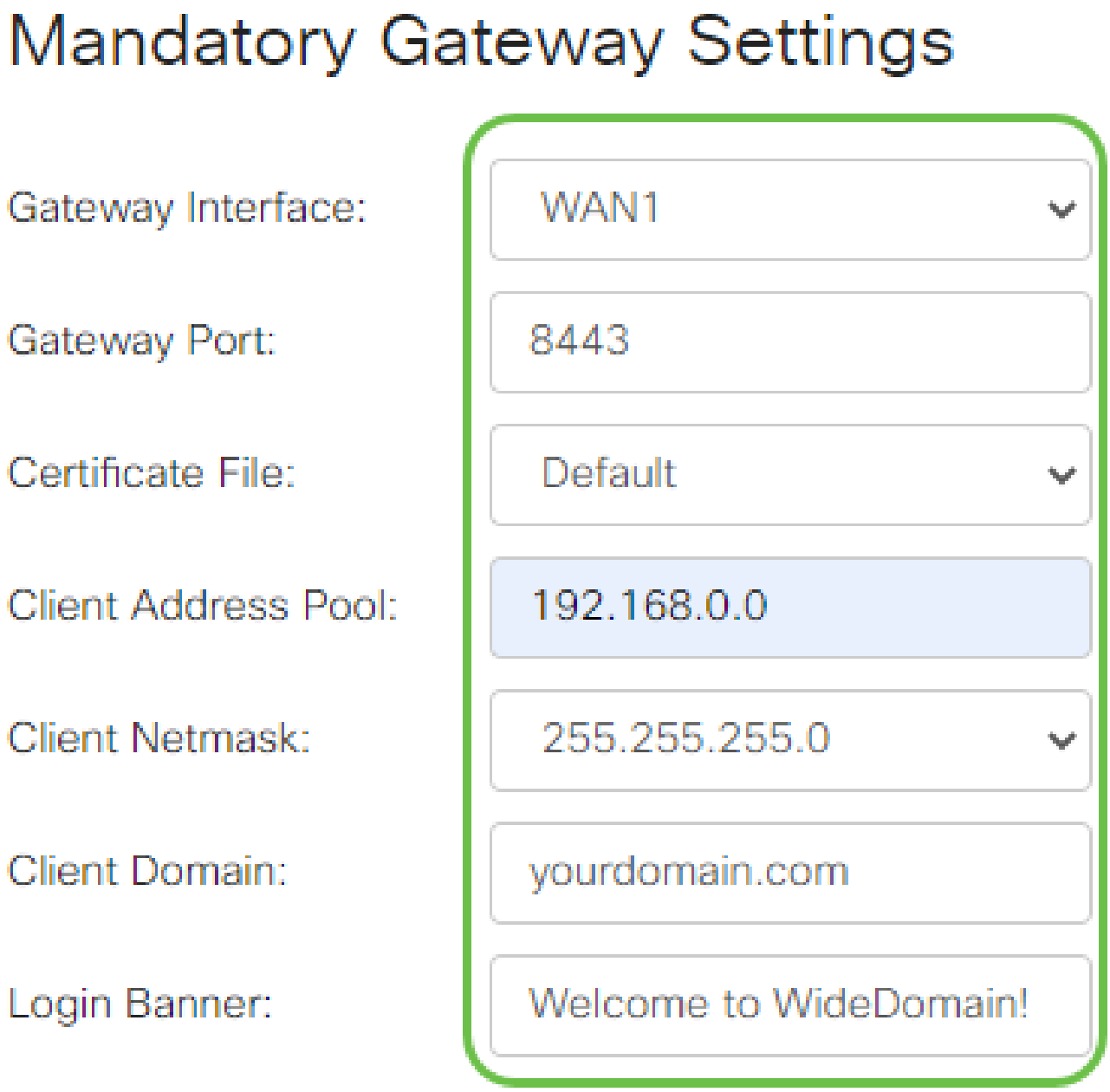
手順 1

次の構成設定は必須です。

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。オプションには、WAN1、WAN2、USB1、USB2があります。
2. SSL VPNゲートウェイに使用するポート番号をGateway Portフィールドに1 ~ 65535の範囲で入力します。
3. ドロップダウンリストから証明書ファイルを選択します。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へのアクセスを試み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ます。
4. Client Address Pool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アドレスの範囲です。

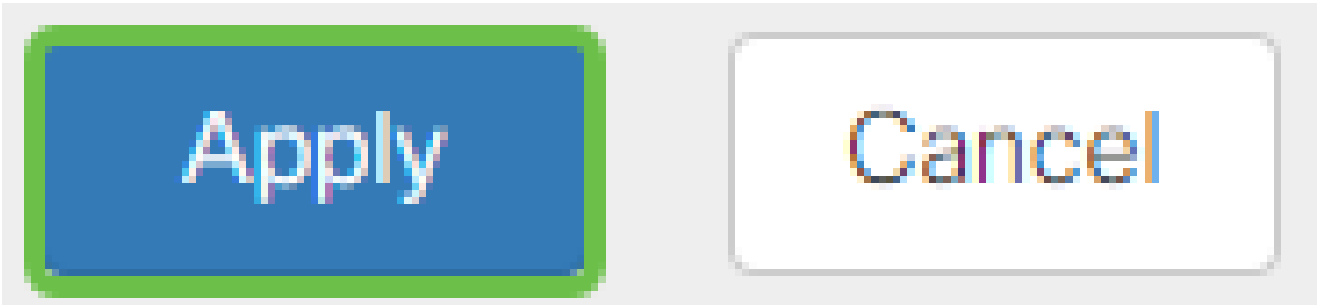
   IPアドレスの範囲がローカルネットワークのどのIPアドレスとも重複していないことを確認します。

5. ドロップダウンリストからクライアントネットマスクを選択します。
6. Client Domainフィールドにクライアントの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するドメイン名になります。
7. Login Banner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。

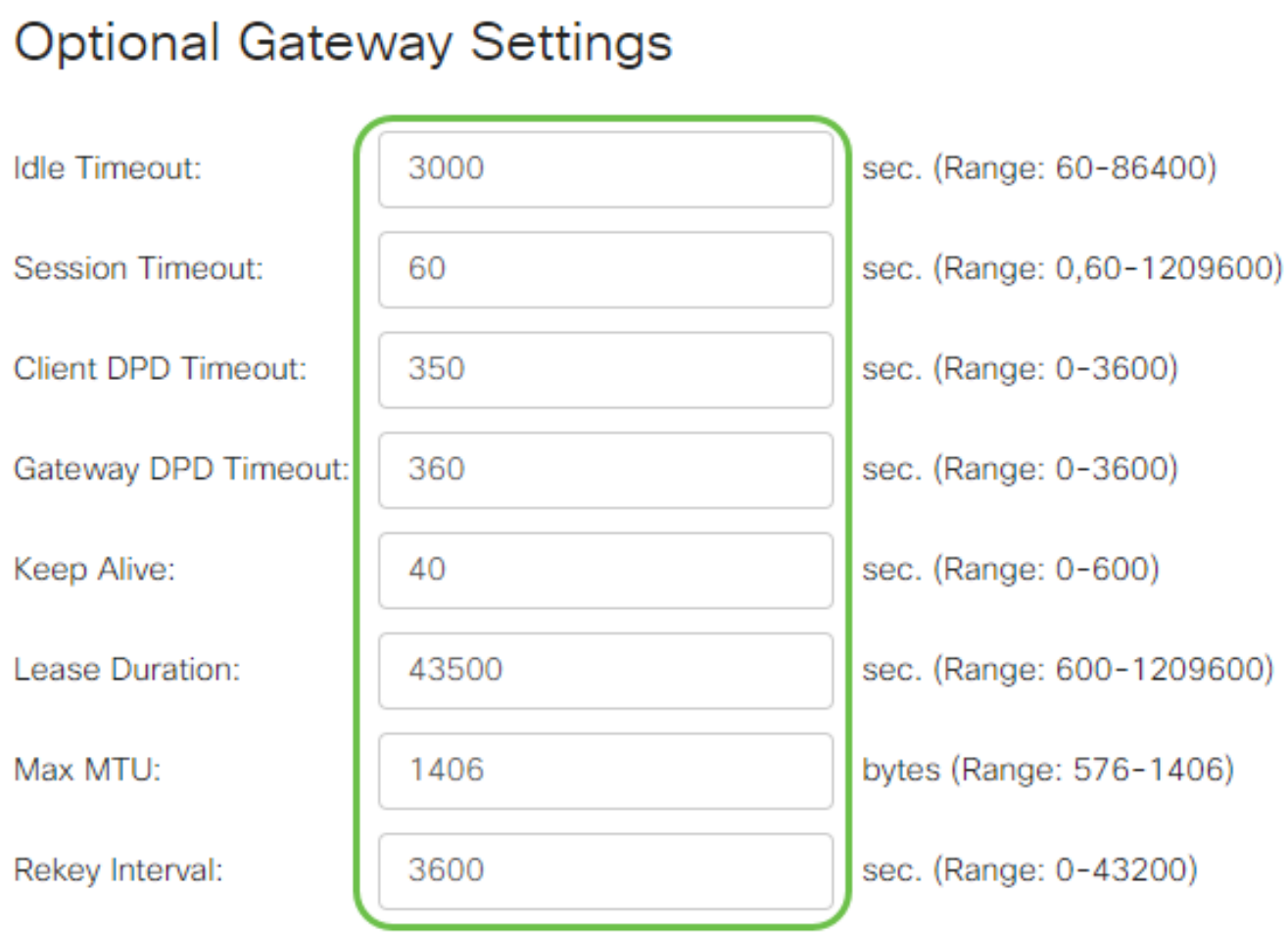


オプションのゲートウェイ設定

手順 1

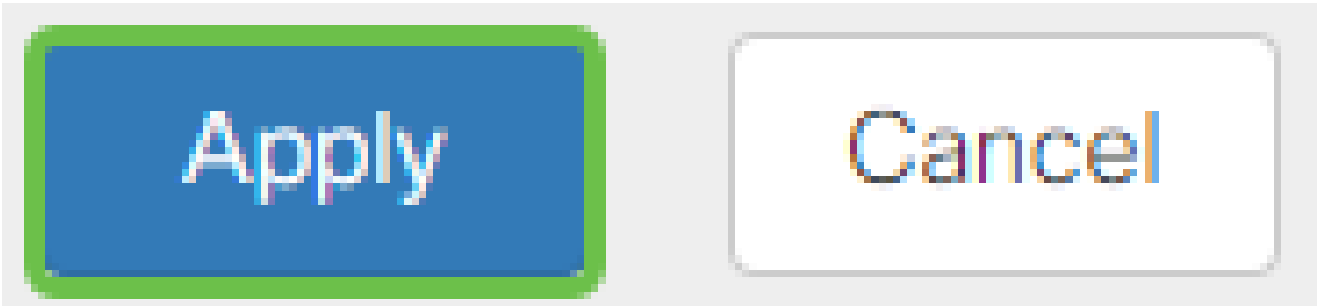
次の設定はオプションです。

1. 60 ~ 86400の範囲のアイドルタイムアウトの値を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. Session Timeoutフィールドに秒単位で値を入力します。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の範囲で秒単位の値を入力します。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の範囲で秒単位の値を入力します。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。ドロップされた場合は、VPN接続の再確立が試行されます。
6. Lease Durationフィールドに、接続するトンネルの継続時間を秒単位で入力します。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をバイト単位で入力します。範囲は 576 ~ 1406 です。
8. Rekey Intervalフィールドにリレー間隔の時間を入力します。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

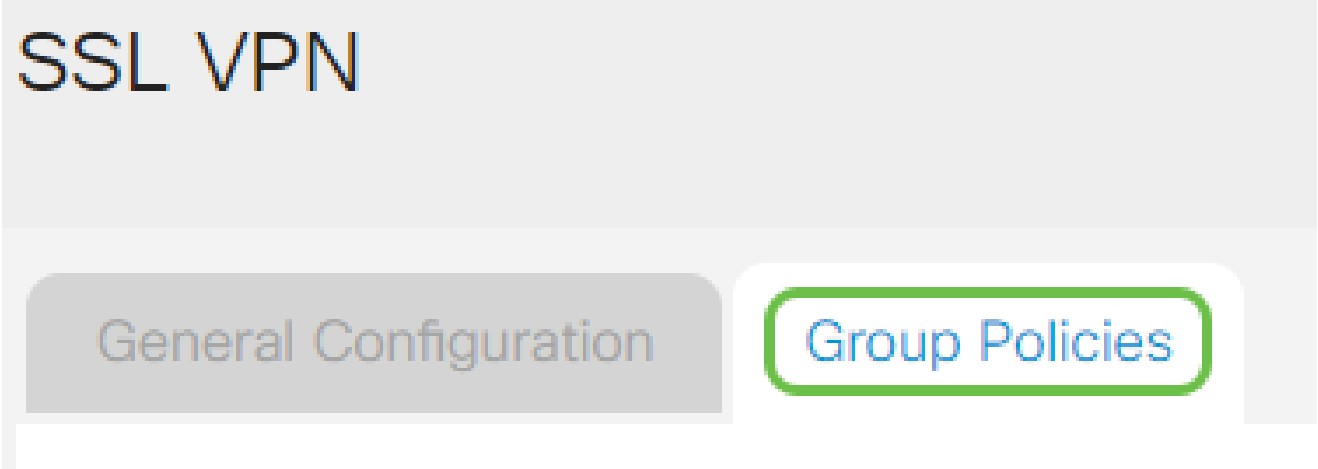
[APPLY] をクリックします。



グループポリシーの設定

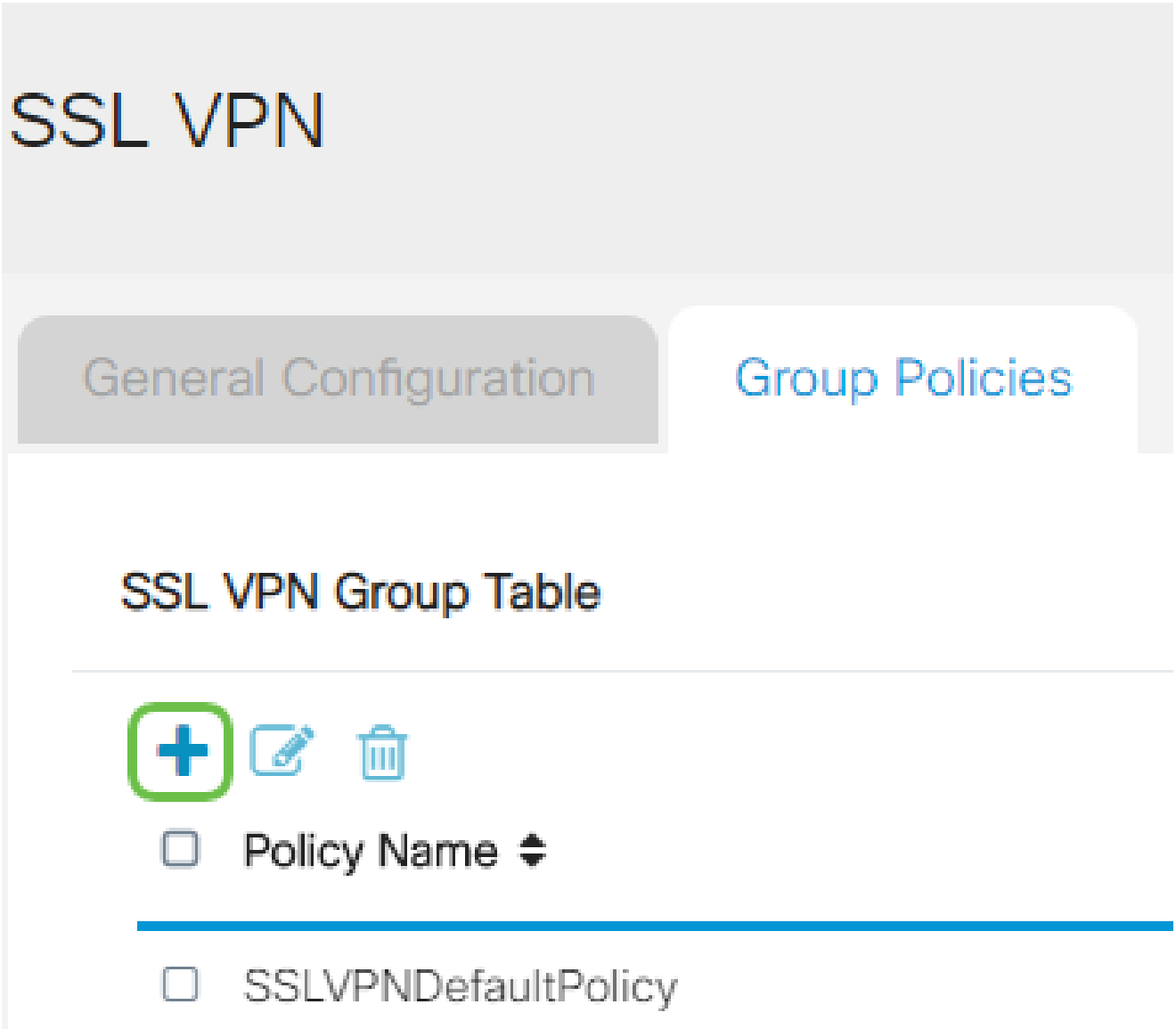
手順 1

Group Policies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にある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。

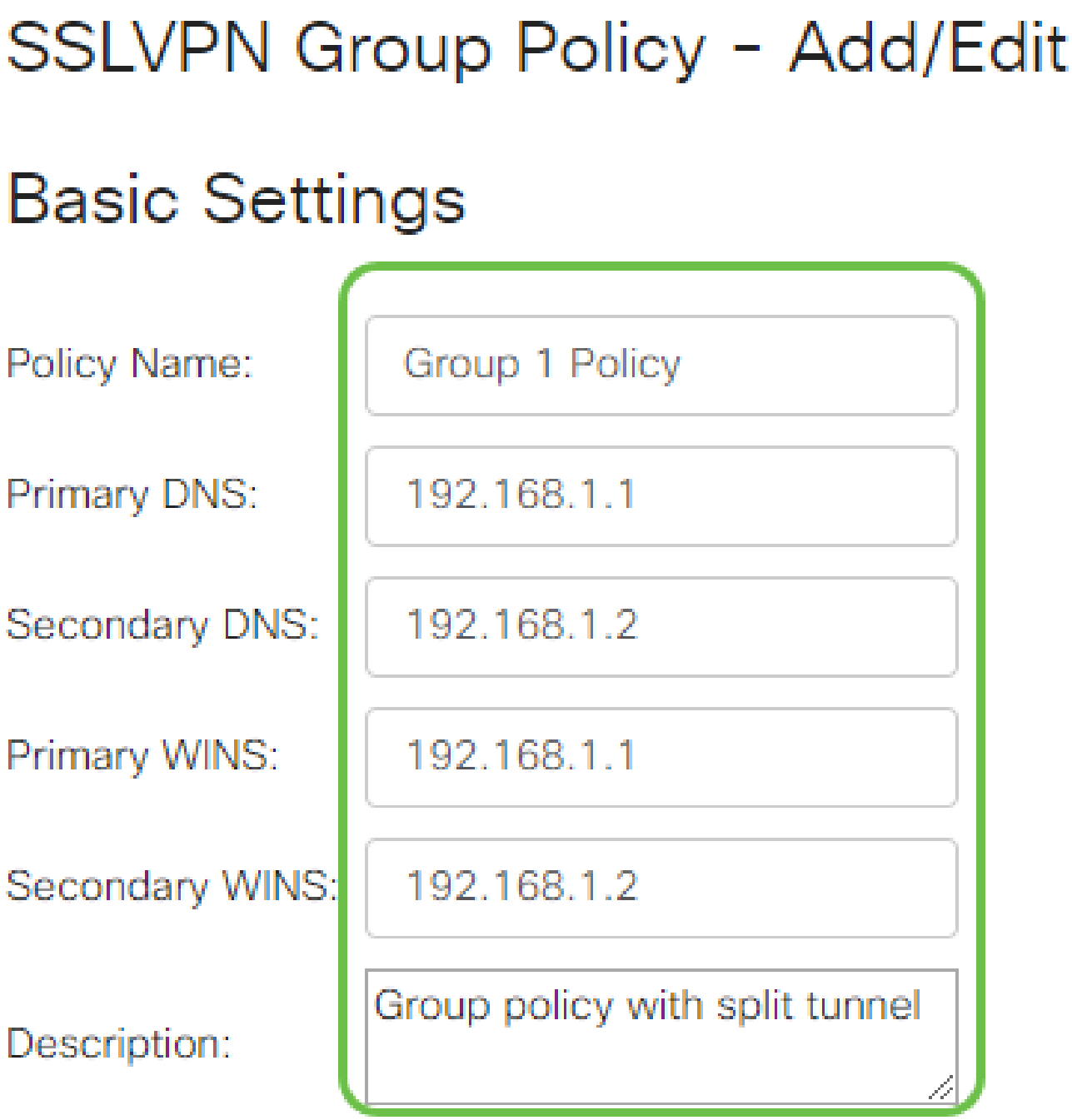


SSL VPNグループテーブルに、デバイスのグループポリシーのリストが表示されます。リストの最初のグループポリシー(SSLVPNDefaultPolicy)を編集することもできます。これは

、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

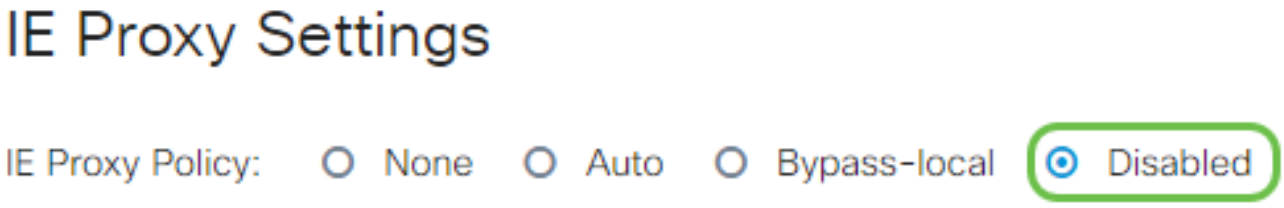
1. Policy Nameフィールドに任意のポリシー名を入力します。
2. 表示されたフィールドにプライマリDNSのIPアドレスを入力します。デフォルトでは、このIPアドレスはすでに指定されています。
3. （オプション）表示されたフィールドにセカンダリDNSのIPアドレスを入力します。これは、プライマリDNSに障害が発生した場合のバックアップとして機能します。
4. （オプション）表示されたフィールドにプライマリWINSのIPアドレスを入力します。
5. （オプション）表示されたフィールドに、セカンダリWINSのIPアドレスを入力します。
6. （オプション）Descriptionフィールドにポリシーの説明を入力します。



手順 4（オプション）

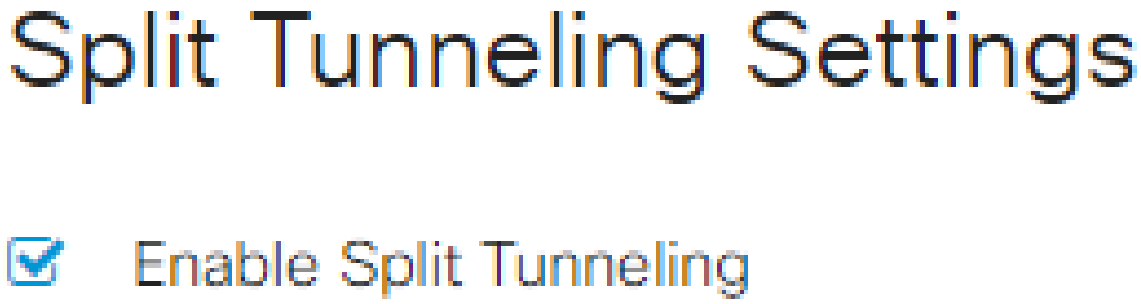
オプションボタンをクリックしてIEプロキシポリシーを選択し、Microsoft Internet Explorer(MSIE)プロキシ設定でVPNトンネルを確立できるようにします。次のオプションがあります。

- 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：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。
- 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チェックボックスにチェックマークを入れて、インターネット宛てのトラフィックが暗号化されずに直接インターネットに送信されるようにします。フルトンネリングでは、すべてのトラフィックがエンドデバイスに送信され、エンドデバイスはその後、宛先リソースにルーティングされます。これにより、Webアクセスのパスから企業ネットワークが除外されます。



ステップ 6（オプション）

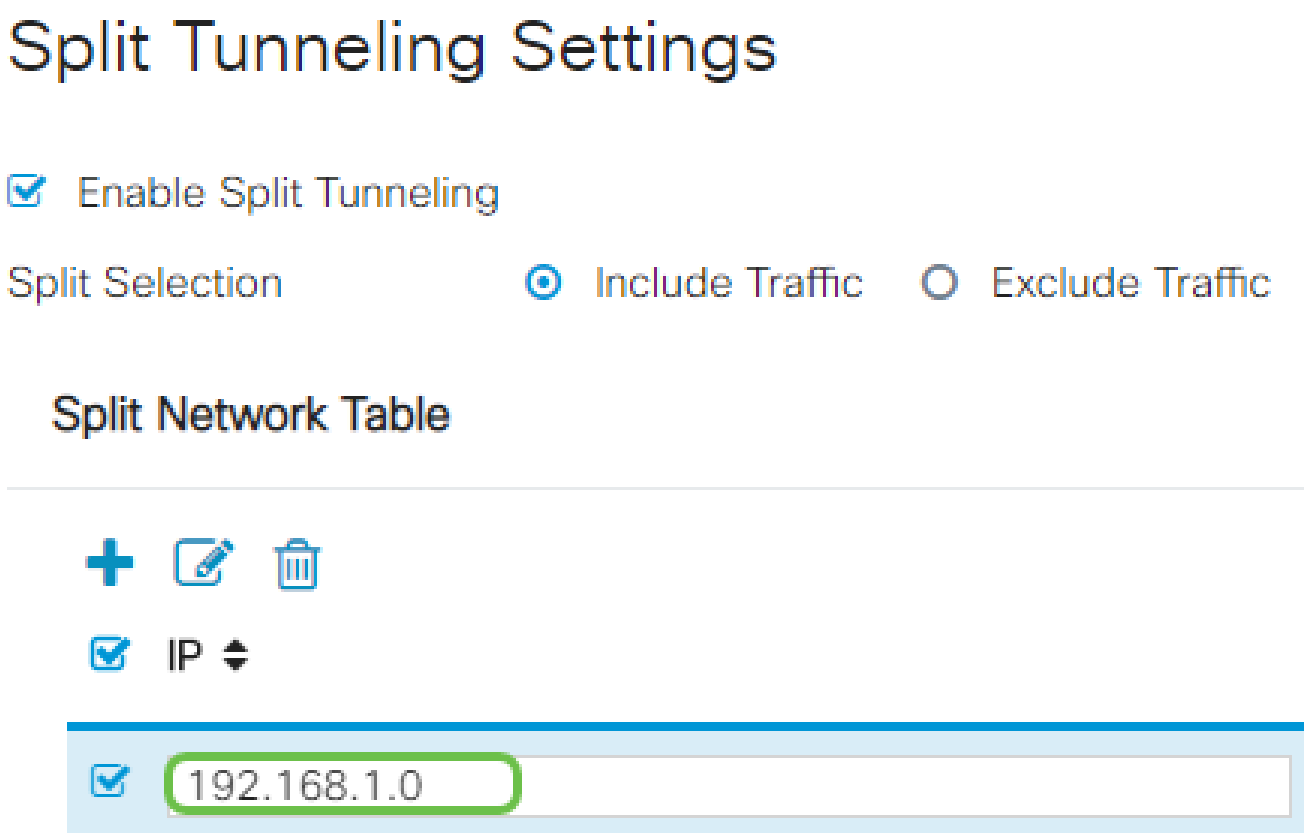
オプションボタンをクリックして、スプリットトンネリングを適用する際にトラフィックを含めるか除外するかを選択します。

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。

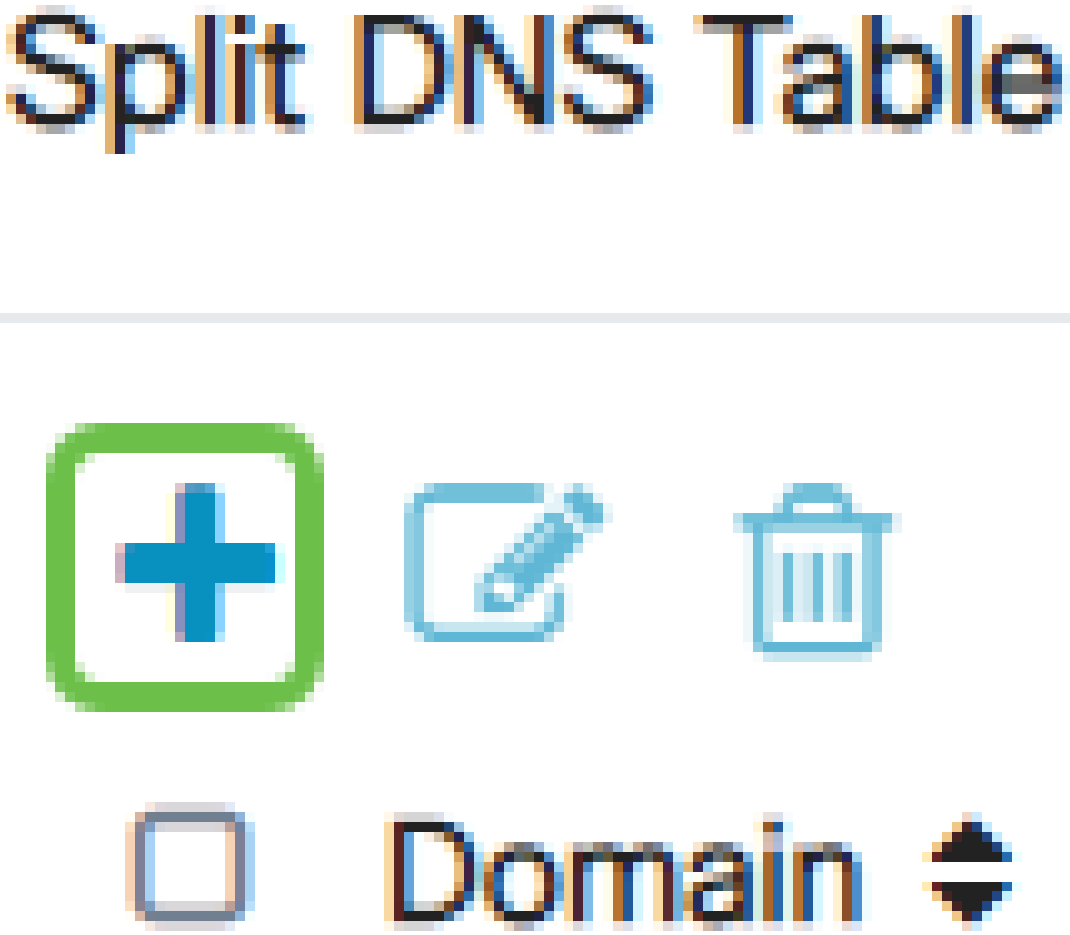
手順 8

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。



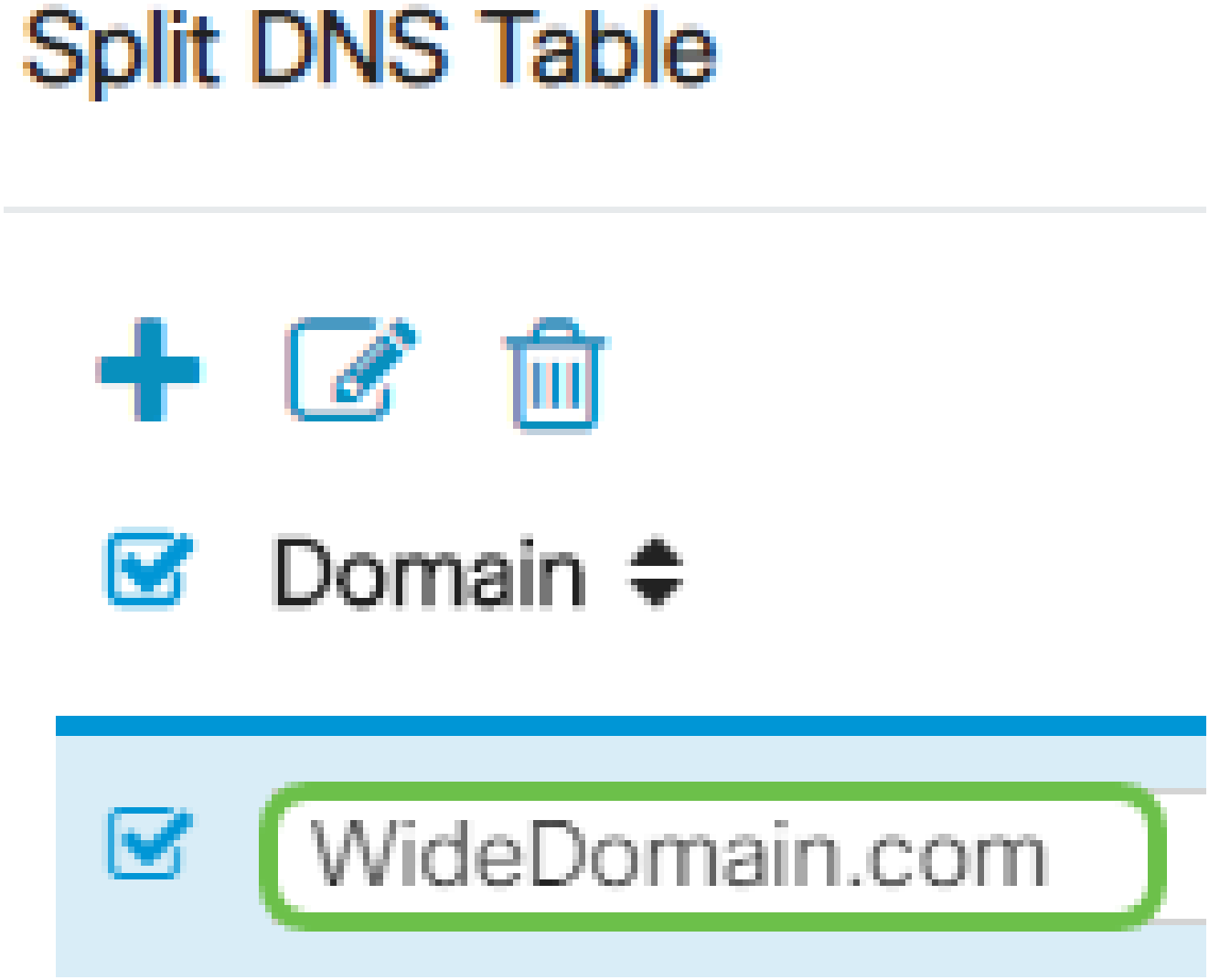
手順 9

スプリットDNSテーブルでadd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、Apply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ライセンスが必要になります。AnyConnectクライアントライセンスを使用すると、デスクトップクライアントとモバイルクライアントが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に接続しようと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設定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

的な場所によっては、VPNクライアントがハードウェアデバイスである場合もあります。これは通常、異なる場所にある2つのネットワークを接続するためにVPN接続が使用され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しているかのように、安全な方法で別のネットワークのリモートリソースにアクセスできるようになります。

ルータがAnyConnectに登録されて設定されると、クライアントは、購入したライセンスの使用可能な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。

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。ライセンスを発注する際には、name@domain.comの形式でシスコスマートアカウントIDまたはドメインIDを提供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、ここから探すことができます。

このドキュメントの作成時点では、次の製品SKUを使用して、25のバンドルで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 Ordering Guide』に記載されているその他のオプションがありますが、記載されている製品IDは、すべての機能を使用するための最小要件です。

最初にリストされているAnyConnectクライアントライセンスの製品SKUは、1年間のライセンスを提供し、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その他の製品SKUも、次に示すさまざまなサブスクリプションレベルで利用できます。

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

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場合は、次のリンクをクライアントに送信する必要があります。

- Windows:WindowsコンピュータへのAnyConnect
- Mac:MacにAnyConnectをインストールします。
- Ubuntuデスクトップ：Ubuntuデスクトップへの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のエラーに関する基本的なトラブルシューティングに関する情報の収集」に移動します。

AnyConnect VPN接続の確認

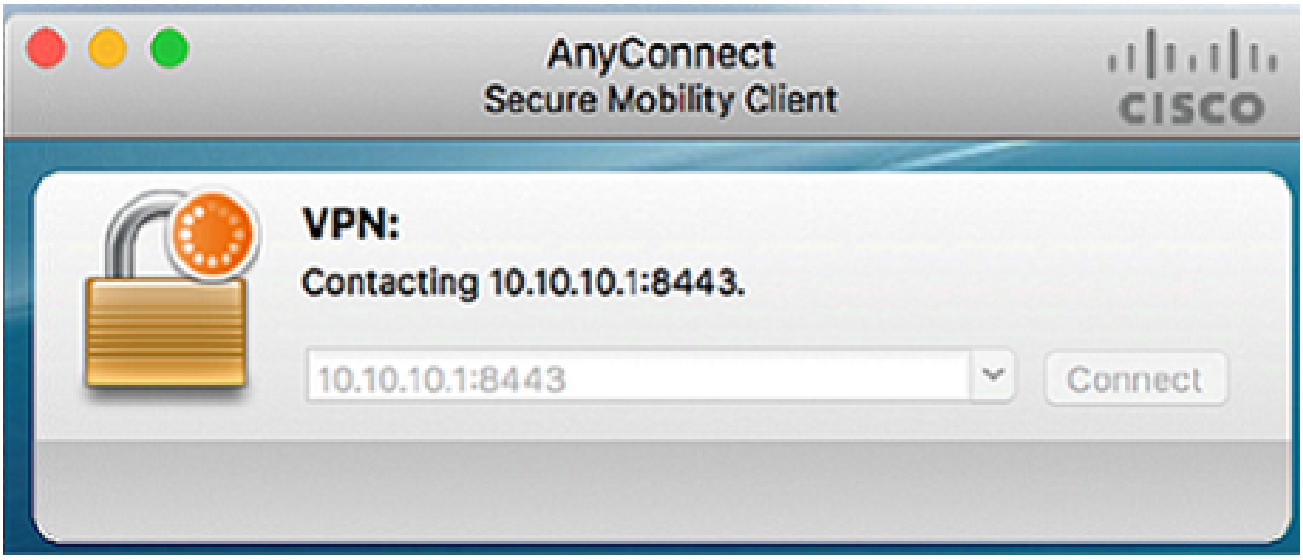
手順 1

AnyConnectセキュアモビリティクライアントのアイコンをクリックします。

手順 2

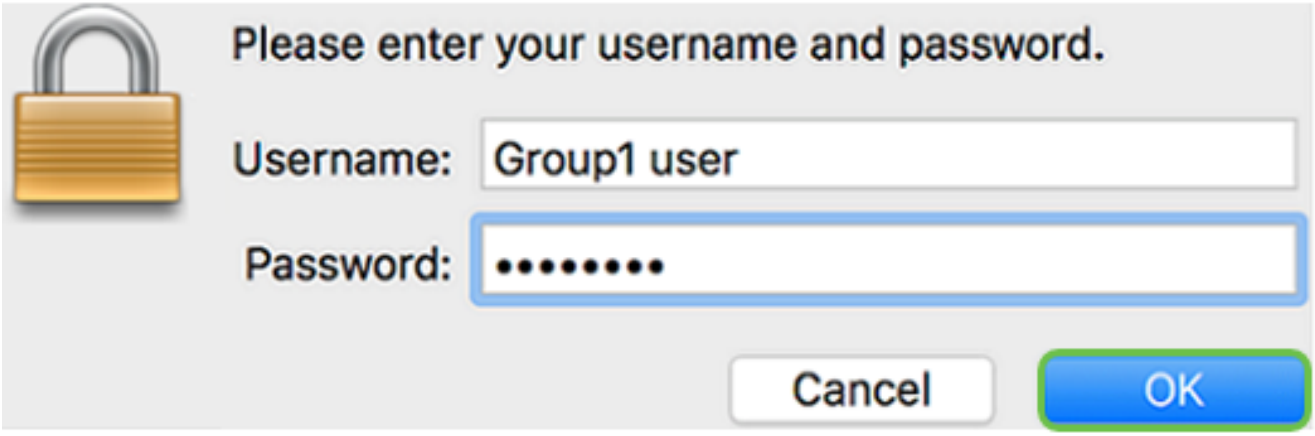
AnyConnectセキュアモビリティクライアントウィンドウで、ゲートウェイIPアドレスとゲートウェイポート番号をコロン(:)で区切って入力し、Connectをクリックします。

これで、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。



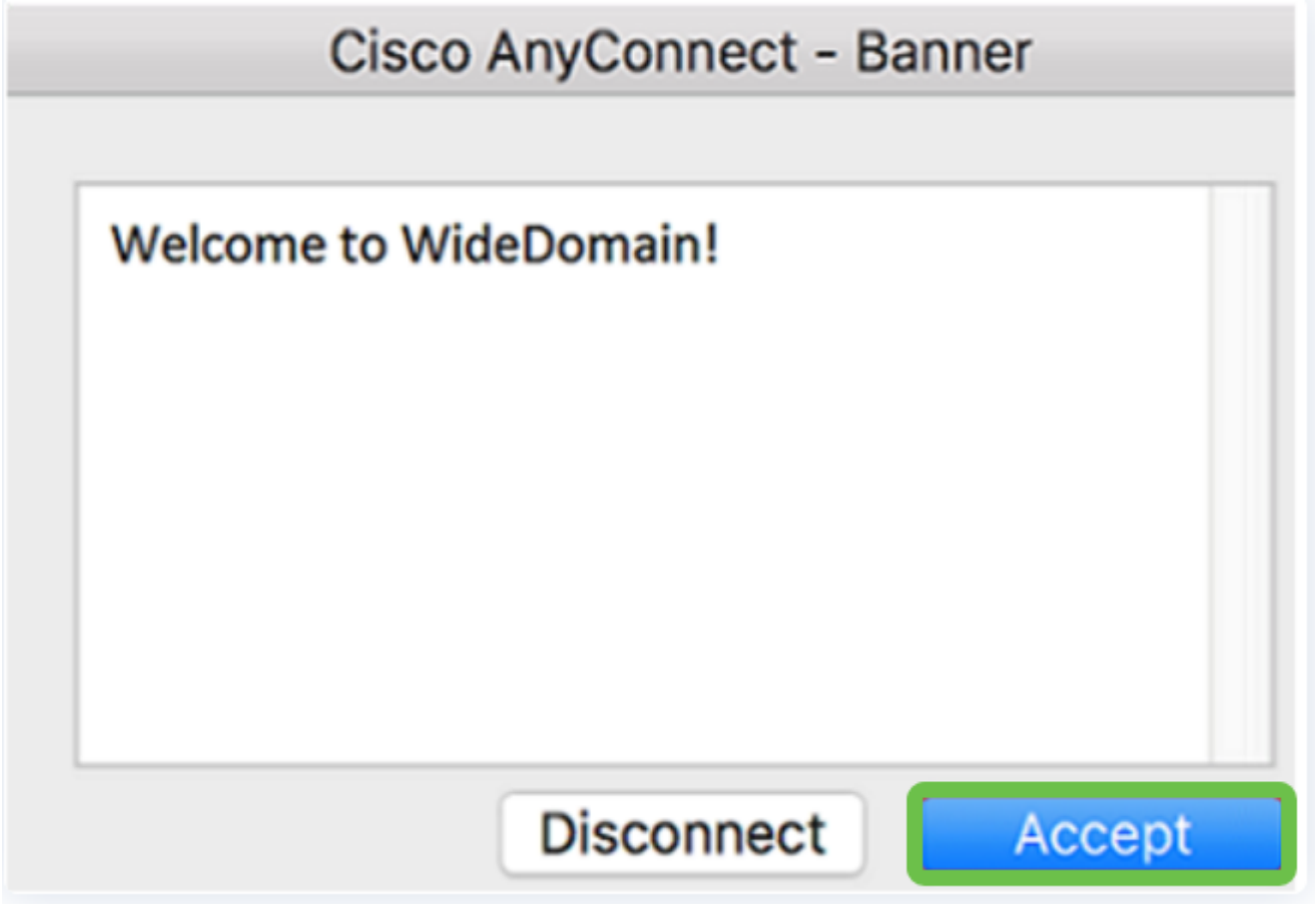
手順 3

それぞれのフィールドにサーバのユーザ名とパスワードを入力し、OKをクリックします。

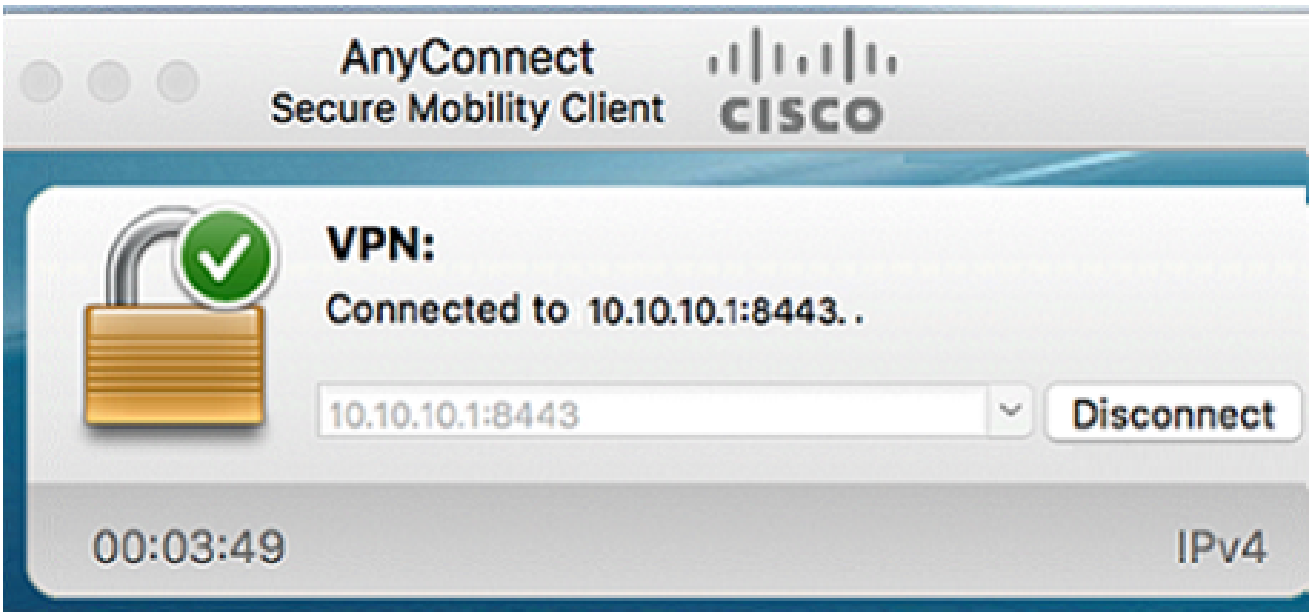


手順 4

接続が確立されるとすぐに、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オプションを省略して、次のセクションに進むことができます。

ShrewソフトVPN

IPsec VPNを使用すると、インターネット上に暗号化されたトンネルを確立して、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を説明します。

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、サポートを受けるために彼らに連絡してください。

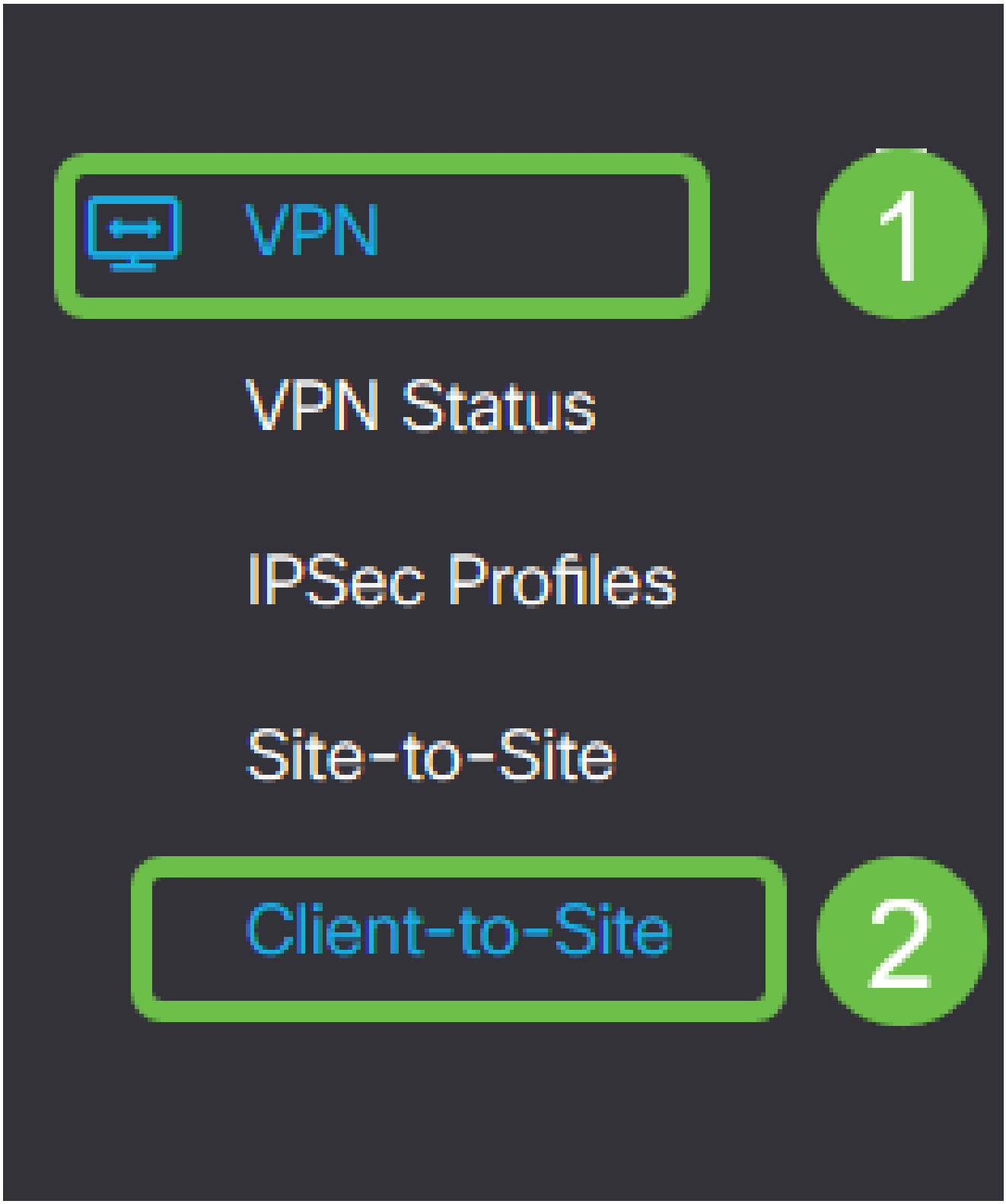
Shrew Soft VPN Clientソフトウェアの最新バージョンは、https://www.shrew.net/download/vpnからダウンロードできます。

RV345Pシリーズルータでの Shrew Softの設定

まず、RV345Pでクライアントとサイト間VPNを設定します。

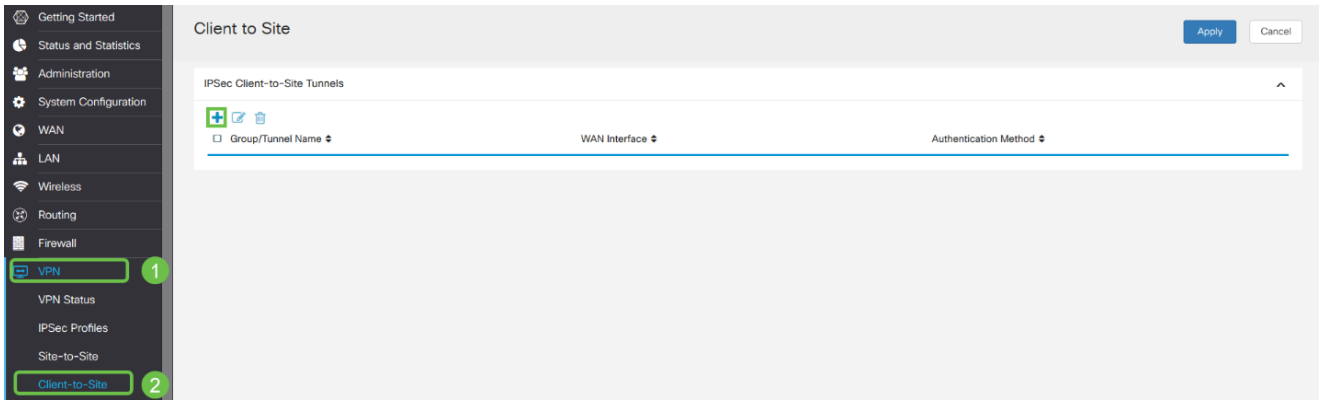
手順 1

VPN > Client-to-Siteの順に移動します。



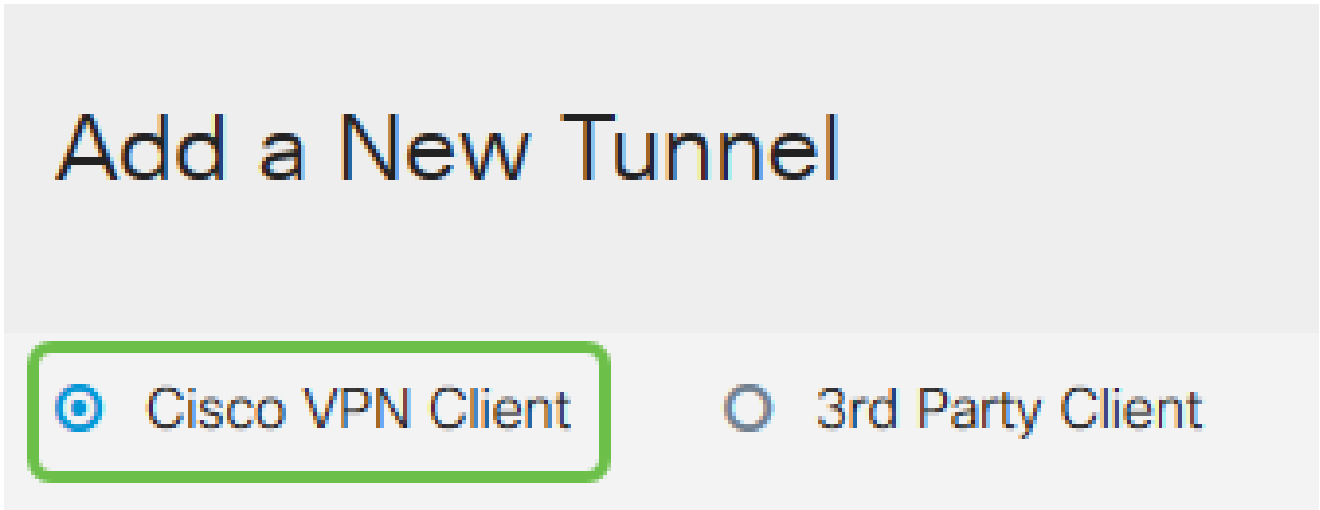
手順 2

Client-to-Site VPNプロファイルを追加します。



手順 3

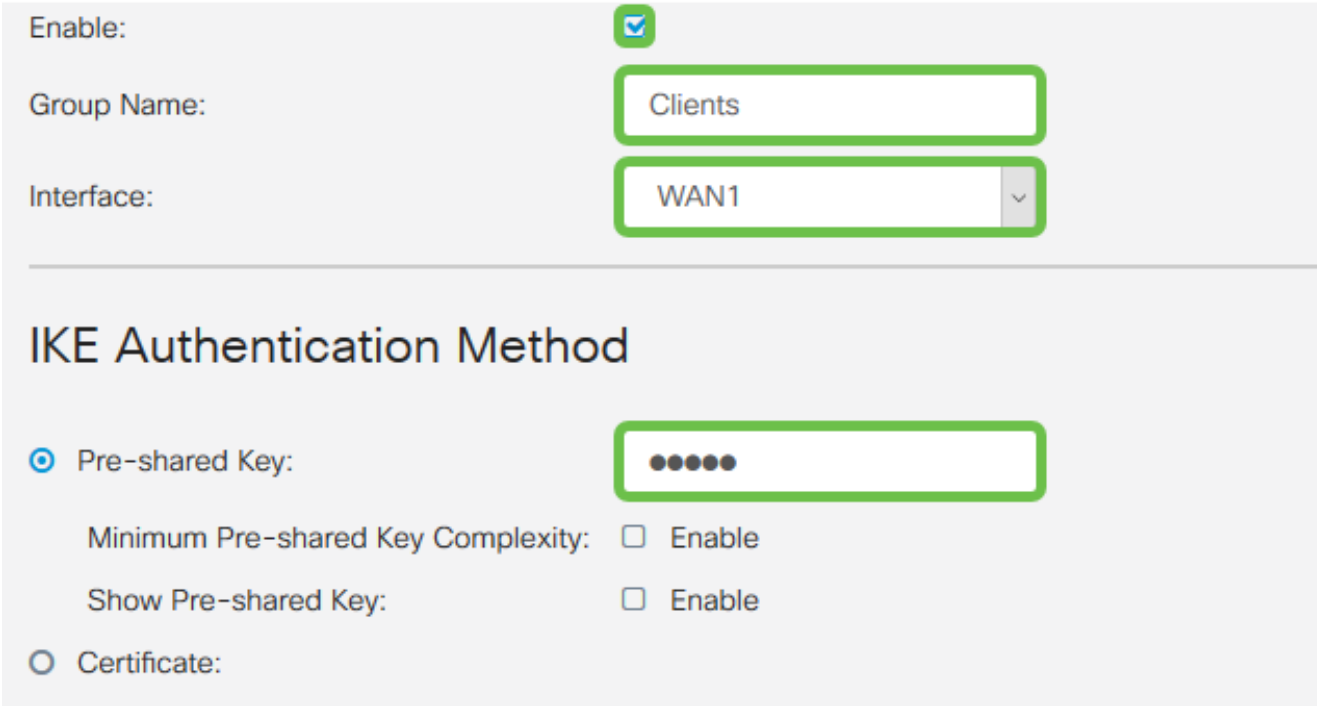
Cisco VPN Clientオプションを選択します。



手順 4

Enableボックスにチェックマークを入れて、VPN Clientプロファイルをアクティブにします。また、グループ名を設定し、WANインターフェイスを選択して、事前共有キーを入力します。

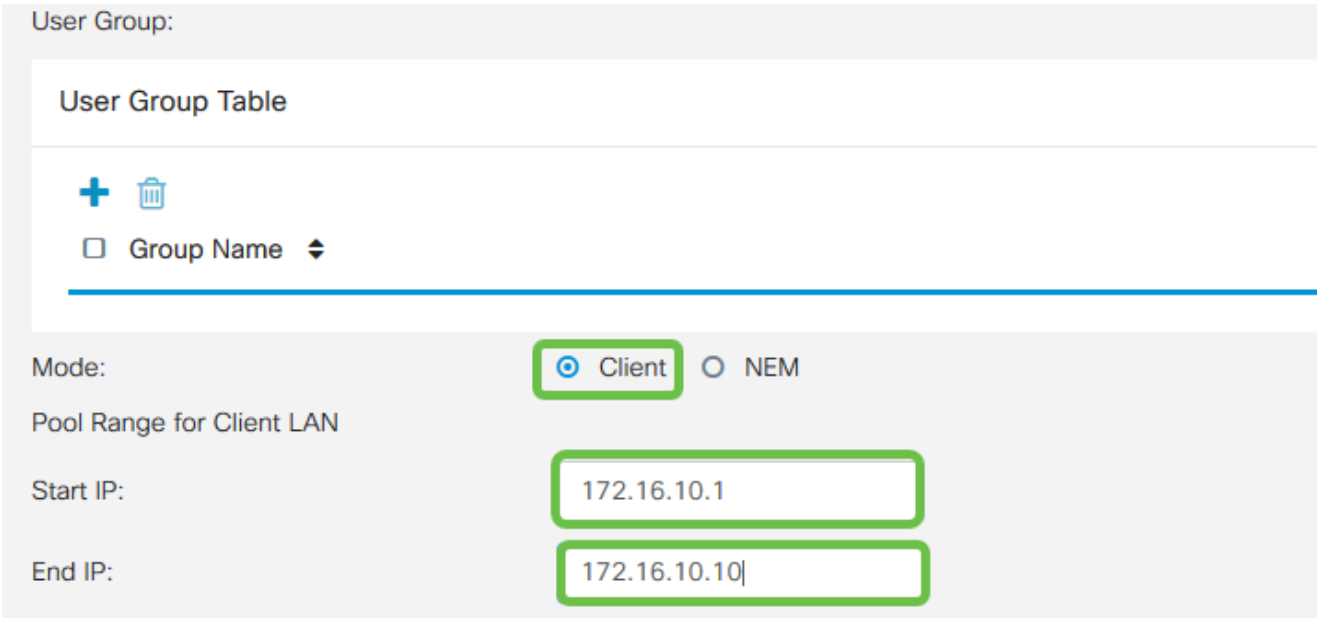
グループ名と 事前共有キーは後でクライアントの設定時に使用するため、注意してください。



手順 5

ここでは、ユーザグループテーブルを空白のままにします。これはルータのユーザグループ用ですが、まだ設定されていません。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。ここでは、172.16.10.1 ~ 172.16.10.10を使用します。

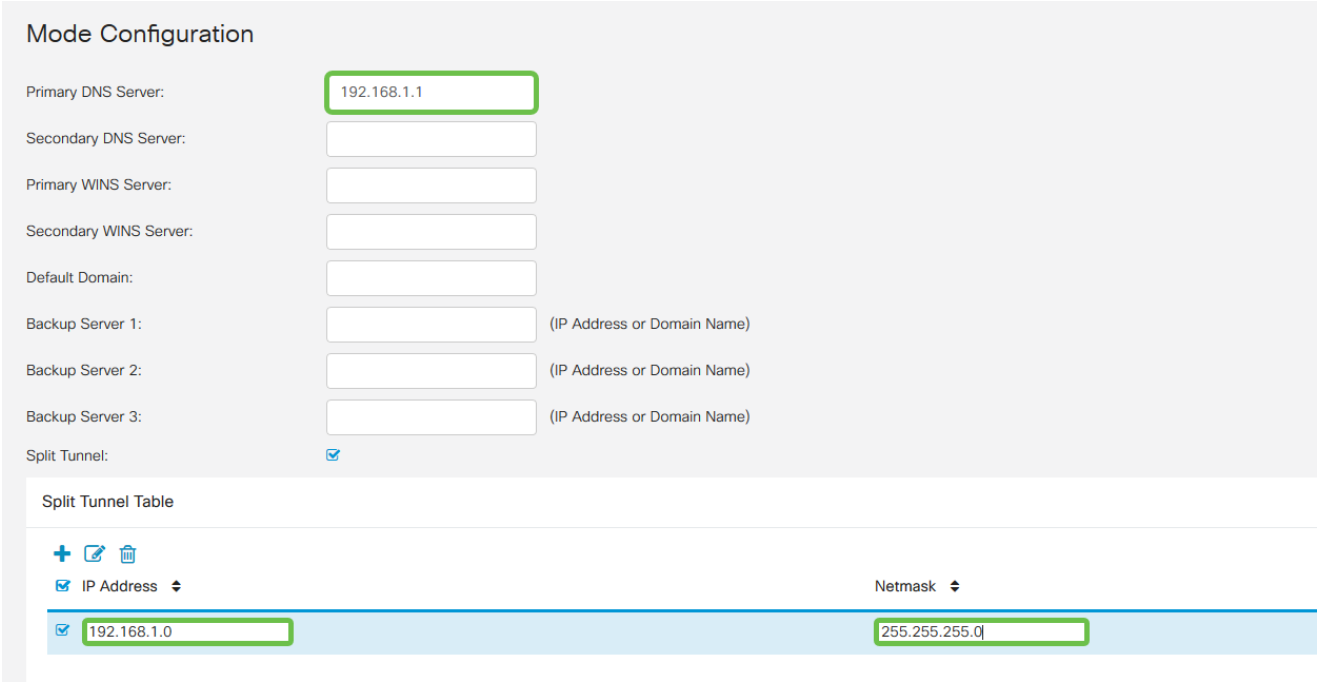
プール範囲は、ネットワーク上の他の場所で使用されていない一意のサブネットを使用する必要があります。



手順 6

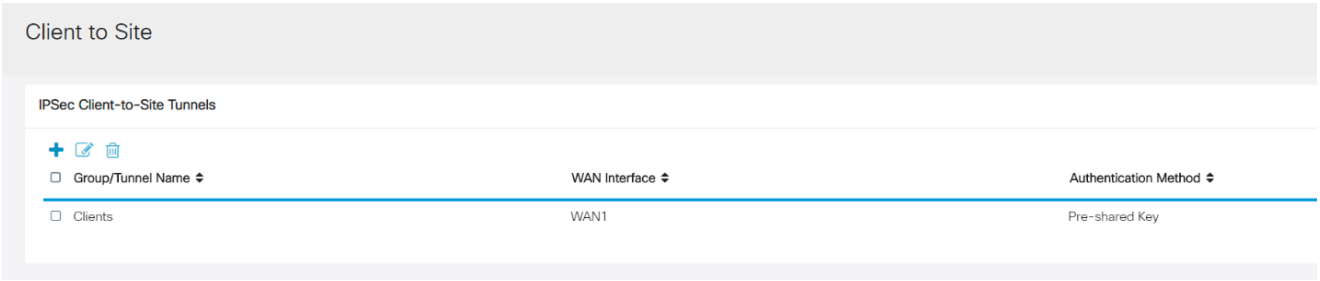
ここでは、Mode Configurationの設定を行います。使用する設定を次に示します。

- 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。
- Split Tunnel:Split Tunnelingを有効にする場合にオンにします。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経由でアクセスす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ます。



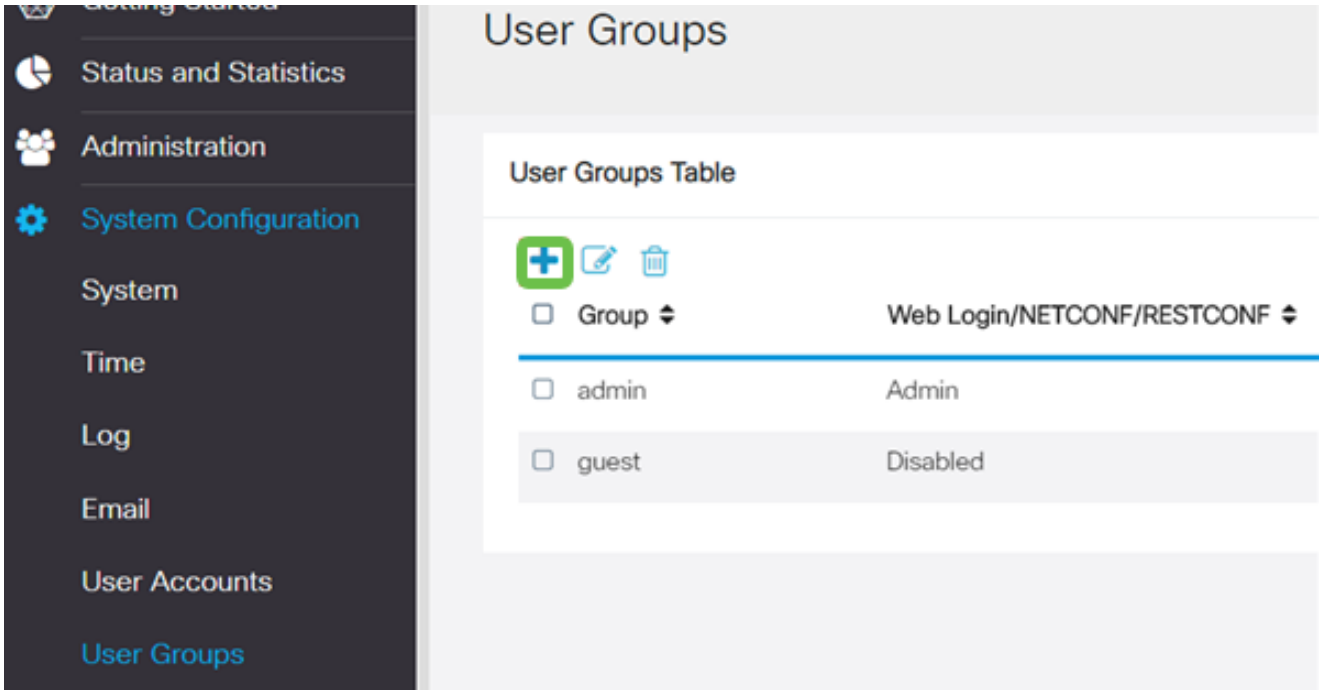
ステップ7

Save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。



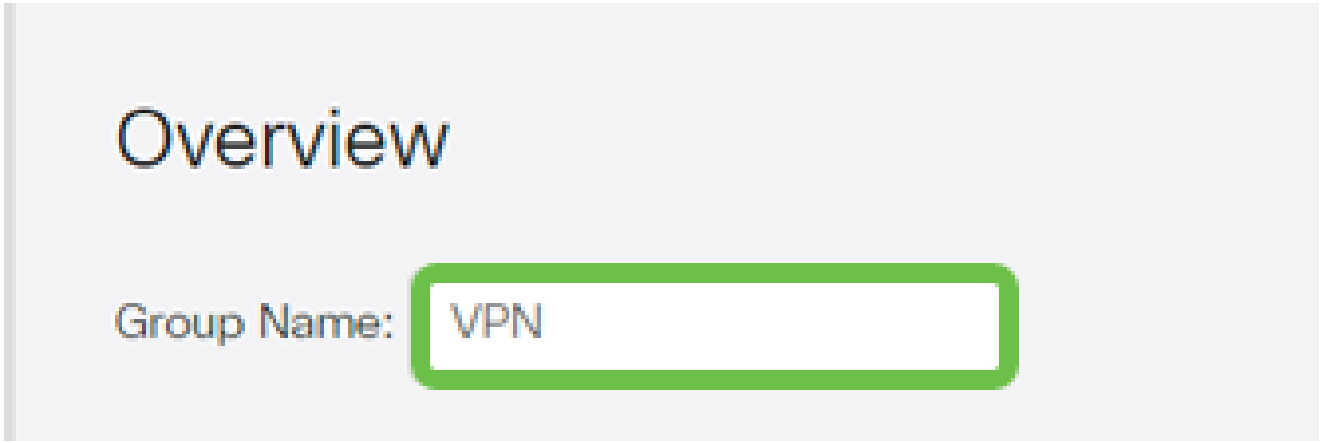
手順 8

VPNクライアントユーザの認証に使用するユーザグループを設定します。System Configuration > User Groupsの下で、プラス記号のアイコンをクリックしてユーザグループを追加します。



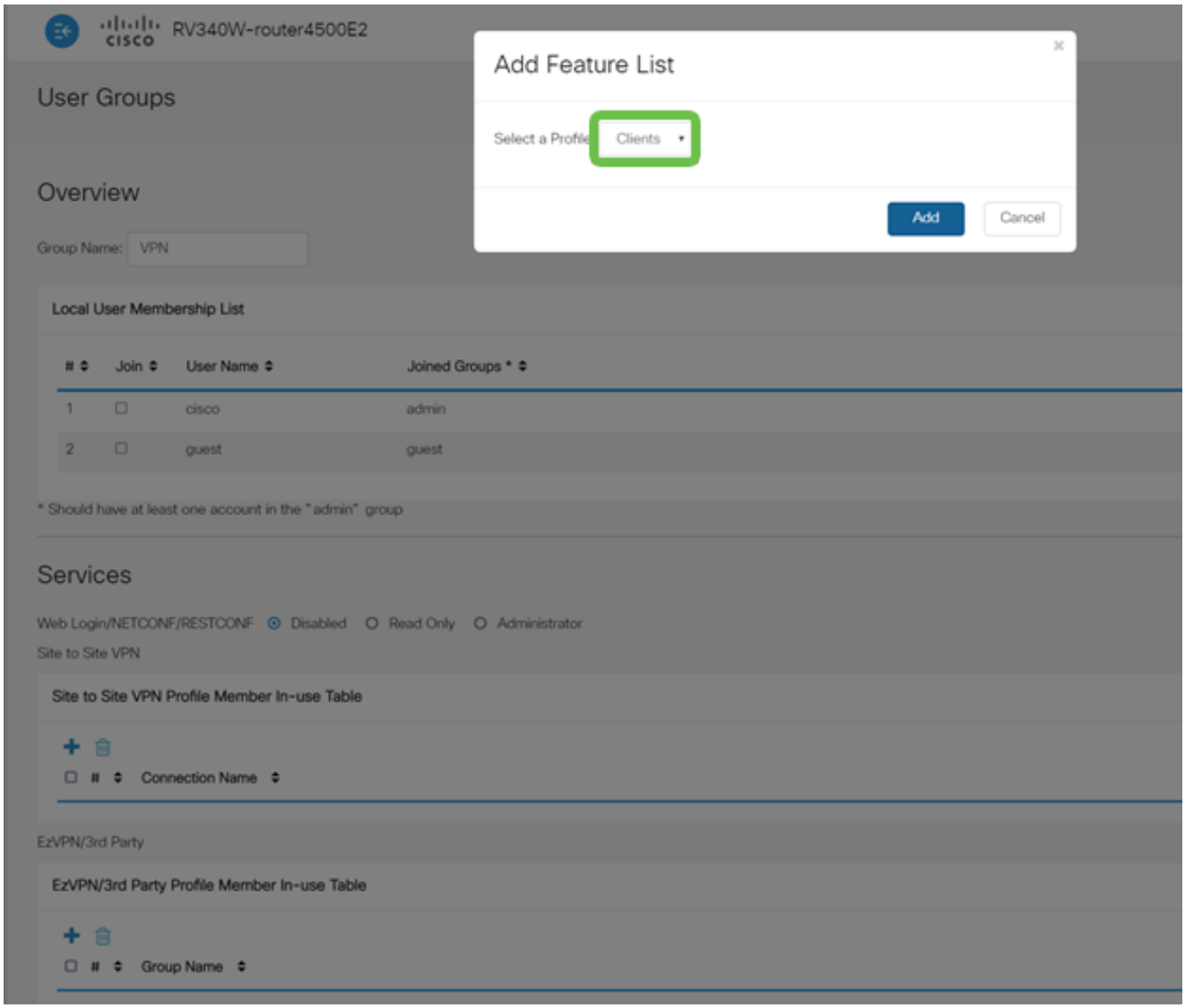
手順 9

グループ名を入力します。



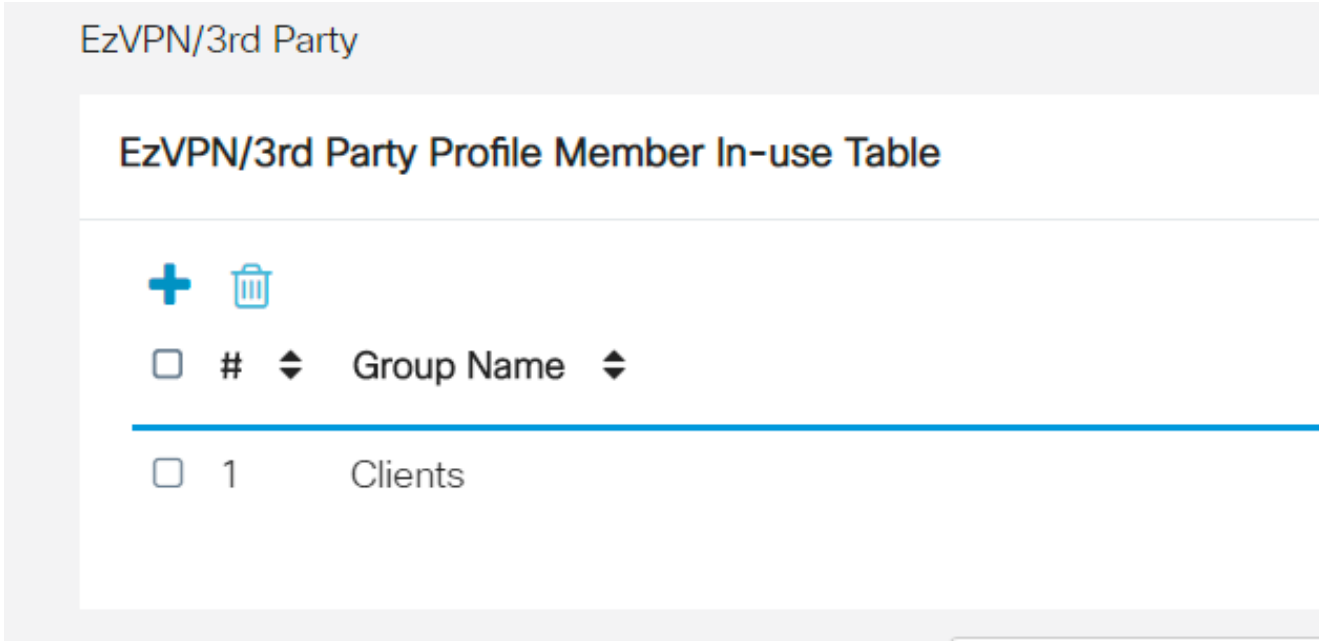
手順 10

Services > EzVPN/3rd Partyの順にクリックし、Addをクリックして、このユーザグループを、以前に設定したClient-to-Siteプロファイルにリンクします。



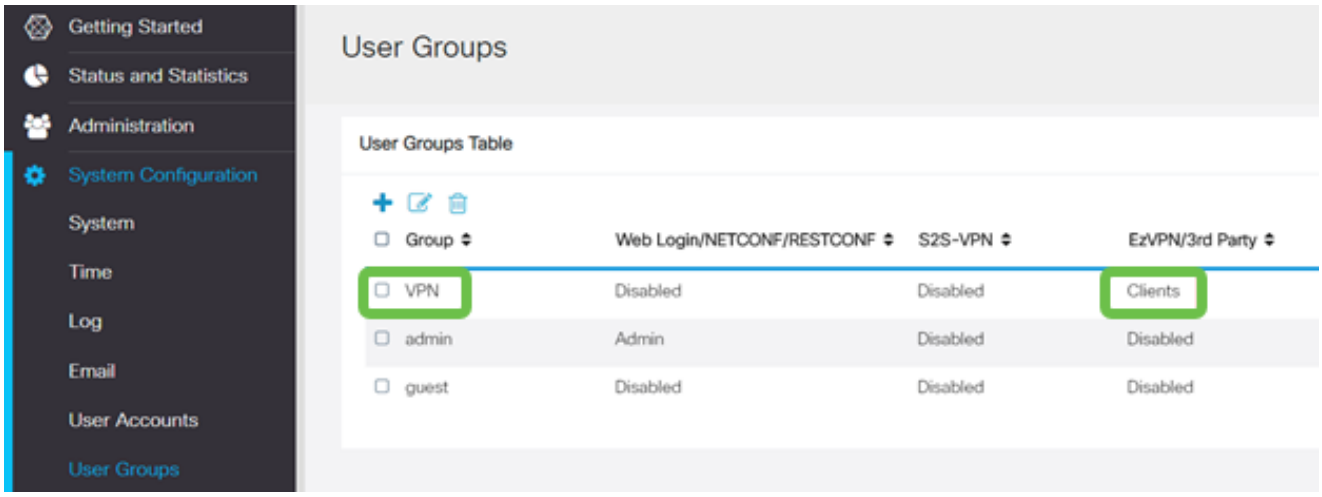
手順 11

Client-to-Siteグループ名がEzVPN/サードパーティのリストに表示されます。



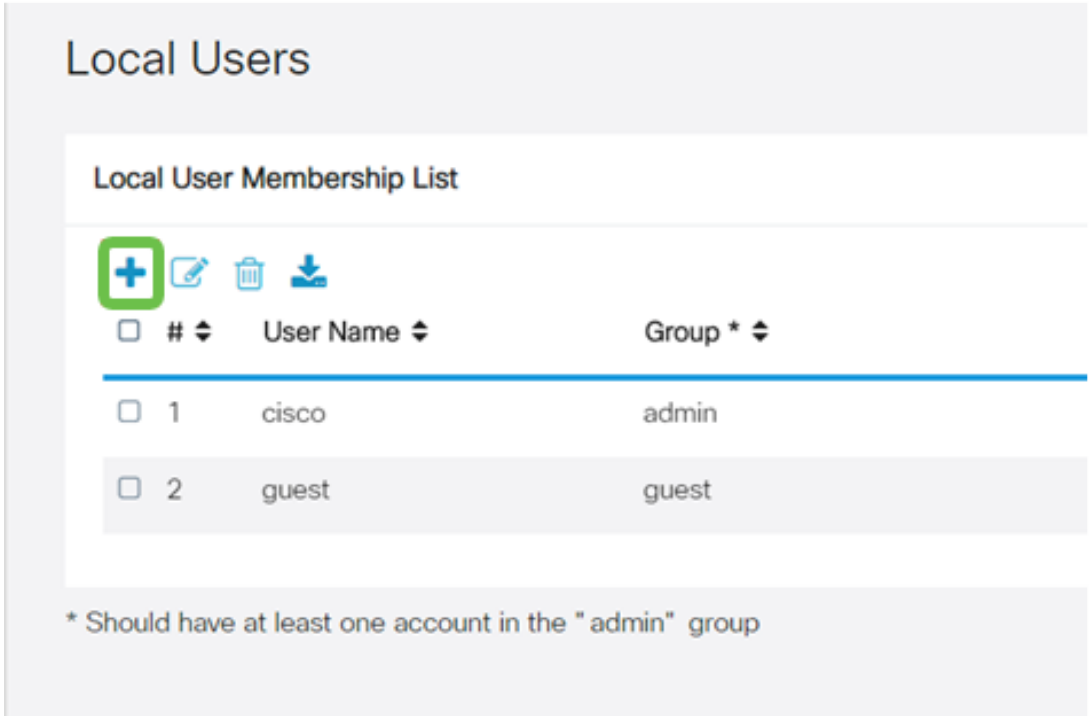
手順 12

ユーザグループの設定を適用すると、ユーザグループのリストにその設定が表示され、先ほど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ることが示されます。



手順 13

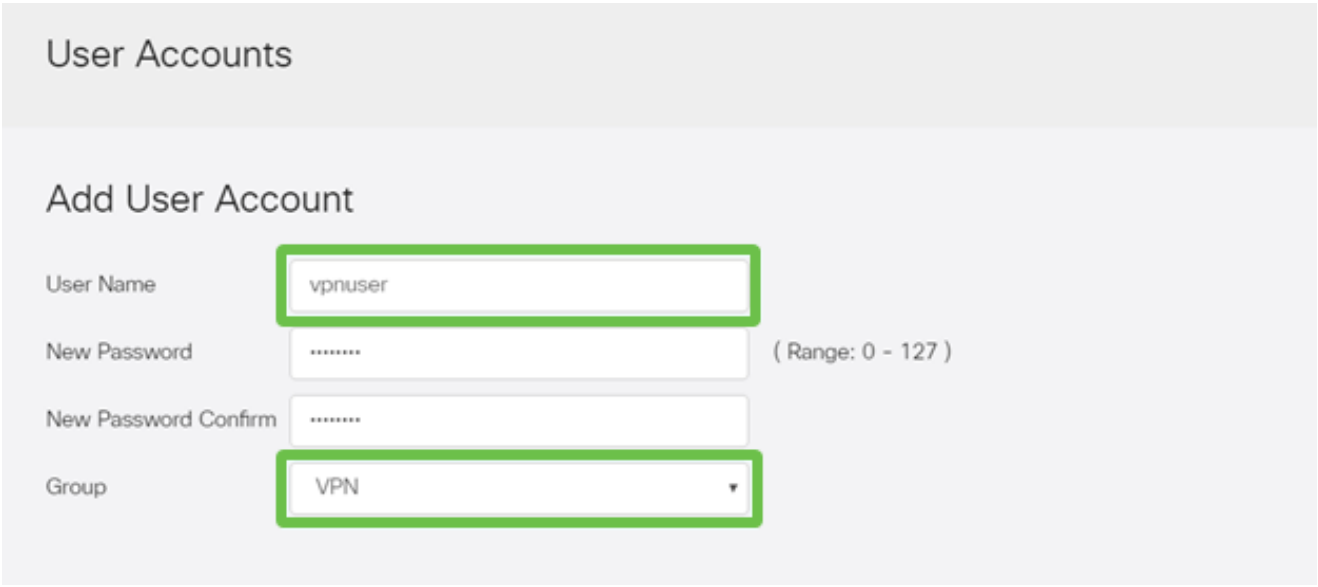
System Configuration > User Accountsで新しいユーザを設定します。プラスアイコンをクリックして、新しいユーザを作成します。



手順 14

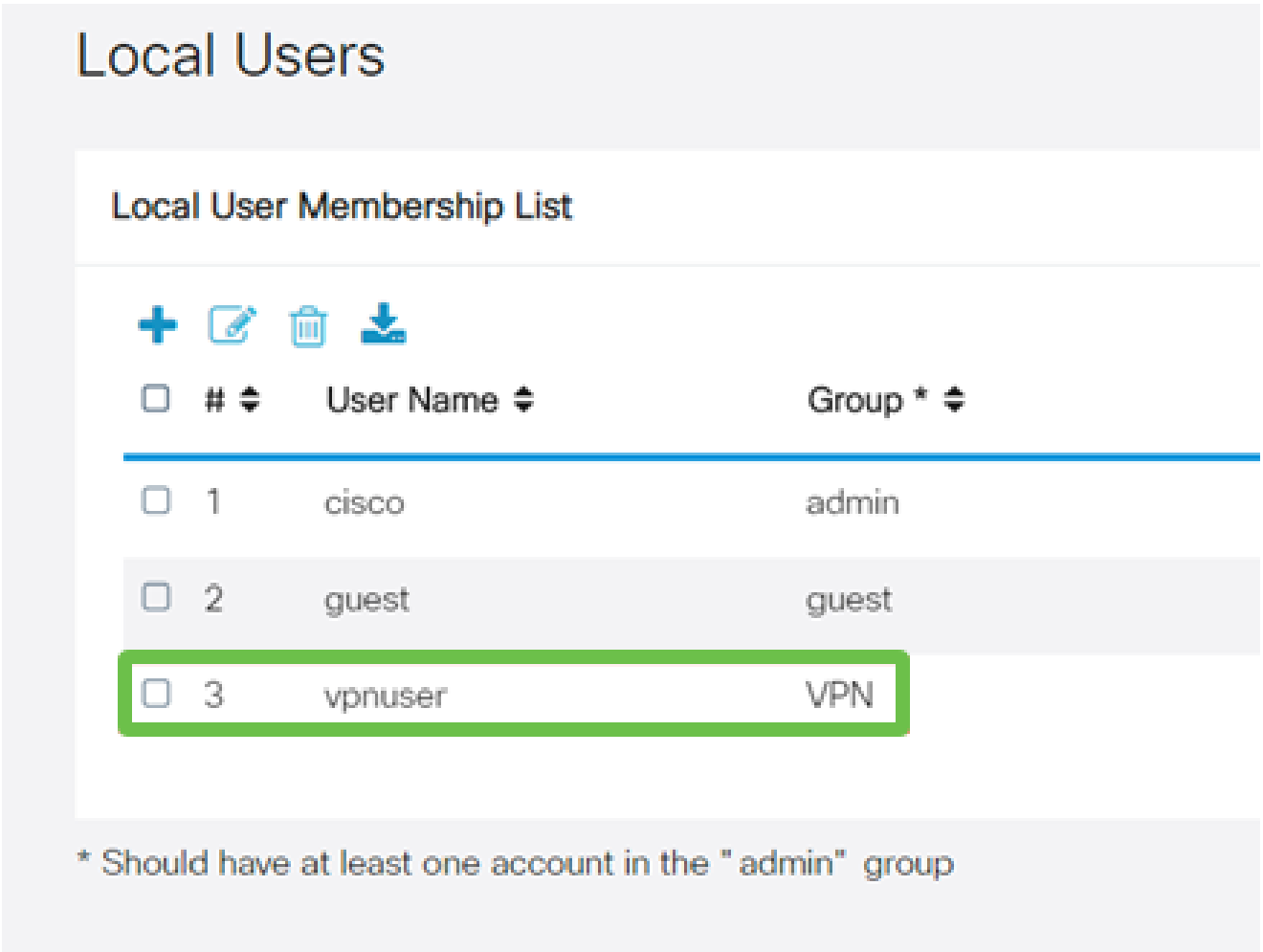
新しいユーザ名と新しいパスワードを入力します。Groupが設定したばかりの新しいUser

Groupに設定されていることを確認します。最後に、[Apply] をクリックします



手順 15

新しいユーザがローカルユーザ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、Shrew Soft VPN Clientを設定します。

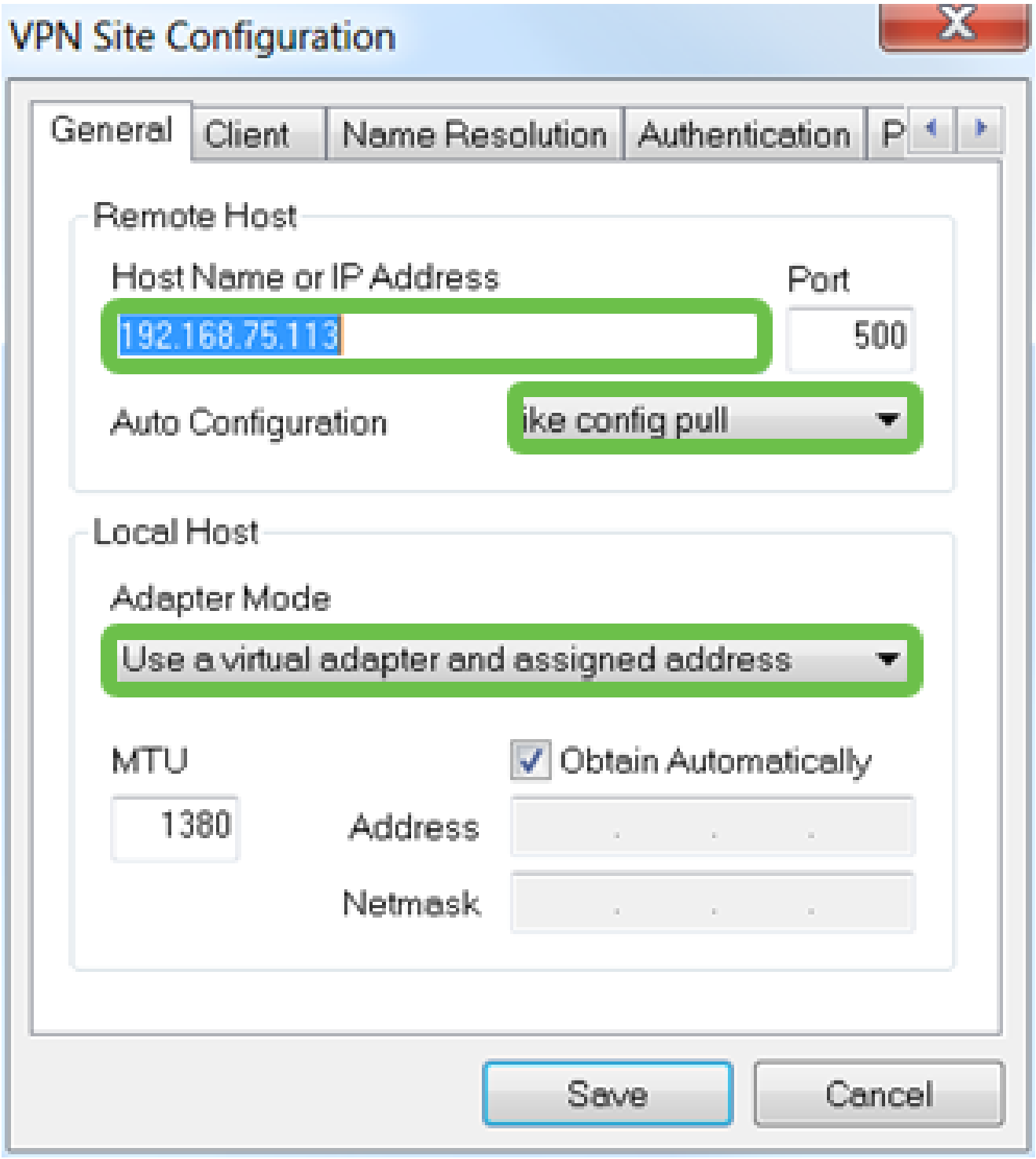
Shrew Soft VPN Clientの設定

次の手順を実行します。

手順 1

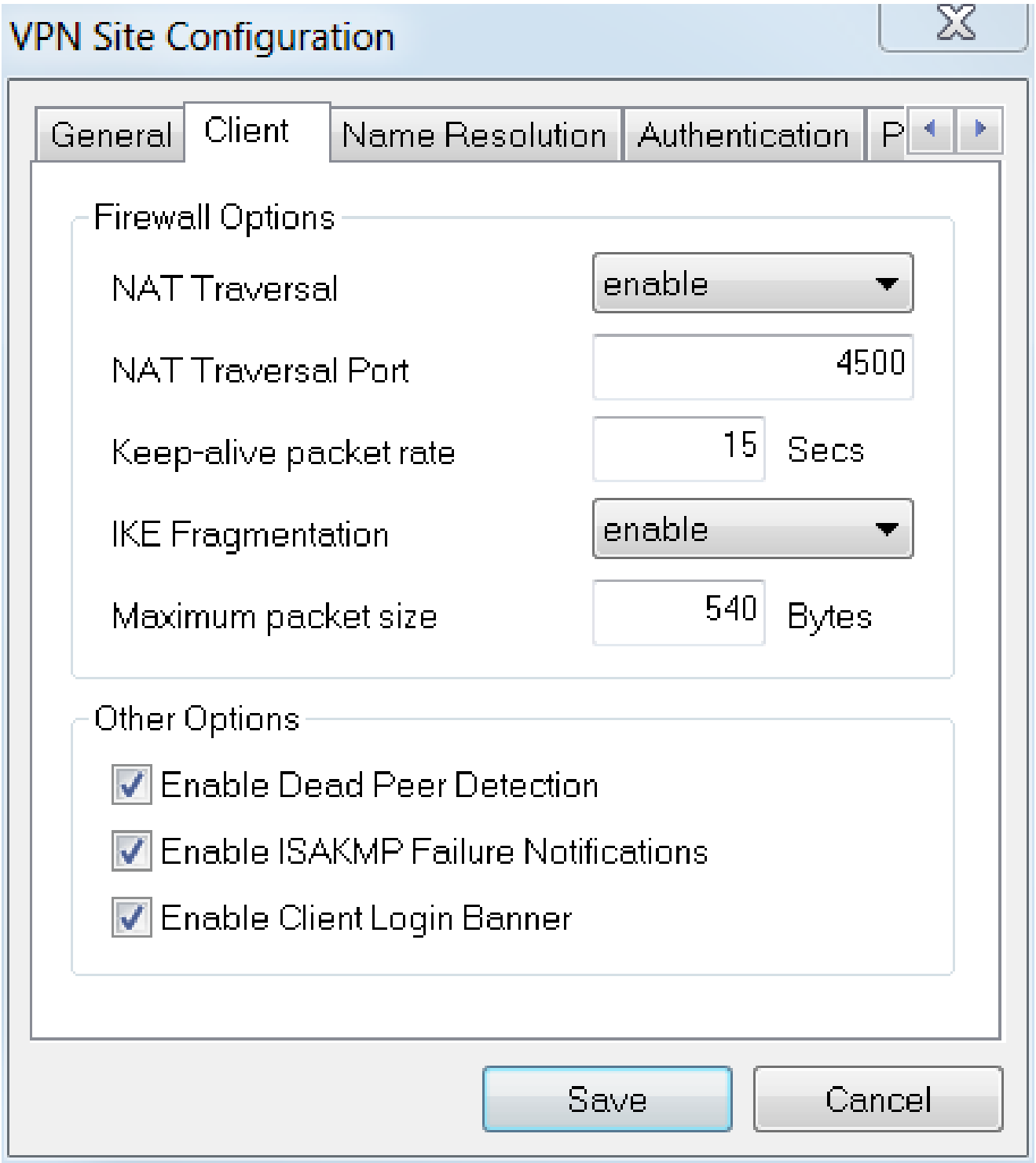
Shrew Soft VPN Access Managerを開き、Addをクリックしてプロファイルを追加します。表示されるVPN Site Configurationウィンドウで、Generalタブを設定します。

- Hostname or IP Address:WAN IPアドレス（またはRV345Pのホスト名）を使用します。
- 自動設定:ike config pullを選択します。
- Adapter Mode:Use a Virtual adapter and assigned addressを選択します。



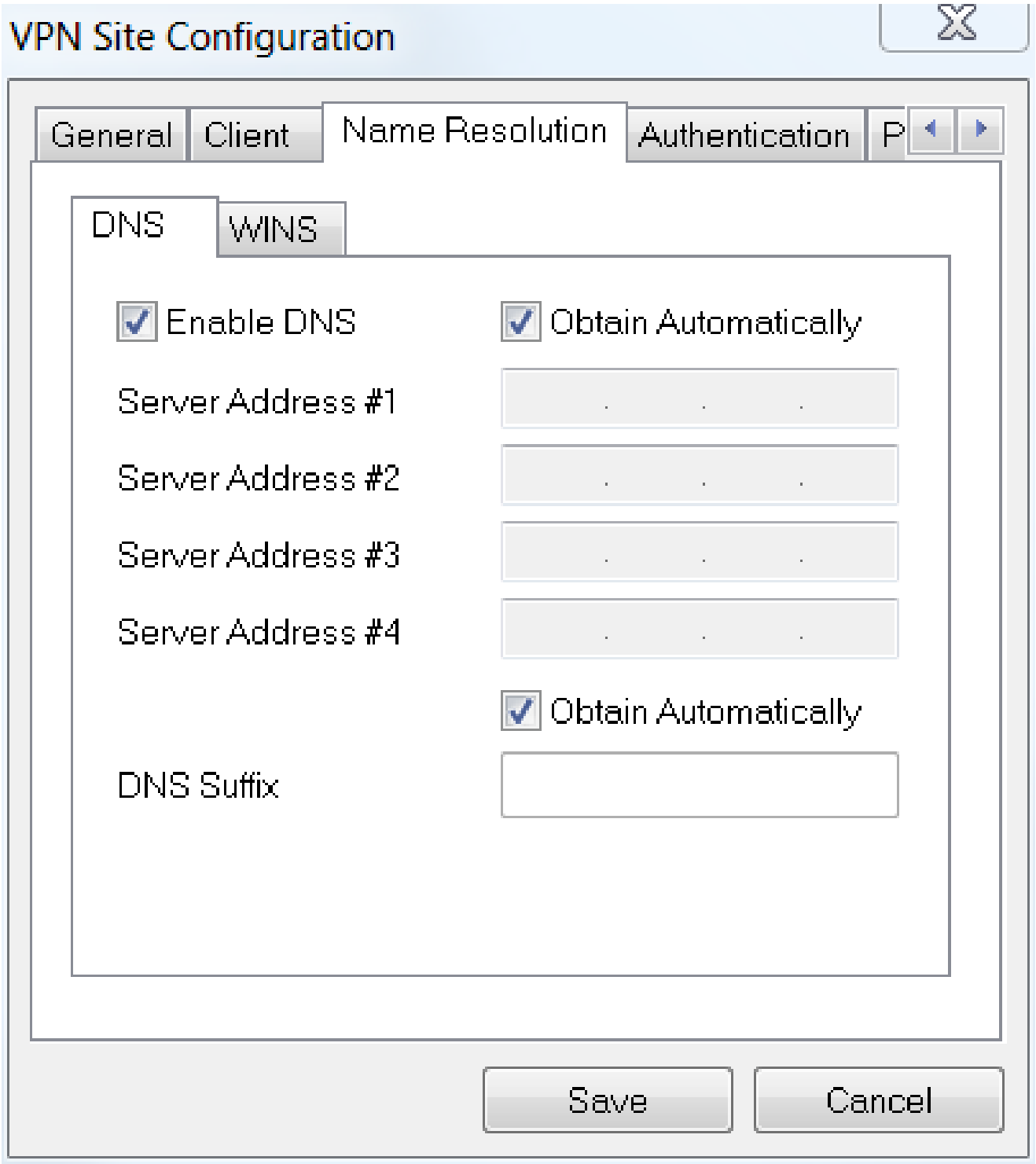
手順 2

Clientタブを設定します。この例では、デフォルト設定のままにしています。



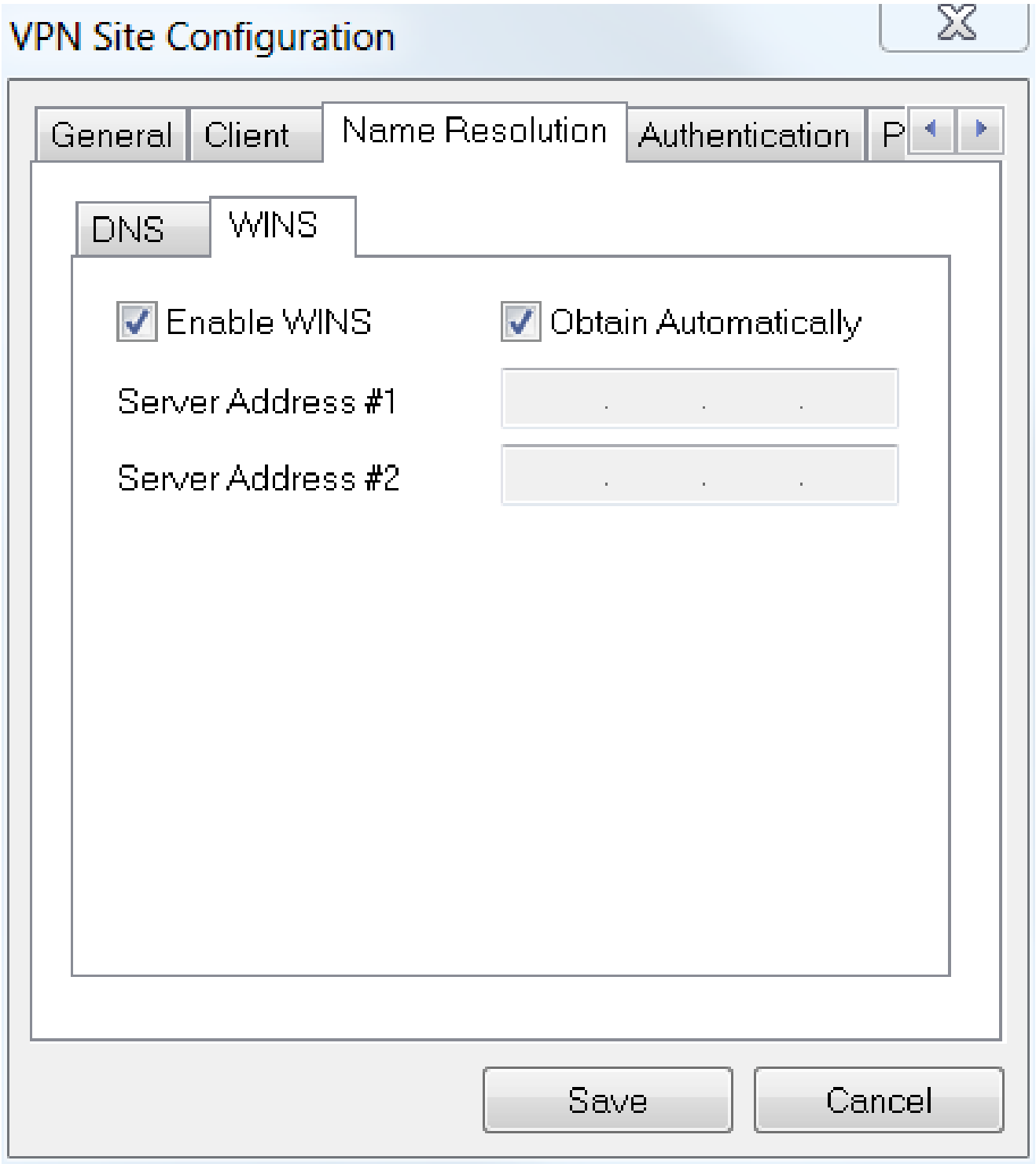
手順 3

Name Resolution > DNSの下で、Enable DNS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たままにします。



手順 4

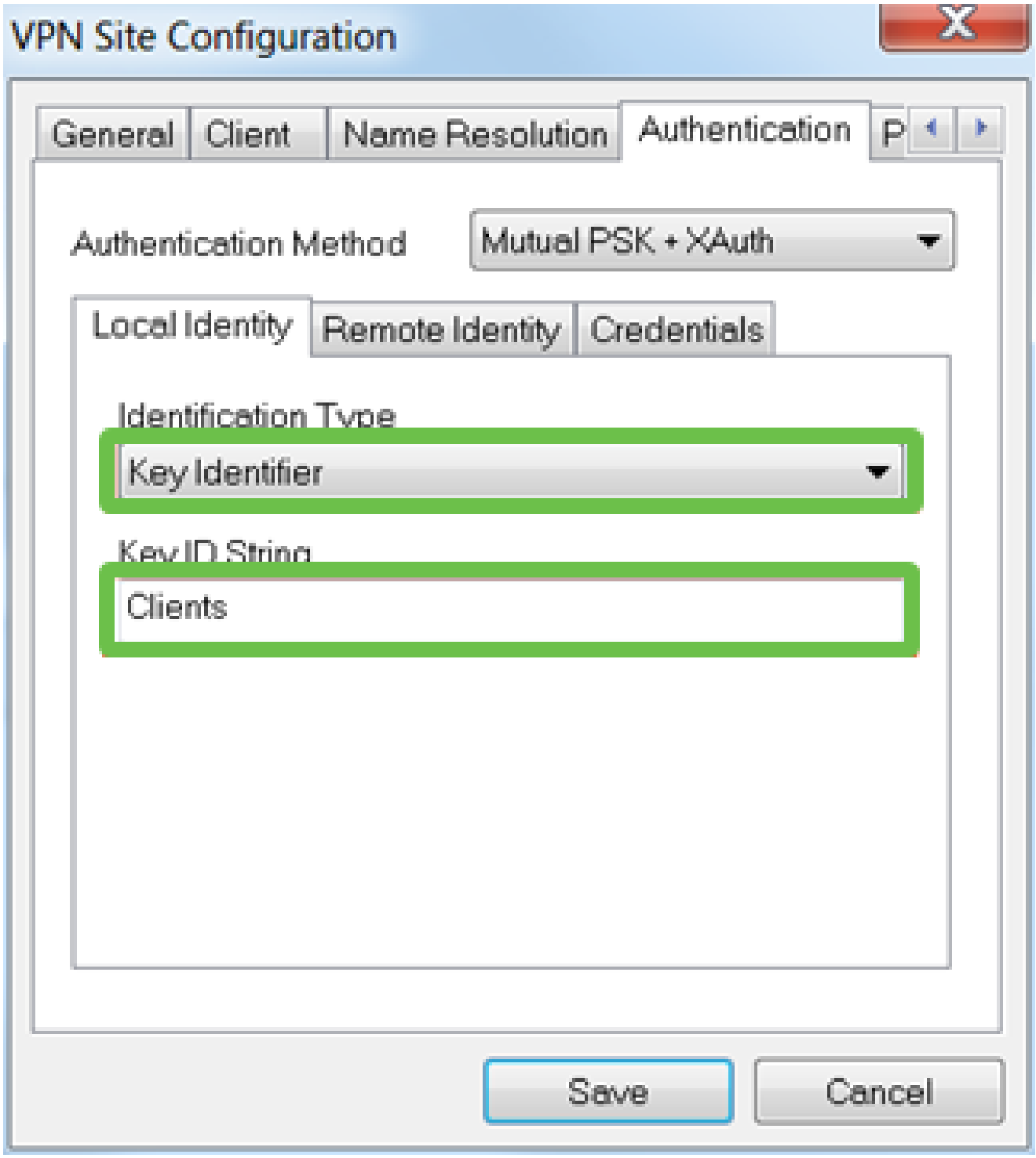
Name Resolution > WINSタブで、Enable WINSボックスにチェックマークを入れ、Obtain Automaticallyボックスにチェックマークを入れたままにします。



手順 5

Authentication > Local Identityの順にクリックします。

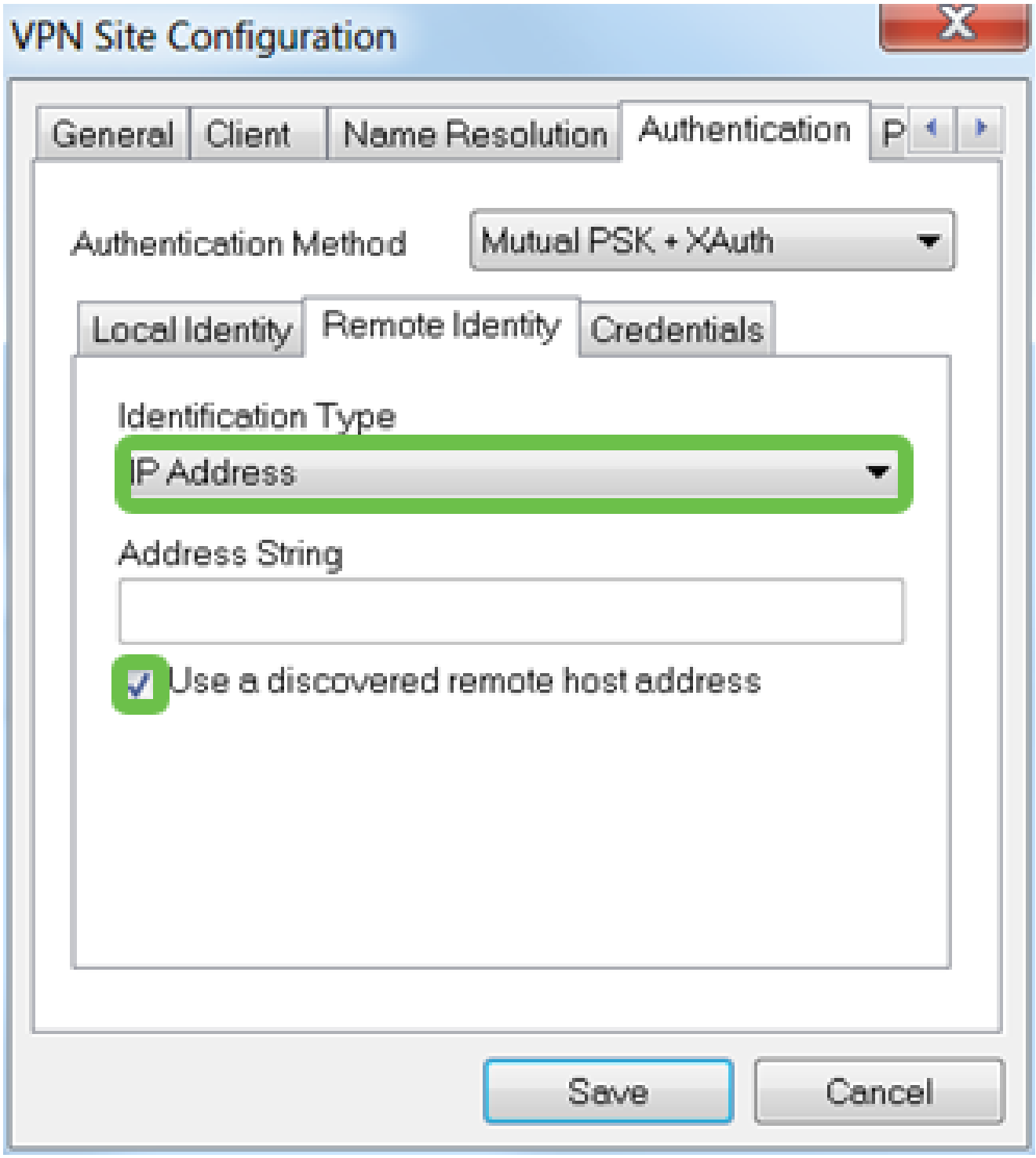
- IDタイプ:キーIDの選択
- Key ID String:RV345Pで設定されたグループ名を入力します。



手順 6

Authentication > Remote Identityの順に選択します。この例では、デフォルト設定のままにしています。

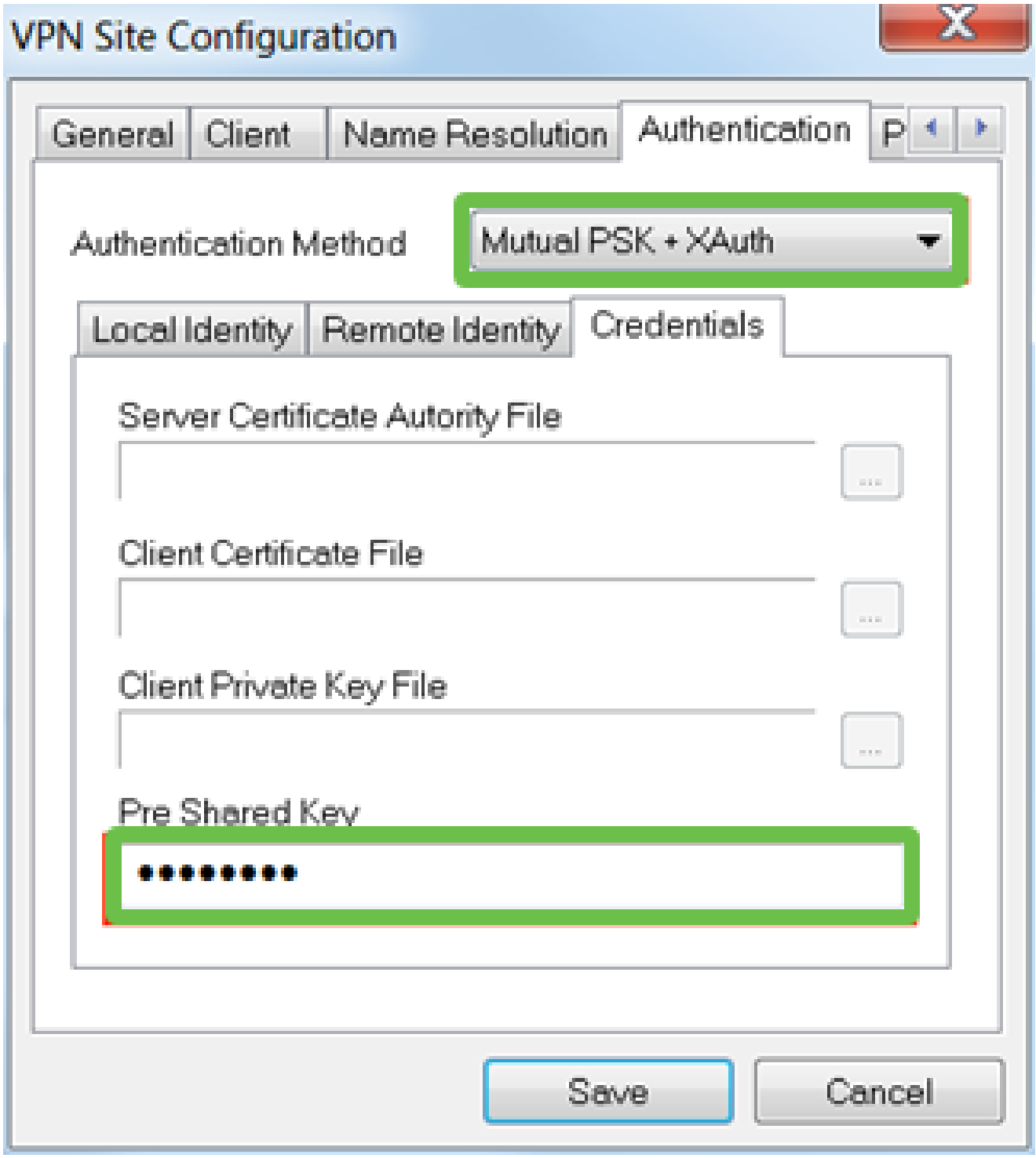
- IDタイプ:IPアドレス
- アドレス文字列: <空白>
- Use a discovered remote host addressボックス：オン



ステップ7

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

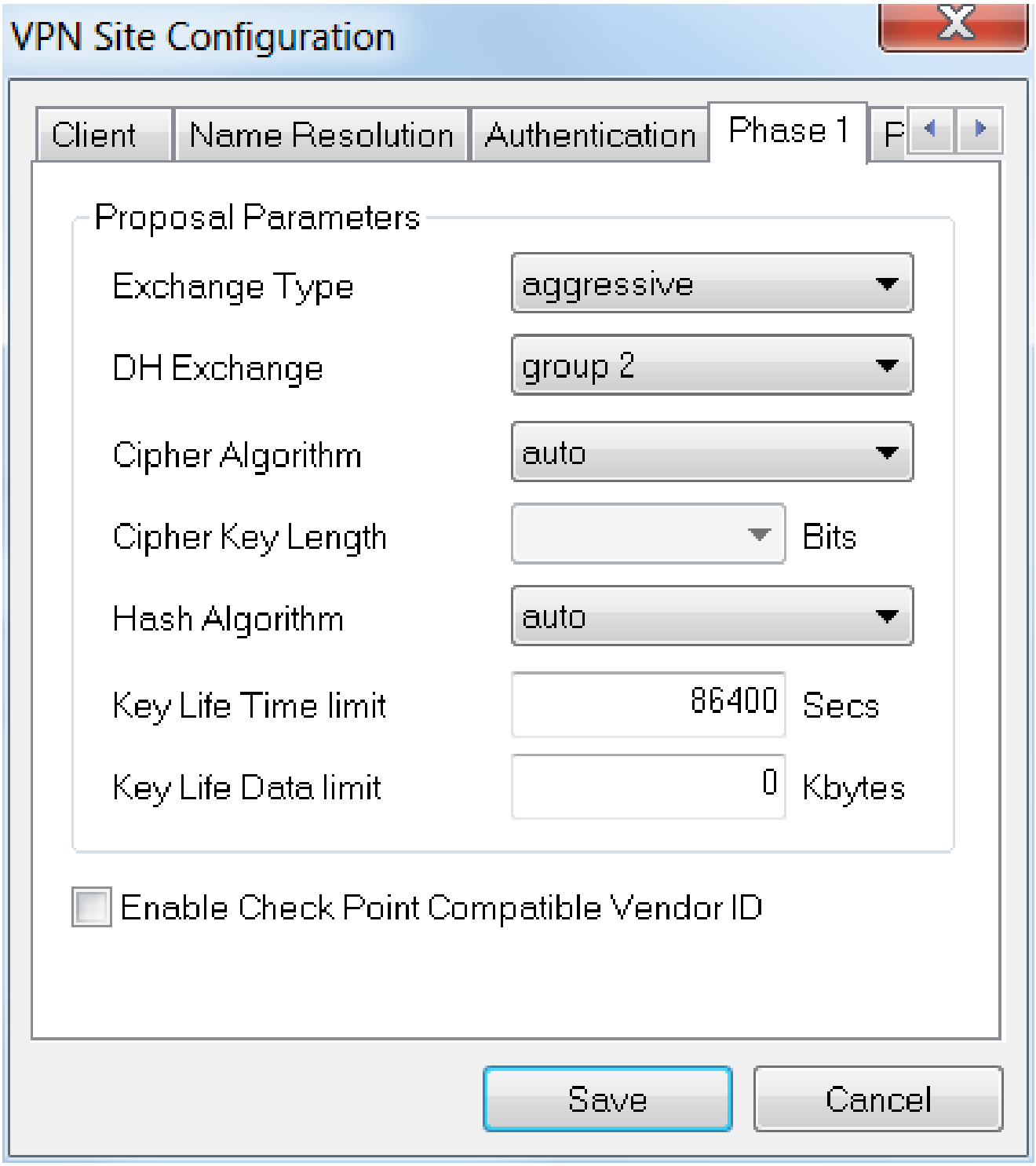
- Authentication Method:Mutual PSK + XAuthを選択します
- 事前共有キー:RV345Pクライアントプロファイルで設定されている事前共有キーを入力します



手順 8

Phase 1タブの場合。この例では、デフォルト設定が維持されています。

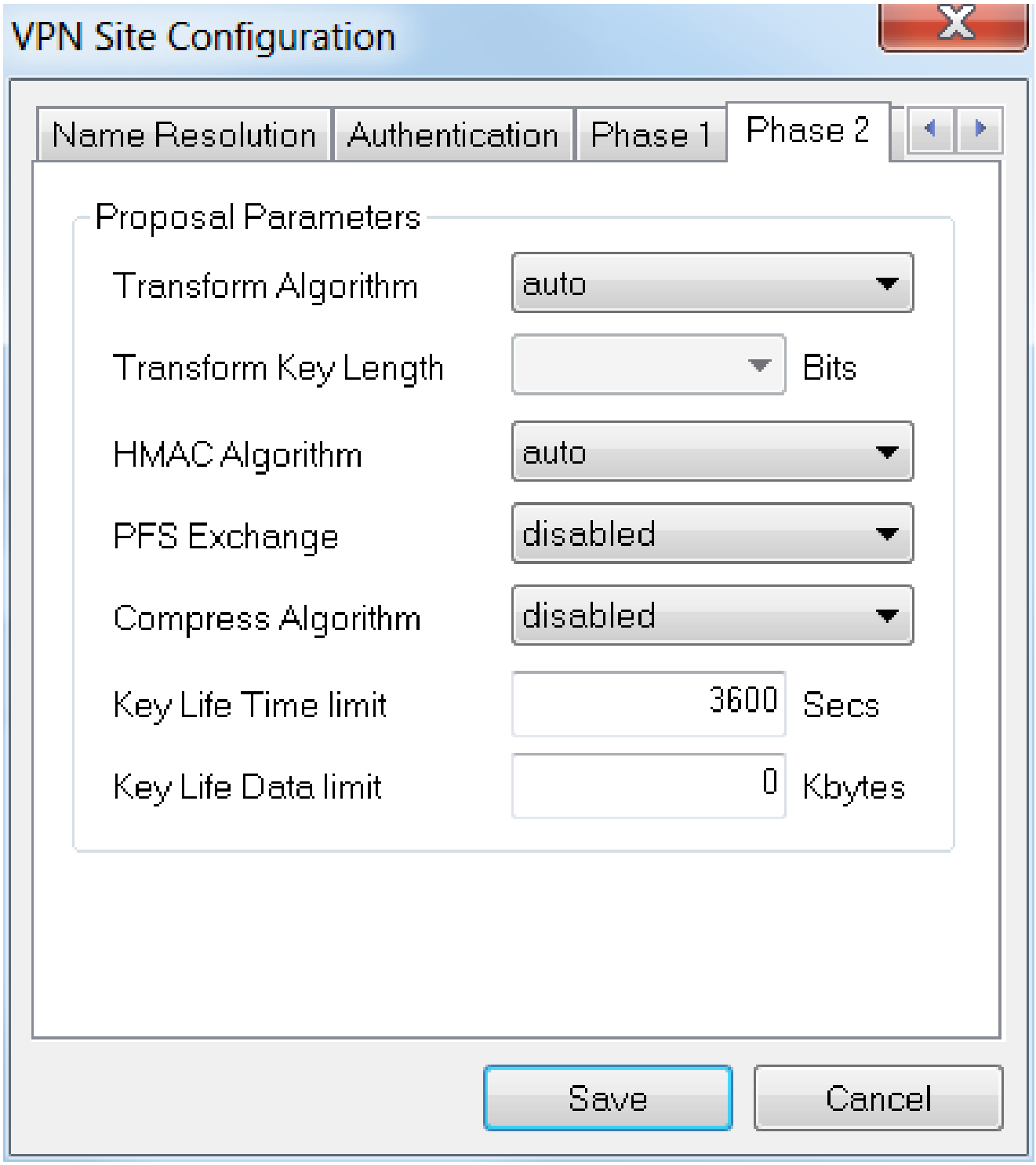
- 交換タイプ：アグレッシブ
- DH交換：グループ2
- 暗号アルゴリズム：自動
- ハッシュアルゴリズム：自動



手順 9

この例では、「Phase 2」タブのデフォルトは同じままです。

- トランスフォームアルゴリズム：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

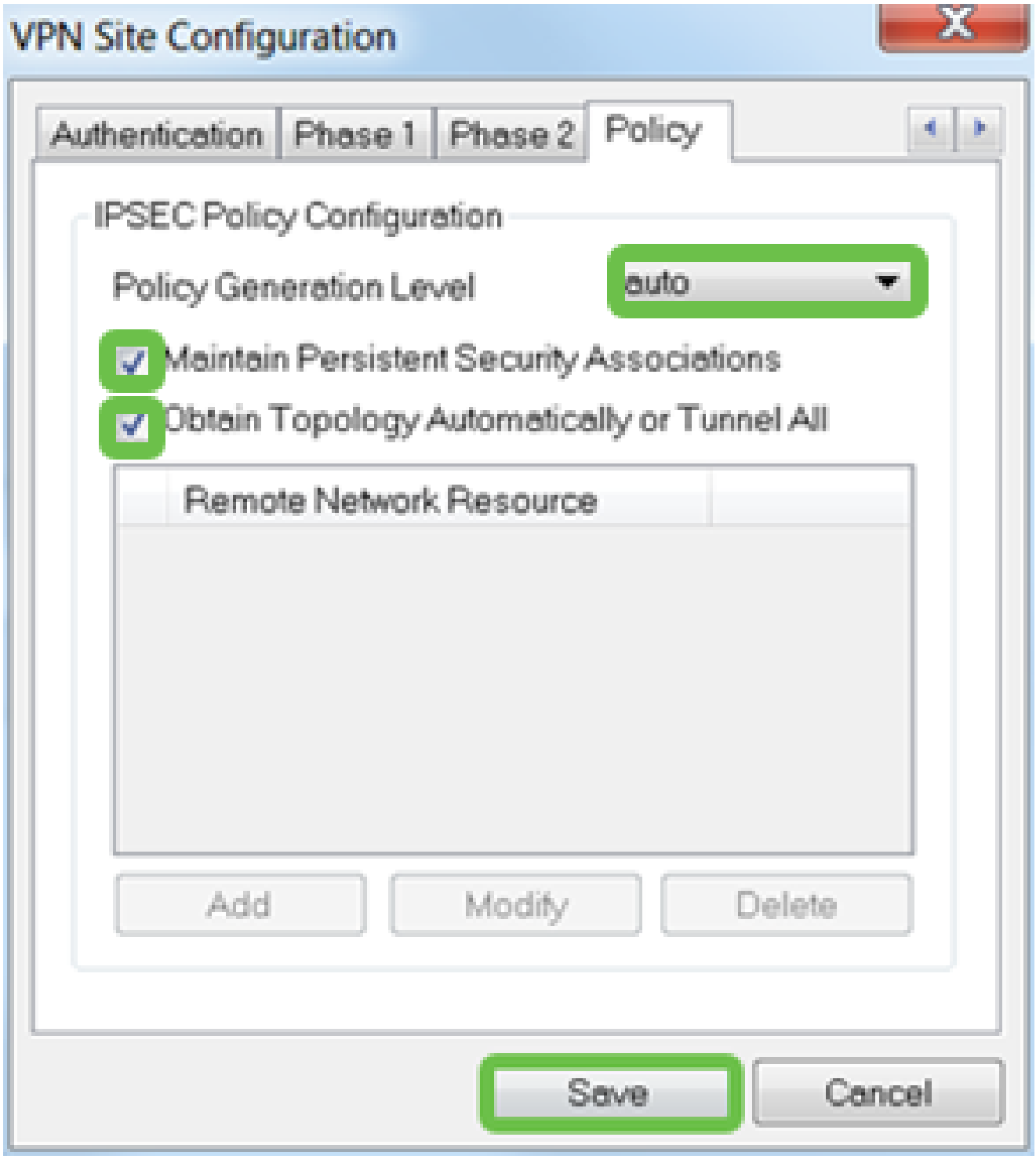


手順 10

Policy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維持：オン
- Obtain Topology AutomaticallyまたはTunnel All:オン

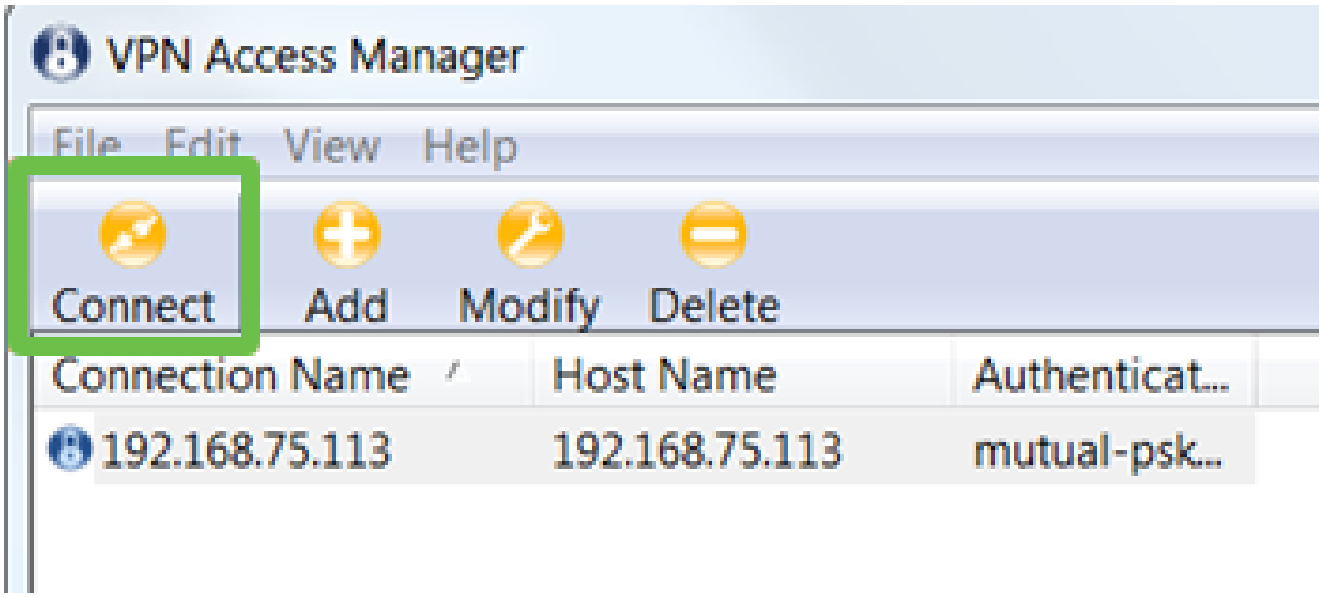
RV345Pでスプリットトンネリングを設定したので、ここで設定する必要はありません。



終了したら、Save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。

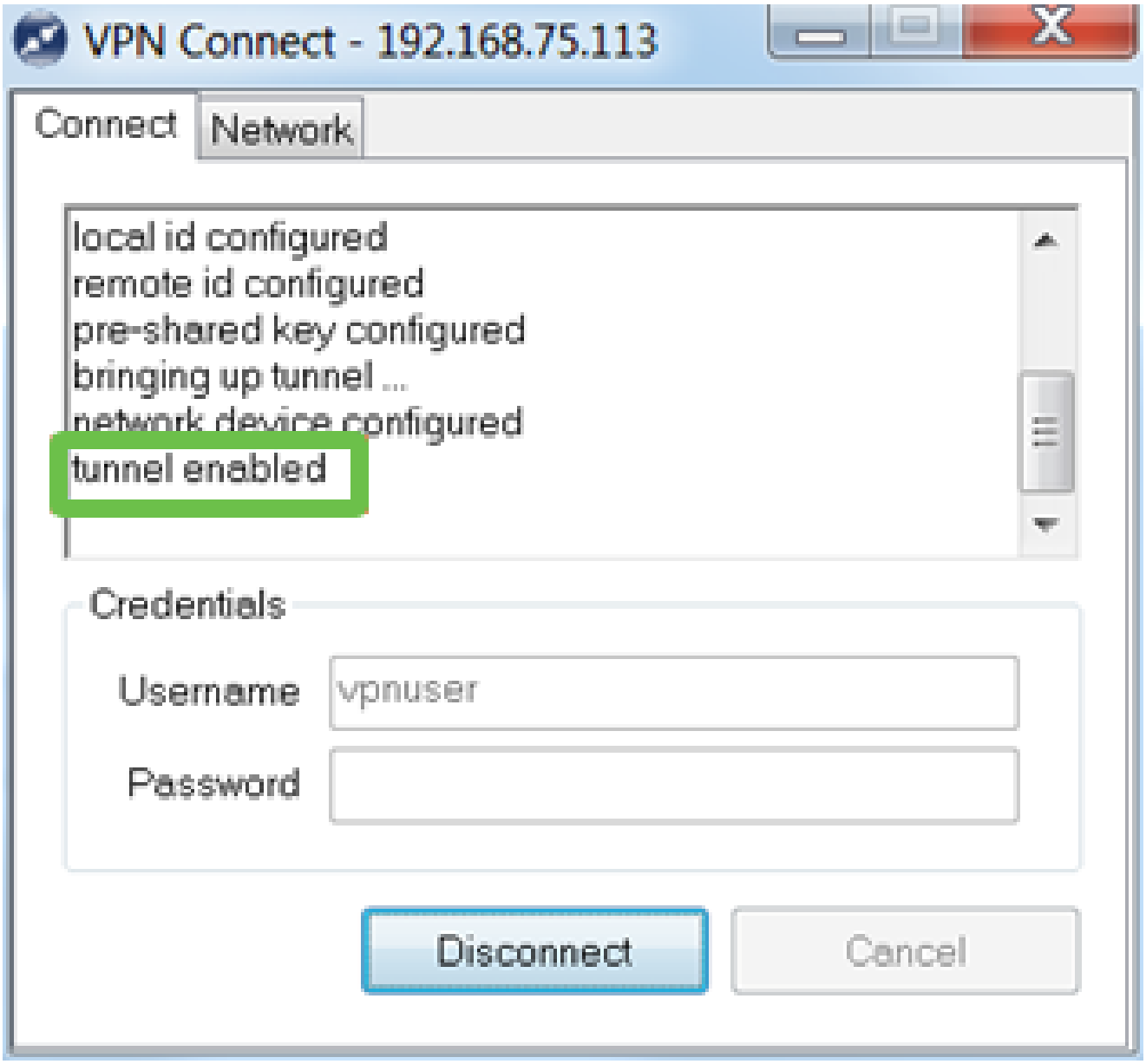


手順 12

表示されるVPN Connectウィンドウで、RV345P（ステップ13および14）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。終了したら、Connect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。tunnel enabledと表示されるはずです。



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、技術的なサポートが必要な場合は、このサードパーティにお問い合わせください。

その他のVPNオプション

VPNを使用するための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シリーズルータとの接続
- RV34xシリーズルータでの在宅勤務者VPNクライアントの設定
- Rv34xシリーズルータでのPoint-to-Point Tunneling Protocol(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ルータでの補足設定

VLANの設定（オプション）

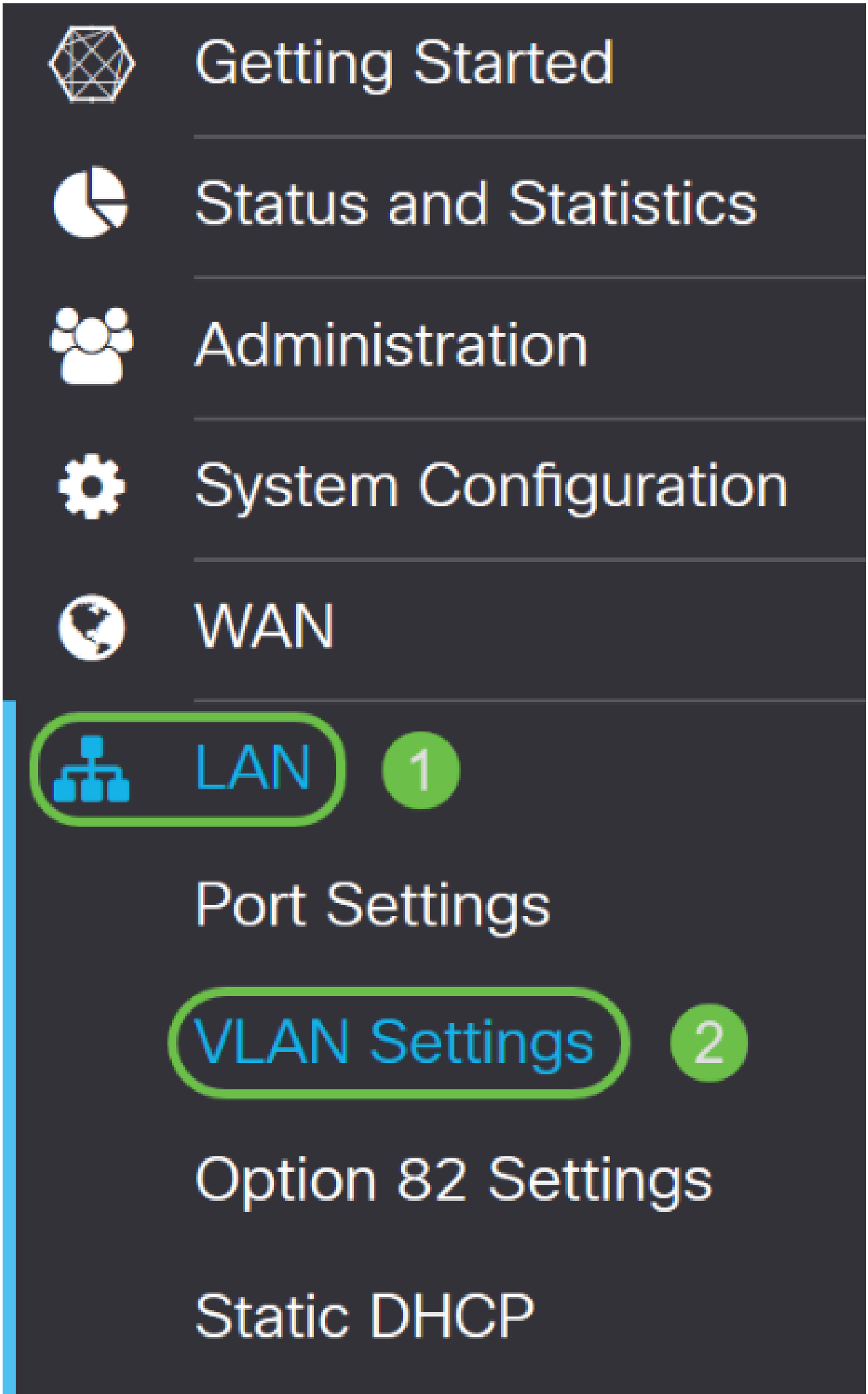
仮想ローカルエリアネットワーク（VLAN）を使用すると、ローカルエリアネットワーク（LAN）を複数のブロードキャストドメインに論理的に分割できます。機密データがネットワーク上でブロードキャストされる可能性があるシナリオでは、特定の VLAN にブロードキャストを指定することで、セキュリティを強化するための VLAN を作成できます。VLAN を使用すると、ブロードキャストやマルチキャストを不要な宛先に送信する必要性を減らし、パフォーマンスを向上させることもできます。VLANを作成できますが、VLANが手動または動的に少なくとも1つのポートに接続されるまでは、これは効果がありません。ポートは常に1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

詳細な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ティップス』を参照してください。

VLANを作成しない場合は、次のセクションに進んでください。

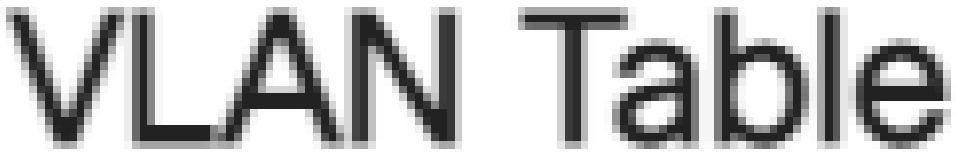
手順 1

LAN > VLAN Settingsの順に移動します。


Getting Started
Status and Statistics
Administration
System Configuration
WAN
LAN
1
Port Settings
VLAN Settings
2
Option 82 Settings
Static DHCP

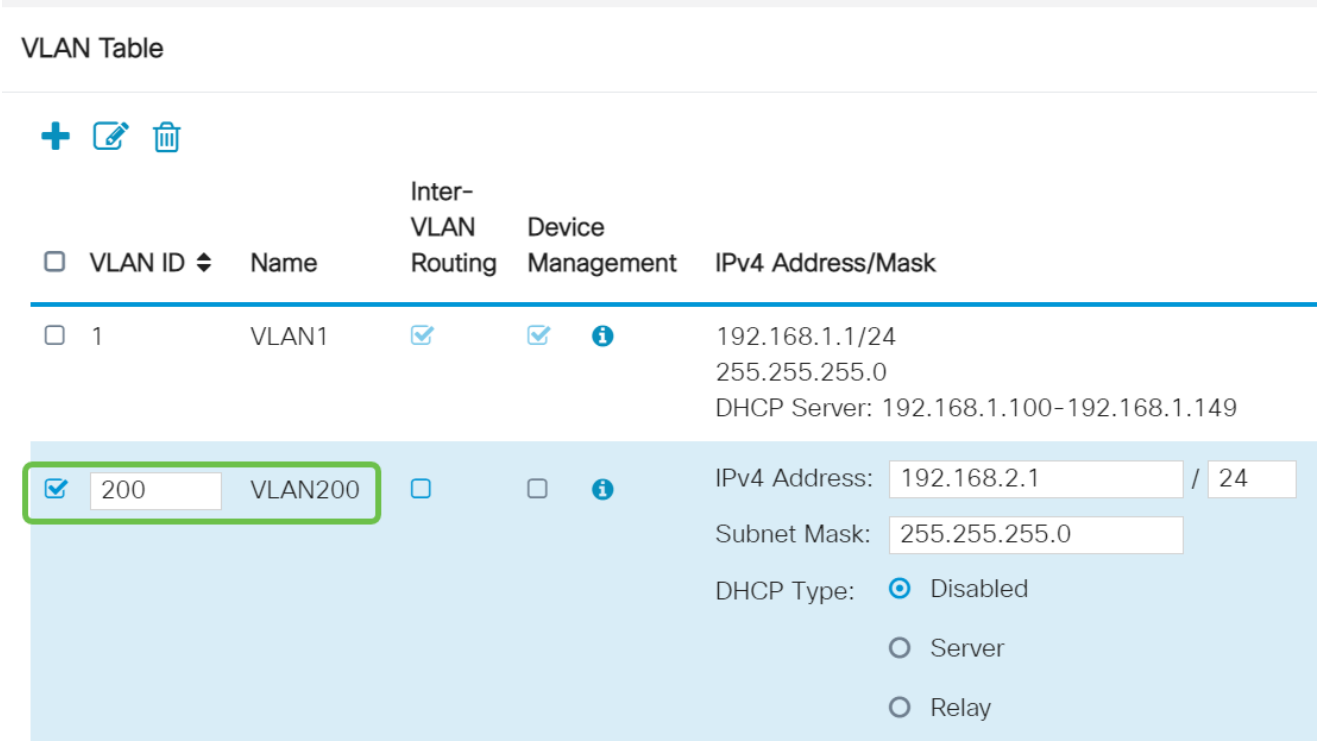
手順 2

addアイコンをクリックして、新しいVLANを作成します。



手順 3

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



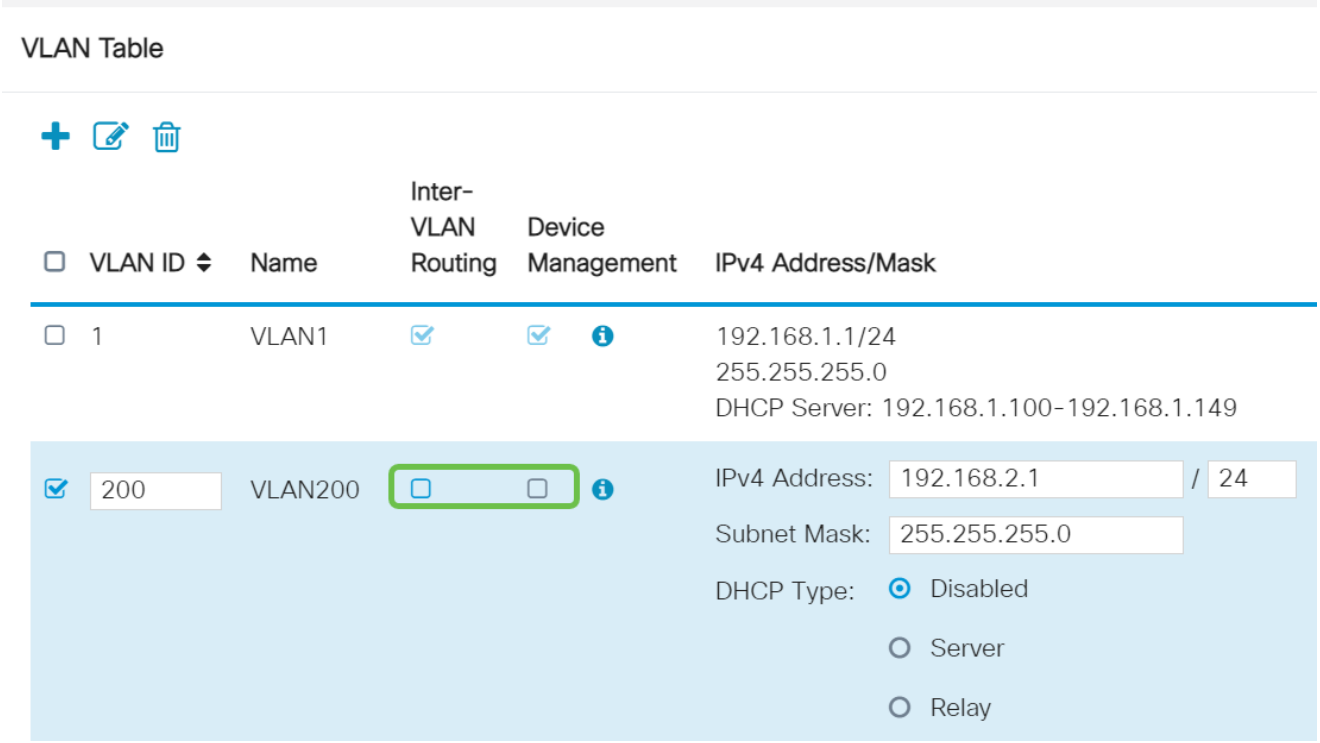
手順 4

必要に応じて、Inter-VLAN RoutingとDevice Managementの両方でEnabledボックスのチェックマークを外します。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。

ゲストユーザを隔離するとVLANのセキュリティが低下するため、ゲストネットワークでは一般的にこの方法は推奨されません。VLAN間のルーティングが必要になる場合があります。その場合は、『ターゲットACL制限がある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。

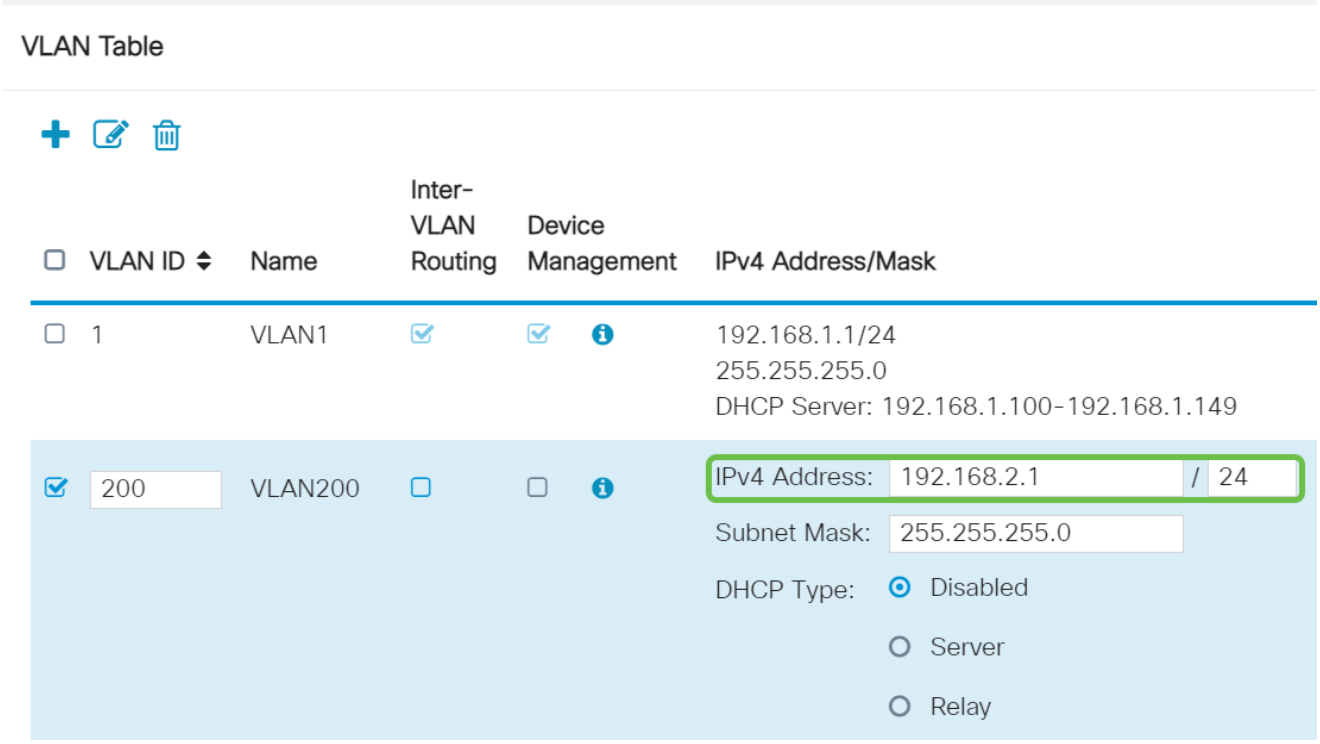
デバイス管理は、ブラウザを使用してVLANからRV345PのWeb UIにログインし、RV345Pを管理できるソフトウェアです。ゲストネットワークでも無効にする必要があります。

この例では、VLANをより安全に保つために、VLAN間ルーティングもデバイス管理も有効にしていません。



手順 5

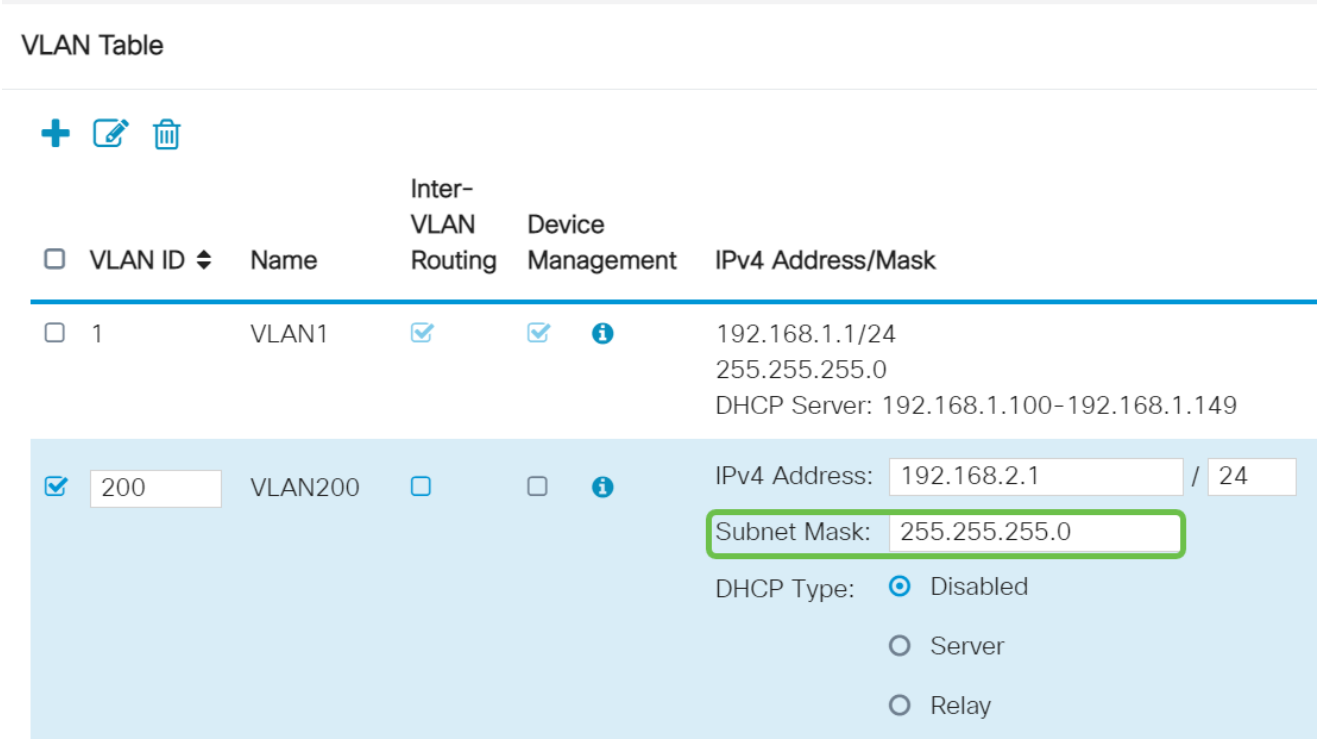
プライベートIPv4アドレスがIP Addressフィールドに自動的に入力されます。必要に応じてこれを調整できます。この例では、サブネットに192.168.2.100-192.168.2.149のIPアドレスがあり、192.168.2.1-192.168.2.99と192.168.2.150-192.168.2.254の固定IPアドレスがあります。



手順 6

Subnet Maskの下のサブネットマスクが自動的に入力されます。変更を加えると、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、サブネットマスクは255.255.255.0または/24のままにしておきます。



ステップ7

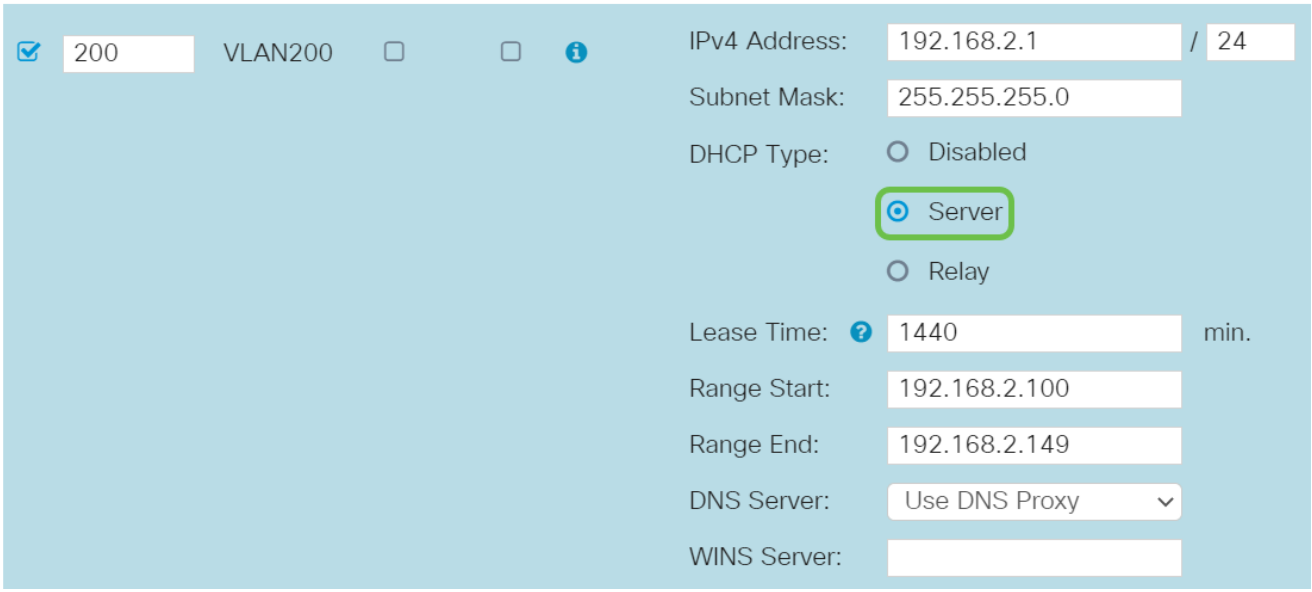
Dynamic Host Configuration Protocol(DHCP)タイプを選択します。次のオプションがあります。

Disabled:VLANで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する必要があり、すべての通信は内部で行われます。

Server：最もよく使用されるオプションです。

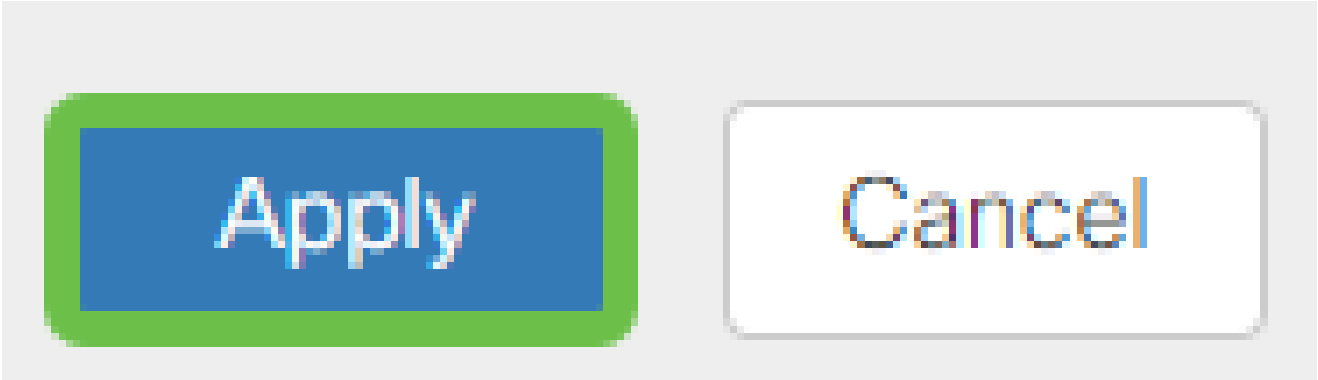
- リース時間：5 ~ 43,200分の時間値を入力します。デフォルトは1440分（24時間）です。
- Range StartおよびRange End：ダイナミックに割り当てることができるIPアドレスの範囲の開始と終了を入力します。
- DNSサーバ：DNSサーバをプロキシとして使用する場合、またはドロップダウンリストからISPを選択します。
- WINSサーバ：WINSサーバ名を入力します。
- DHCP オプション:
  - オプション66:TFTPサーバのIPアドレスを入力します。
  - オプション150:TFTPサーバのリストのIPアドレスを入力します。
  - オプション67：コンフィギュレーション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をクリックして、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、1つのVLANでワイドエリアネットワーク(WAN)を実現します。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、そのポート上のトラフィックは、ユーザが明示的に割り当てたVLAN/VLANに対してのみ保持されます。これは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として設定できます。

- アクセスポート：1つのVLANを割り当てます。 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をタグなしにできます。トランク上で不要な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ました。

- アクセスポートと見なされる

- このポートに割り当てられたVLANには、Untaggedというラベルを付ける必要があります。
- その他すべてのVLANには、そのポートに対してExcludedというラベルを付けます。

1つのポートを共有する複数のVLAN:

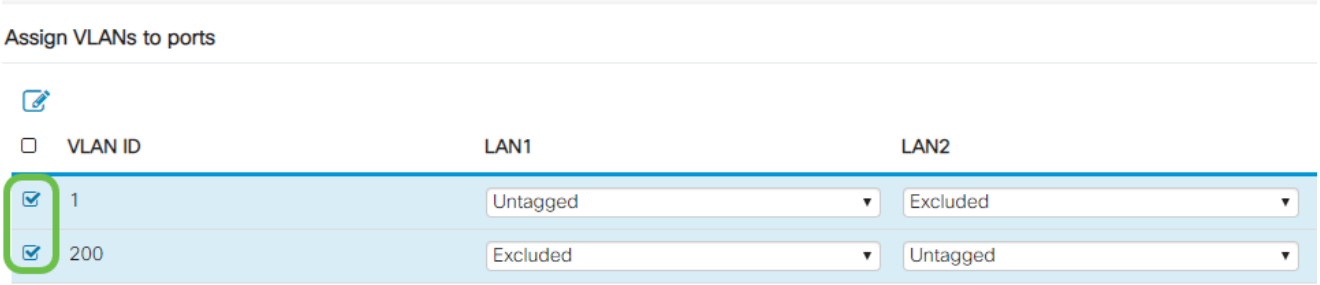
- トランクポートと見なされます。
- VLANの1つにUntaggedというラベルを付けることができます。
- トランクポートの一部である残りのVLANには、Taggedというラベルを付ける必要があります。
- トランクポートの一部ではないVLANには、そのポートについてExcludedというラベルを付ける必要があります。

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。

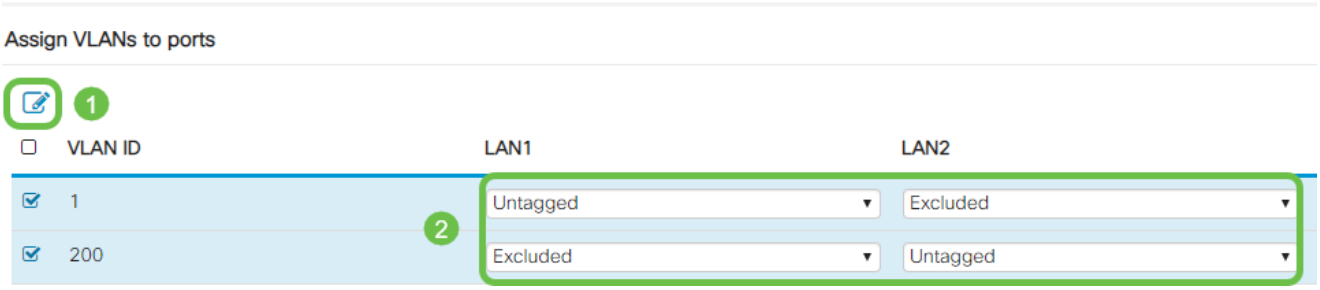
この例では、VLAN 1とVLAN 200を選択しています。



手順 2

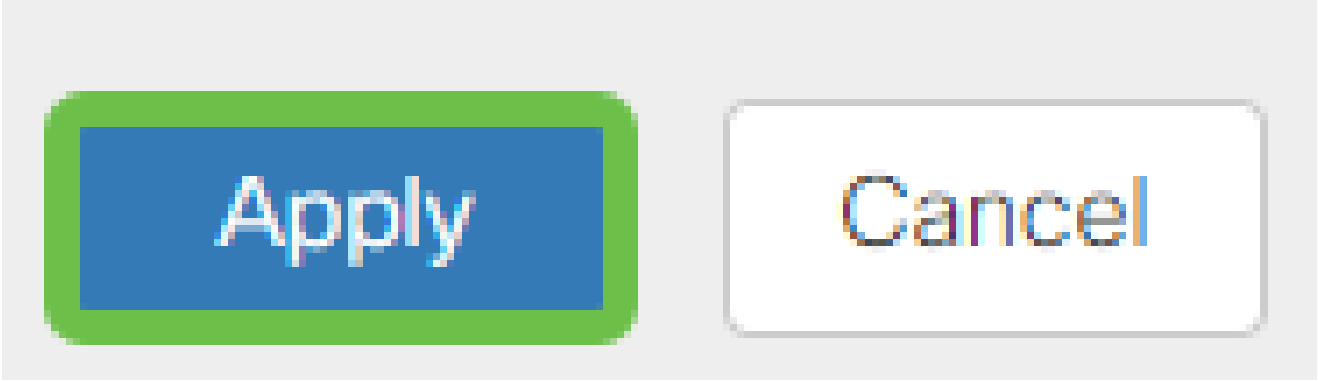
Editをクリックしてを LANポートに割り当て、各設定をTagged、Untagged、またはExcludedとして指定します。

この例では、LAN1でVLAN 1をUntaggedとして割り当て、VLAN 200をExcludedとして割り当てています。LAN2では、VLAN 1を除外として割り当て、VLAN 200をタグなし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はマーケティング用にサブネット192.168.3.xで作成され、VLAN400はアカウンティング用にサブネット192.168.4.xで作成されます。

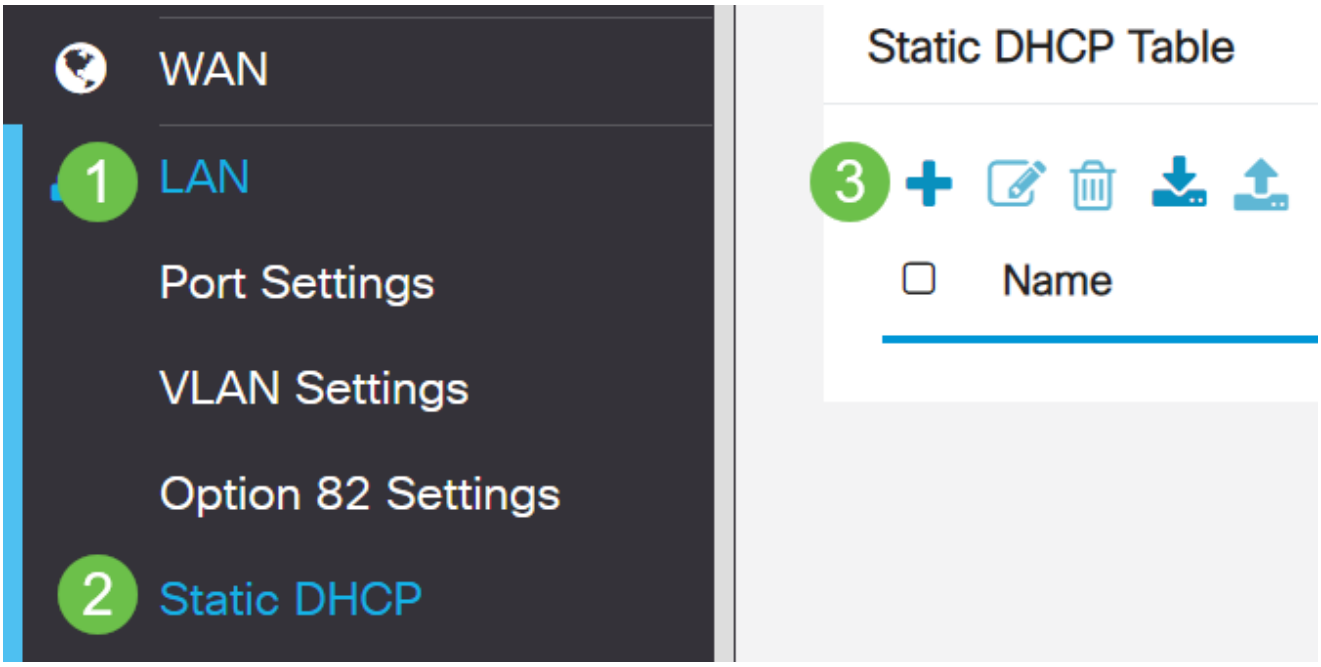
スタティックIPの追加（オプション）

特定のデバイスが他のVLANに到達できるようにする場合は、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ためのアクセスルールを作成します。これは、VLAN間ルーティングがイネーブルになっている場合にのみ機能します。他にも、スタティックIPが役立つ状況があります。固定IPアドレスの設定の詳細については、『Ciscoビジネスハードウェアでの固定IPアドレスの設定に関するベストプラクティス』を参照してください。

スタティック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進んでください。

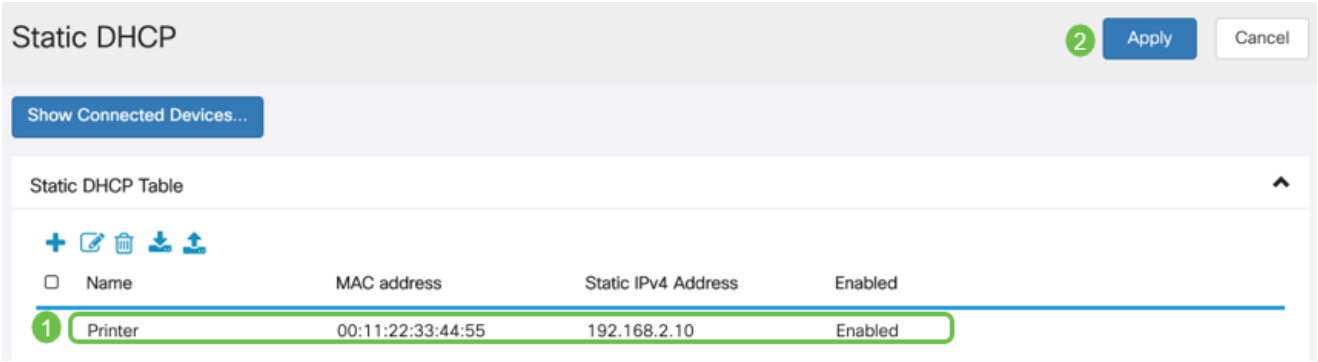
手順 1

LAN > Static DHCPの順に移動します。プラスアイコンをクリックします。



手順 2

デバイスのスタティック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）

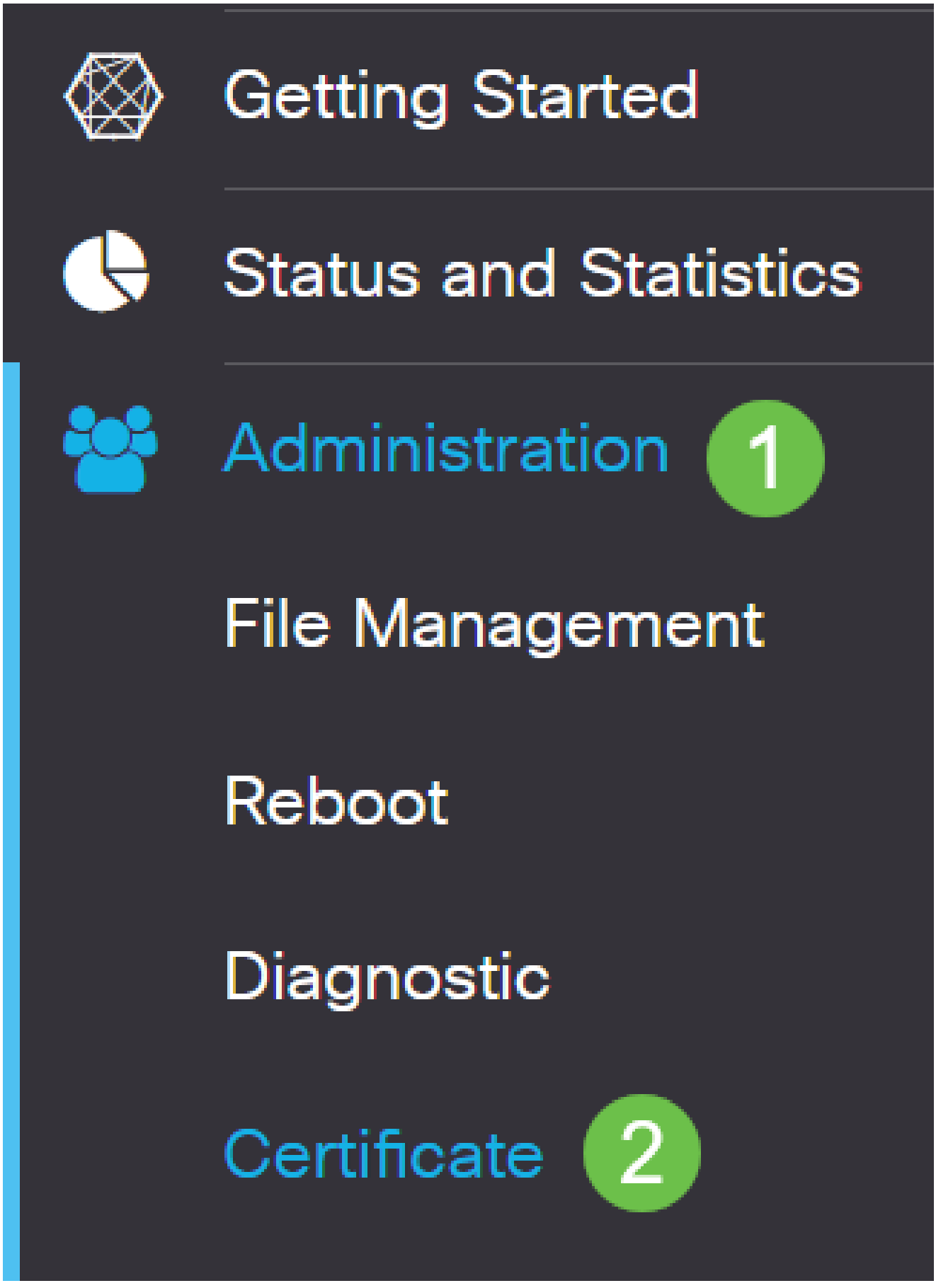
デジタル証明書は、証明書の名前付きサブジェクトによって公開キーの所有権を証明します。これにより、証明書利用者は、認証された公開キーに対応する秘密キーによって作成された署名またはアサーションに依存できます。ルータは、自己署名証明書（ネットワーク管理者が作成した証明書）を生成できます。また、デジタルID証明書を申請する要求を認証局(CA)に送信することもできます。サードパーティ製アプリケーションからの正規の証明書を保持することが重要です。

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。それはあなたのサイトが安全であることを証明するための公式の方法です。基本的に、CAは、ユーザが正当な企業であり、信頼できることを検証する信頼できる送信元です。必要に応じて、最小限のコストで証明書を作成します。CAによってチェックアウトされ、CAが情報を確認すると、証明書が発行されます。この証明書は、コンピュータに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、そこでアップロードできます。

CSR/証明書の生成

手順 1

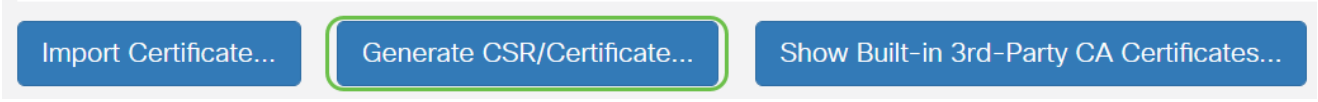
ルータのWebベースのユーティリティにログインし、Administration > Certificateの順に選択します。



手順 2

Generate CSR/Certificateをクリックします。「CSR/証明書の生成」ページが表示されます

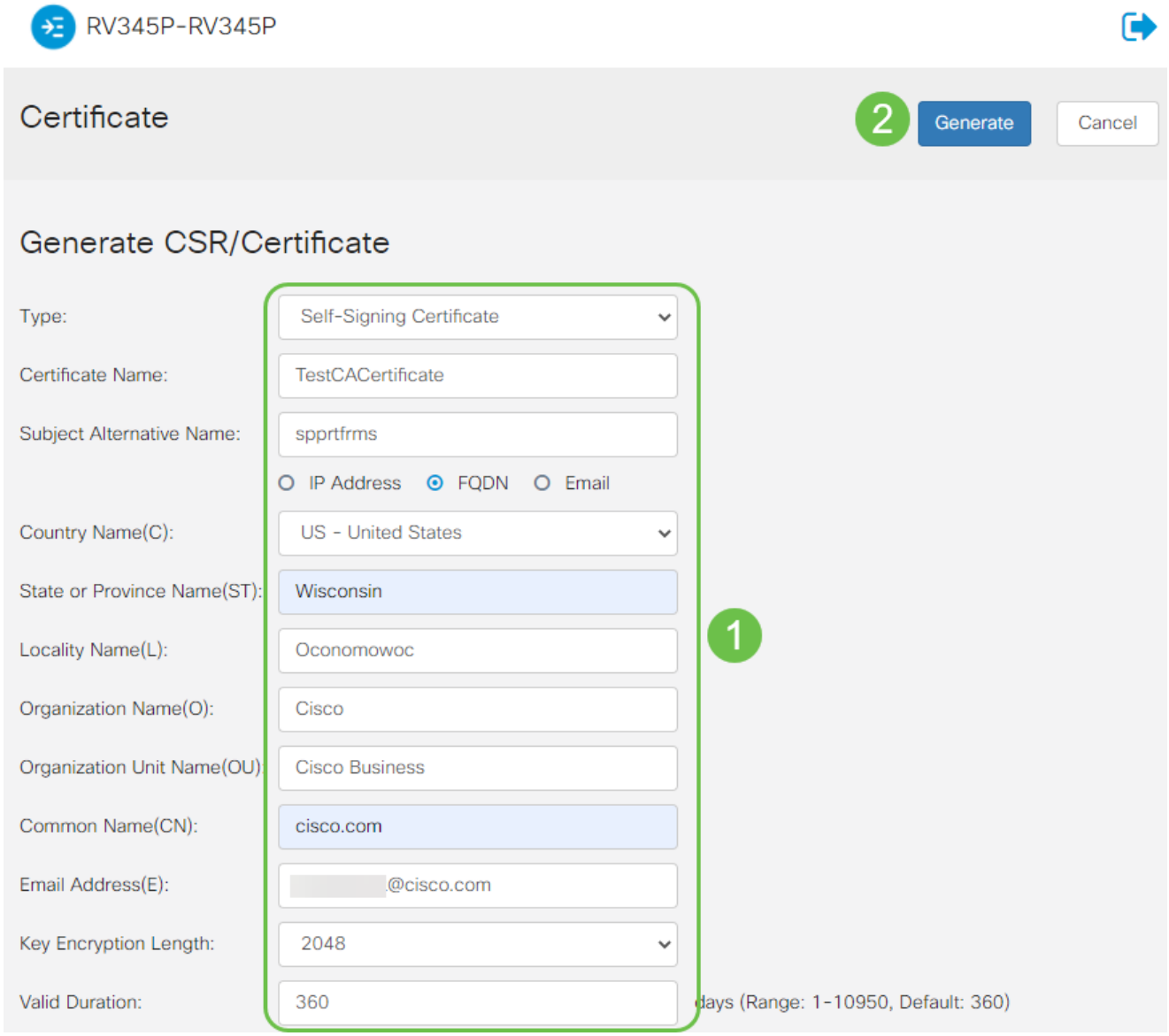
。



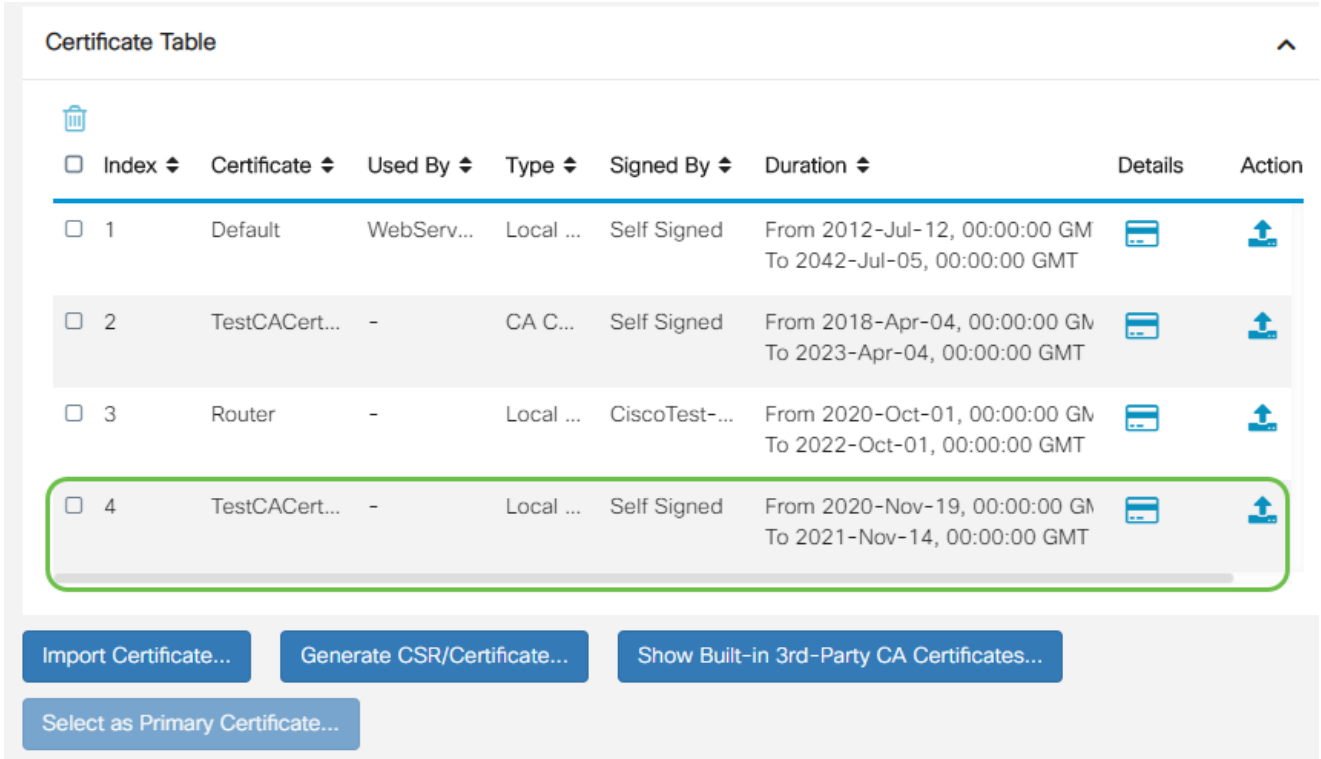
手順 3

ボックスに次のように入力します。

- 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、秘密キーが攻撃者によって何らかの形で侵害された場合はキャンセルできないため、あまり信頼されません。
  - 証明書署名要求(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。秘密鍵は秘密に保持されるため、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することも、スペースや特殊文字を含めることもできません。
- （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
  - Email – 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」ドロップダウンリストから、組織が正式に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[都道府県または地域名(ST)]フィールドに入力します。
- 「地域名」フィールドに、組織が登録されている地域または市の名前を入力します。
- ビジネスが正式に登録されている名前を入力します。スモールビジネスまたは個人事業主として登録する場合は、「組織名」フィールドに証明書依頼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」フィールドに名前を入力して、組織内の部門間を区別します。
- 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。
- 証明書を生成する担当者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。
- Valid Duration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。

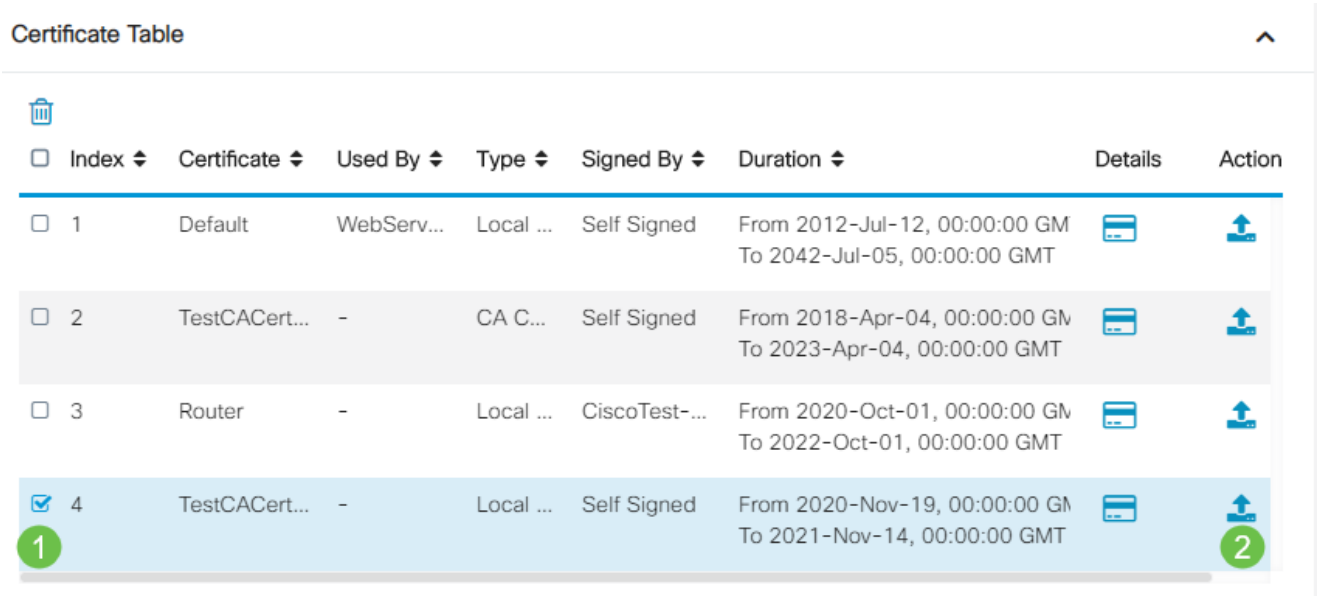


これで、RV345Pルータに証明書が正常に作成されました。

証明書のエクスポート

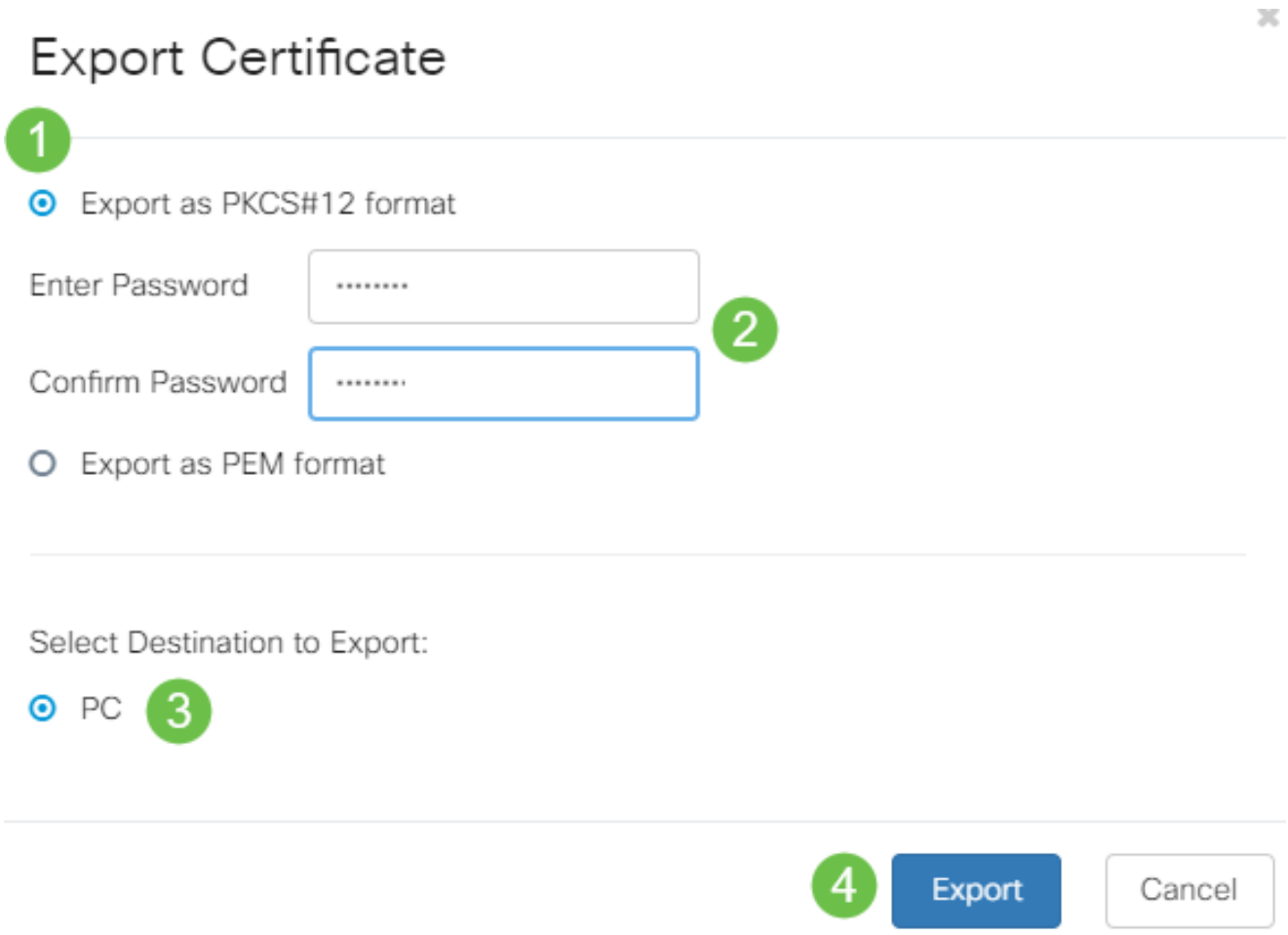
手順 1

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。



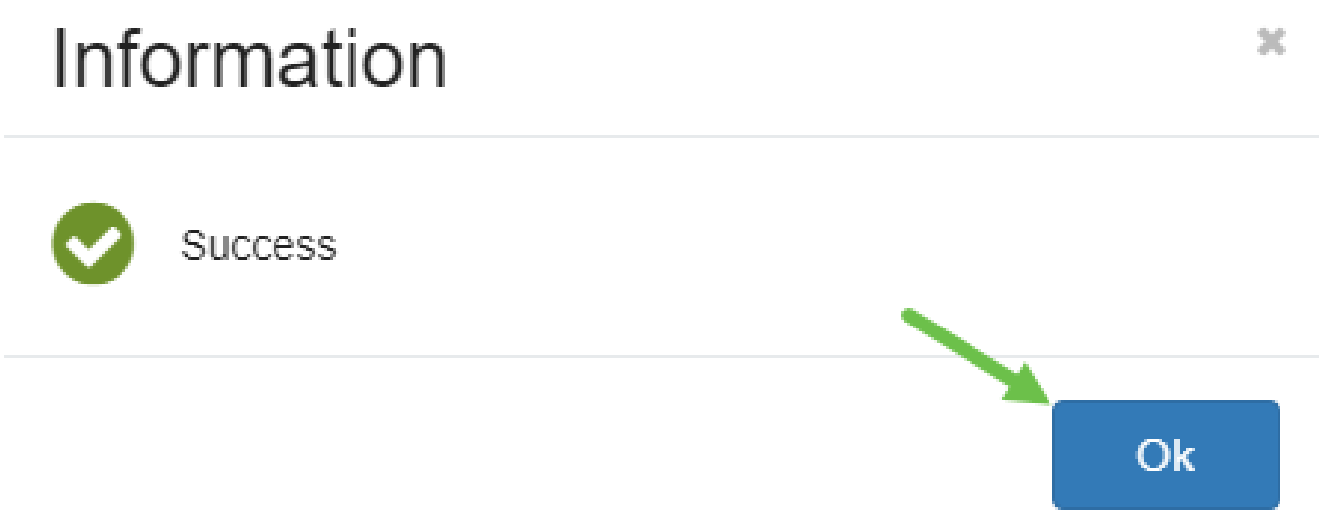
手順 2

- 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：公開キー暗号規格(PKCS)#12は、.p12拡張子で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保護するには、パスワードが必要です。
  - PEM：プライバシー強化メール(PEM)は、メモ帳などの簡単なテキストエディタを使用して読み取り可能なデータに簡単に変換する機能を備えたWebサーバでよく使用されます。
- PEMを選択した場合は、Exportをクリックするだけです。
- Enter Passwordフィールドに、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領域では、PCが選択されており、現在利用できる唯一のオプションです。
- [Export] をクリックします。



手順 3

ダウンロードが成功したことを示すメッセージがダウンロードボタンの下に表示されます。ブラウザでファイルのダウンロードが開始されます。[OK] をクリックします。

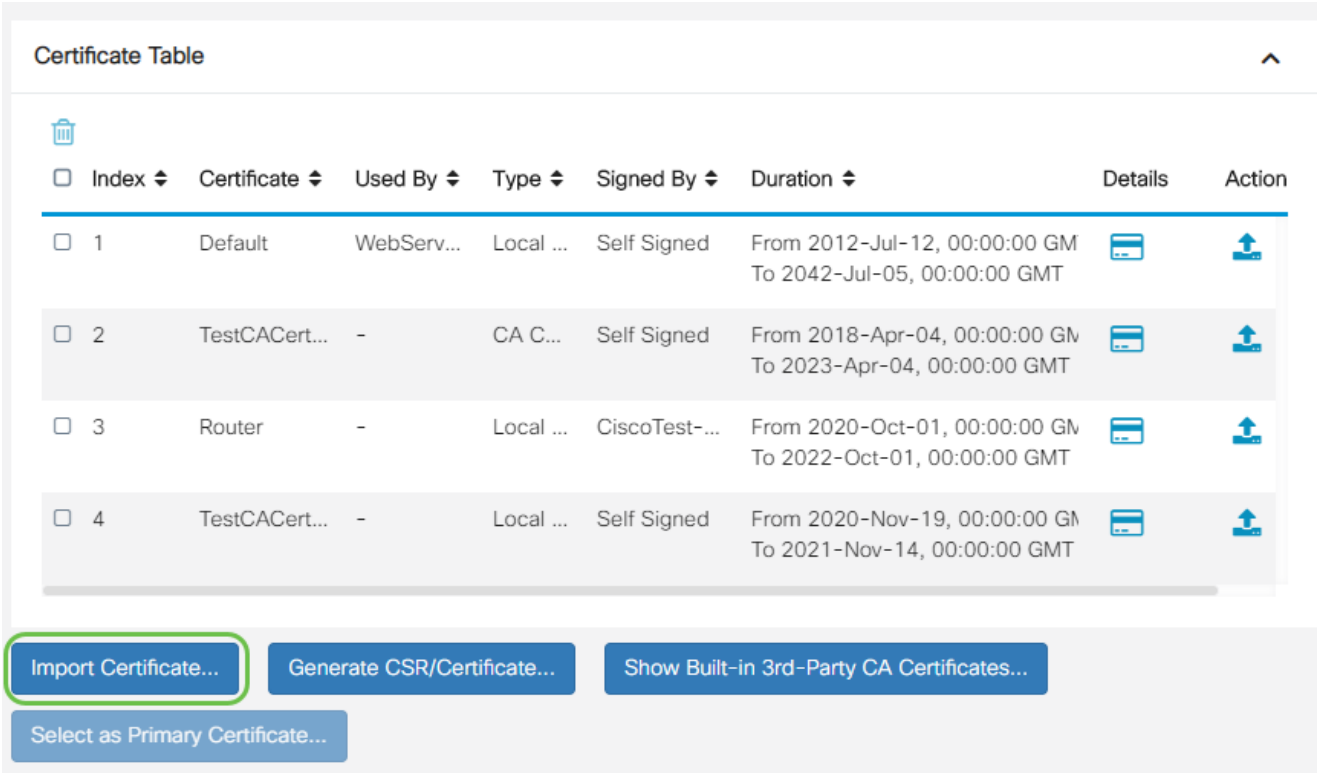


これで、RV345Pシリーズルータの証明書が正常にエクスポートされました。

証明書のインポート

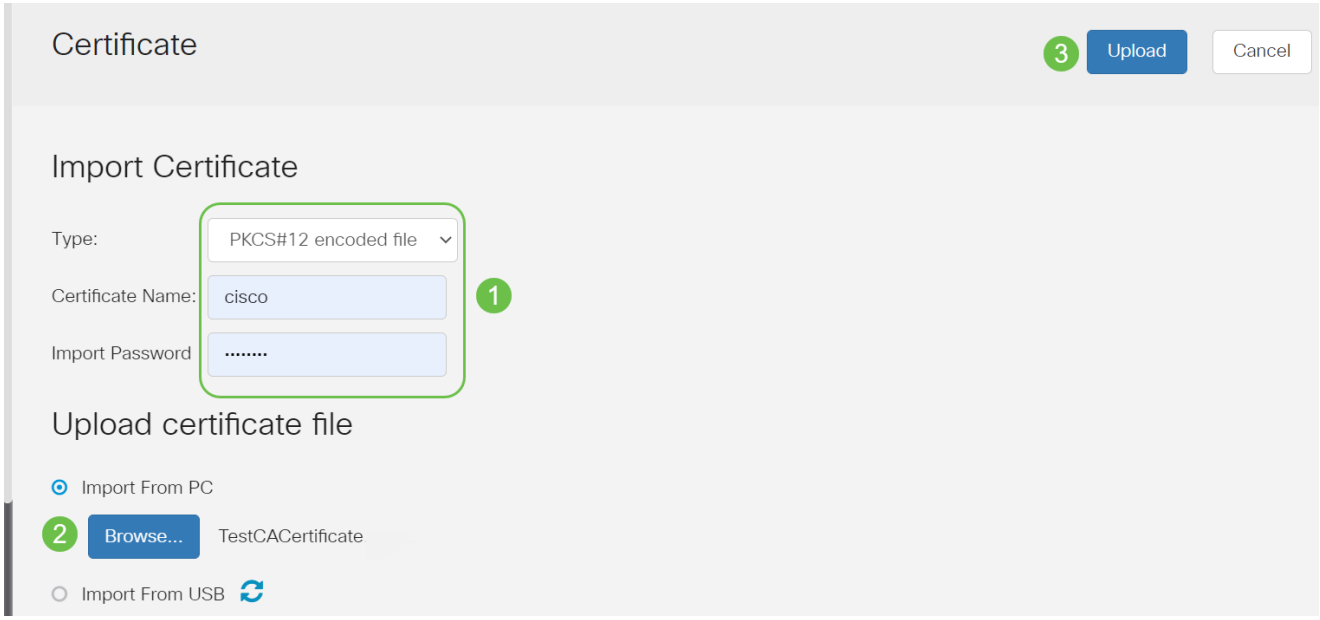
手順 1

Import Certificate...をクリックします。

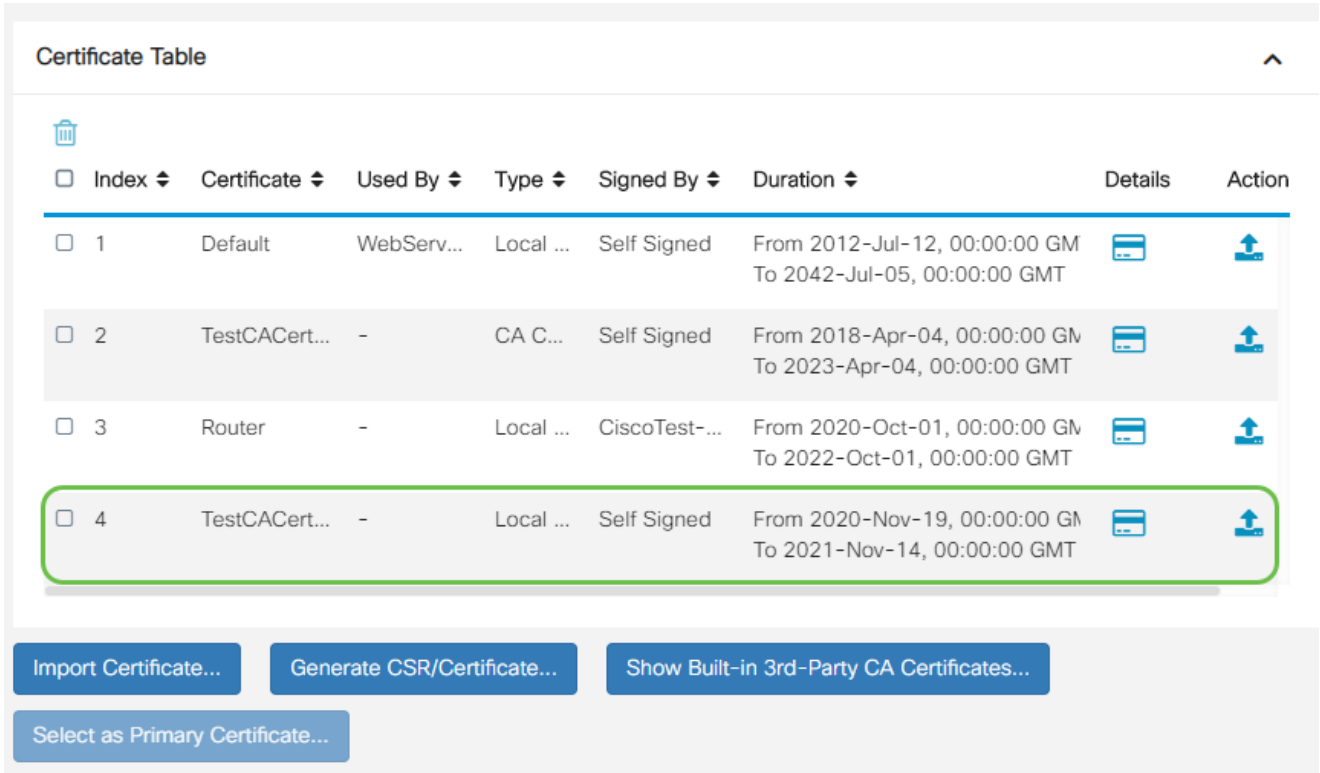


手順 2

- 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：ルータ上で生成された証明書。
  - CA証明書：信頼できるサードパーティ認証局によって認証され、証明書に含まれる情報が正確であることを確認した証明書。
  - PKCS #12エンコードファイル：Public Key Cryptography Standards(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、[USBからインポート]オプションはグレー表示されます。
- [USBからインポート]を選択したときに、USBがルータに認識されない場合は、[最新の情報に更新]をクリックします。
- Choose Fileボタンをクリックして、適切なファイルを選択します。
- [Upload] をクリックします。



正常に完了すると、メインの証明書ページが自動的に表示されます。証明書テーブルに、最近インポートし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ました。

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。その場合は、「ドングルとRV34xシリーズルータを使用してモバイルネットワークを設定する」を参照してください。

これで、RV345Pルータの設定は完了です。次に、シスコビジネスワイヤレスデバイスを設定します。

ワイヤレスメッシュネットワークの設定

CBW140AC設定済み

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のポートの半分はPoEを供給できるため、これらのいずれも使用できます。

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が複数のパターンで緑色に点滅し、緑、赤、およびオレンジ色の間で急速に交互に点灯した後、再び緑色に変わります。LEDの色の強さと色相には、ユニットごとに多少の違いがあります。LEDライトが緑色に点滅したら、次の手順に進みます。

モバイルアプリケーション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にのみ使用でき、他のモバイルアプリケーション対応デバイスやメッシュエクステンダデバイスへの接続には使用できません。

新しいアクセスポイントではない場合は、工場出荷時のデフォルト設定にリセットして、CiscoBusiness-Setup SSIDをWi-Fiオプションに表示してください。これに関するサポートについては、『RV345xルータのリブートおよび工場出荷時のデフォルト設定へのリセット方法』を参照してください。

140ACモバイルアプリケーションワイヤレスアクセスポイントの設定

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

アプリケーションは頻繁に更新され、外観やレイアウトは時間の経過とともに変更される可能性があることに注意してください。

140ACの背面で、APに付属のケーブルを黄色のPoEに差し込み、140 ACを差し込みます。もう一方の端をRV345P LANポートの1つに接続します。

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

手順 1

Google PlayまたはモバイルデバイスのApple App Storeで入手できるCisco Business Wireless Appをダウンロードします。次のいずれかのオペレーティングシステムが必要です。

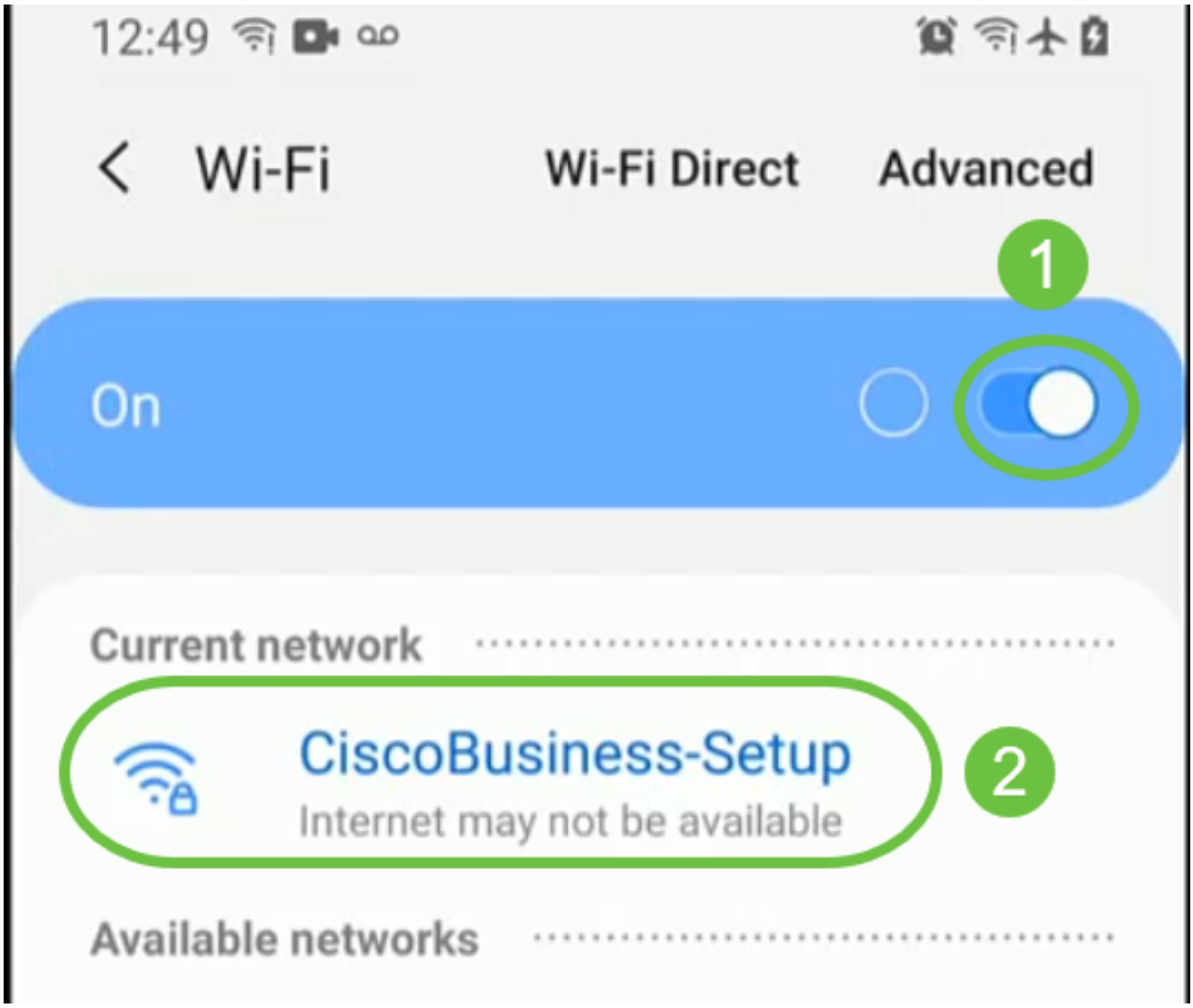
- Androidバージョン5.0以降
- iOSバージョン8.0以降

手順 2

モバイルデバイスでCisco Business Applicationを開きます。

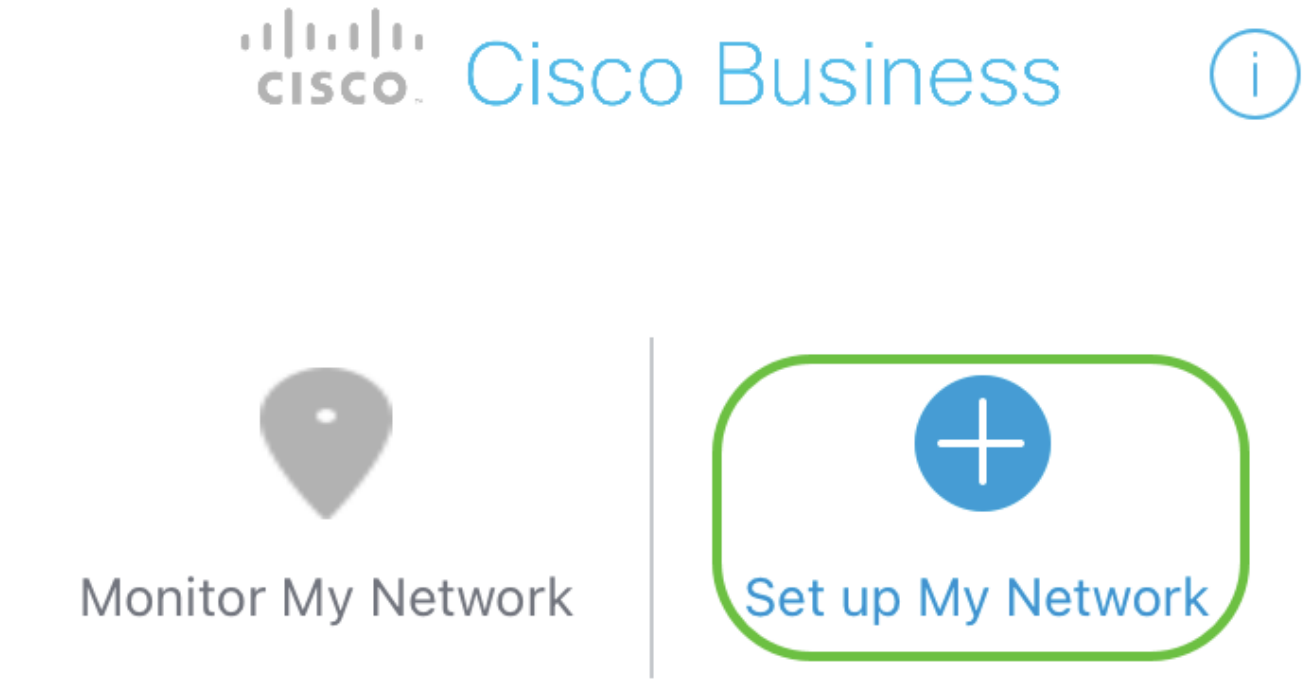
手順 3

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



手順 4

アプリは自動的にモバイルネットワークを検出します。Set up My Networkを選択します。

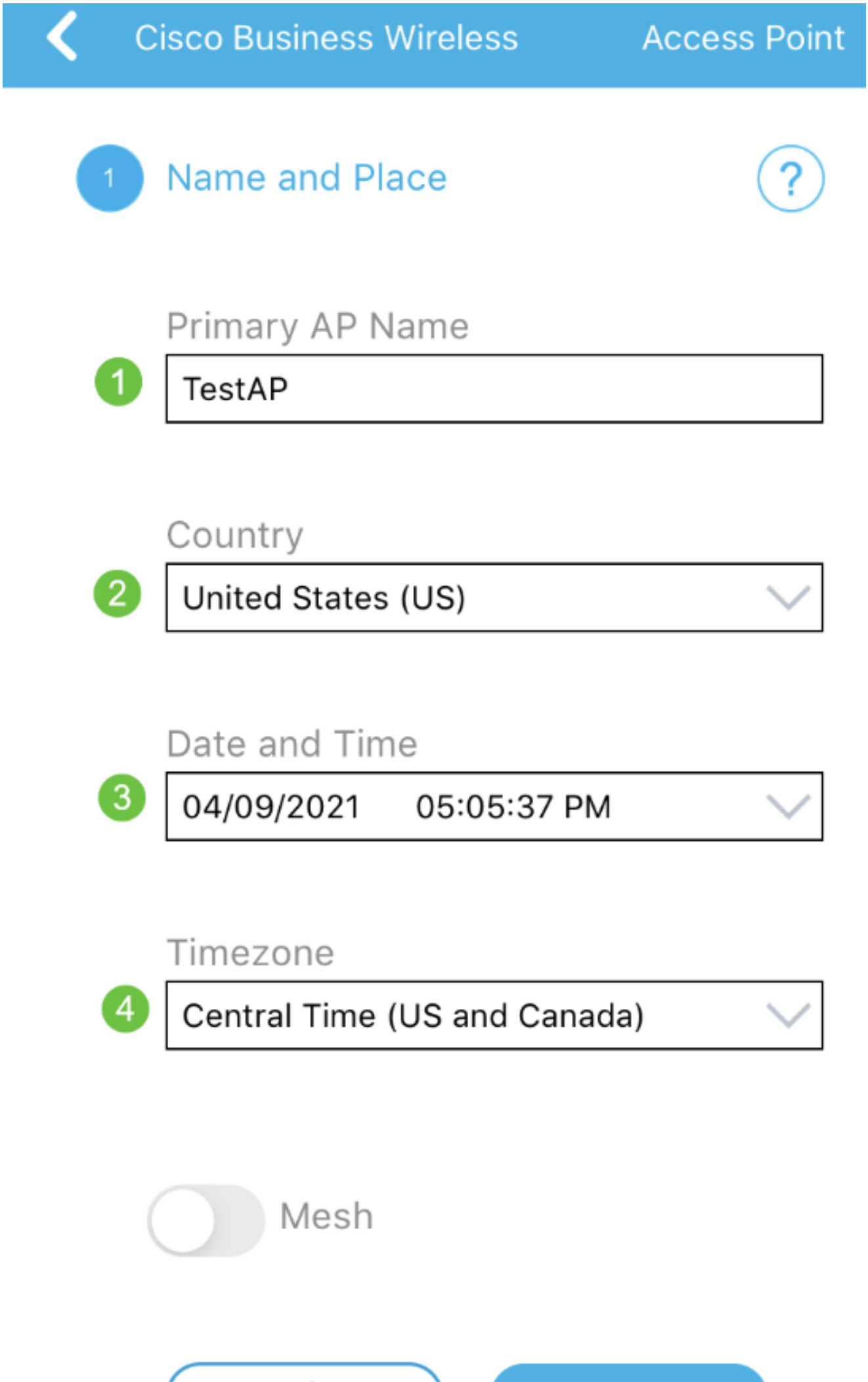


手順 5

ネットワークをセットアップするには、次のコマンドを入力します。

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

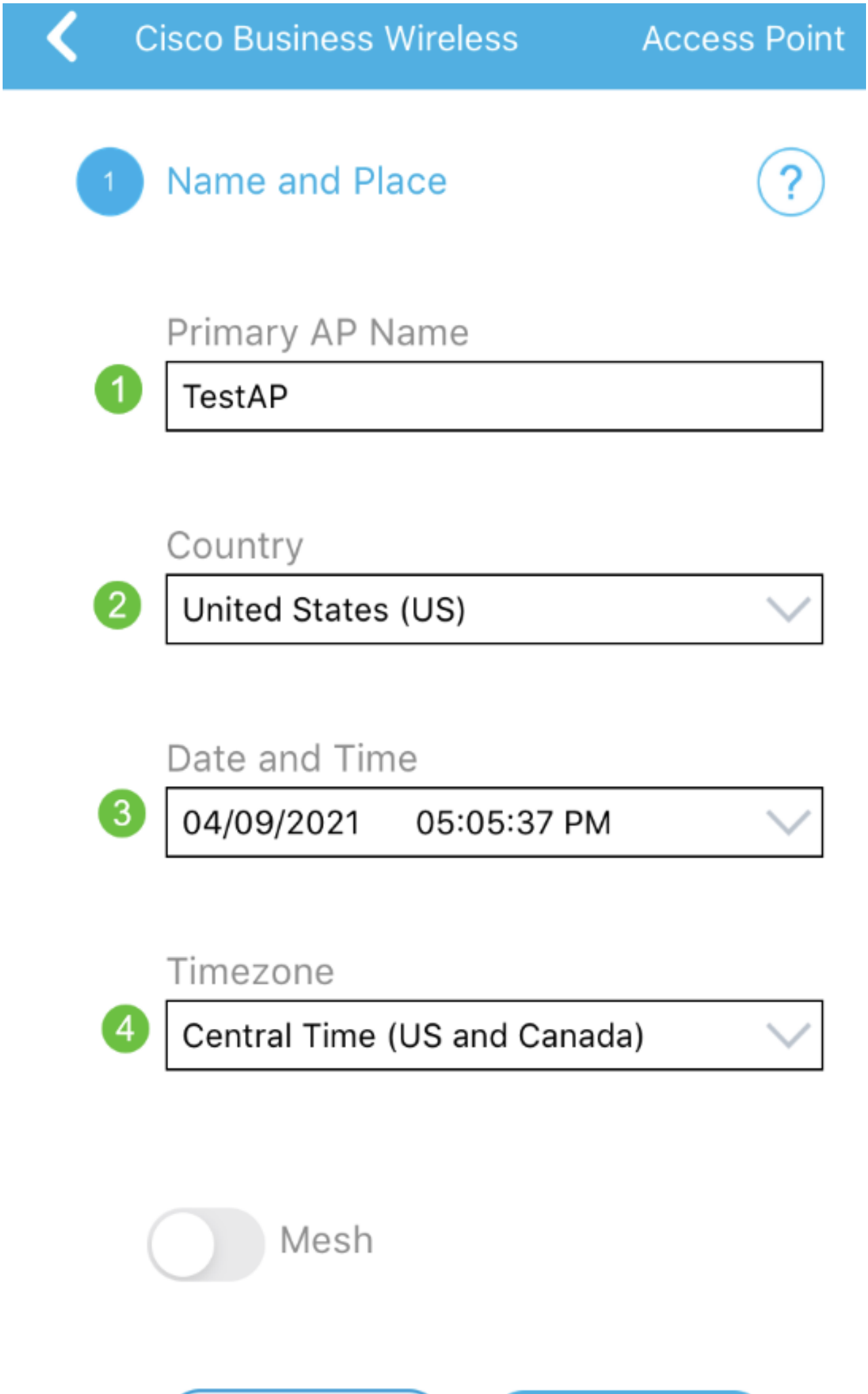
Get Startedを選択します。


Cisco Business Wireless
Access Point
1
Name and Place
?
Primary AP Name
1
TestAP
Country
2
United States (US)
Date and Time
3
04/09/2021 05:05:37 PM
Timezone
4
Central Time (US and Canada)
Mesh

手順 6

Name and Placeを設定するには、次の情報を正確に入力します。矛盾する情報を入力すると、予期しない動作が発生する可能性があります。

- Mobile Application AP Name」を参照してください。
- Country
- 日付
- 時間
- TimeZone


Cisco Business Wireless
Access Point
1
Name and Place
Primary AP Name
1
TestAP
Country
2
United States (US)
Date and Time
3
04/09/2021 05:05:37 PM
Timezone
4
Central Time (US and Canada)
Mesh

ステップ7

Meshのトグルをオンにします。[Next] をクリックします。

1 Name and Place

Primary AP Name

TestAP

Country

United States (US)

Date and Time

04/09/2021 05:05:37 PM

Timezone

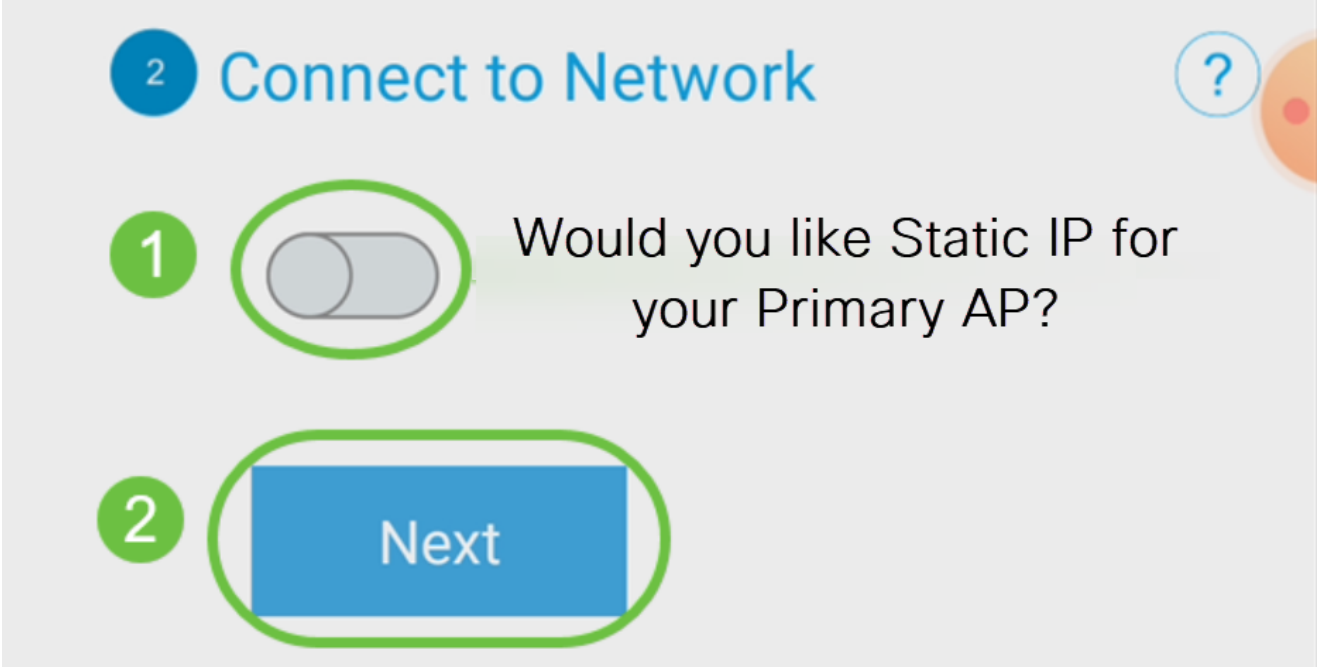
Central Time (US and Canada)

1

Mesh

手順 8

（オプション）モバイルアプリケーションAPのスタティックIPを管理目的で有効にすることができます。そうでない場合は、DHCPサーバがIPアドレスを割り当てます。アクセスポイントにスタティックIPを設定しない場合は、Nextをクリックします。

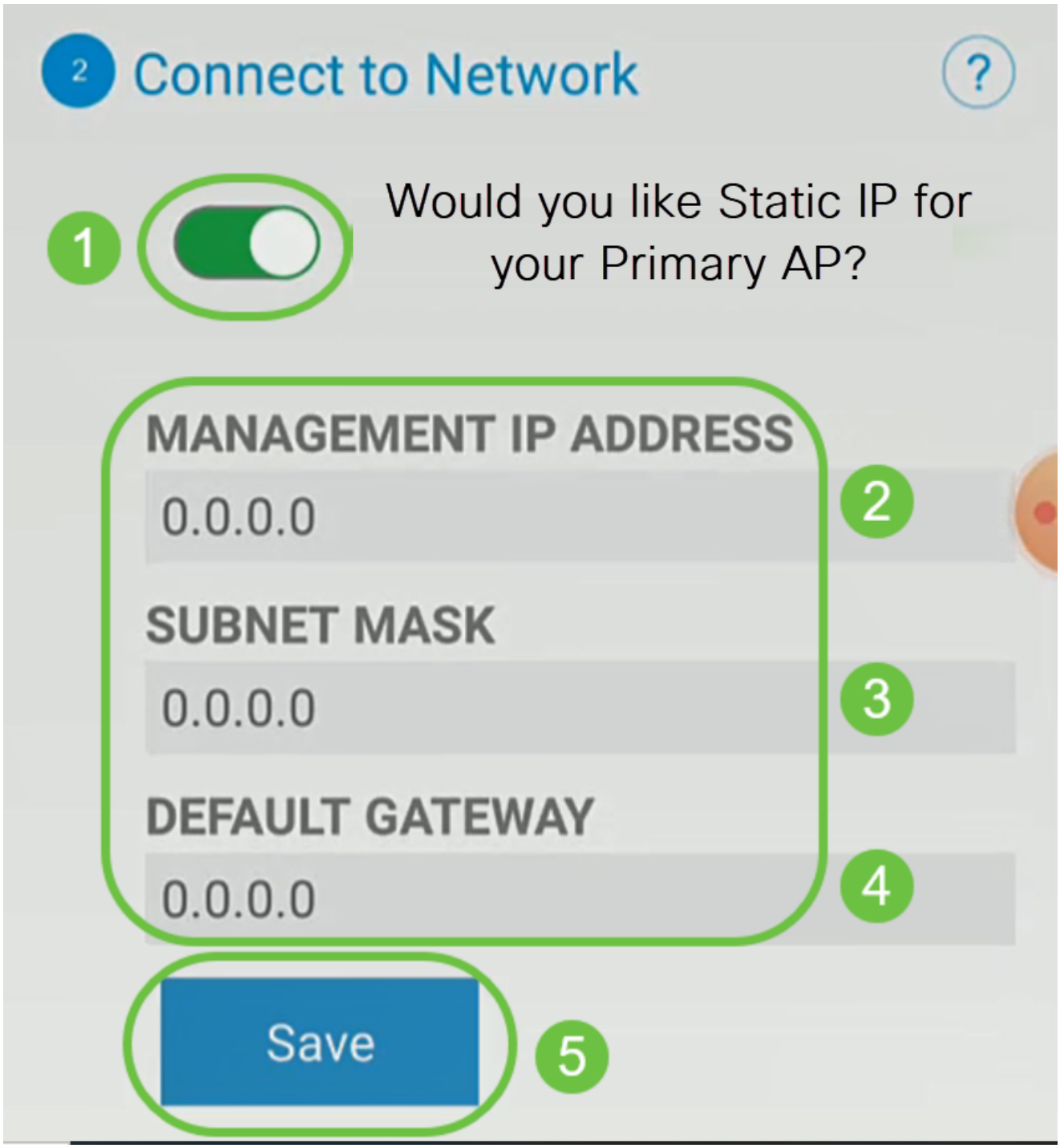


または、ネットワークに接続するには、次の手順を実行します。

Static IP for your Mobile Application APを選択します。デフォルトでは、このオプションは無効になっています。

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

[Save] をクリックします。

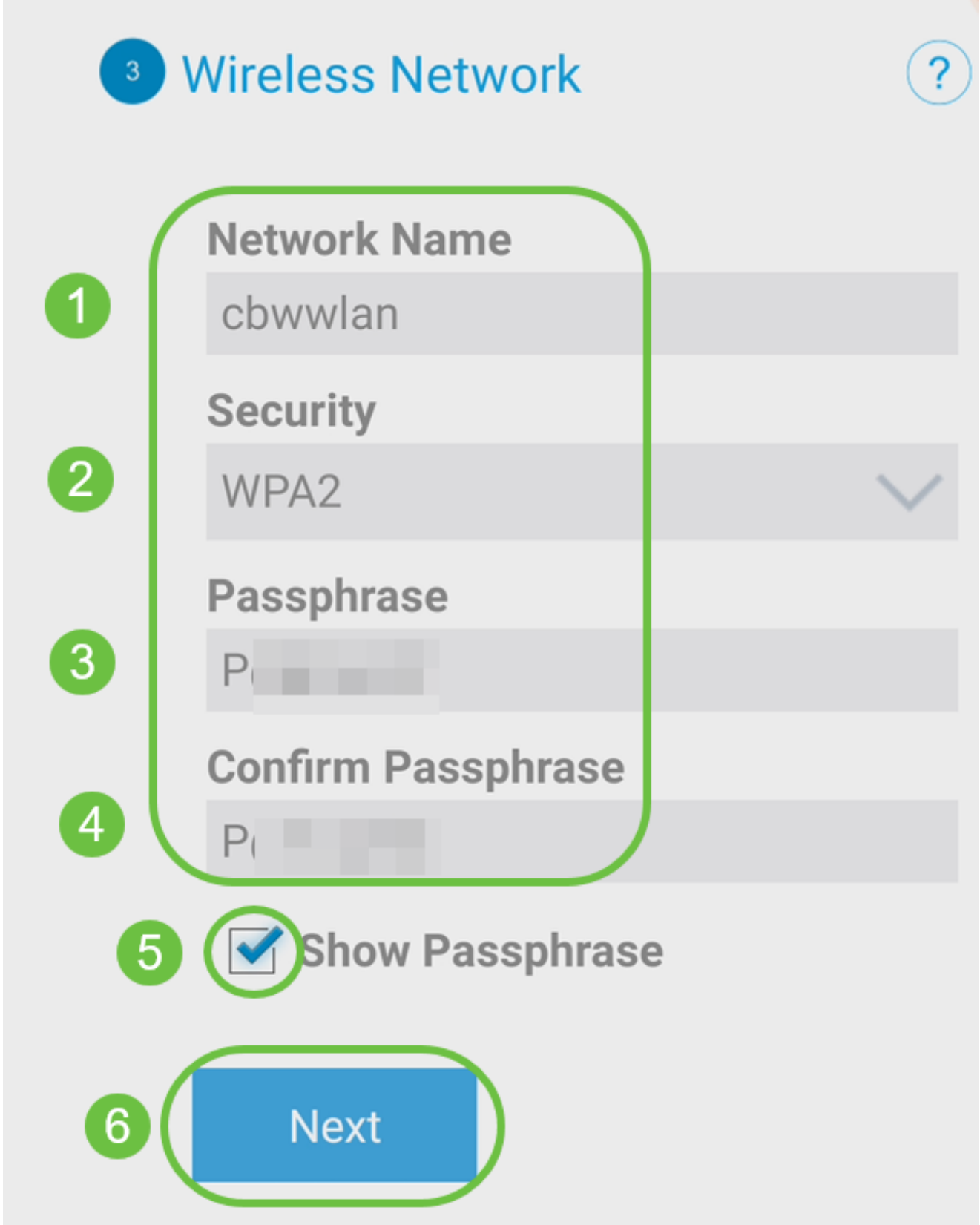


手順 9

次のように入力して、ワイヤレスネットワークを設定します。

- ネットワーク名/SSID
- セキュリティ
- パスフレーズ
- パスフレーズの確認
- （オプション）Show Passphraseにチェックマークを付けます。

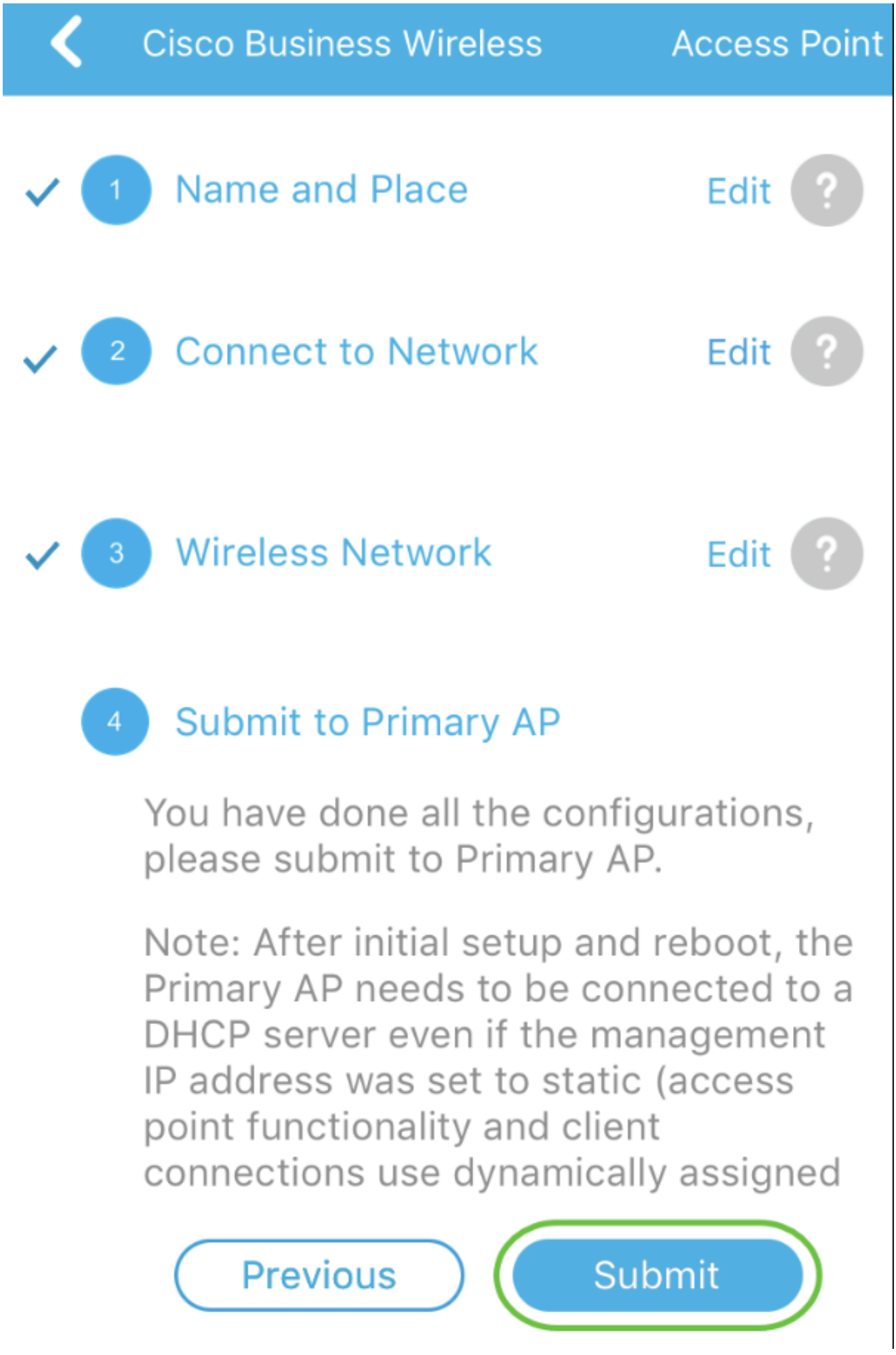
[Next] をクリックします。



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

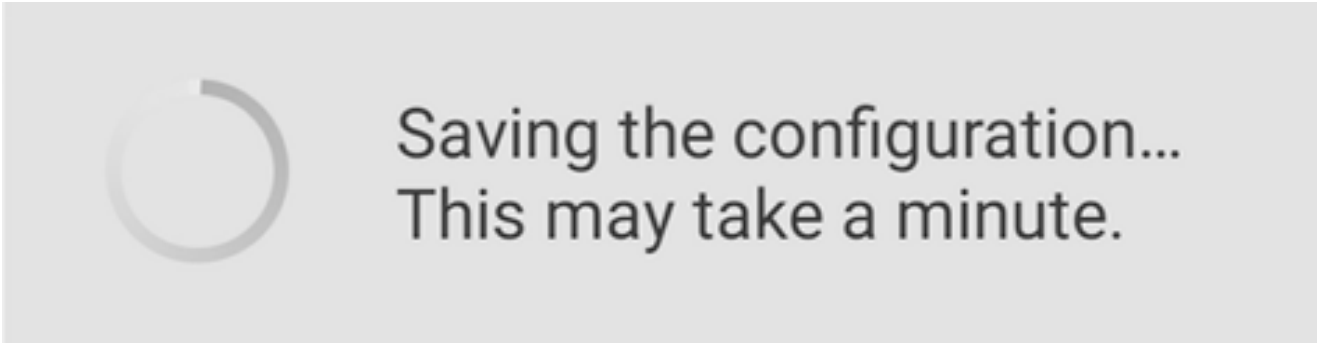
手順 10

Submit to Mobile Application AP画面で設定を確認するには、Submitをクリックします。


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

手順 11

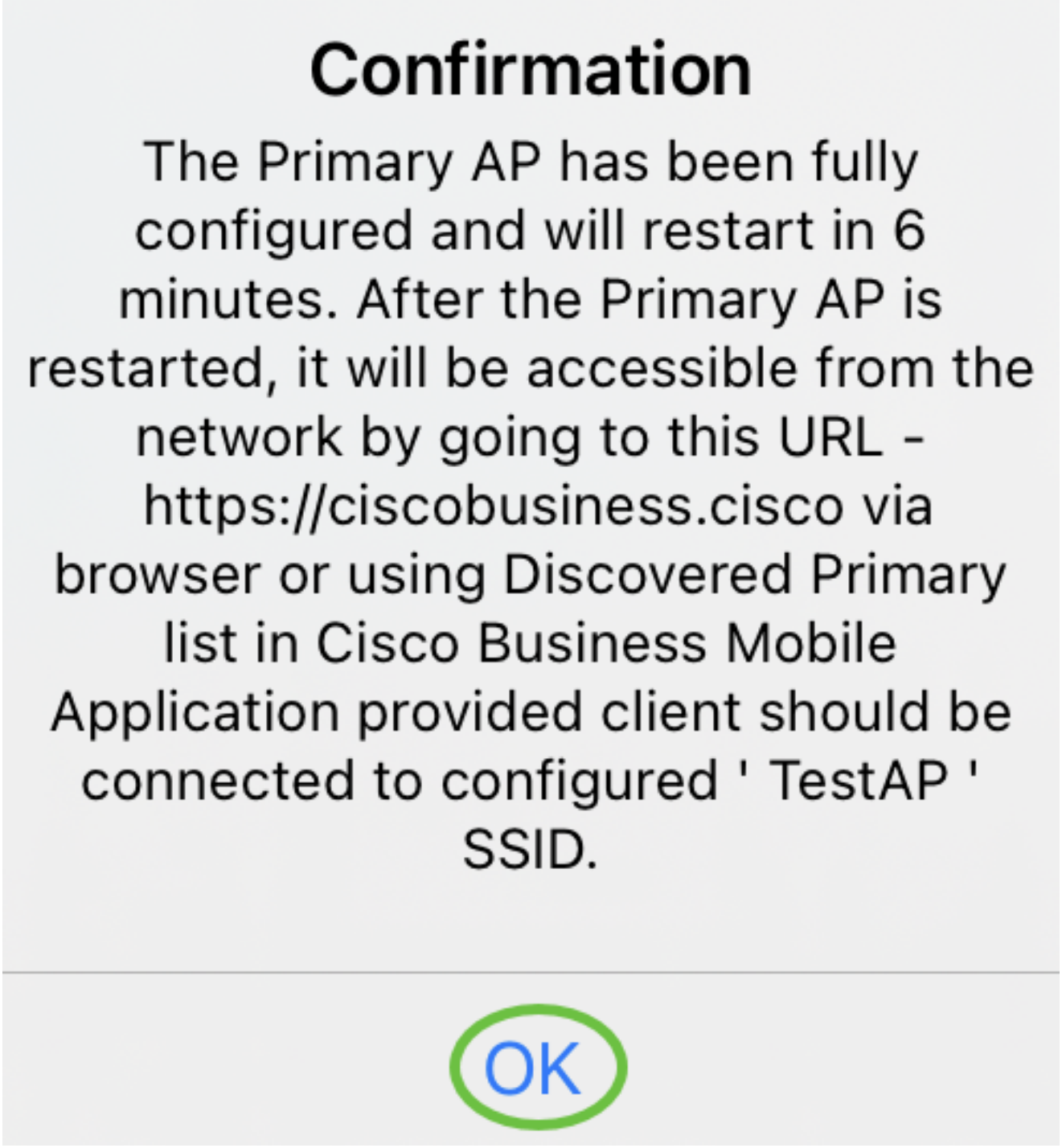
リブートが完了するまで待ちます。



リブートには最大10分かかることがあります。リブート中は、アクセスポイントのLEDが複数のカラーパターンに変化します。LEDがグリーンに点滅したら、次の手順に進みます。LEDが赤い点滅パターンを通過しない場合は、ネットワークにDHCPサーバがないことを示しています。APがDHCPサーバを使用して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 12

次の確認画面が表示されます。[OK] をクリックします。



手順 13

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

ワイヤレスのトラブルシューティングのヒント

問題がある場合は、次のヒントを確認してください。

- 正しいService Set Identifier(SSID)が選択されていることを確認します。これは、ワイヤレスネットワーク用に作成した名前です。
- モバイルアプリまたはラップトップのVPNを切断します。モバイルサービスプロバイ

ダーが使用しているVPNに接続している可能性があり、そのVPNを知らない可能性もあります。たとえば、Google Fiをサービスプロバイダーとして使用するAndroid(Pixel 3)電話には、通知なしで自動接続する組み込みVPNがあります。モバイルアプリケーションAPを見つけるには、これを無効にする必要があります。

- https://<IP address of the Mobile Application AP>を使用して、モバイルアプリケーションAPにログインします。
- 初期設定を行ったら、ciscobusiness.ciscoにログインしているか、Webブラウザに IPアドレスを入力して、https:// isが使用されていることを確認します。設定によっては、最初にログインしたときに使用したhttp:// sinceがコンピュータに自動入力されている場合があります。
- APの使用中にWeb UIまたはブラウザの問題へのアクセスに関連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の順に選択して、Refresh Firefoxをクリックします。

CBW142ACMメッシュエクステンダの設定

このネットワークの設定は非常に簡単です。メッシュエクステンダを追加するだけです。

モバイルデバイスでCisco Businessアプリケーションにログインします。

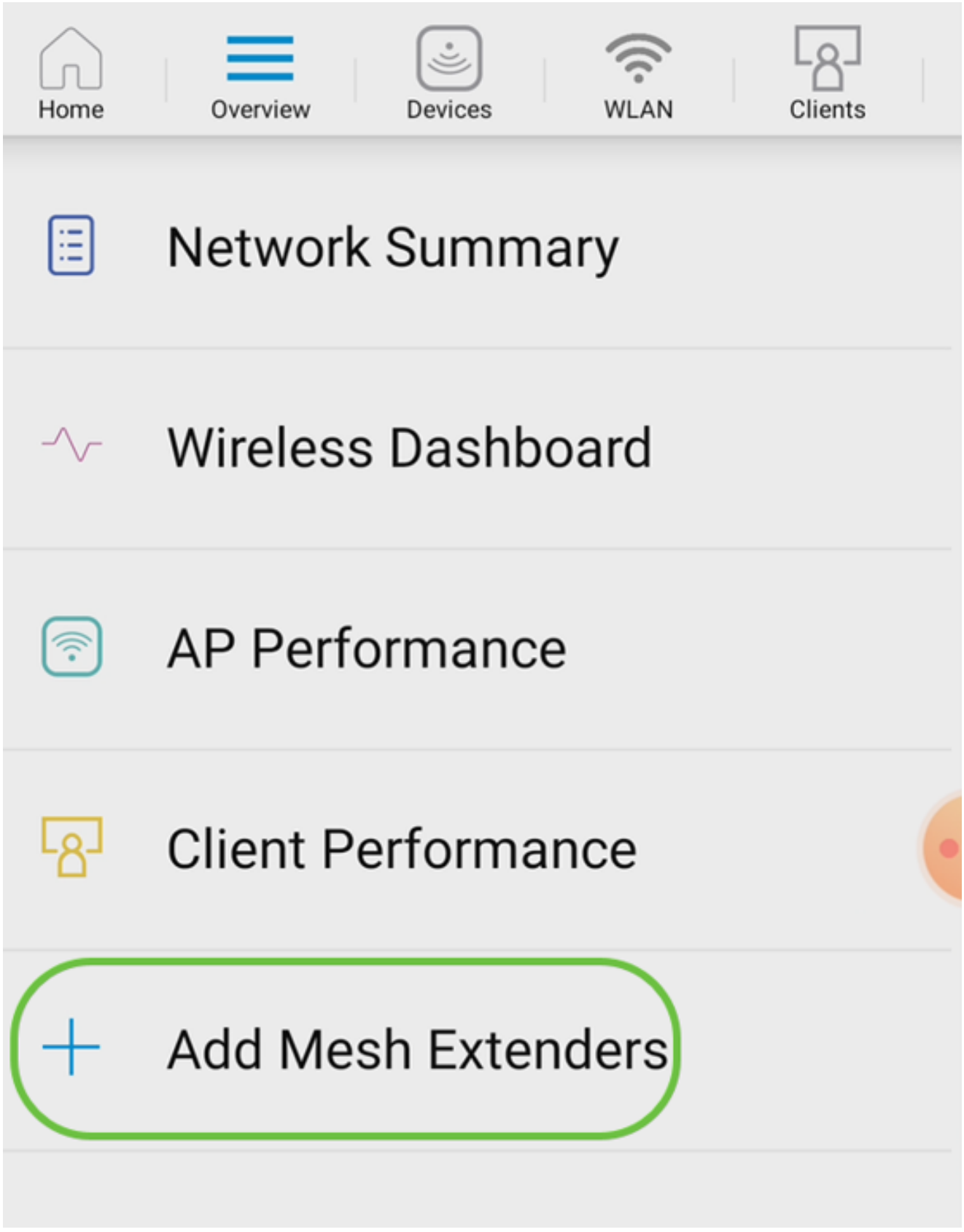
手順 1

Devicesに移動します。Meshが有効になっていることを再確認します。

Name	Clients	Usage
APA453.0E1E.2338*	0	0 Bytes
AP4CBC.48C0.74B8	0	0 Bytes
APA453.0E22.0A70	0	0 Bytes
AP68CA.E46E.1650	0	2 MB
AP68CA.E470.0500	0	11 MB

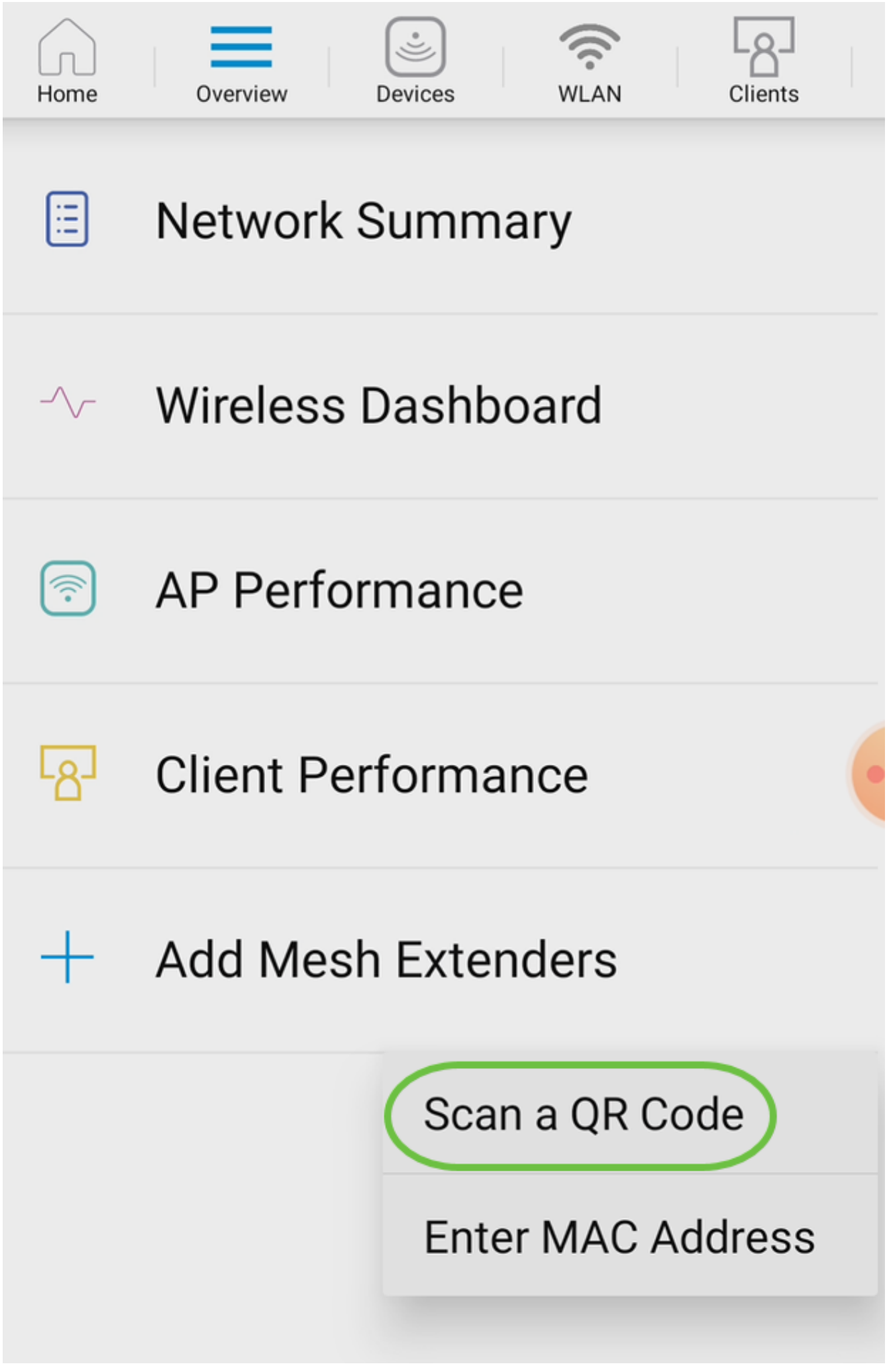
手順 2

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



手順 3

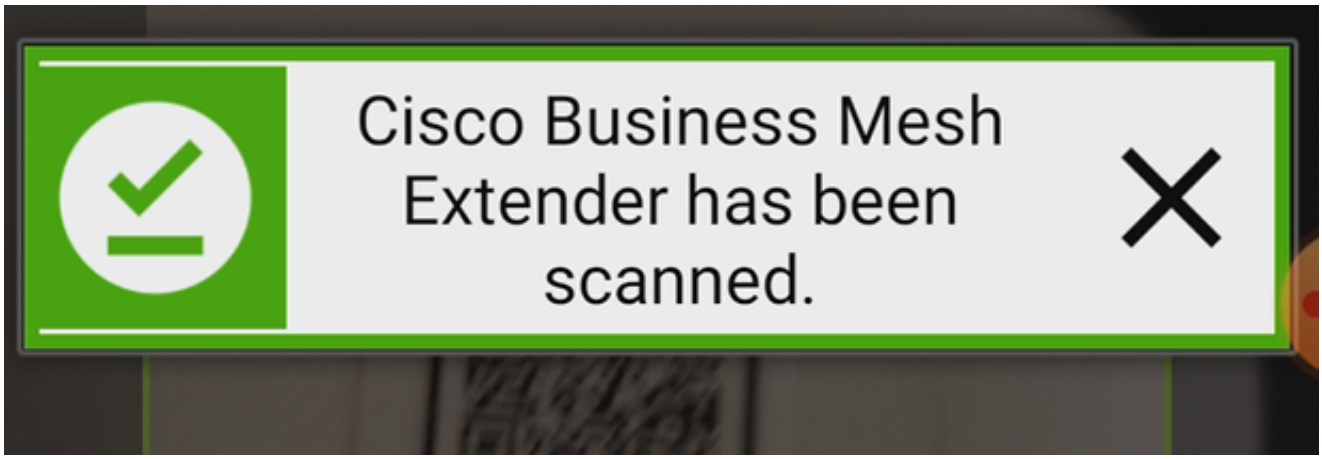
MACアドレスを追加するには、QRコードをスキャンするか、MACアドレスを手動で入力します。この例では、QRコードのスキャンが選択されています。


Home
Overview
Devices
WLAN
Clients
Network Summary
Wireless Dashboard
AP Performance
Client Performance
Add Mesh Extenders
Scan a QR Code
Enter MAC Address

手順 4

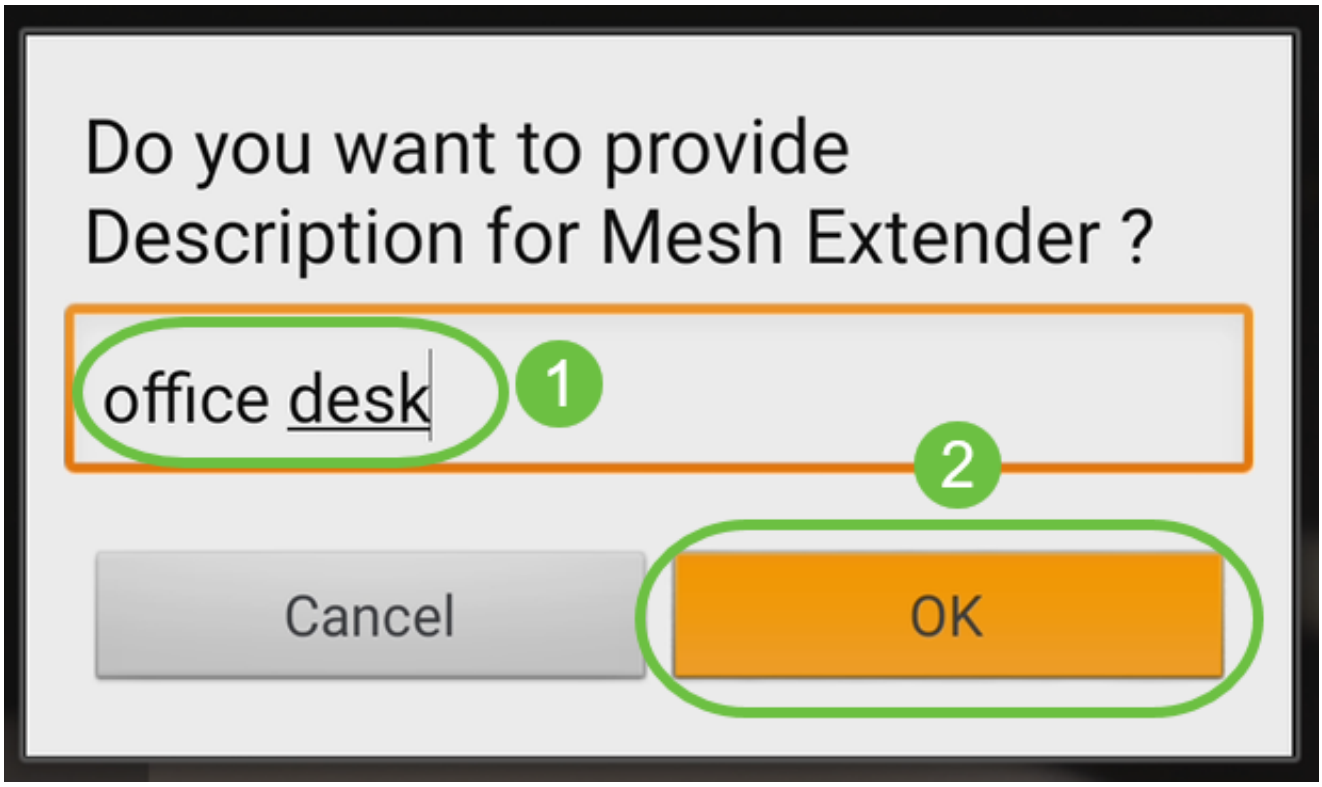
QRコードリーダーがQRコードをスキャンするように表示されます。

Mesh ExtenderのQRコードをスキャンすると、以下の画面が表示されます。



手順 5 (オプション)

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



手順 6

Summaryを確認し、Submitをクリックします。

Summary

Almost done. The following Mesh Extenders will be added to your site. If you are done adding Mesh Extenders, click submit.

Mesh Extenders To Be Added

Scanned MAC Address

A4 0 office desk

ステップ7

Add More Mesh Extenderをクリックして、ネットワークに他のメッシュエクステンダを追加します。メッシュエクステンダをすべて追加したら、Doneをクリックします。

Done! Your Mesh Extender has been added

Good News! You've successfully added your Mesh Extender

Mesh Extender Status

A4 0 SUCCESS

What's Next ?

Add More Mesh Extenders

各メッシュエクステンダに対して同じ手順を繰り返します。

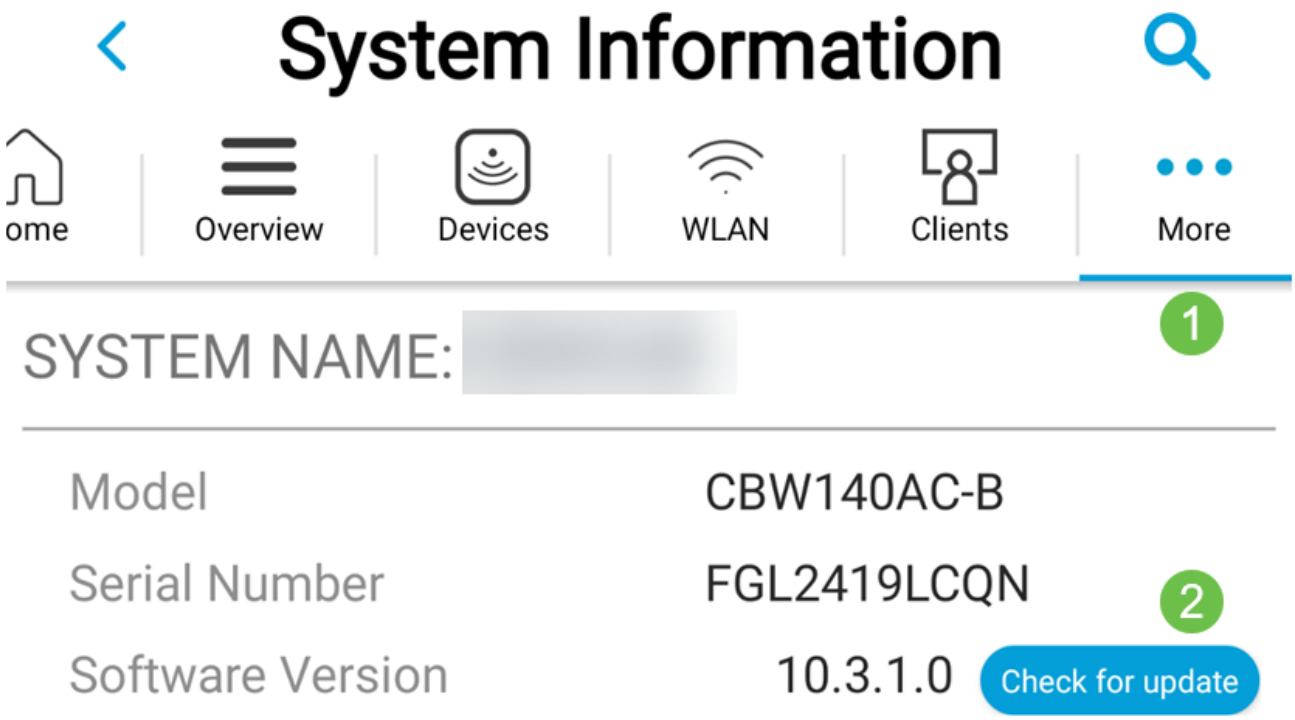
これで基本設定をロールする準備ができました。先に進む前に、必要に応じてソフトウェアを確認して更新してください。

モバイルアプリでのソフトウェアの確認と更新

ソフトウェアの更新は非常に重要です。この部分は飛ばさないでください。

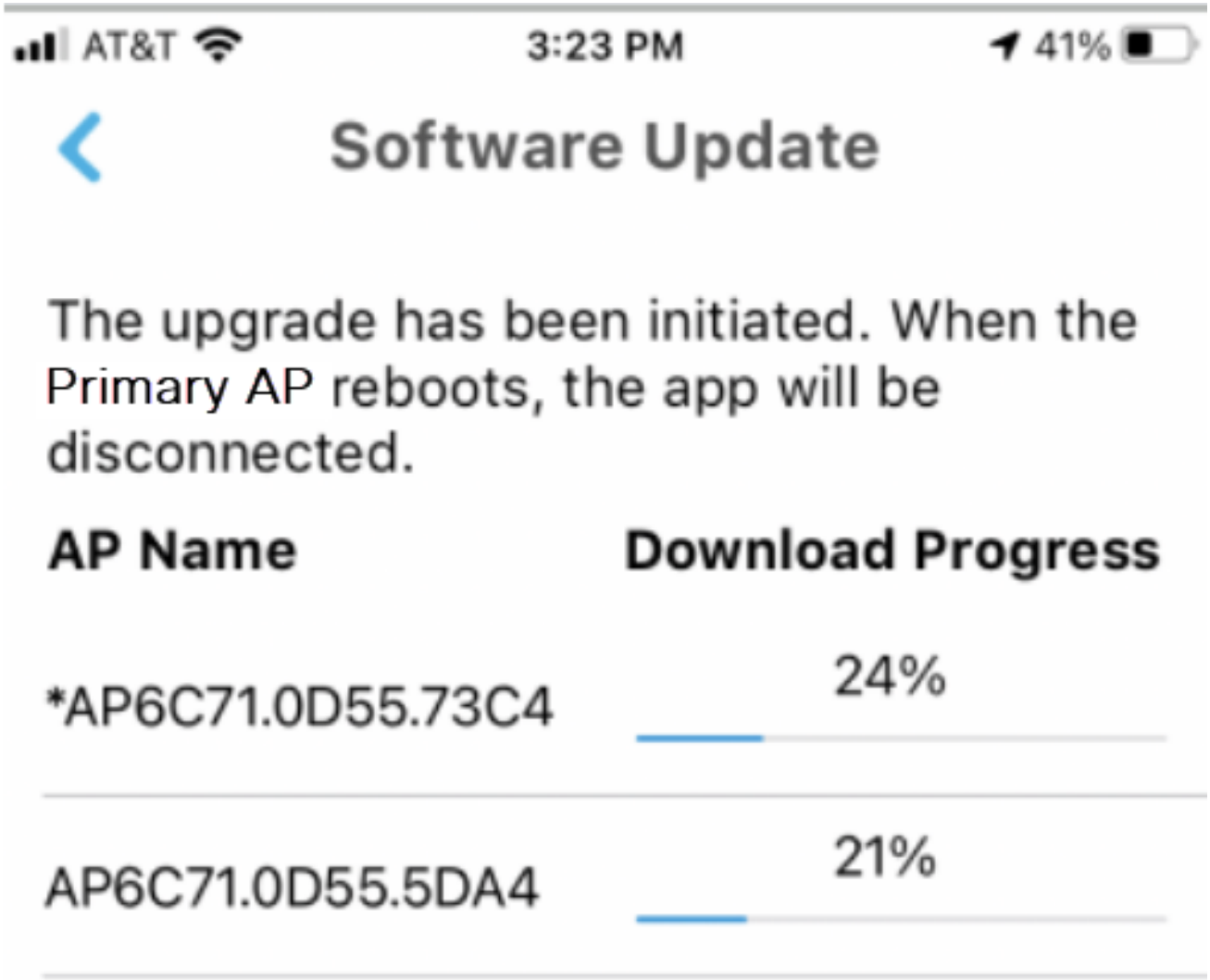
手順 1

モバイルアプリのMoreタブで、Check for updateボタンをクリックします。プロンプトに従ってソフトウェアを最新バージョンに更新します。



手順 2

ロード中にダウンロードの進行状況が表示されます。


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

手順 3

ソフトウェアアップグレードの完了を知らせるポップアップが表示されます。[OK] をクリックします。

モバイルアプリを使用したWLANの作成

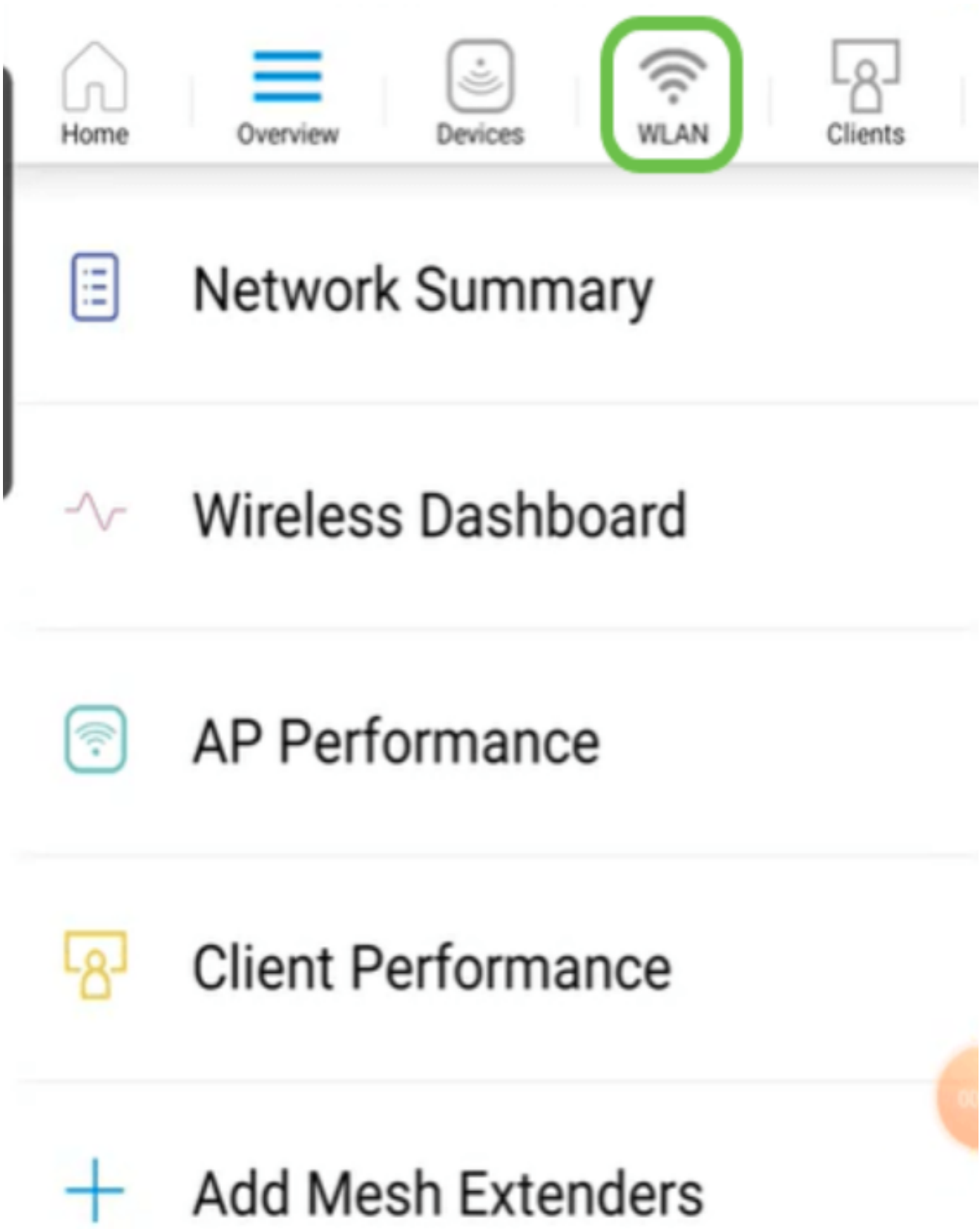
このセクションでは、ワイヤレスローカルエリアネットワーク(WLAN)を作成できます。

手順 1

Cisco Business Wireless Appを開きます。

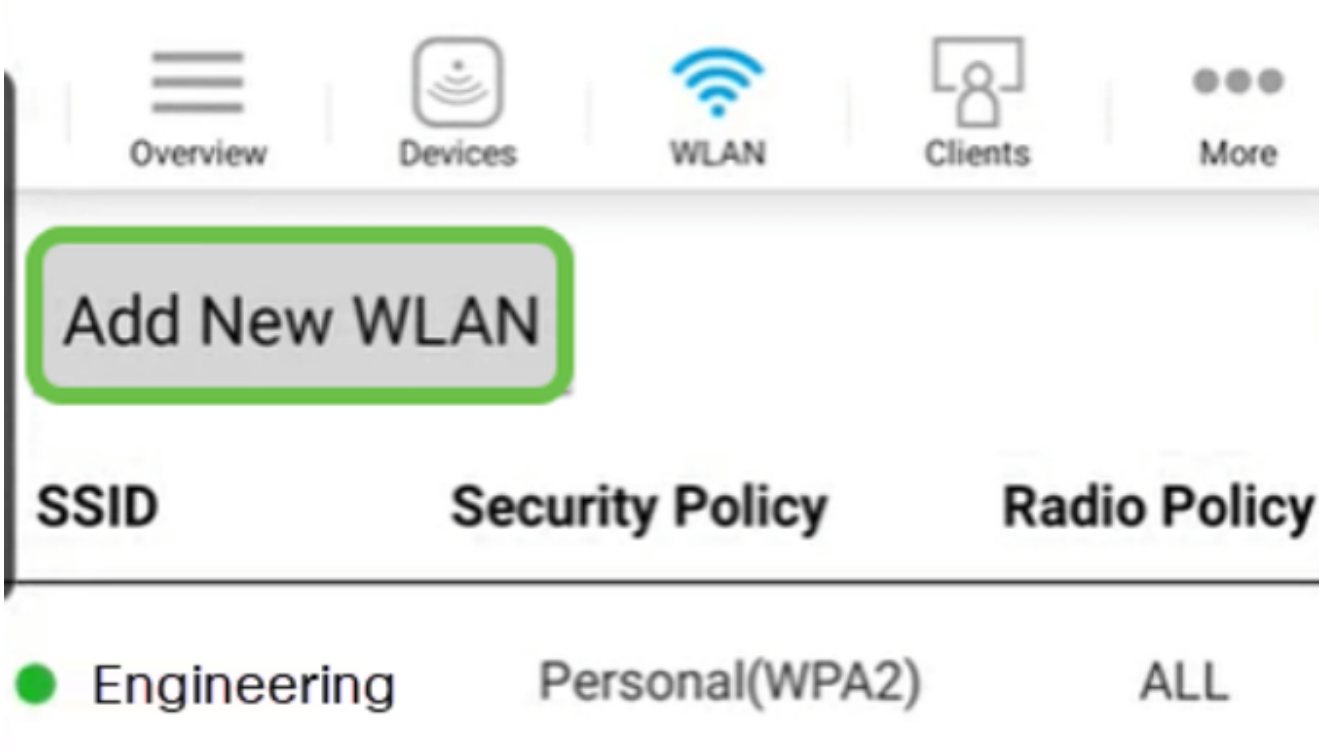
手順 2

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



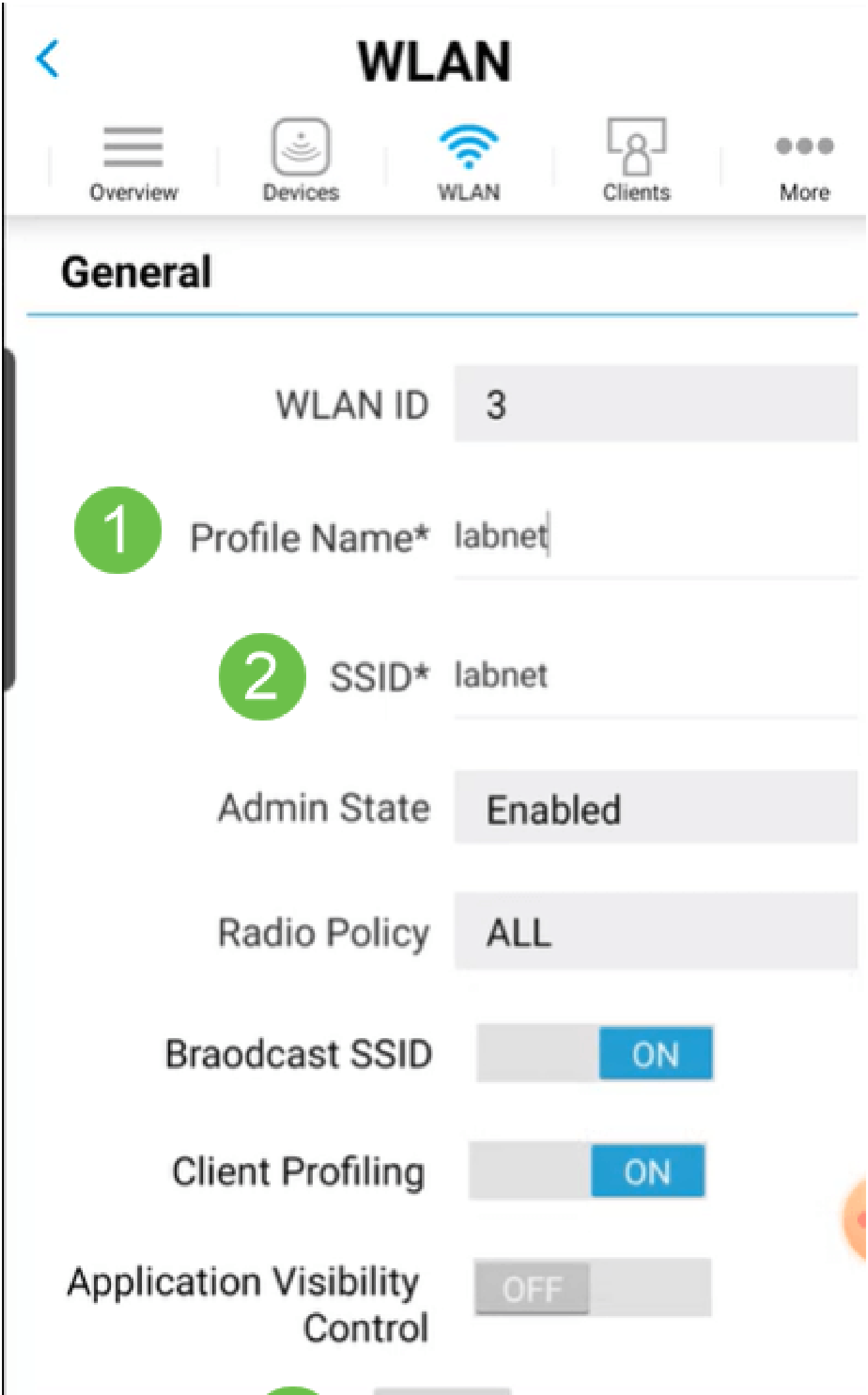
手順 3

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



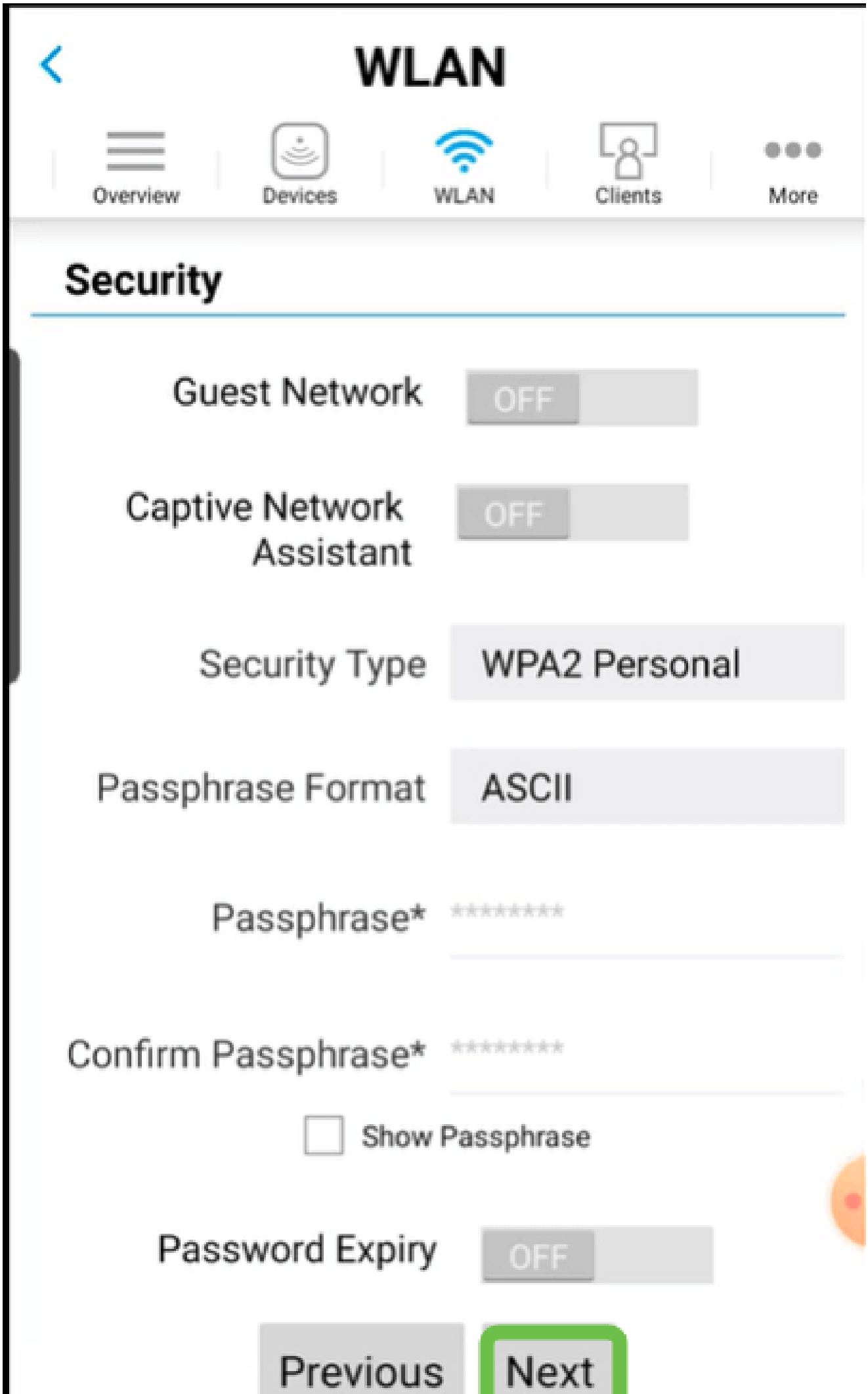
手順 4

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


WLAN
Overview
Devices
WLAN
Clients
More
General
WLAN ID
3
1
Profile Name*
labnet
2
SSID*
labnet
Admin State
Enabled
Radio Policy
ALL
Braodcast SSID
ON
Client Profiling
ON
Application Visibility Control
OFF

手順 5（オプション）

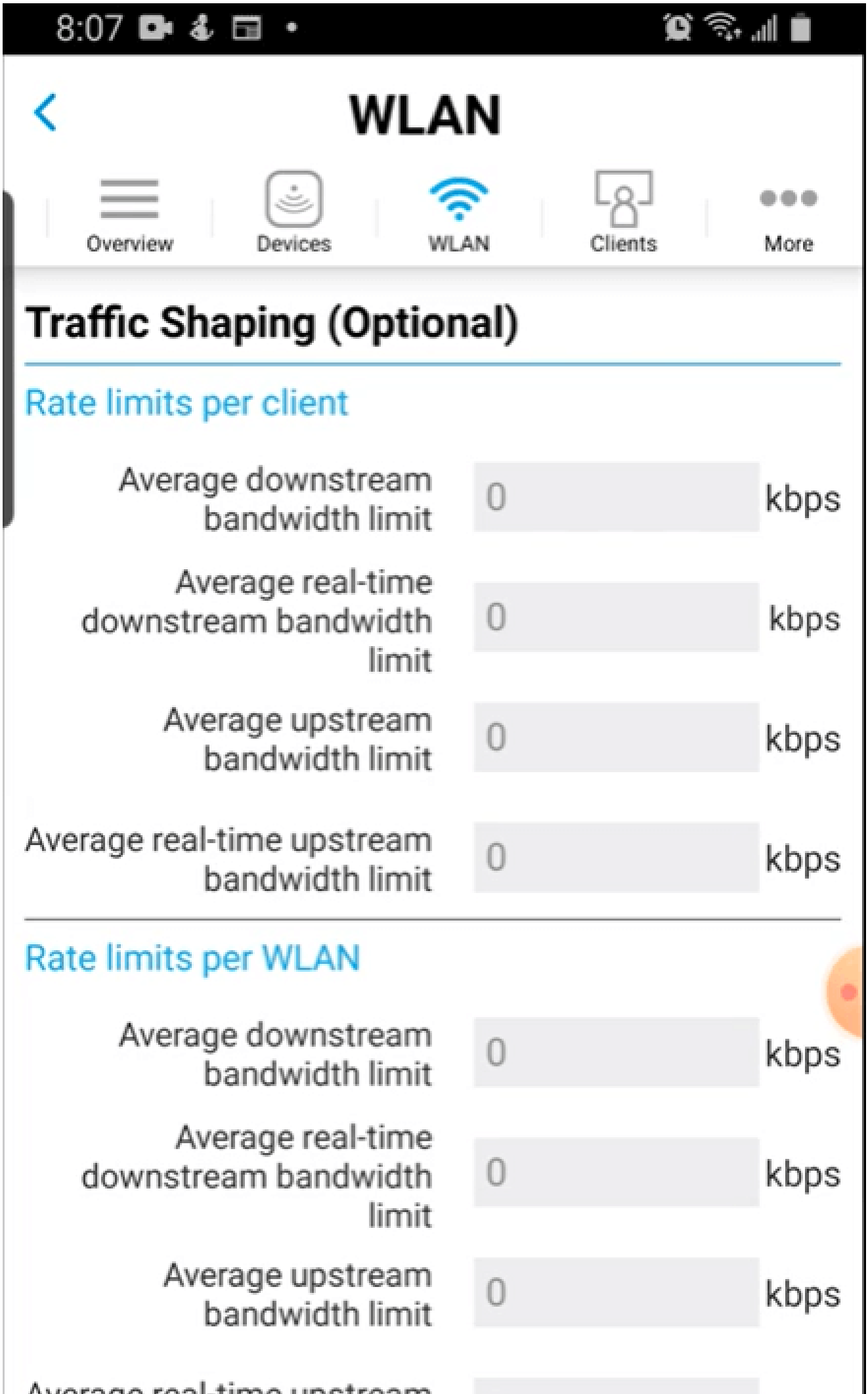
ステップ4でApplication Visibility Controlを有効にした場合は、ゲストネットワークなどの他の設定を構成できます。詳細については、次のセクションを参照してください。 Captive Network Assistant、Security Type、Passphrase、およびPassword Expiryもここに追加できます。すべての設定を追加したら、Nextをクリックします。


WLAN
Overview
Devices
WLAN
Clients
More
Security
Guest Network
OFF
Captive Network Assistant
OFF
Security Type
WPA2 Personal
Passphrase Format
ASCII
Passphrase*
Confirm Passphrase*
Show Passphrase
Password Expiry
OFF
Previous
Next

モバイルアプリケーションを使用する場合、Security TypeのオプションはOpenまたは WPA2 Personalのみです。より高度なオプションを使用する場合は、代わりにモバイルアプリケーションAPのWeb UIに口グインします。

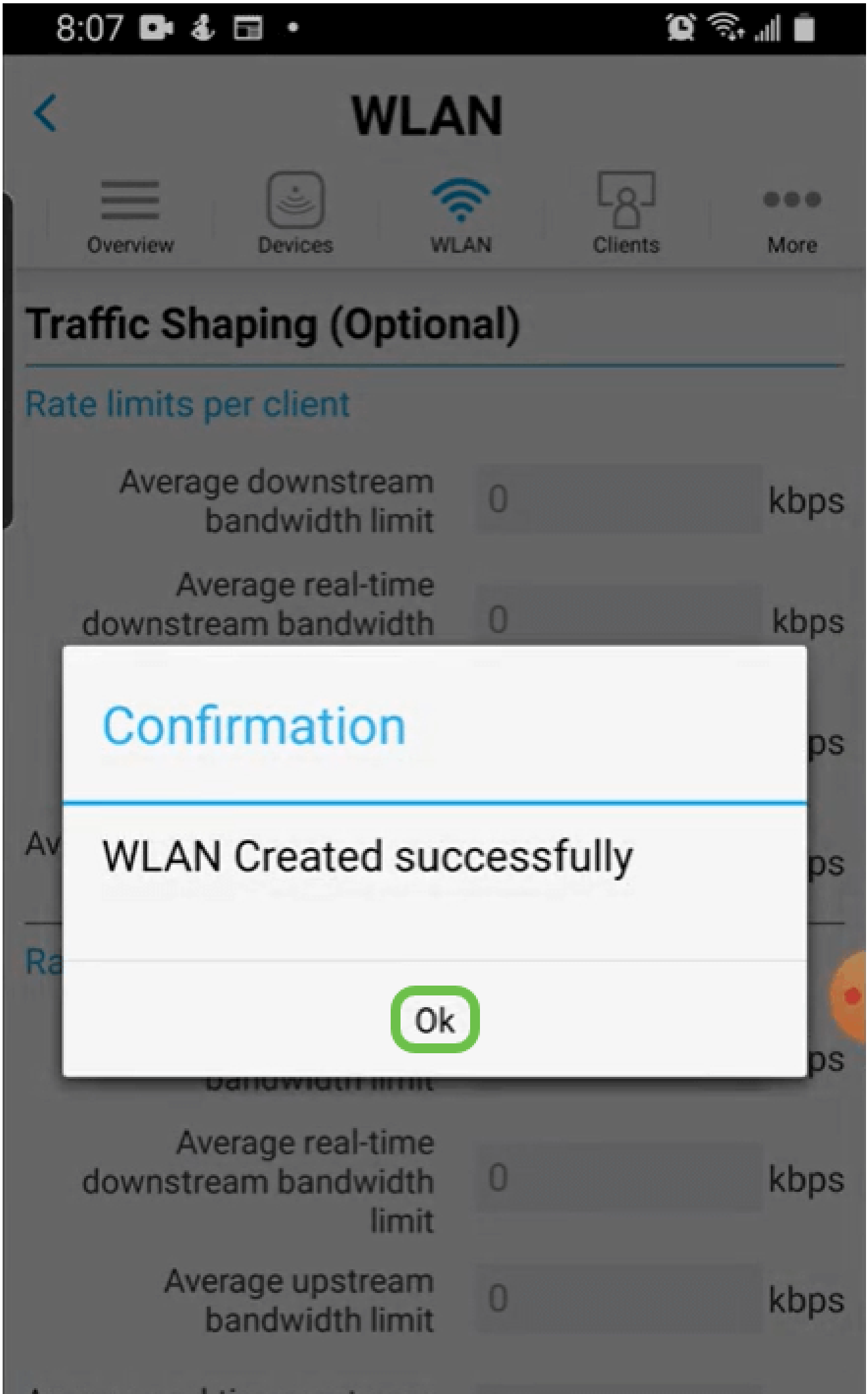
ステップ 6（オプション）

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


8:07
WLAN
Overview
Devices
WLAN
Clients
More
Traffic Shaping (Optional)
Rate limits per client
Average downstream bandwidth limit
0
kbps
Average real-time downstream bandwidth limit
0
kbps
Average upstream bandwidth limit
0
kbps
Average real-time upstream bandwidth limit
0
kbps
Rate limits per WLAN
Average downstream bandwidth limit
0
kbps
Average real-time downstream bandwidth limit
0
kbps
Average upstream bandwidth limit
0
kbps

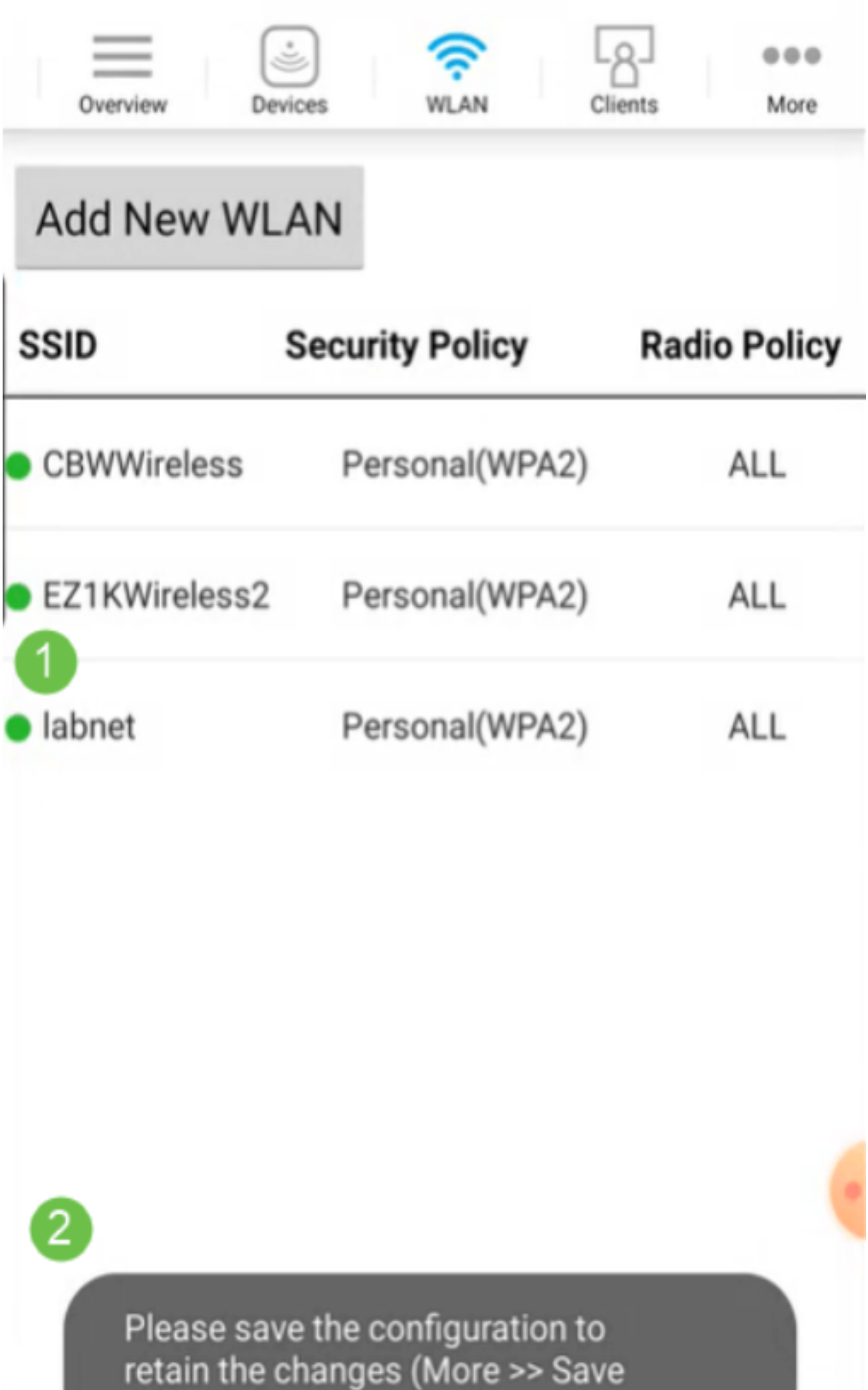
ステップ7

確認ポップアップが表示されます。[OK] をクリックします。


8:07
WLAN
Overview
Devices
WLAN
Clients
More
Traffic Shaping (Optional)
Rate limits per client
Average downstream bandwidth limit
0
kbps
Average real-time downstream bandwidth
0
kbps
Confirmation
WLAN Created successfully
Ok
Average real-time downstream bandwidth limit
0
kbps
Average upstream bandwidth limit
0
kbps

手順 8

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


Overview
Devices
WLAN
Clients
More
Add New WLAN
SSID
Security Policy
Radio Policy
CBWWireless
Personal(WPA2)
ALL
EZ1KWireless2
Personal(WPA2)
ALL
1
labnet
Personal(WPA2)
ALL
2
Please save the configuration to
retain the changes (More >> Save

手順 9

Moreタブをクリックし、ドロップダウンメニューからSave Configurationを選択して、設定を保存します。

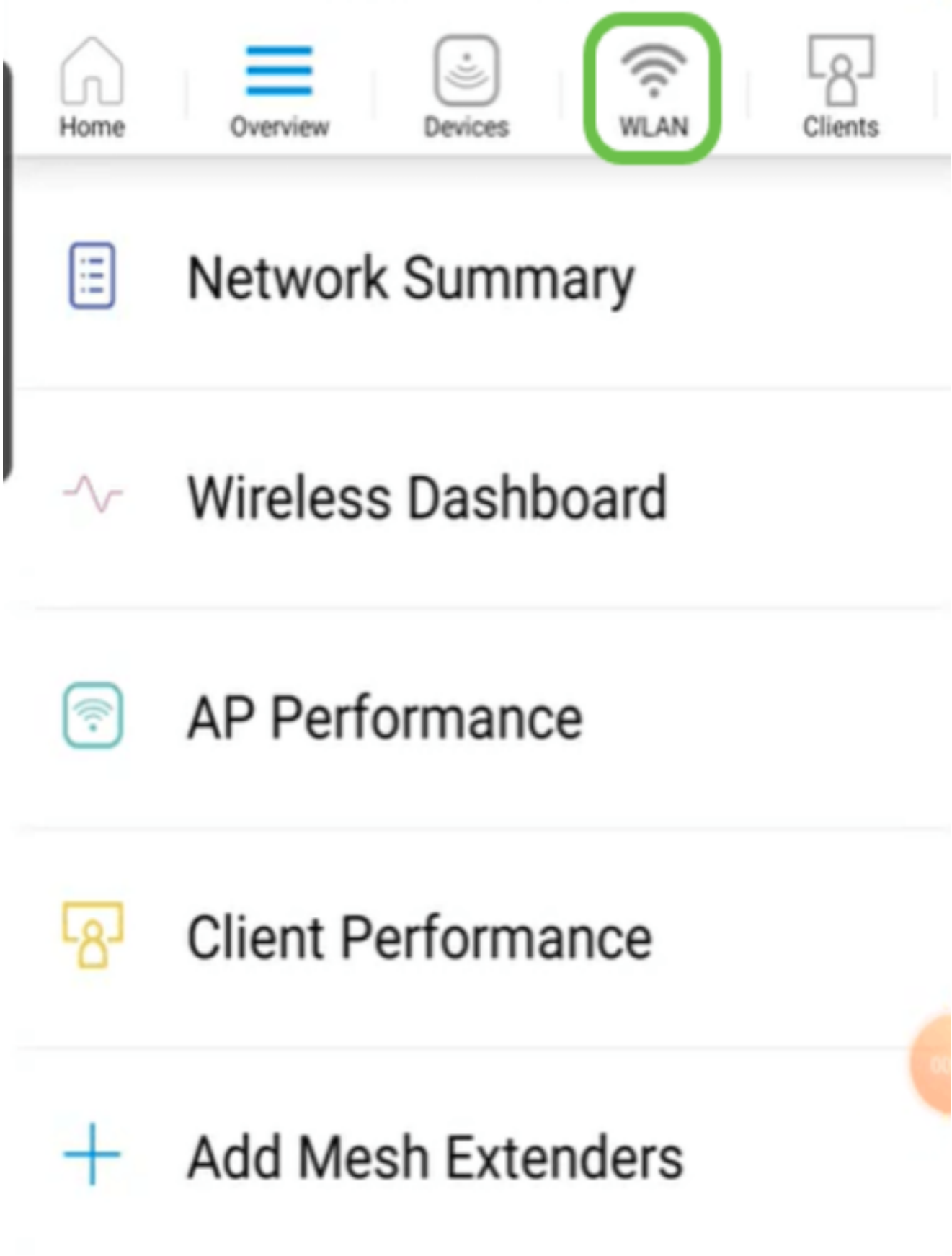
モバイルアプリを使用したゲストWLANの作成

手順 1

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

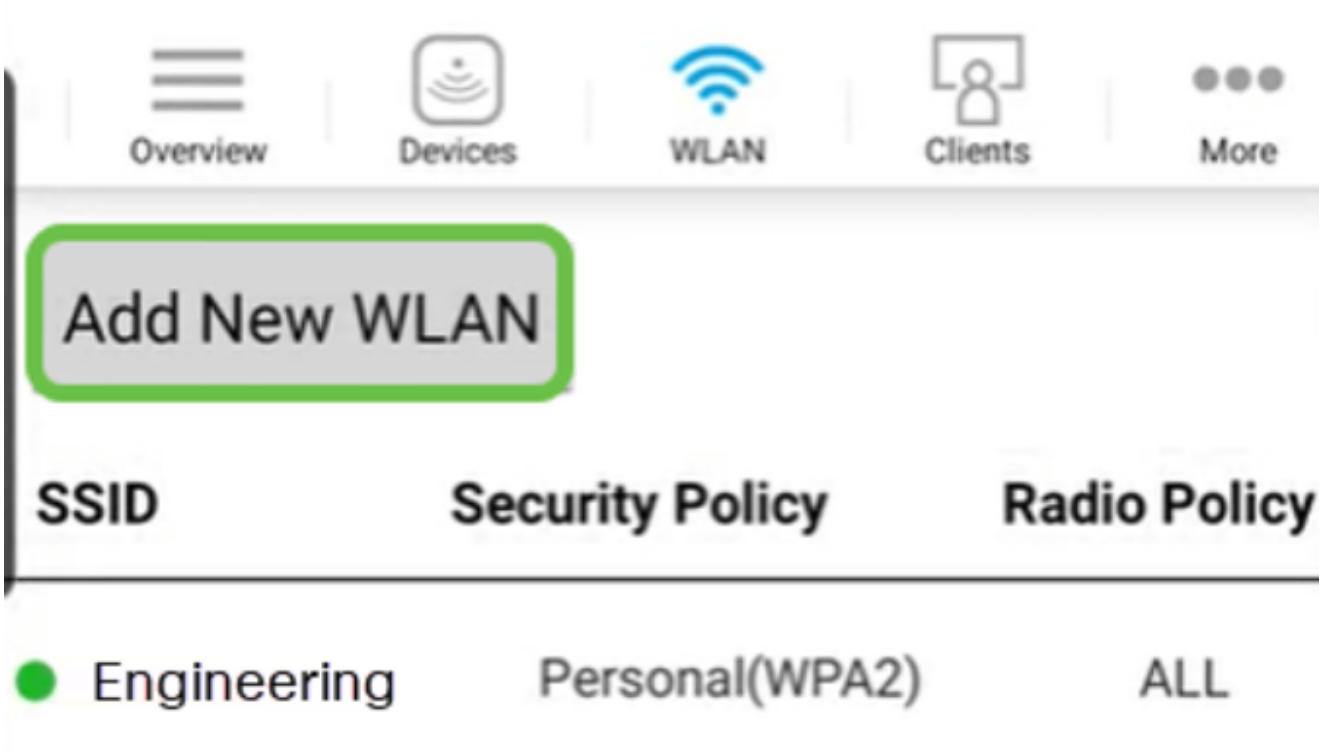
手順 2

ページの上部にあるWLANアイコンをクリックします。



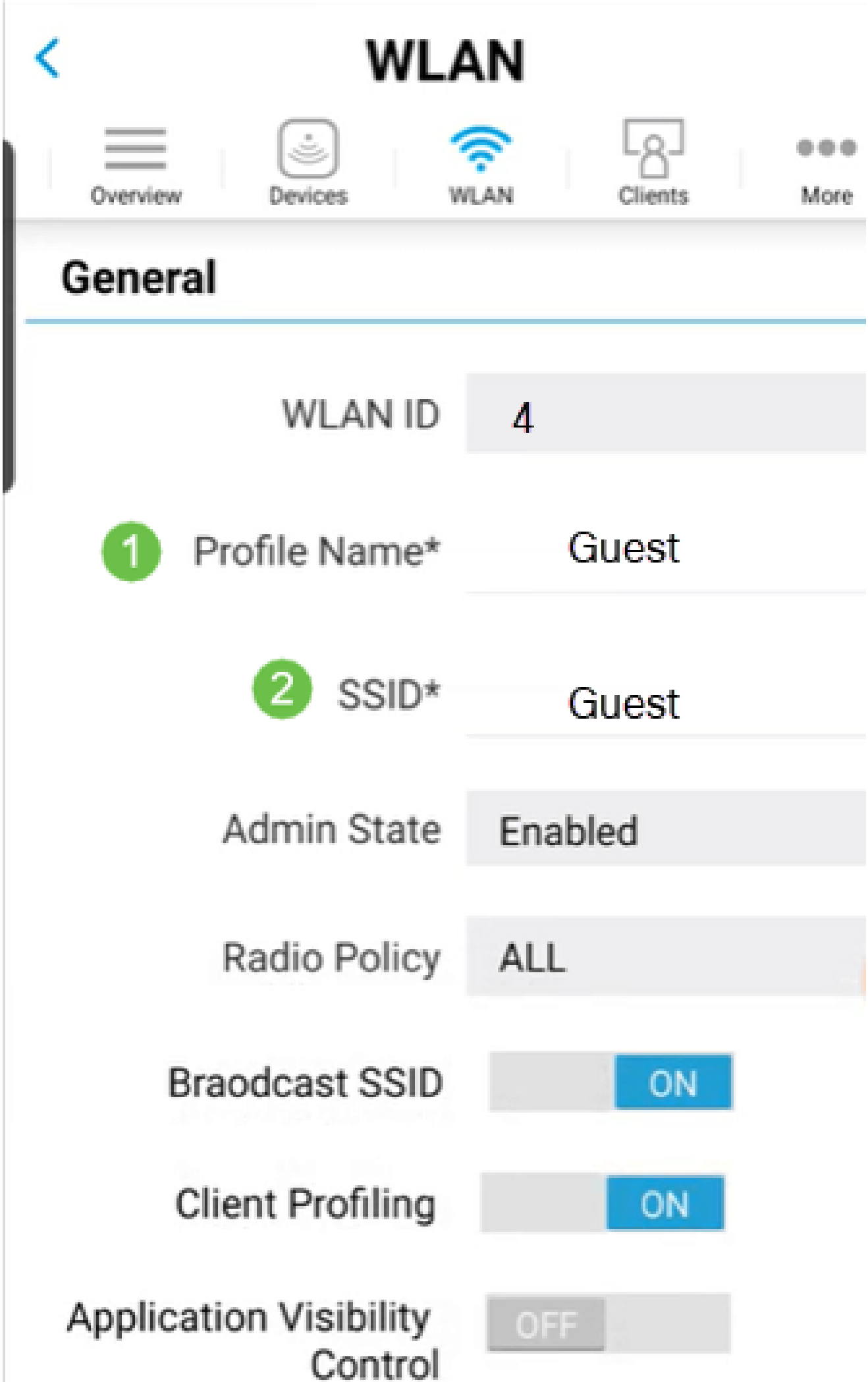
手順 3

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



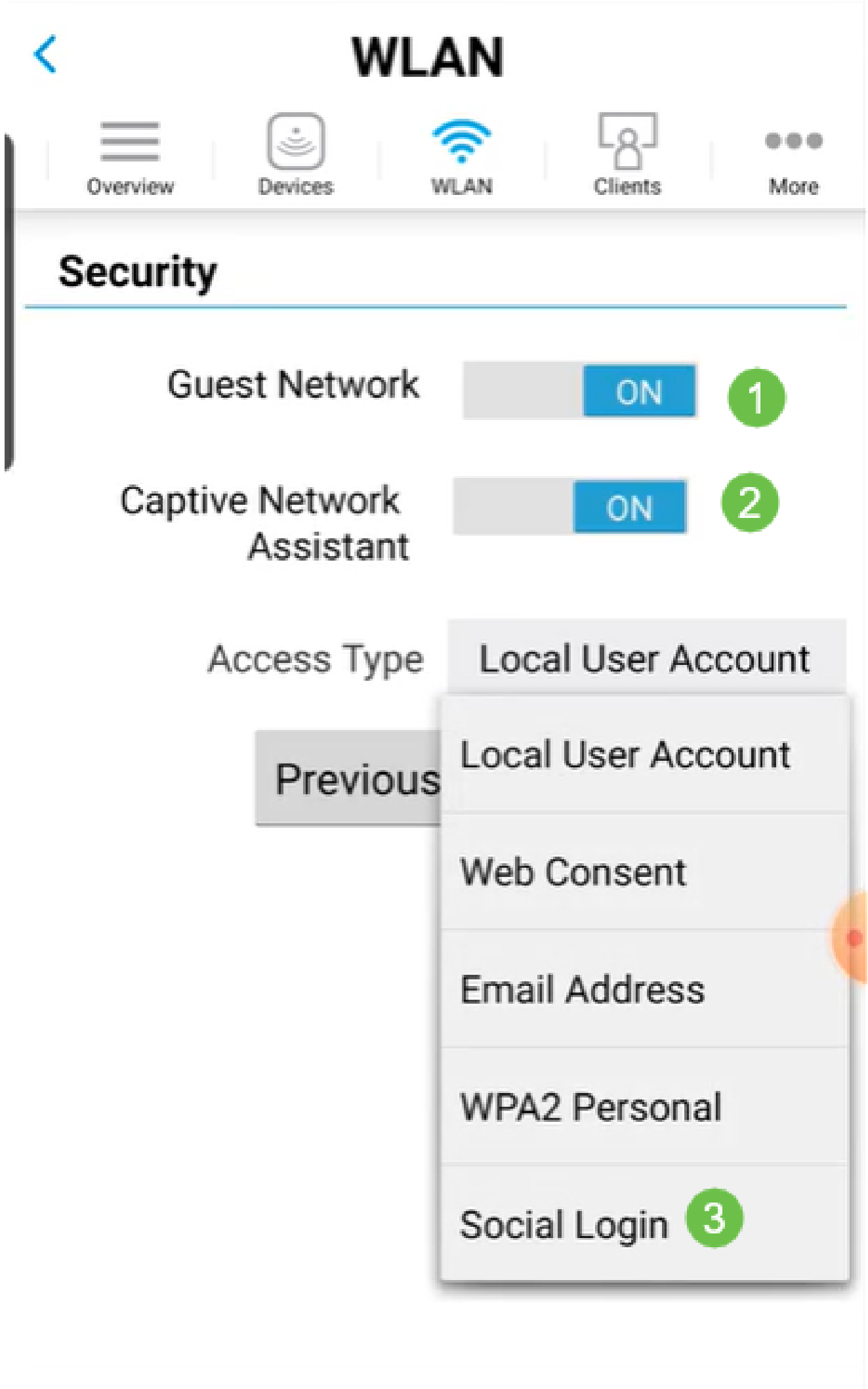
手順 4

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


WLAN
Overview
Devices
WLAN
Clients
More
General
WLAN ID
4
1
Profile Name*
Guest
2
SSID*
Guest
Admin State
Enabled
Radio Policy
ALL
Braodcast SSID
ON
Client Profiling
ON
Application Visibility Control
OFF

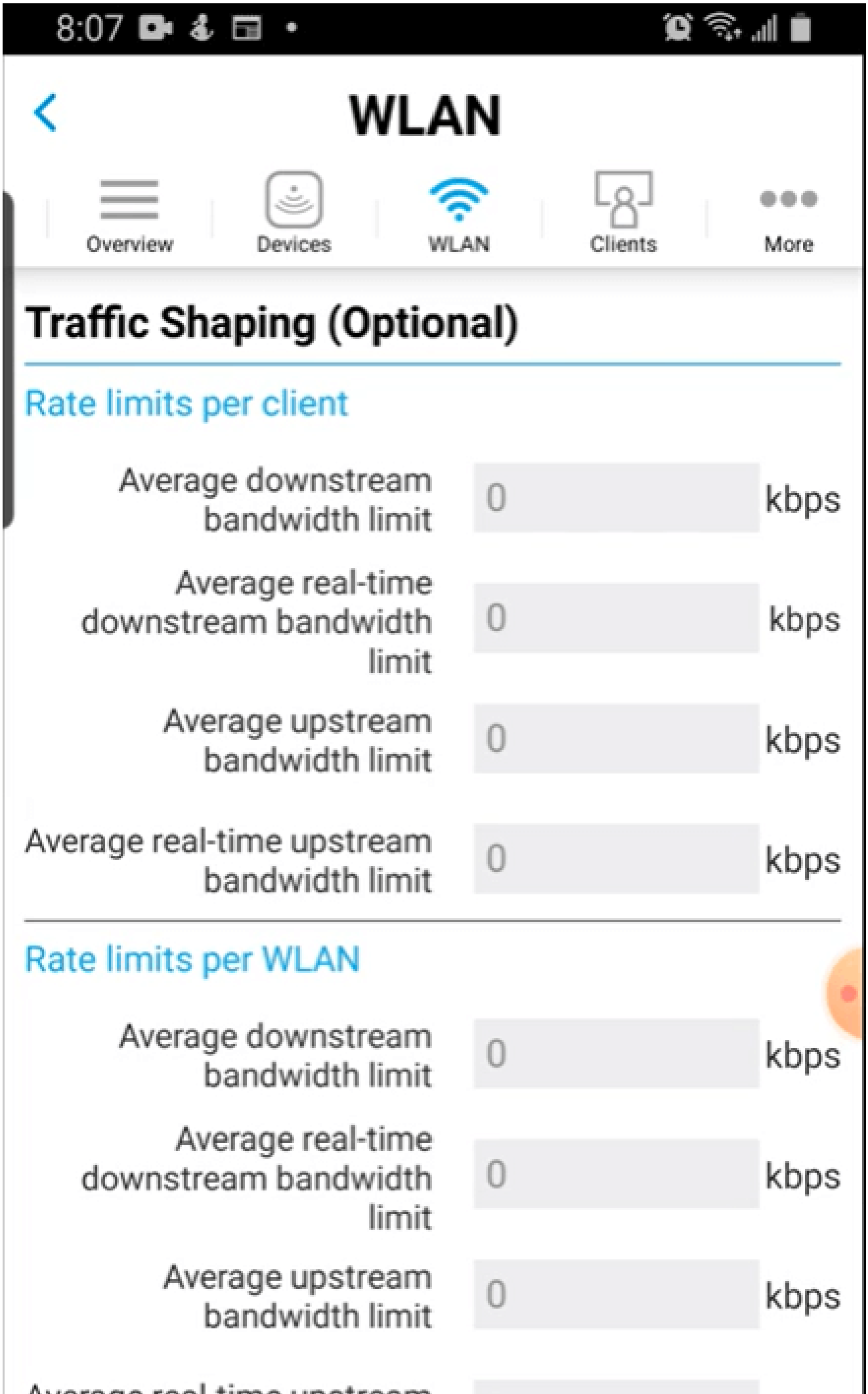
手順 5

Guest Networkをオンにします。この例では、Captive Network Assistantもオンになっていますが、これはオプションです。アクセスタイプのオプションがあります。この場合は、Social Loginが選択されています。


WLAN
Overview
Devices
WLAN
Clients
More
Security
Guest Network
ON
1
Captive Network Assistant
ON
2
Access Type
Local User Account
Previous
Local User Account
Web Consent
Email Address
WPA2 Personal
Social Login
3

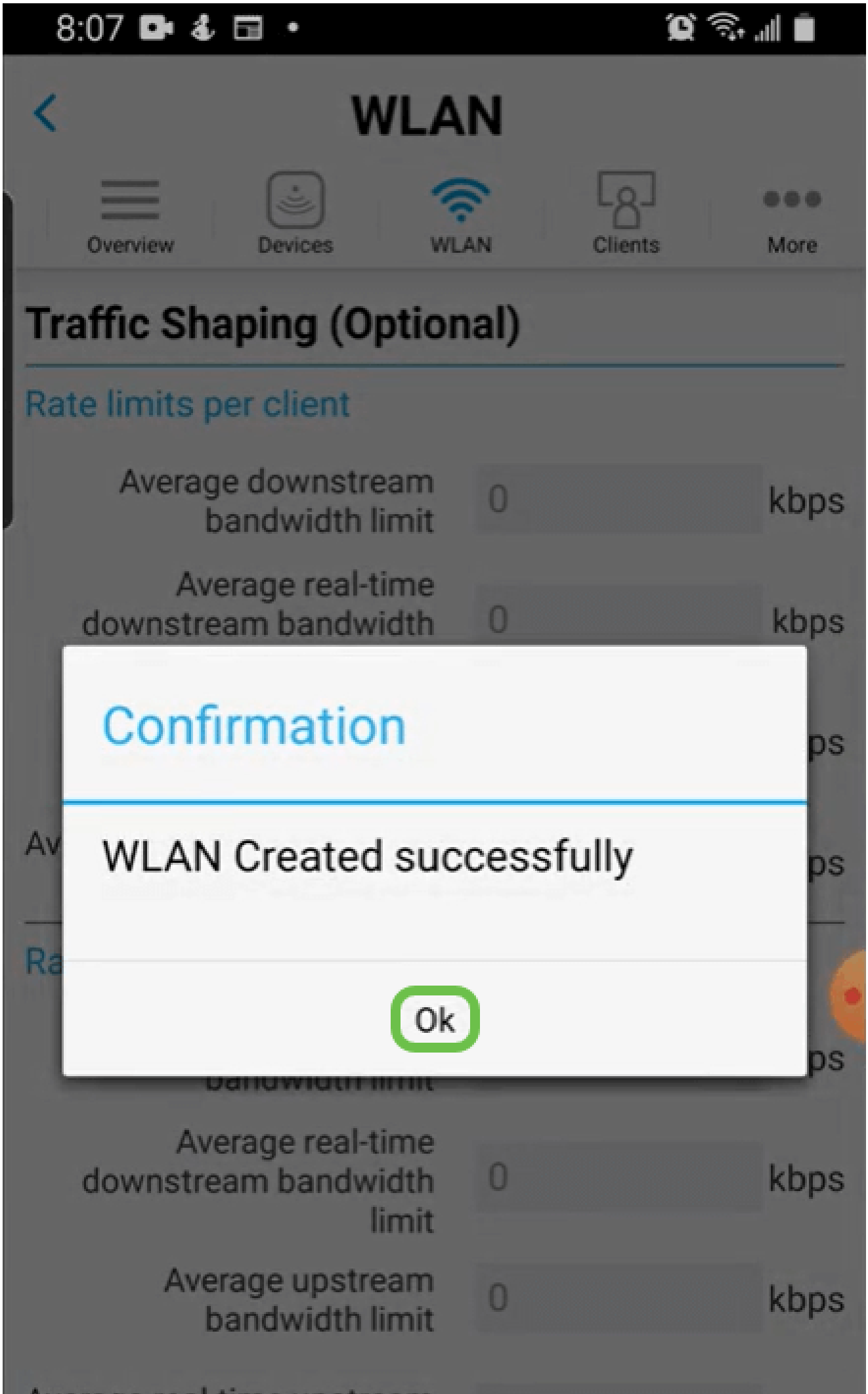
手順 6

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


8:07
WLAN
Overview
Devices
WLAN
Clients
More
Traffic Shaping (Optional)
Rate limits per client
Average downstream bandwidth limit
0
kbps
Average real-time downstream bandwidth limit
0
kbps
Average upstream bandwidth limit
0
kbps
Average real-time upstream bandwidth limit
0
kbps
Rate limits per WLAN
Average downstream bandwidth limit
0
kbps
Average real-time downstream bandwidth limit
0
kbps
Average upstream bandwidth limit
0
kbps

ステップ7

確認ポップアップが表示されます。[OK] をクリックします。


8:07
WLAN
Overview
Devices
WLAN
Clients
More
Traffic Shaping (Optional)
Rate limits per client
Average downstream bandwidth limit
0
kbps
Average real-time downstream bandwidth
0
kbps
Confirmation
WLAN Created successfully
Ok
Average real-time downstream bandwidth limit
0
kbps
Average upstream bandwidth limit
0
kbps

手順 8

Moreタブをクリックし、ドロップダウンメニューからSave Configurationを選択して、設定を保存します。

結論

これで、ネットワークの設定が完了しました。お祝いに時間を取り、その後、仕事に行く！

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

シスコでは、お客様に最善を尽くしたいと考えています。このトピックに関するご意見やご提案については、シスコのコンテンツチームまで電子メールでお送りください。

他の記事やドキュメントを読みたい場合は、ご使用のハードウェアのサポートページを参照してください。

- 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

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