RV160およびRV260ルータ上のOpenVPN

目的

この記事の目的は、RV160またはRV260ルータでのOpenVPNのセットアップ、およびコンピュータでのOpenVPNのVPNクライアントのセットアップについて説明することです。

該当するデバイス

- RV160
- RV260

[Software Version]

- 1.0.00.15

目次

概要

OpenVPNは、仮想プライベートネットワーク(VPN)用にセットアップおよび使用できる無料のオープンソースアプリケーションです。 クライアント/サーバ接続を使用して、インターネット経由でサーバとリモートクライアントロケーション間のセキュアな通信を提供します。

OpenVPNは、トラフィックの伝送にUDPとTCPの暗号化にOpenSSLを使用します。VPNは保護の安全なトンネルを提供します。これは、VPN接続を介してコンピュータから送信されるデータを暗号化するため、ハッカーに対する脆弱性が少ないためです。たとえば、空港などの公共の場所でWiFiを使用している場合は、データ、トランザクション、およびクエリが他のユーザに表示されないようにします。HTTPSと同様に、2つのエンドポイント間で送信されるデータを暗号化します。

OpenVPNをセットアップする際の最も重要な手順の1つは、認証局(CA)から証明書を取得することです。 これは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します。これは、あなたのサイトが安全であることを証明する公式の方法です。基本的に、CAは正当なビジネスであり、信頼できることを検証する信頼できるソースです。OpenVPNの場合は、低レベルの証明書を最小限のコストで使用できます。CAによってチェックアウトされ、情報を確認すると、証明書が発行されます。この証明書は、コンピュータ上のファイルとしてダウンロードできます。その後、ルータ（またはVPNサーバ）に移動し、そこにアップロードできます。クライアントはOpenVPNを使用するために証明書を必要としないことに注意してください。これはルータを介した検証のためだけです。

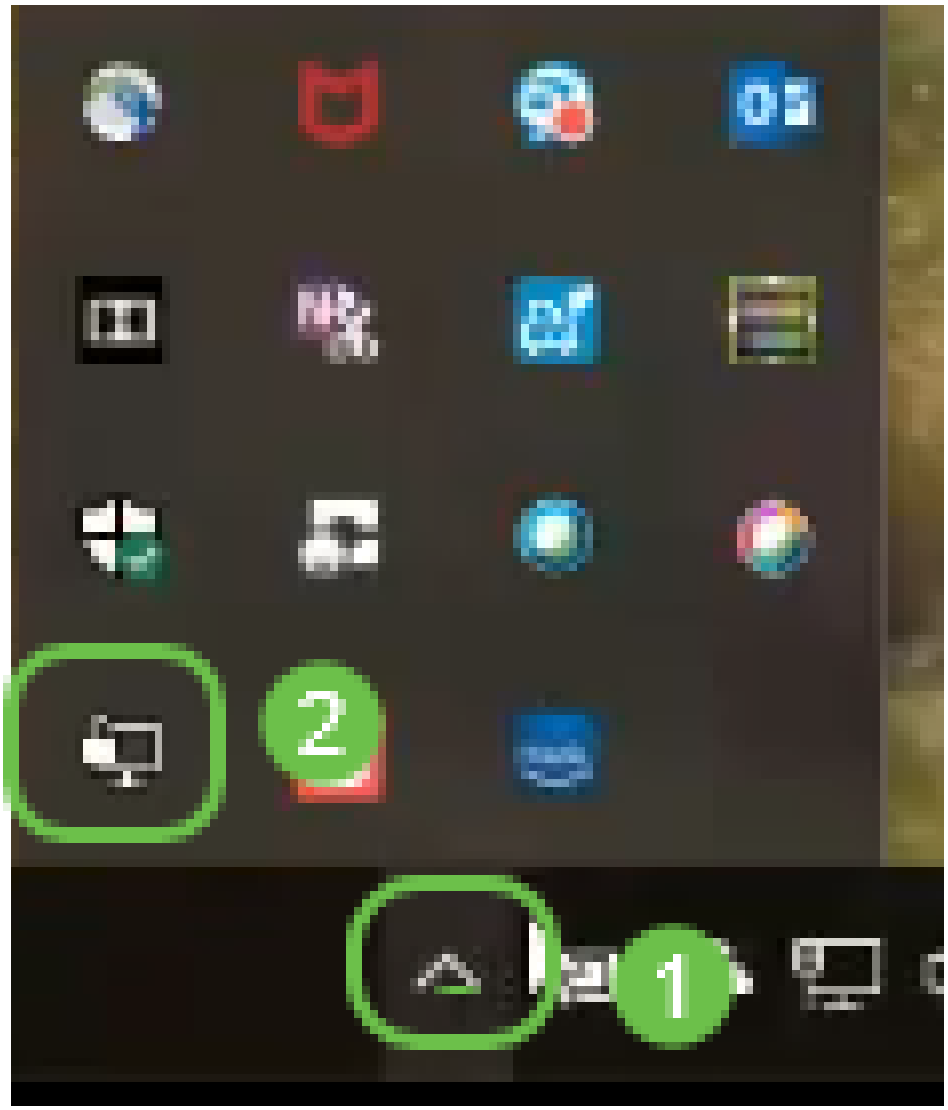
前提条件

OpenVPNアプリケーションをシステムにインストールします。ここをクリックして、OpenVPN Webサイトにアクセスしてください。

OpenVPNの詳細と多くの質問への回答については、ここをクリックしてください。

注：この設定は、Windows 10に固有のものです。

OpenVPNをインストールすると、アプリケーションがデスクトップに表示されるか、タスクバーの右側に小さなアイコンとして表示されます。OpenVPNクライアントにも、このインストールが必要です。



すべてのデバイスに適切なシステム時刻が設定されていることを確認します。証明書を作成する

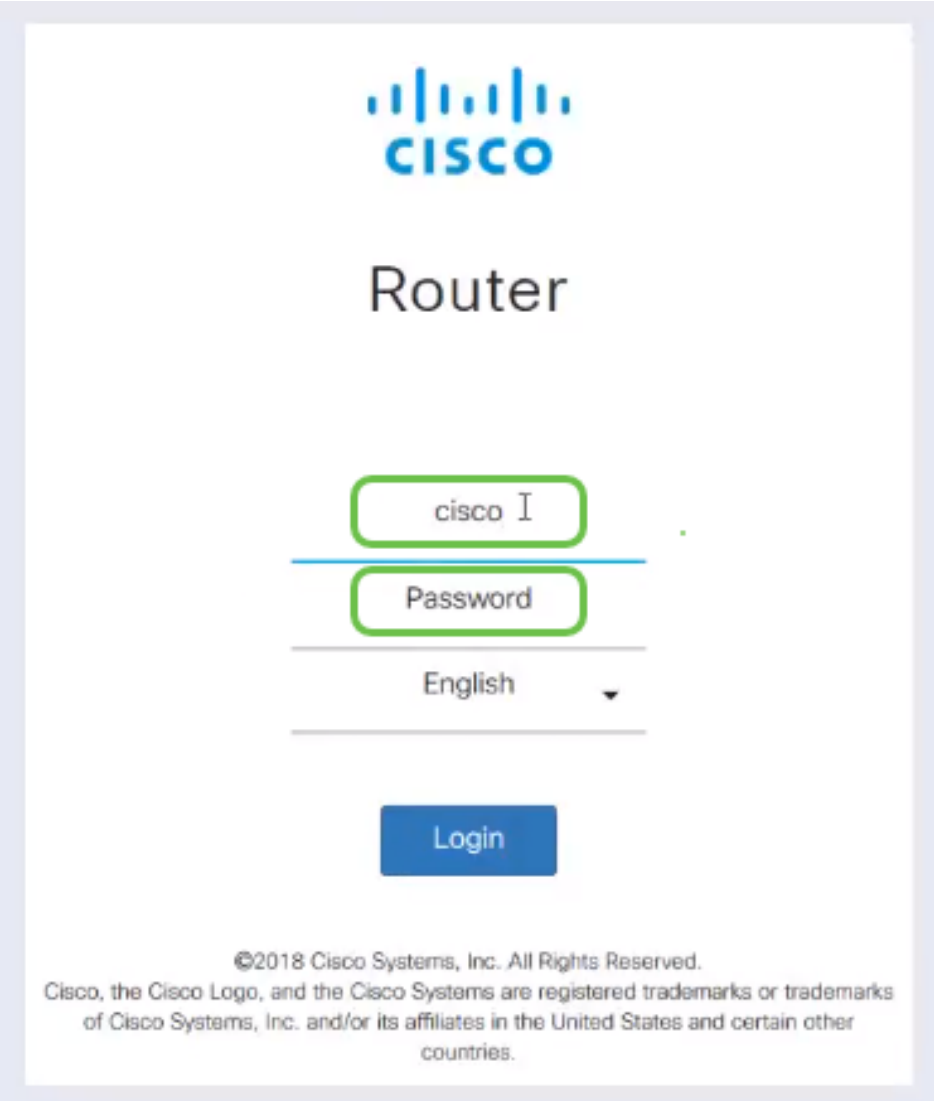
前に、ルータで適切なシステム時刻を完全に同期する必要があります。これは自動的に行われることが多いですが、問題が発生した場合は、チェックに適した場所です。

RV160/RV260ルータでのデモOpenVPNの設定

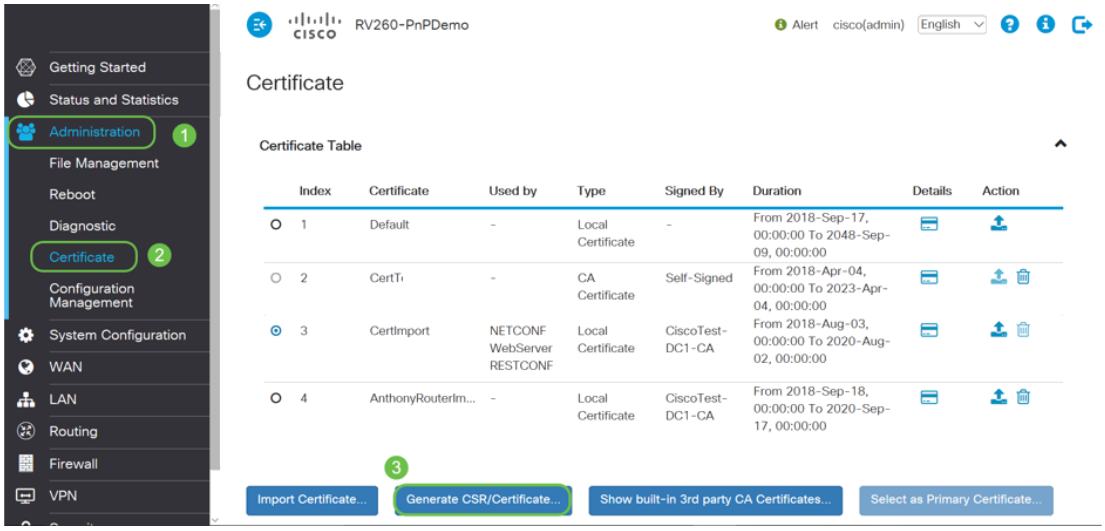
CAの支払い前にOpenVPNを試してみたい場合は、自己署名証明書を作成できます。これは、OpenVPNがビジネスに導入する必要があるかどうかをコストなしで確認する方法です。CAを購入する必要がある場合は、この記事のセクションをスキップして、直接「RV160/RV260ルータでのOpenVPNの設定」に進んでください。

ステップ1：クレデンシャルを使用してルータにログインします。デフォルトのユーザ名とパスワードは*cisco*です。

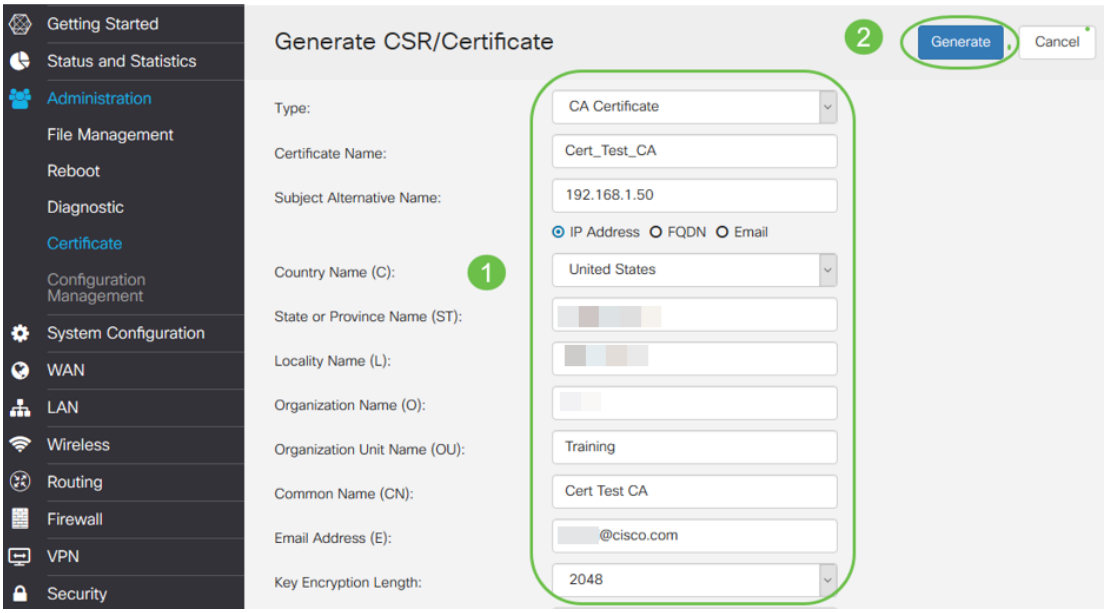
注：すべてのパスワードをより複雑なものに変更することを強く推奨します。それ以外の場合は、鍵をドアのステップに鍵を鍵を置いておくようなものです。



ステップ2：ルータで証明書を取得することが要件です。[Administration] > [Certificate] > [Generate CSR/Certificate...] に移動します。これは、証明書の要求を作成する方法です。



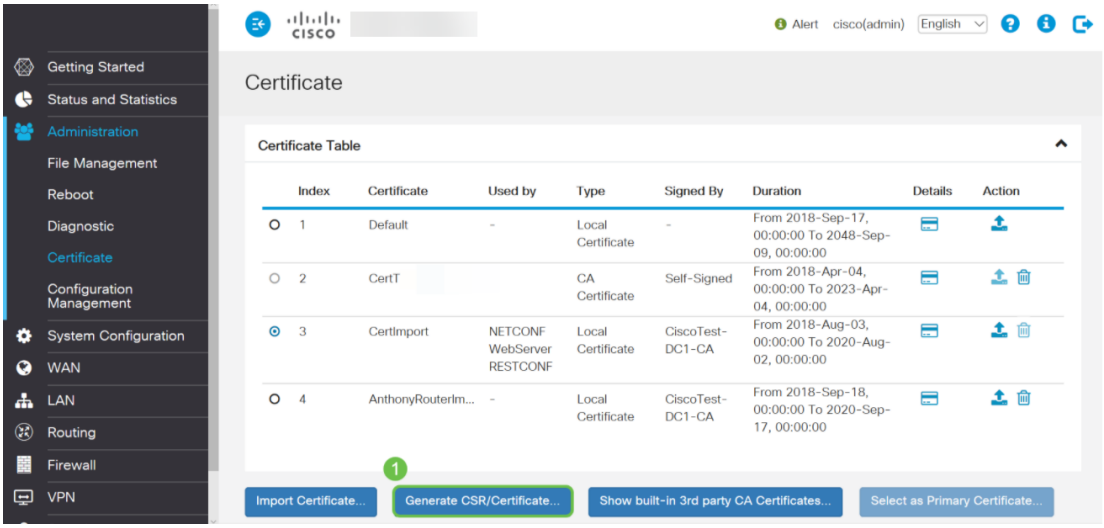
ステップ3:CA証明書を要求します。



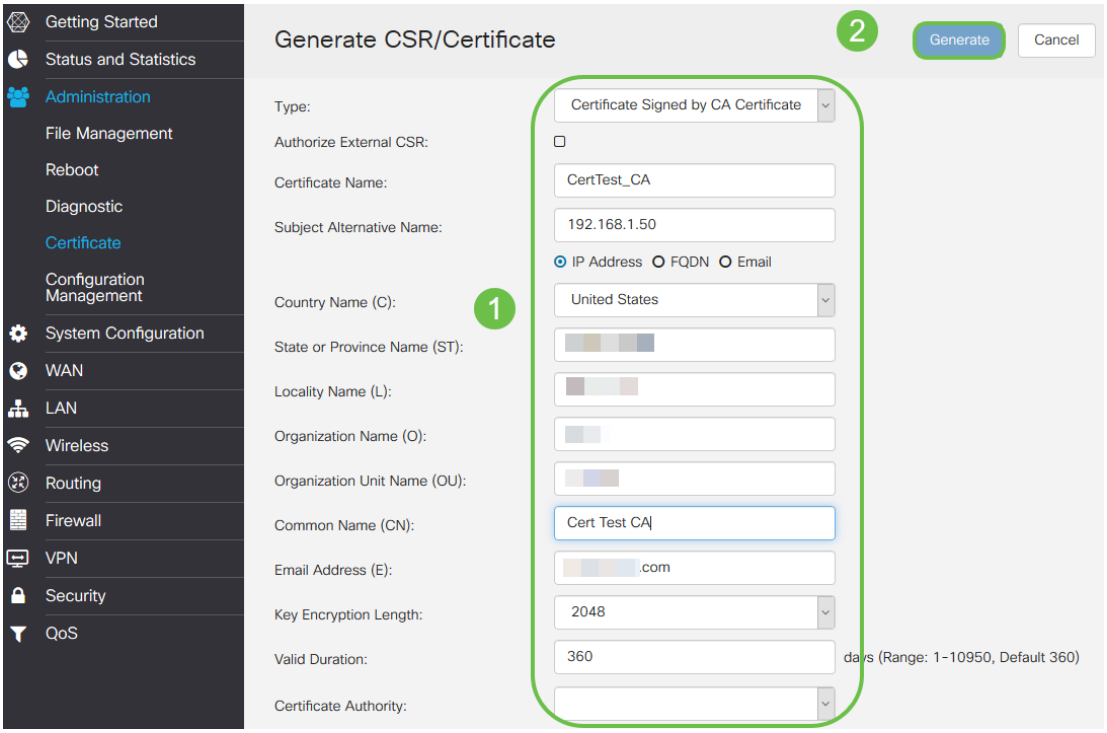
- ドロップダウンメニューから[CA Certificate]を選択します
- 証明書名の入力
- IPアドレス、完全修飾ドメイン名(FQDN)、または電子メールを入力します。IPアドレスの入力が最も一般的な選択肢です。
- 国を入力
- 状態を入力
- [Locality Name]（通常は市）を入力します
- 組織名の入力
- 組織ユニット名の入力
- メールアドレスを入力します
- Enter Key Encryption Length, 2048 is recommended

右上の[生成]ボタンをクリックします。

ステップ4：サーバ証明書も必要です。この証明書は、*作成したCA証明書*によって署名されます。



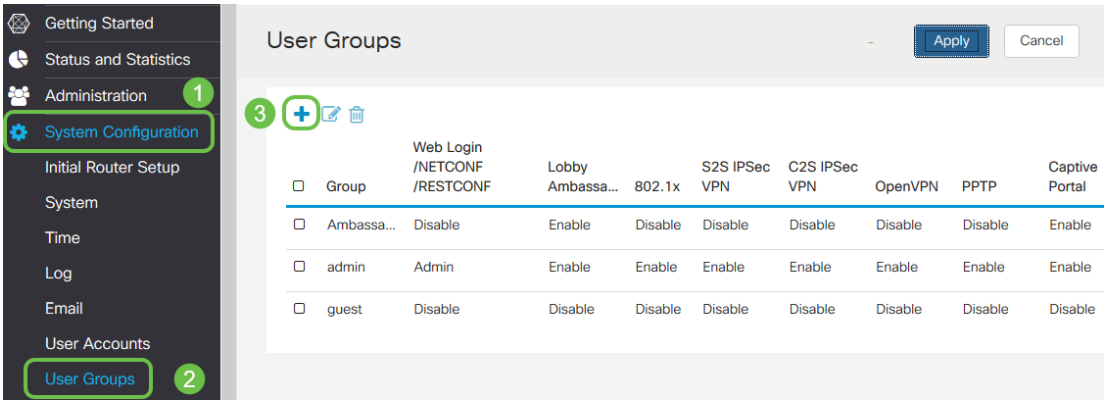
ステップ5:CA証明書によって署名された*証明書を要求します*。



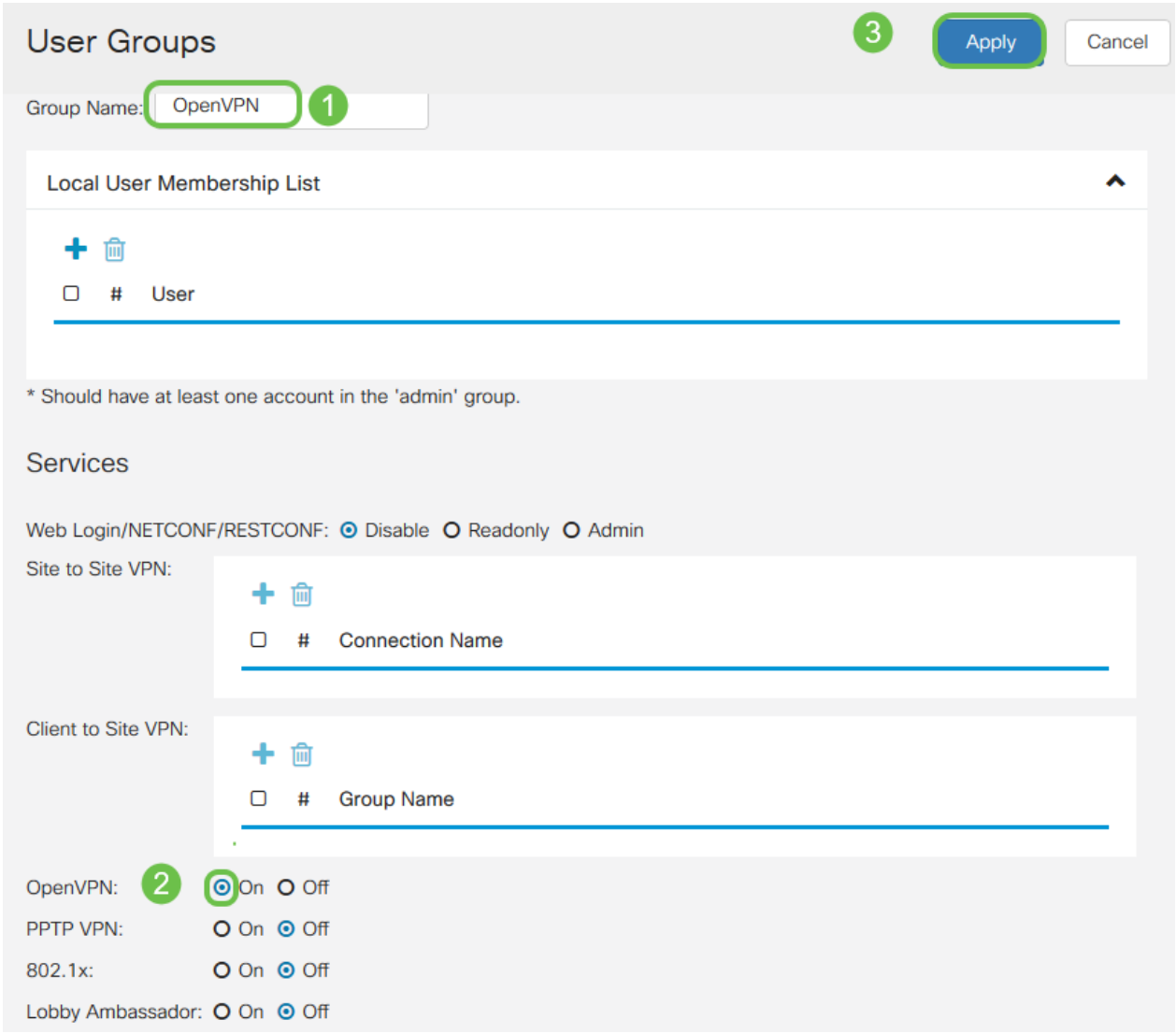
- ドロップダウンメニューから*[証明書*署名要求]を選択します
- 証明書名の入力
- IPアドレス、完全修飾ドメイン名(FQDN)、または電子メールを入力します。IPアドレスの入力が最も一般的な選択肢です。
- 国を入力
- 状態を入力
- [Locality Name]（通常は市）を入力します
- 組織名の入力
- 組織ユニット名の入力
- メールアドレスを入力します
- Enter Key Encryption Length, 2048 is recommended
- ドロップダウンメニューから適切な認証局を選択します

右上の[生成]ボタンをクリックします。

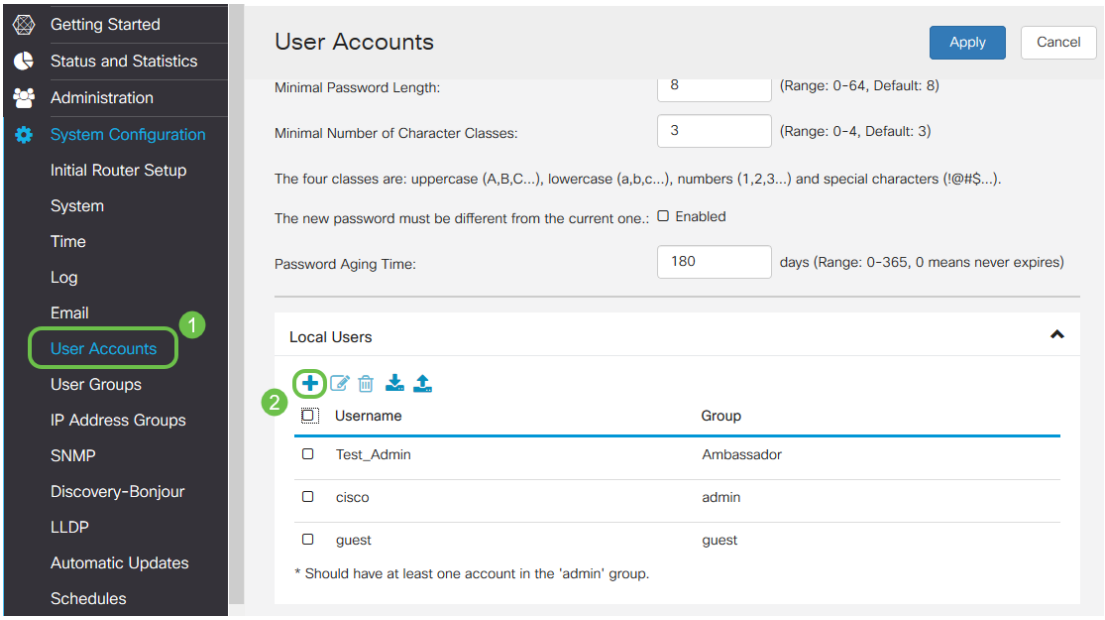
ステップ6:[System Configuration] > [User Groups]に移動します。新しいグループを追加するには、プラスのアイコンを選択します。



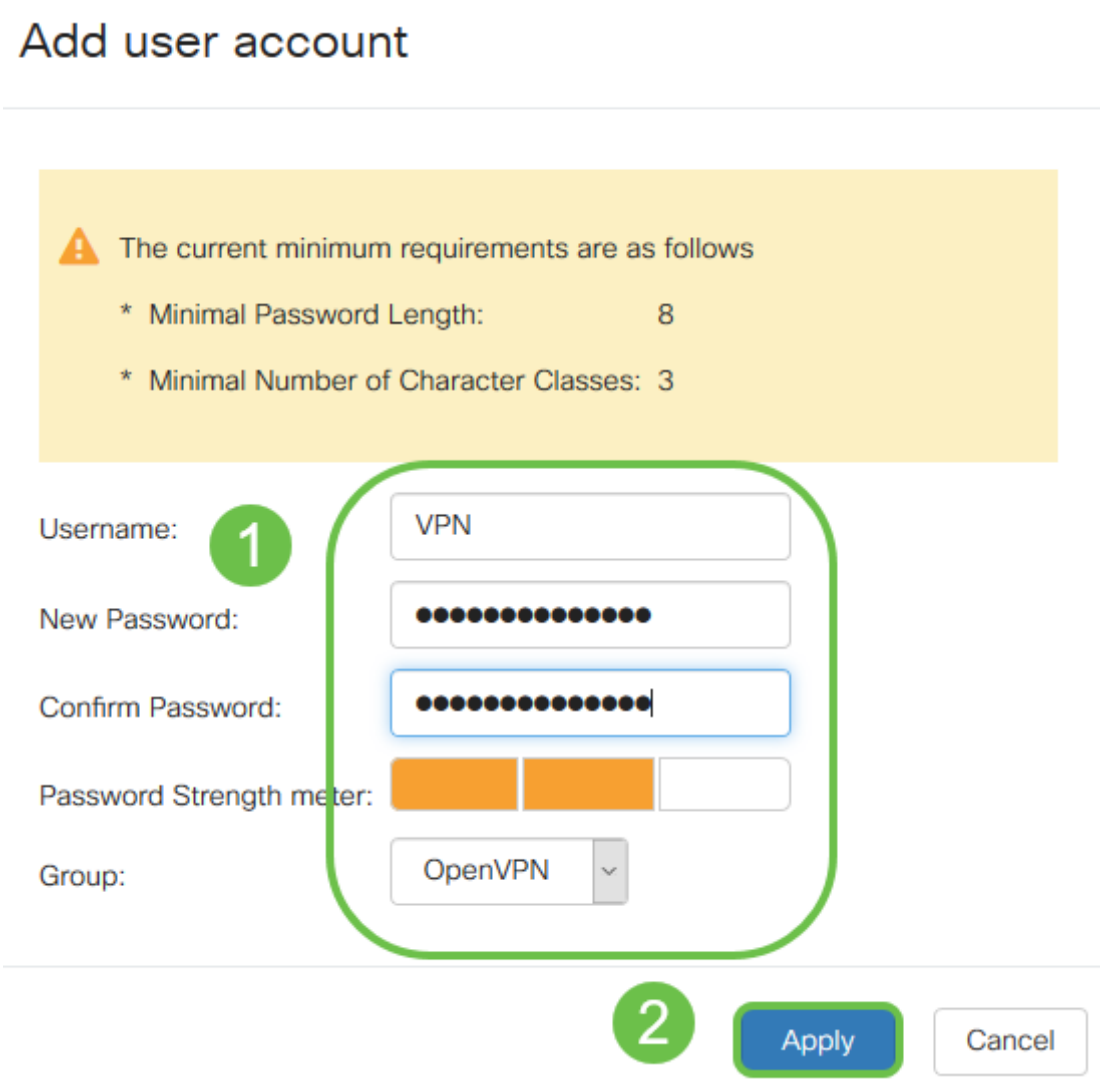
ステップ7：グループの名前を入力し、ラジオボタンの[*On*]をクリックしてOpenVPNをオンにします。[Apply] をクリックします。



ステップ8:[System Configuration]メニュー内を移動し、[**User Accounts**]をクリックします。[ローカルユーザー]の下のプラス記号アイコンをクリックします。

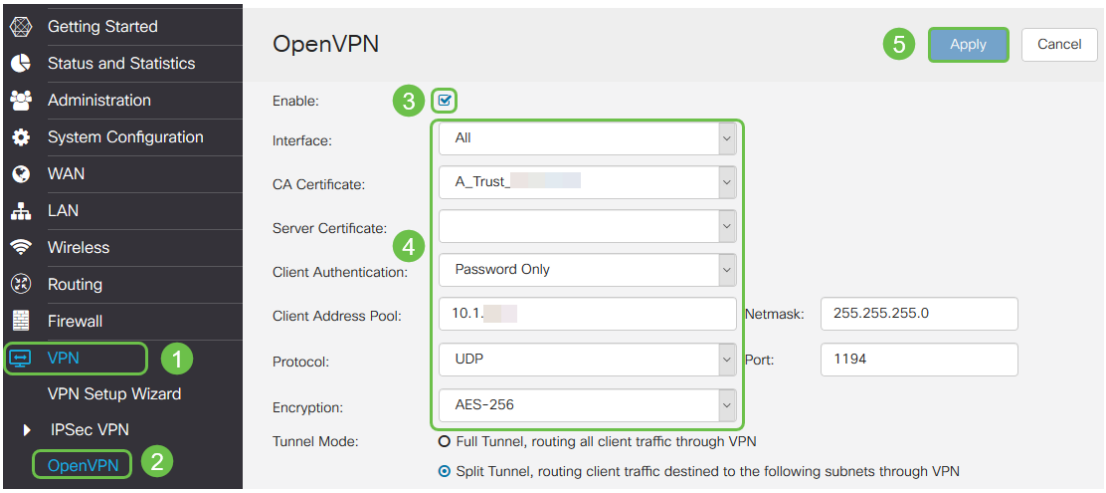


ステップ9：次の情報を入力します。ドロップダウンメニューから[OpenVPN]を選択します。[Apply] をクリックします。



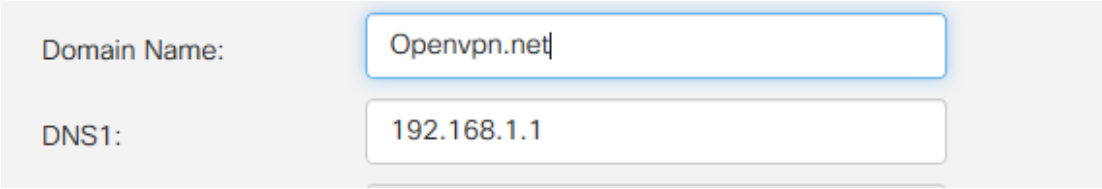
すべての依存関係が完了し、ルータをOpenVPN用に設定できるようになりました。

ステップ10:[VPN] > [OpenVPN] に移動します。[OpenVPN]ページが開きます。ページの各ボックスに入力し、ドロップダウンメニューから以前に作成した証明書を選択します。



- [有効]ボックスをオンにします。トラフィックで許可するインターフェイスを選択します。この場合、ワイドエリアネットワーク(WAN)を使用して、認証局(CA)証明書を選択します。
- ドロップダウンメニューから[CA Certificate]を選択します
- ドロップダウンメニューから、ダウンロードしたサーバ証明書を選択します
- [*Client Authentication*]を選択します。[Password]を選択した場合は、パスワードで認証する必要があります。[Password + Certificate]を選択する場合、クライアントにも証明書が必要です。これは、より安全ですが、VPNは別のCAを購入する必要があるため、コストが増加します。
- クライアント・アドレス・プールを入力します。社内の他の場所で使用されていないネットワークサブネットのIPアドレスを選択します。予約済みの範囲から選択し、他の場所で使用されていない範囲を選択します。
- 暗号化の形式を選択します。暗号化がクライアントと同じであることを確認します。DESおよび3DESは推奨されず、後方互換性のためだけに使用する必要があります。
- VPNを通過するトラフィックだけを指定する場合は、[Split tunnel]を選択します。VPNには、スプリットトンネルが必要です。*Full Tunnel Mode*は、すべてのクライアントトラフィックをVPNを通過させる他の状況で選択されます。

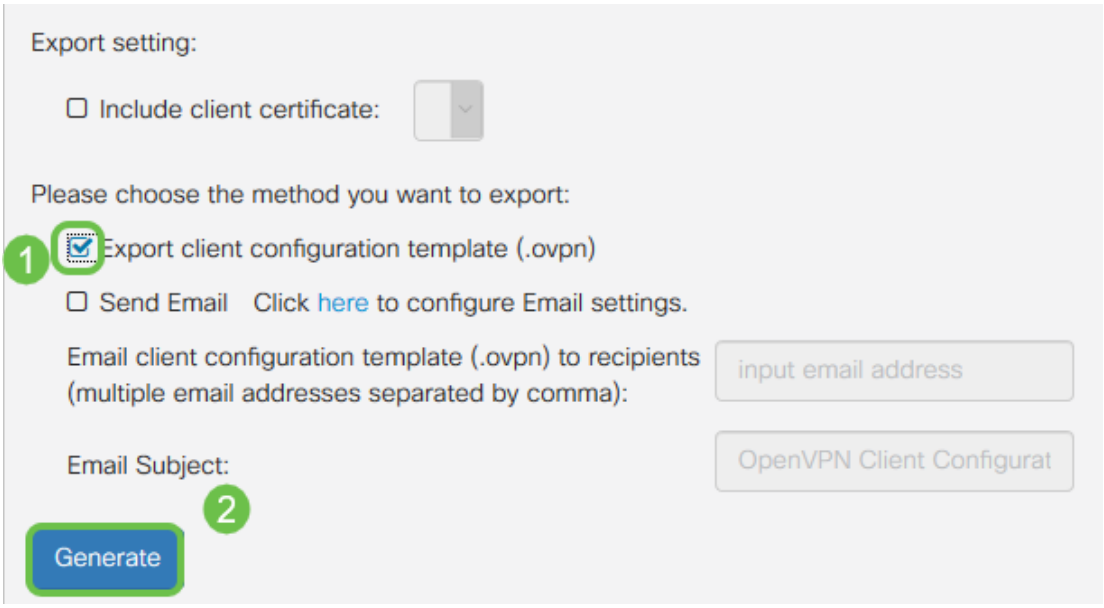
ステップ11：ページを下にスクロールし、ドメイン名とDNS*1*を入力してください。



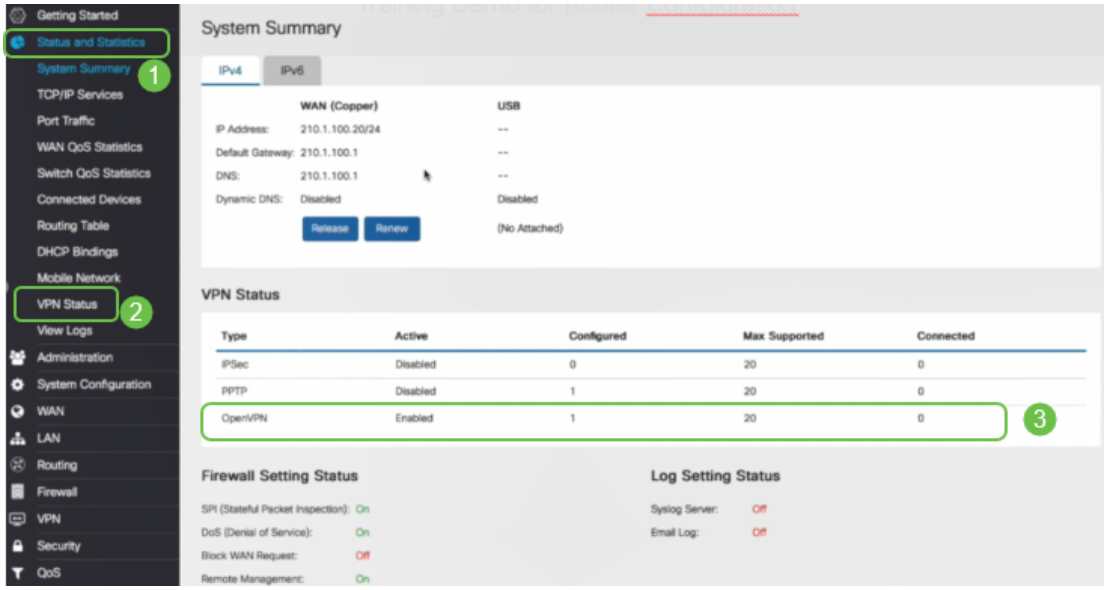
注：DNS1 IPアドレスは、専用の内部DNSサーバ、インターネットサービスプロバイダー(ISP)が提供するデフォルトゲートウェイと同じIPアドレス、仮想マシン上のIPアドレス、またはインターネット上の信頼できるDNSサーバにすることができます。

ステップ12:[**Apply**]をクリックして、ルータの設定を保存します。

ステップ13：同じページを表示したまま、さらにスクロールします。OpenVPN Clientにインストールする設定テンプレートを生成します。このファイルの拡張子*は.ovpn*で、OpenVPN Clientによって使用されます。[Export client configuration template (.ovpn)]のボックスをオンにし、[**Generate**]をクリックします。これにより、ファイルがコンピュータにダウンロードされます。



ステップ14:[Status and **Statistics**] > [**VPN Status**]に移動**します**。詳細については、下にスクロールできます。



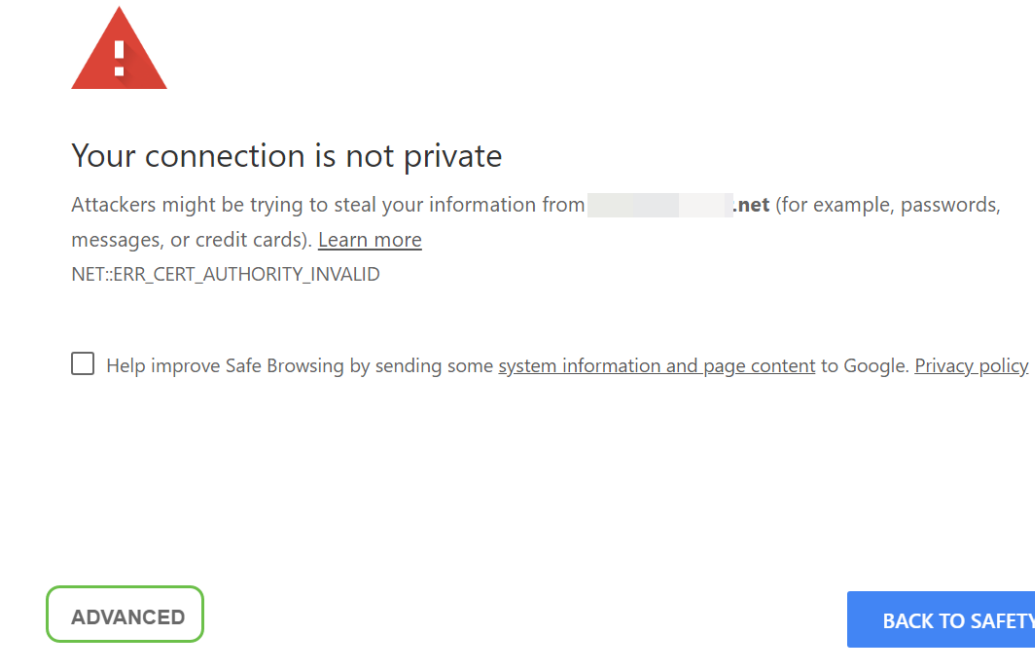
自己署名証明書を使用してログインする方法を説明しているため、この記事の次のセクションを確認することが重要です。

Demo OpenVPNの設定後の自己署名証明書によるログイン

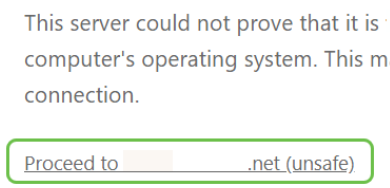
自己署名証明書を使用してログインすると、ログインしようとすると警告ポップアップが表示されることがあります。続行するには、Webブラウザに応じて[Advanced]、[Proceed]、[Trust]またはその他のオプションをクリックする必要があります。

この時点で、安全ではないという警告が表示されることがあります。続行、例外の追加、または詳細を選択できます。これはWebブラウザによって異なります。

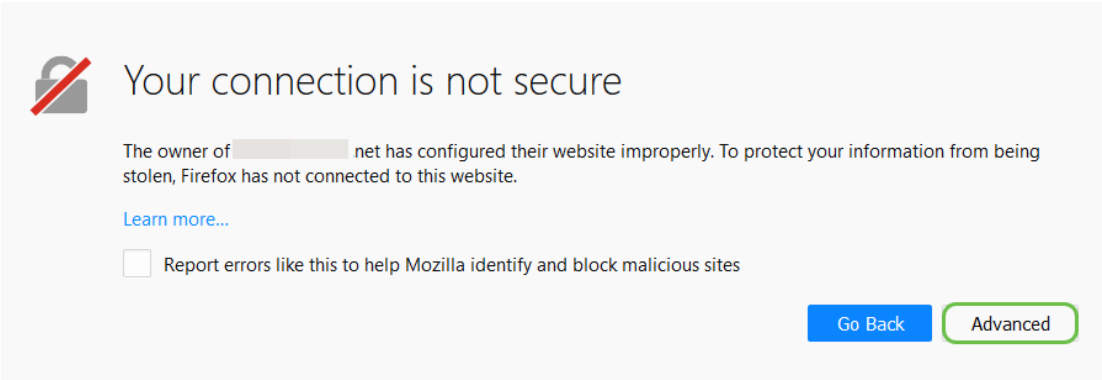
この例では、ChromeがWebブラウザに使用されています。このメッセージが表示されたら、[**Advanced**]をクリック**します**。



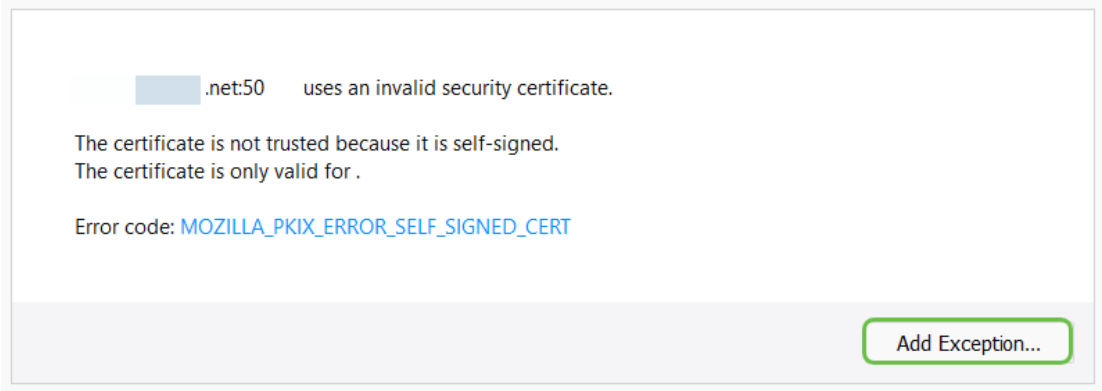
新しい画面が開き、「Proceed to your website.net (unsafe)」をクリックする必要があります



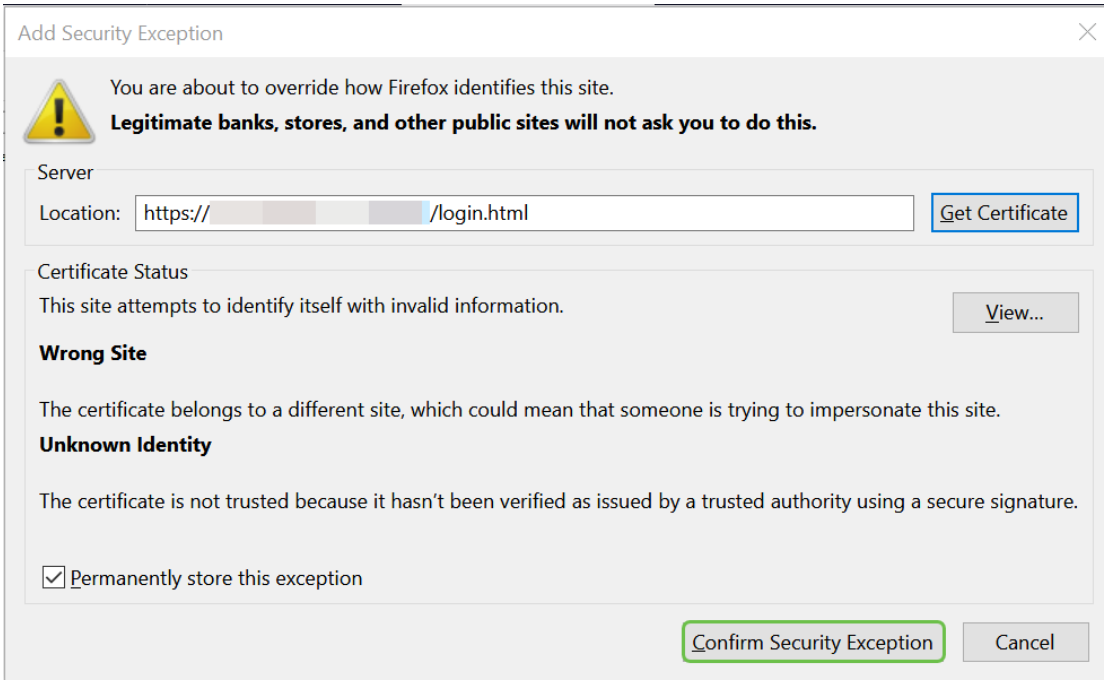
FirefoxをWebブラウザとして使用する場合のデバイス警告へのアクセス例を次に示します。[Advanced]をクリックします。



「例外の追加....」をクリックします。



最後に、[セキュリティ例外の確認]をクリックする必要があります。



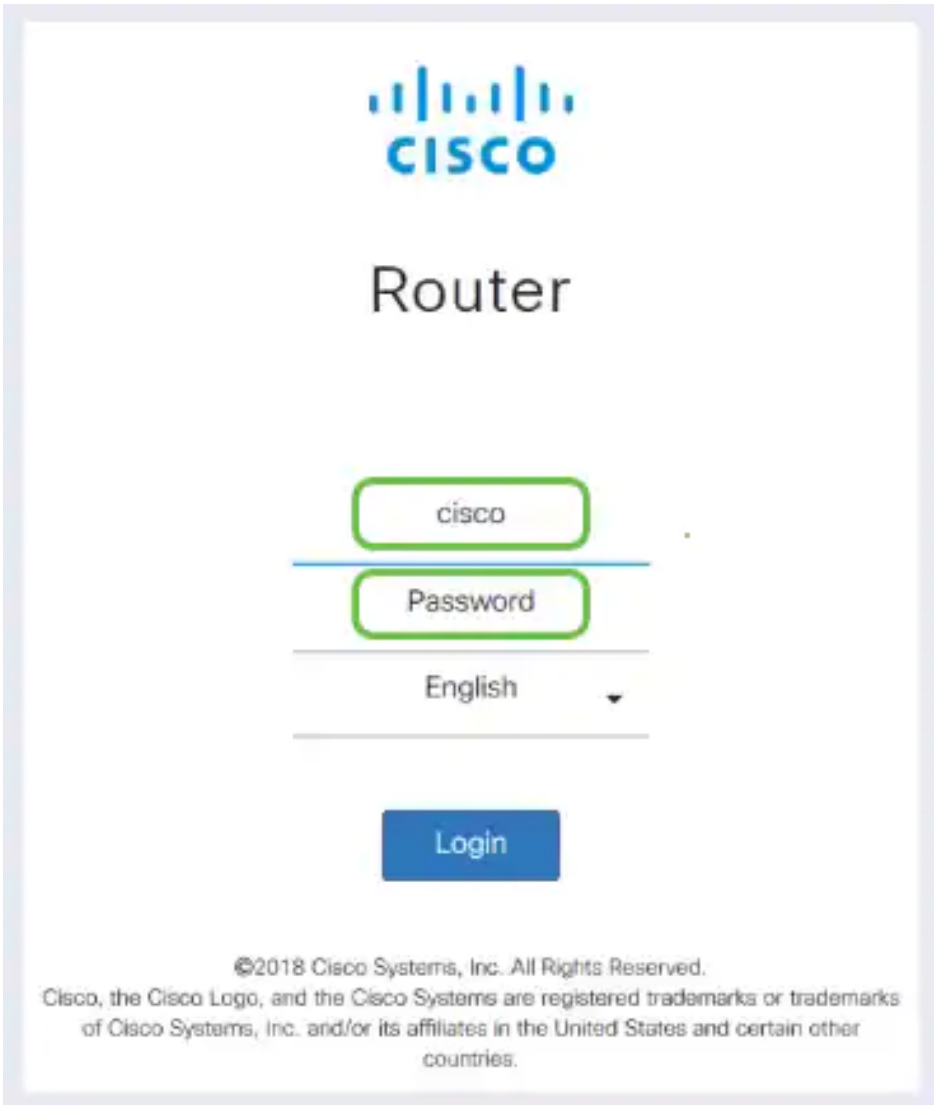
これで、ルータはOpenVPN Client接続をサポートするために必要なすべてのパラメータで設定されます。すでにクライアント設定テンプレートをデバイスにダウンロードしているため、*.ovpn*で終わるテンプレートをダウンロードし、「OpenVPN Client Setup on Computer」セクションに進むことができます。会社にOpenVPNを導入する場合は、次のセクションの手順に従います。

RV160/RV260ルータでのOpenVPNの設定

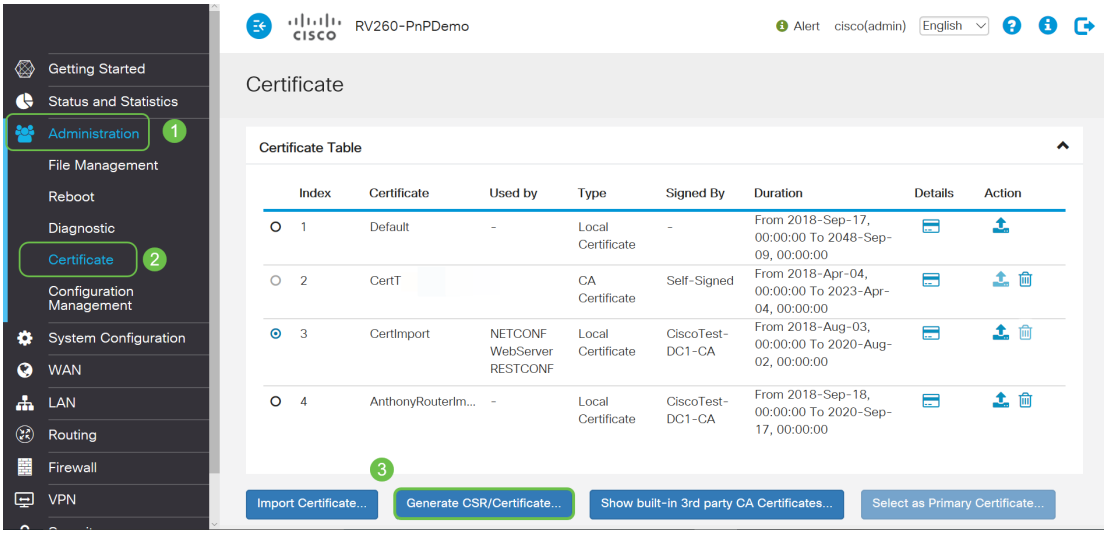
これは、サードパーティからCAを取得する必要があるため、より複雑なプロセスであり、コストがかかります。また、VPNクライアント設定テンプレートを送信する必要があります。このテンプレートの末尾は*.ovpn*です。これにより、クライアントはデバイス上でセットアップできます。クライアントが通信するには、ルータと同じ設定が必要です。最も重要な点は、最小限のコストでインターネットを使用し、ビジネスをより安全に遂行できることです。

ステップ1：クレデンシャルを使用してルータにログインします。デフォルトのユーザ名とパスワードは*cisco*です。

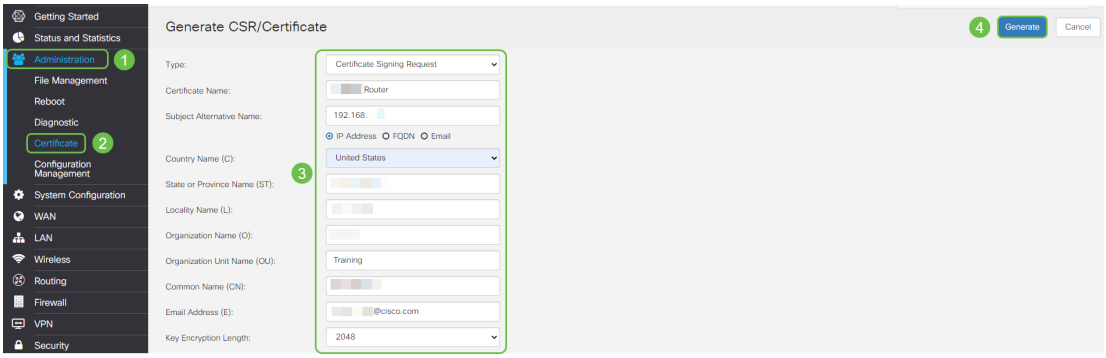
注：すべてのパスワードをより複雑なものに変更することを強く推奨します。それ以外の場合は、鍵をドアのステップに鍵を鍵を置いておくようなものです。



ステップ2：証明書を取得する必要があります。[Administration] > [Certificate] > [Generate CSR/Certificate...] に移動します。これは、証明書の要求を作成する方法です。



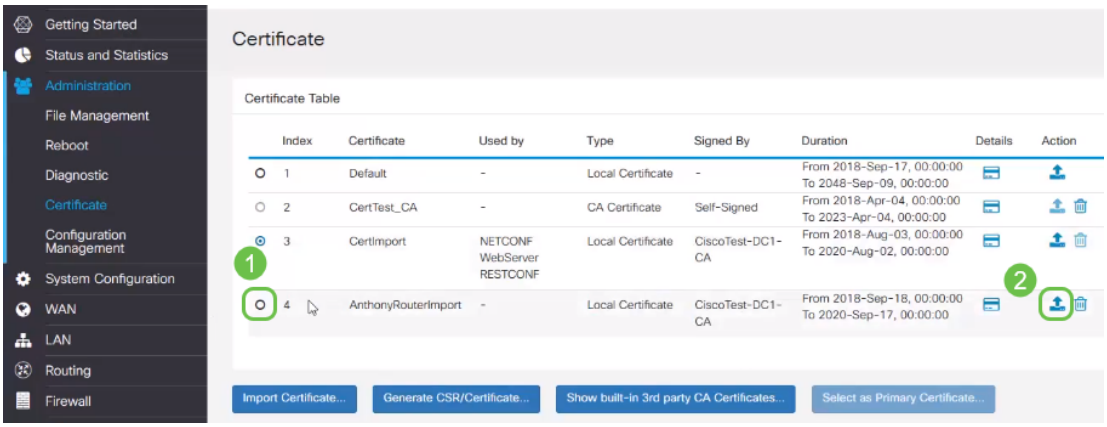
ステップ3:CA証明書によって署名された*証明書を要求します*。これは、[**Administration**] > [**Certificate**]の順に移動することで確認できます。



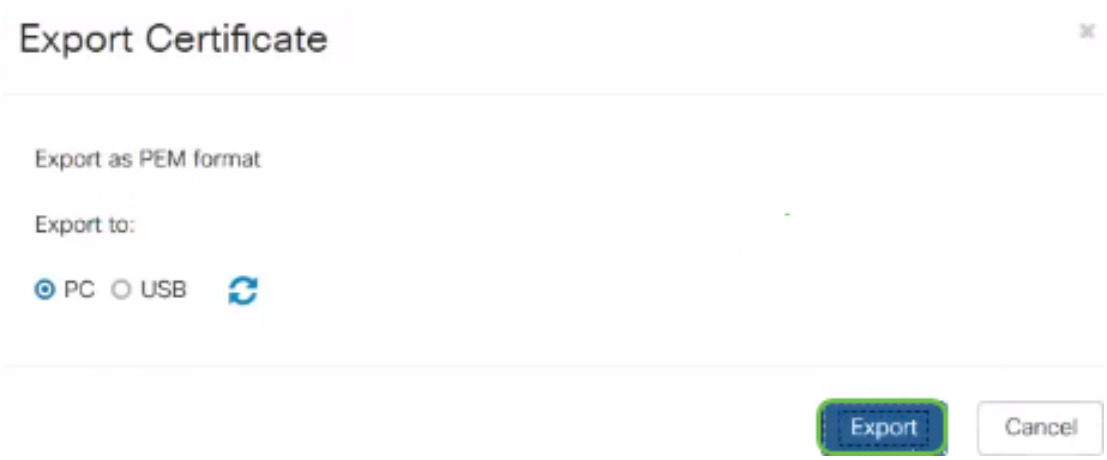
- ドロップダウンメニューから*[証明書*署名要求]を選択します
- 証明書名の入力
- IPアドレス、完全修飾ドメイン名(FQDN)、または電子メールを入力します。IPアドレスの入力が最も一般的な選択肢です。
- 国を入力
- 状態を入力
- [Locality Name]（通常は市）を入力します
- 組織名の入力
- 組織ユニット名の入力
- メールアドレスを入力します
- Enter Key Encryption Length, 2048 is recommended

右上の[生成]ボタンをクリックします

ステップ4:[Action（アクション）]の下の上矢印をクリックして、エクスポートすることを選択します。

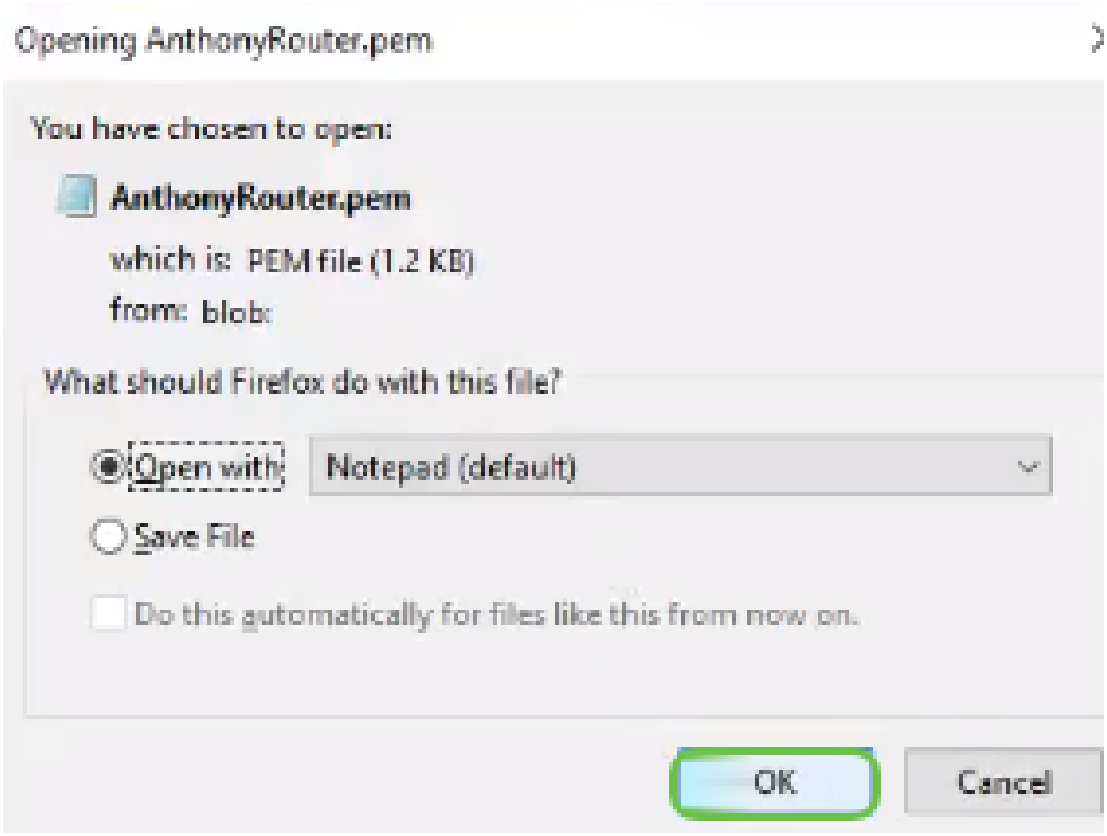


ステップ5：この画面が表示されます。[Export] をクリックします。



ステップ6：ドロップダウンメニューから*[Open with and Notepad*（デフォルト）]を選択します。

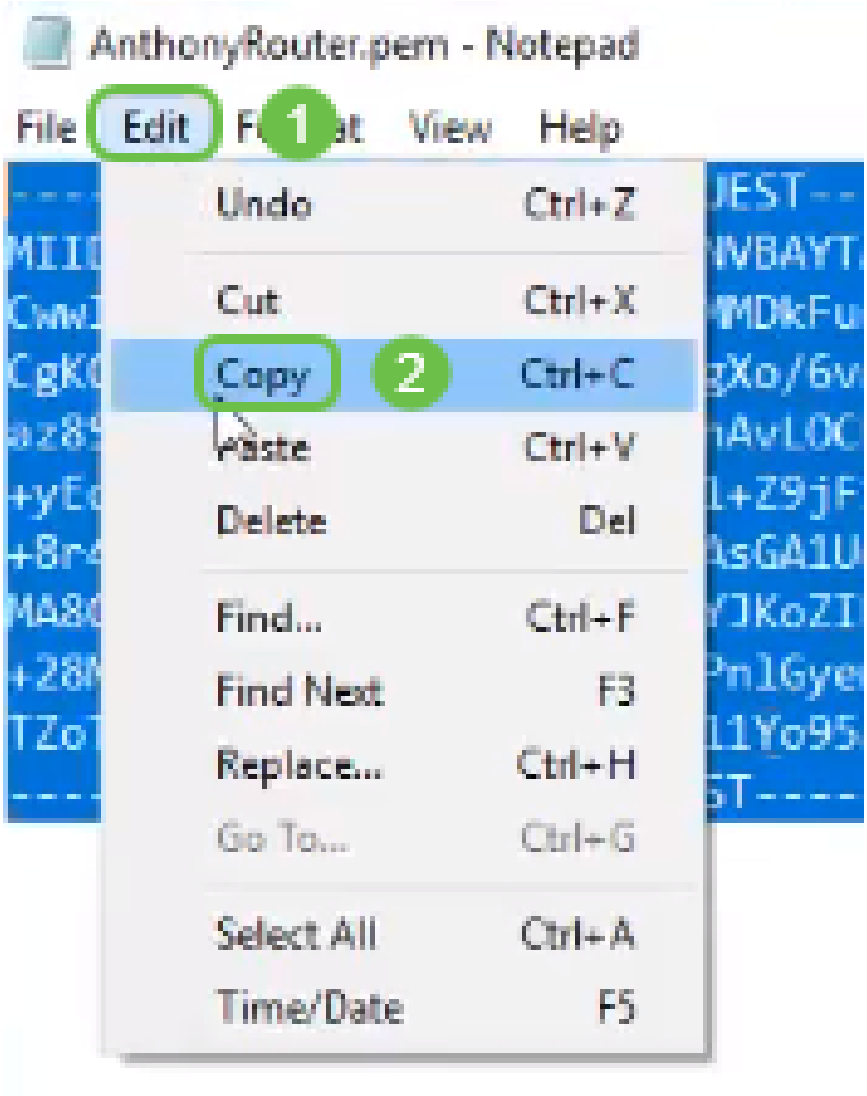
[OK] をクリックします。



ステップ7:XMLファイルが開きます。

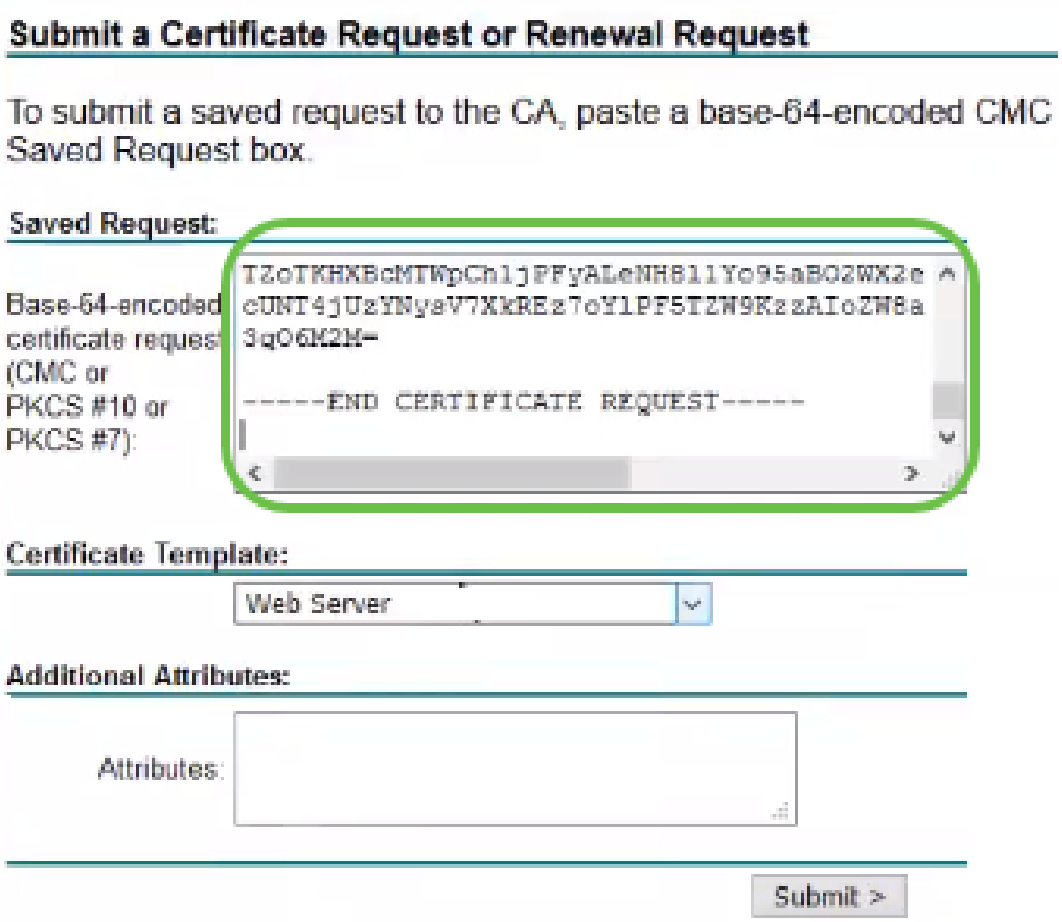
注：上記のように、BEGIN CERTIFICATE REQUESTとEND CERTIFICATE REQUESTがそれぞれ独自の行にあることを確認します。

ステップ8：画面の上部で[Edit]をクリックし、ダウン**ダウン**· メニュー**から**[Copy]を選択します。

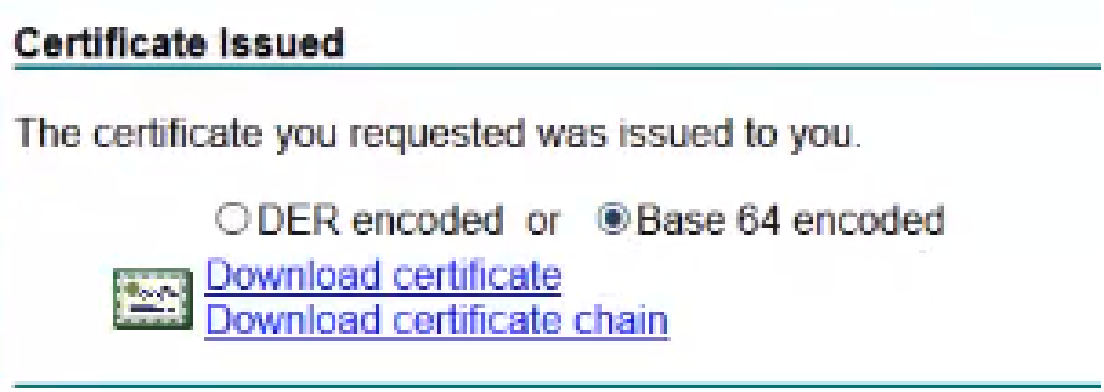


ステップ9：信頼できるサードパーティサイトを選択して、証明書要求を行います。コピーしたXMLファイルを要求の一部として貼り付ける必要があります。

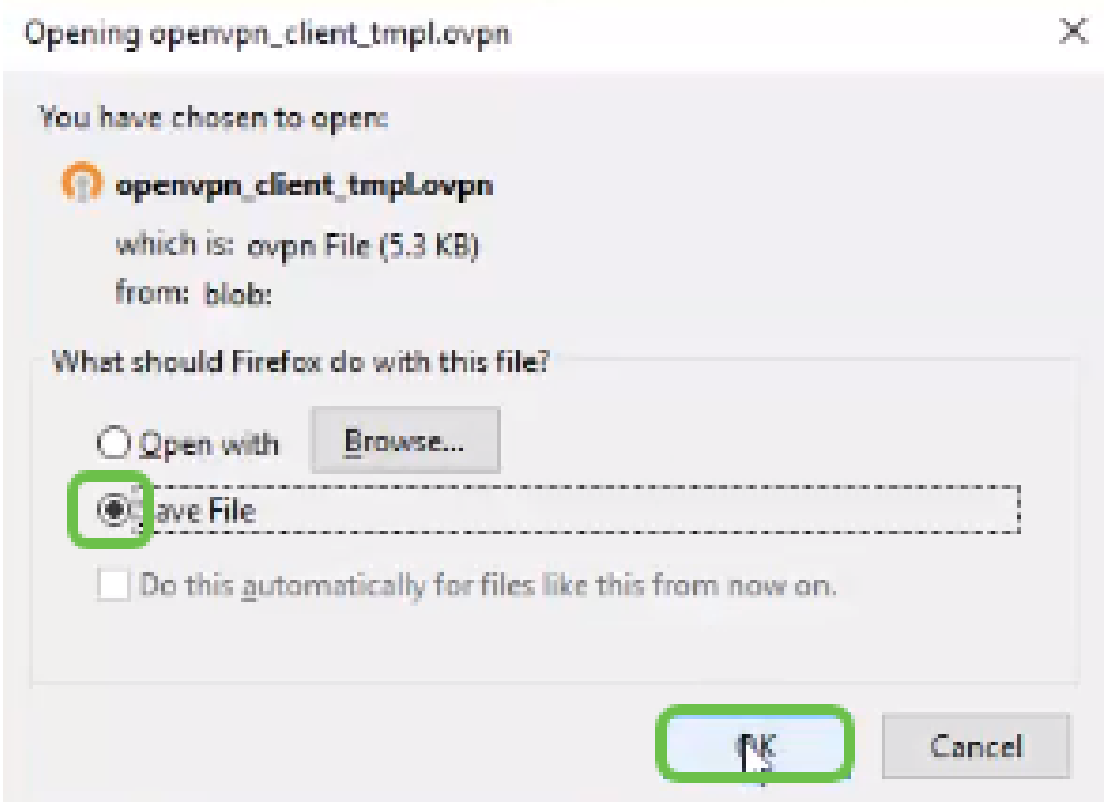
注：ネットワーク上に内部証明書サーバがある場合は、その代わりに使用できますが、これは一般的ではありません。



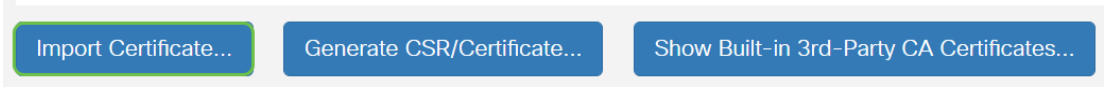
ステップ10：確認したら、[Download certificate]を選択できます。



ステップ11:[Save File]のラジオボタンをクリックし、[OK]をクリックします。

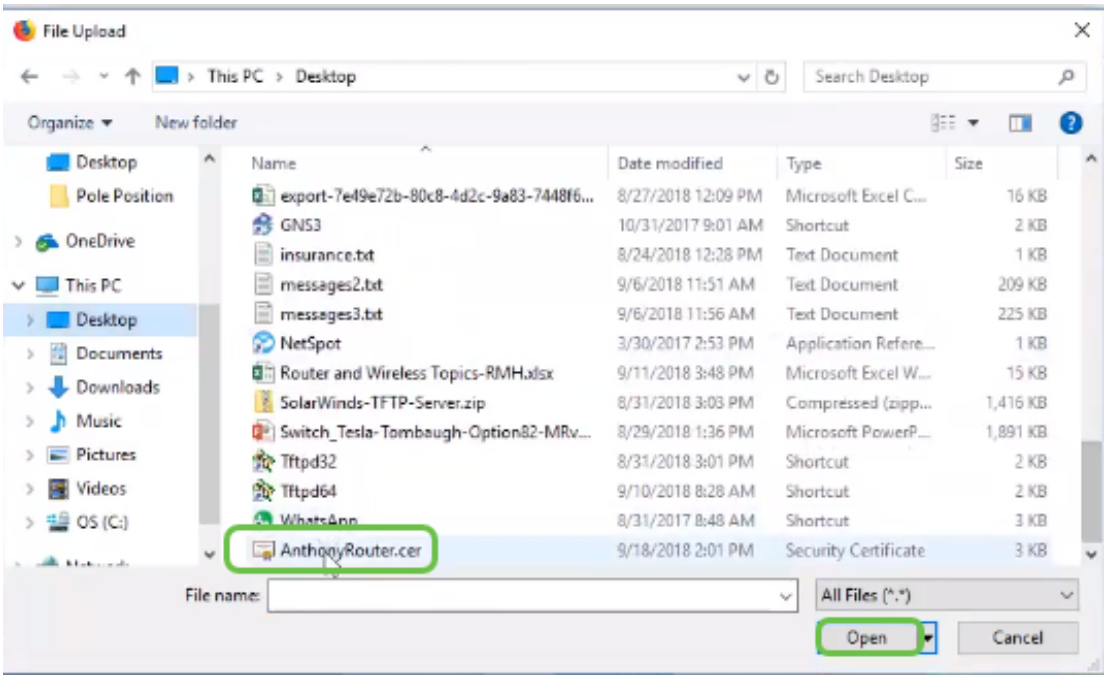


ステップ12：証明書が保存されたら、その証明書のオプションボタンを選択し、下矢印アイコンをクリックします。

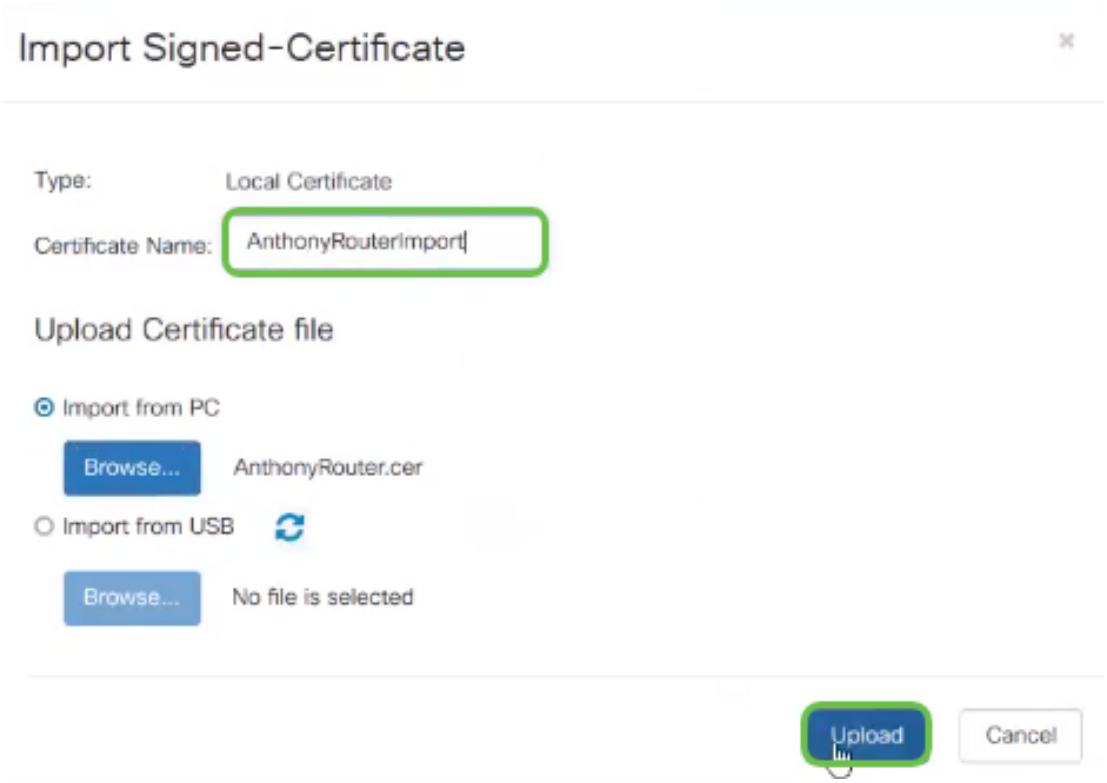


ステップ13：この画面が開きます。参照....

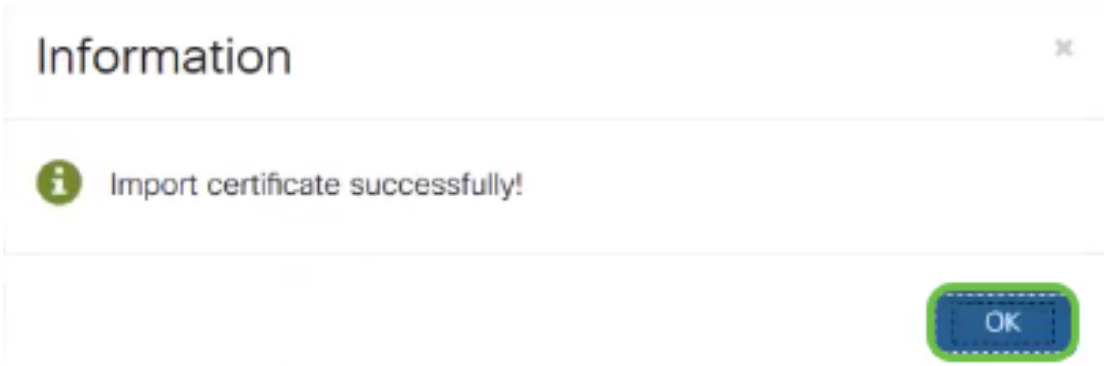
ステップ14：証明書のファイルを選択し、[開く]をクリックします。



ステップ15：インポートする証明書名を入力し、[Upload]をクリックします。

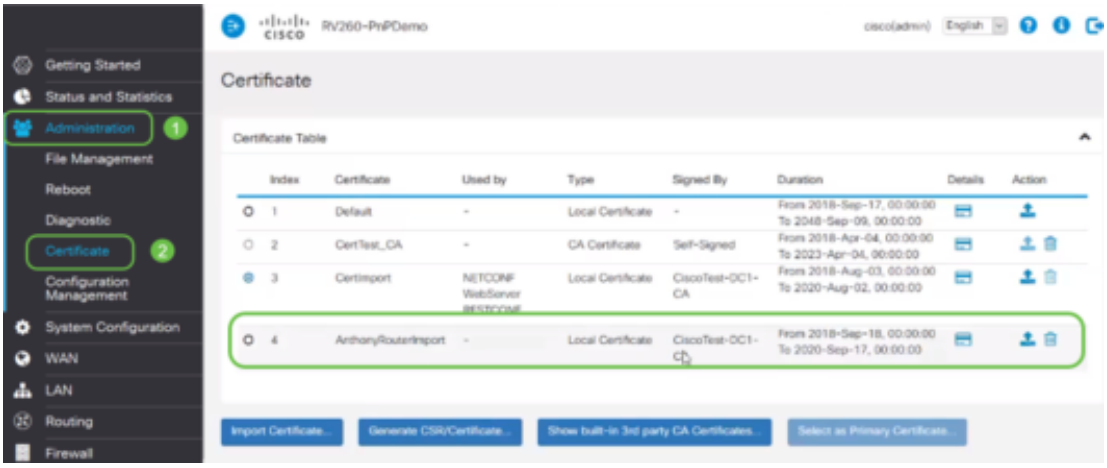


ステップ16：証明書が正常にインポートされたことが通知されます。[OK] をクリックします。

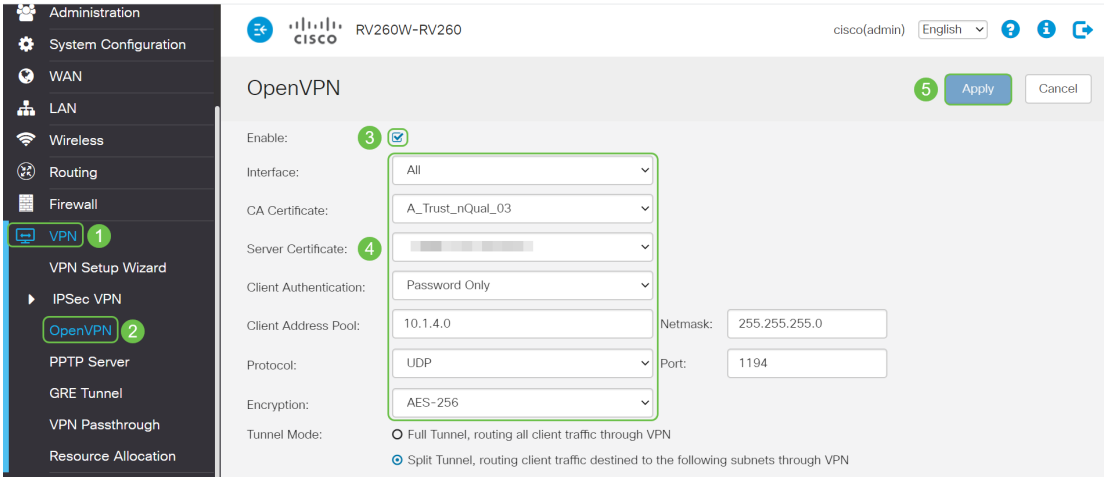


ステップ17:[Administration] > [Certificate]に移動します。証明書が読み込まれました。

注：この例では、ローカル証明書サーバが使用されています。



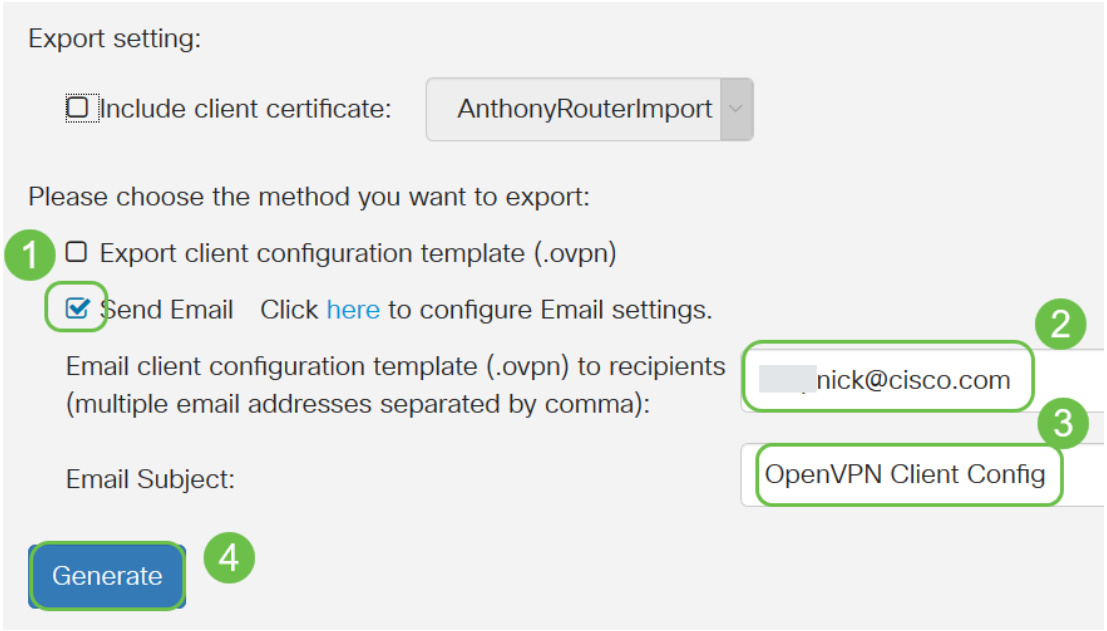
ステップ18:[VPN] > [OpenVPN] に移動します。[OpenVPN]ページが開きます。次の情報を入力します。



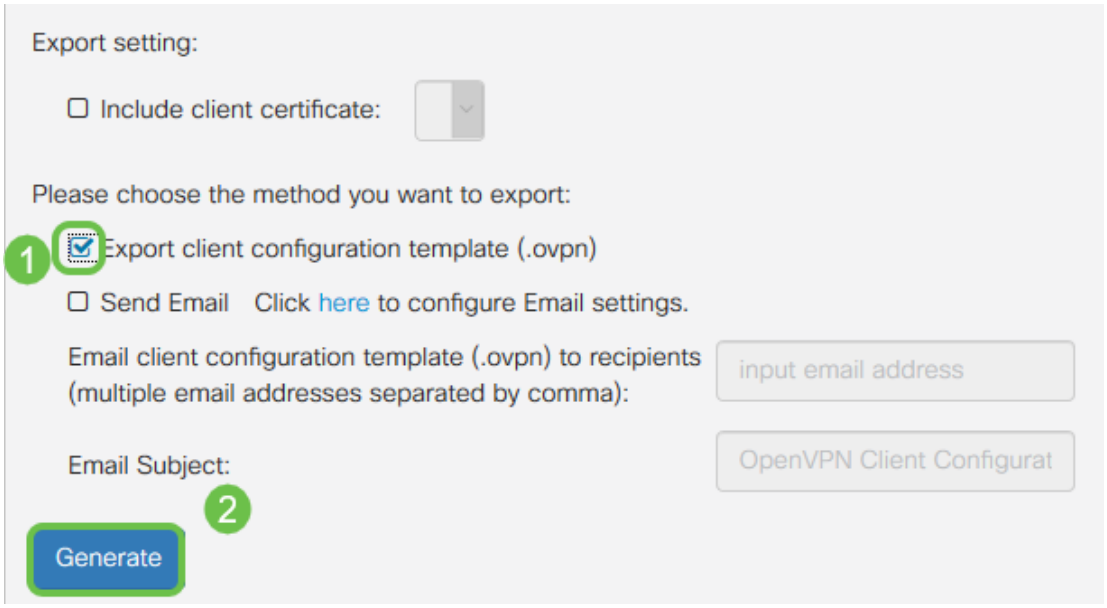
- [有効]ボックスをオンにします。トラフィックで許可するインターフェイスを選択します。この場合、ワイドエリアネットワーク(WAN)を使用して、認証局(CA)証明書を選択します
- ドロップダウンメニューから[CA Certificate]を選択します
- ドロップダウンメニューからダウンロードしたサーバ証明書を選択します
- [*Client Authentication*]を選択します。[Password]を選択した場合は、パスワードで認証する必要があります。[Password + Certificate]を選択する場合、クライアントにも証明書が必要です。これは、より安全ですが、VPNは別のCAを購入する必要があるため、コストが増加します。
- クライアント・アドレス・プールを入力します。社内の他の場所で使用されていないネットワークサブネットのIPアドレスを選択します。予約済みの範囲から選択し、他の場所で使用されていない範囲を選択します。
- 暗号化の形式を選択します。暗号化がクライアントと同じであることを確認します。DESおよび3DESは推奨されず、後方互換性のためだけに使用する必要があります。
- すべてのクライアントトラフィックをVPNを通過させる場合は[Full Tunnel Mode] を、VPNを通過するトラフィックだけを指定する場合は[Split tunnel]を選択します
- *DNS1* IPアドレスは、専用の内部DNSサーバ、インターネットサービスプロバイダー(ISP)から提供されるデフォルトゲートウェイの同じIPアドレス、仮想マシン、またはインターネット上の信頼できるDNSサーバにすることができます。

[Apply]をクリックし、設定を保存します。

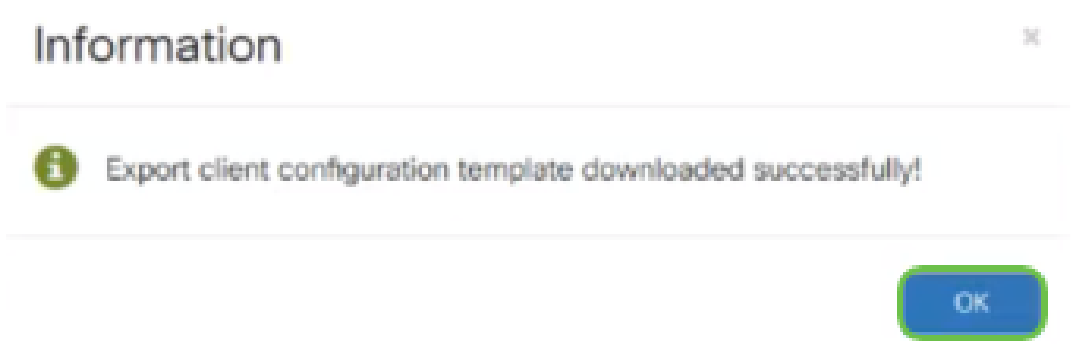
ステップ19（オプション1）。 この設定をクライアントに電子メールで送信できます。[Send Email]チェックボックスをオンにします。電子メールアドレスを入力します。電子メールの件名を追加します。[Generate] をクリックします。



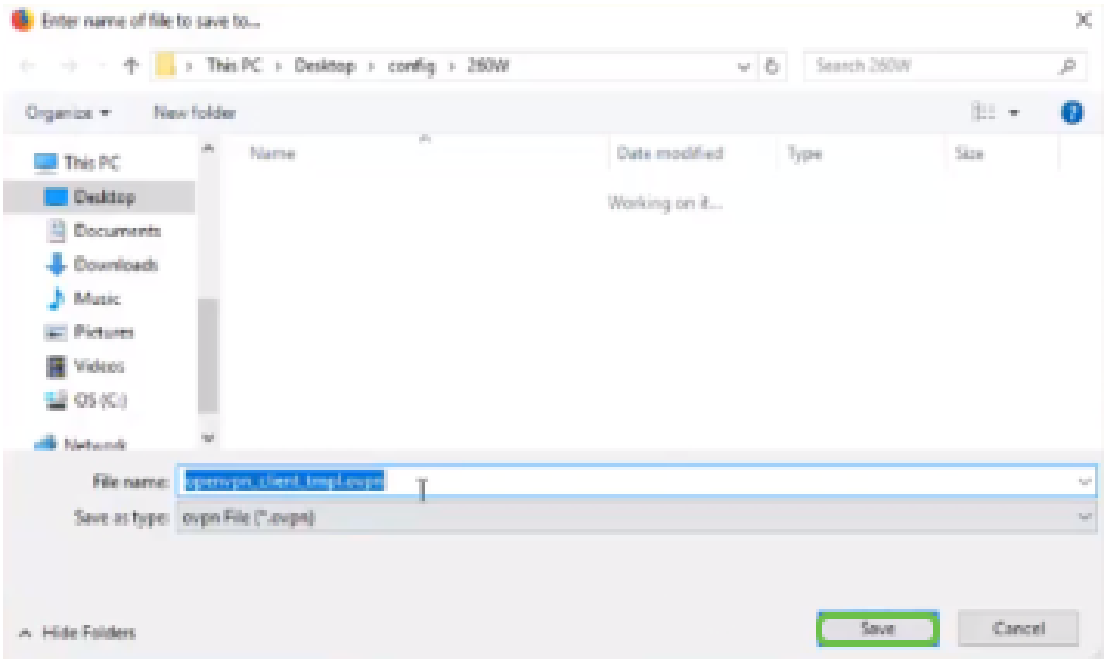
ステップ20:（オプション2）。 [Export *client configuration template (.ovpn)]を選択し、[***Generate***]をクリックします。*



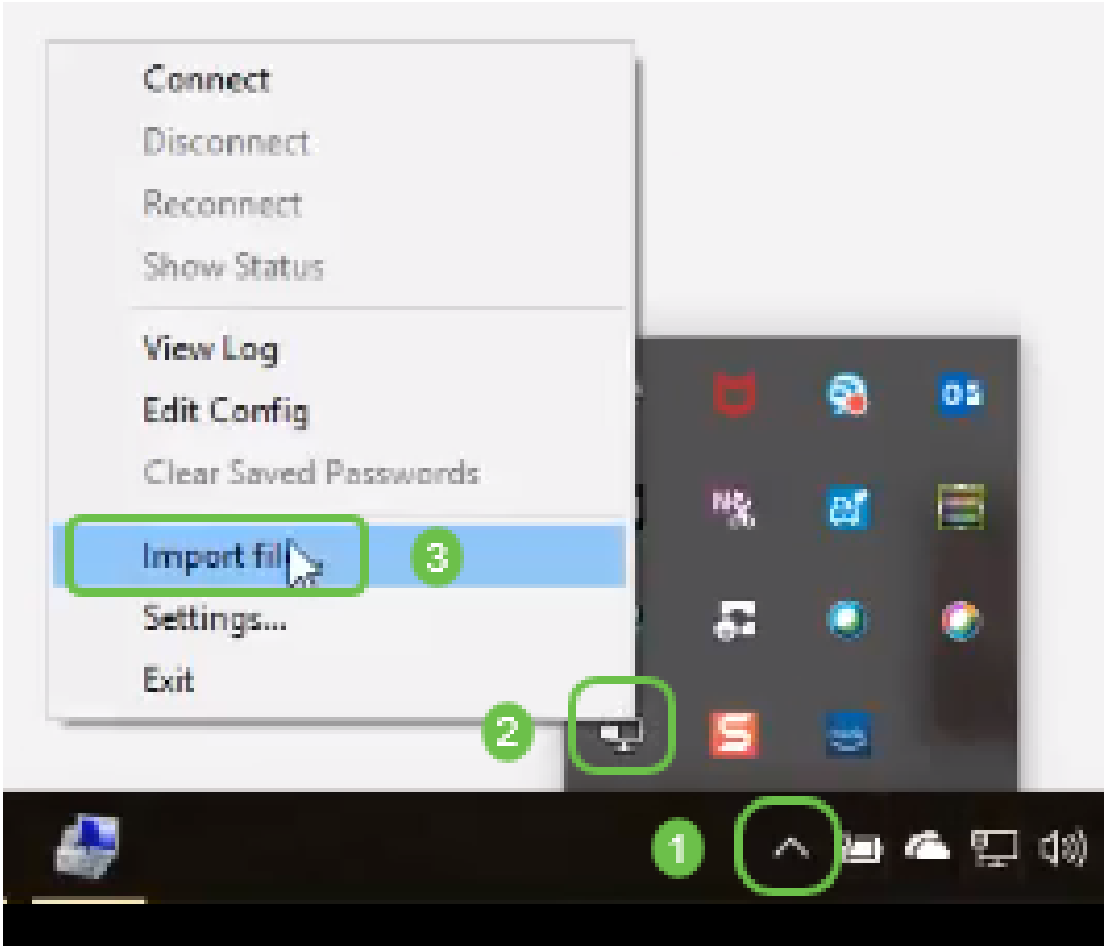
ステップ21：成功したことを確認するメッセージが表示されます。[OK] をクリックします。



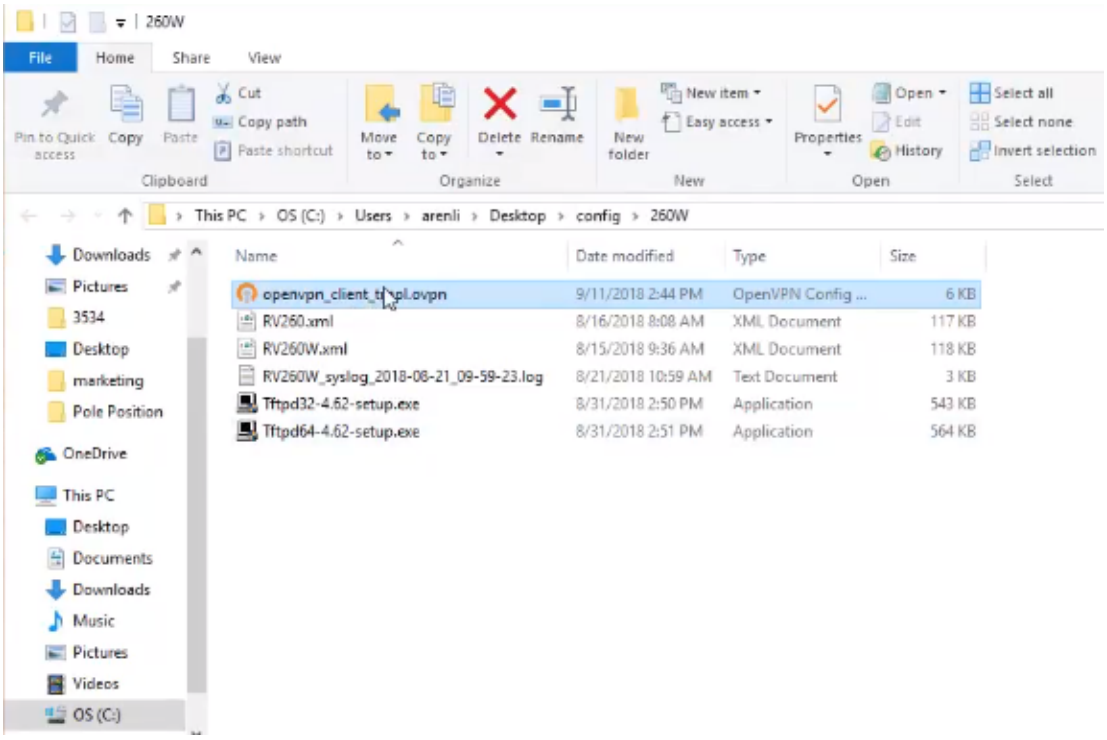
ステップ22:[Save]をクリックします。



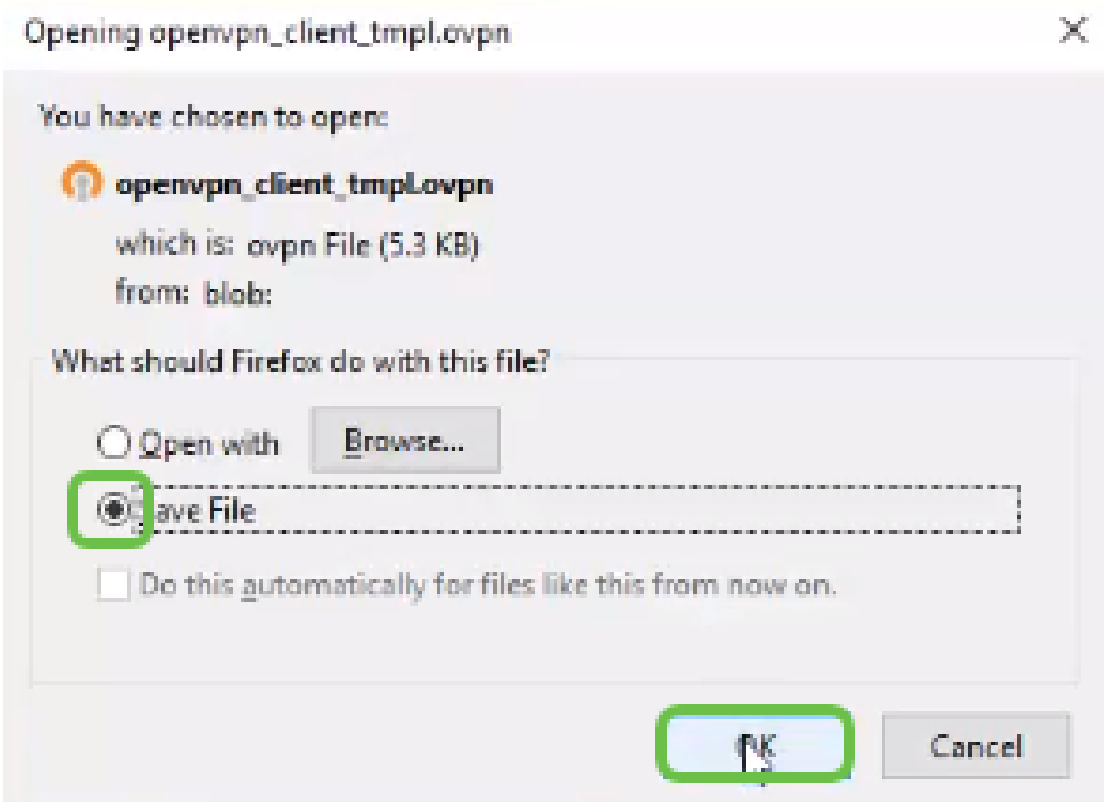
ステップ23：デスクトップの右下で、クリックしてOpenVPNを開きます。右クリックしてドロップダウンメニューを開きます。[ファイルのインポート]をクリックします。



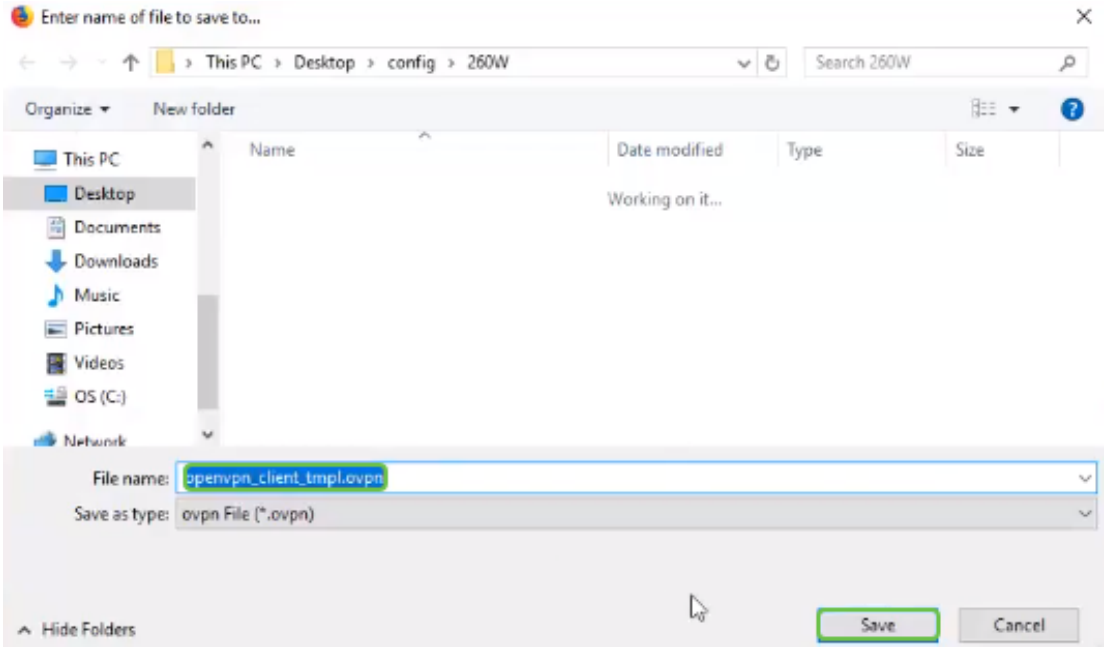
ステップ24:.ovpnで終わるOpenVPNファイルを選択します。



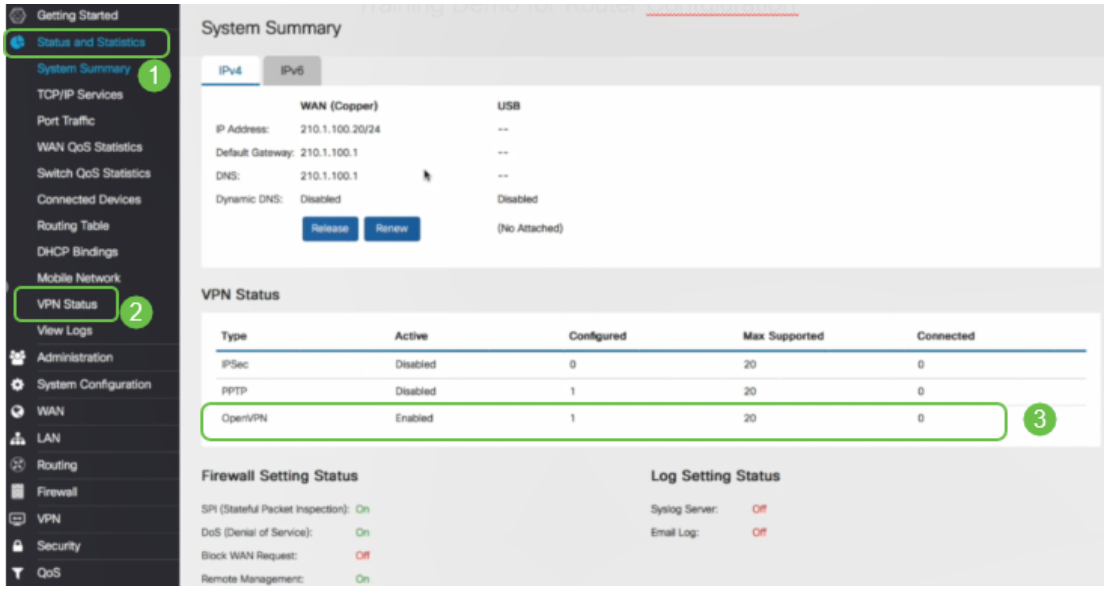
ステップ25:[Save File]ラジオボタンをクリックし、[OK]をクリックします。



ステップ26：選択した場合はファイル名を変更し、ファイル名の最後に*.ovpn*を残します。[Save]をクリックします。



ステップ27:[Status and **Statistics**] > [**VPN Status**]**に移動**します。詳細については、下にスクロールできます。



これで、ルータは、個人試用版のOpenVPN Client接続をサポートするために必要なすべてのパラメータで設定されます。

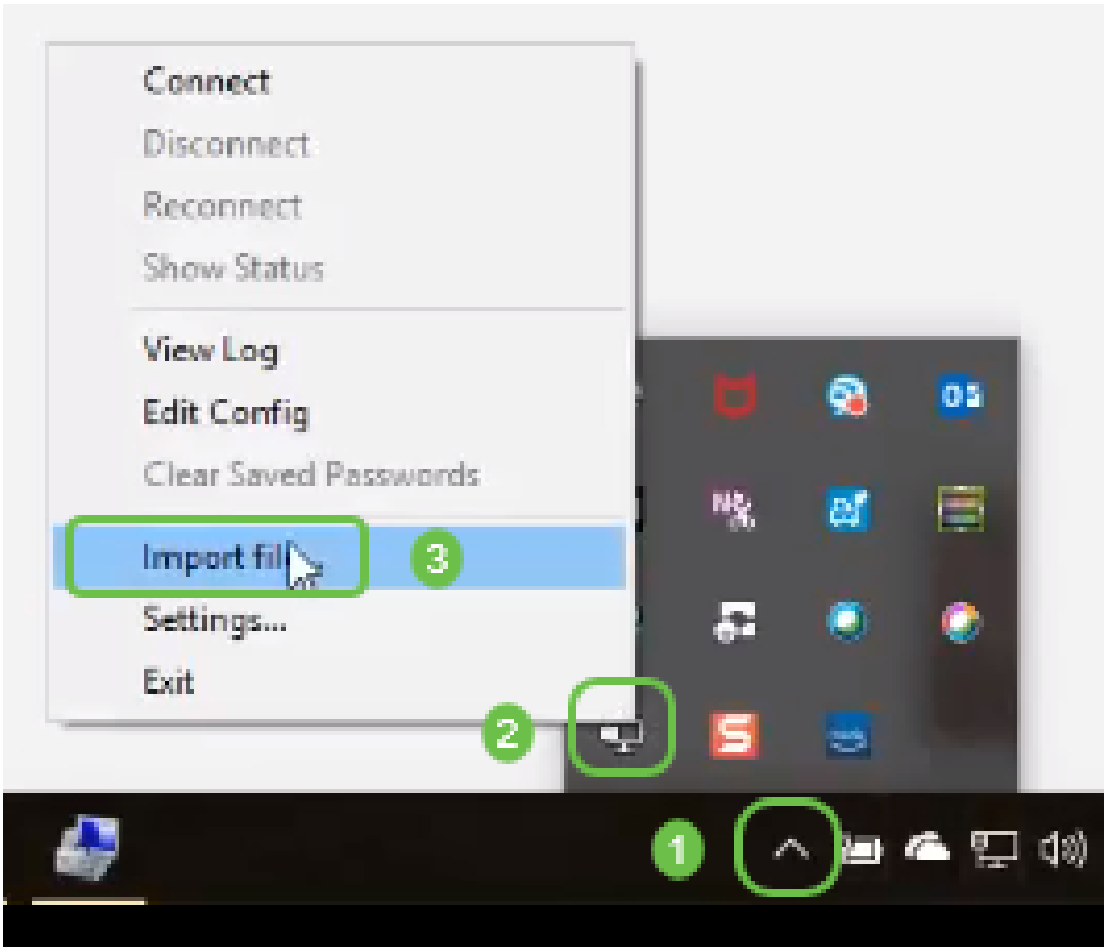
コンピュータでのOpenVPN Clientのセットアップ

各OpenVPN Clientは、前提条件として次のタスクを実行する必要があります。

- デバイスにOpenVPNアプリケーションをダウンロードします。
- 前のセクションのステップ19 ~ 22で送信されたコンフィギュレーションファイルを開き、保存します。設定ファイルの末尾は*.ovpn*です。

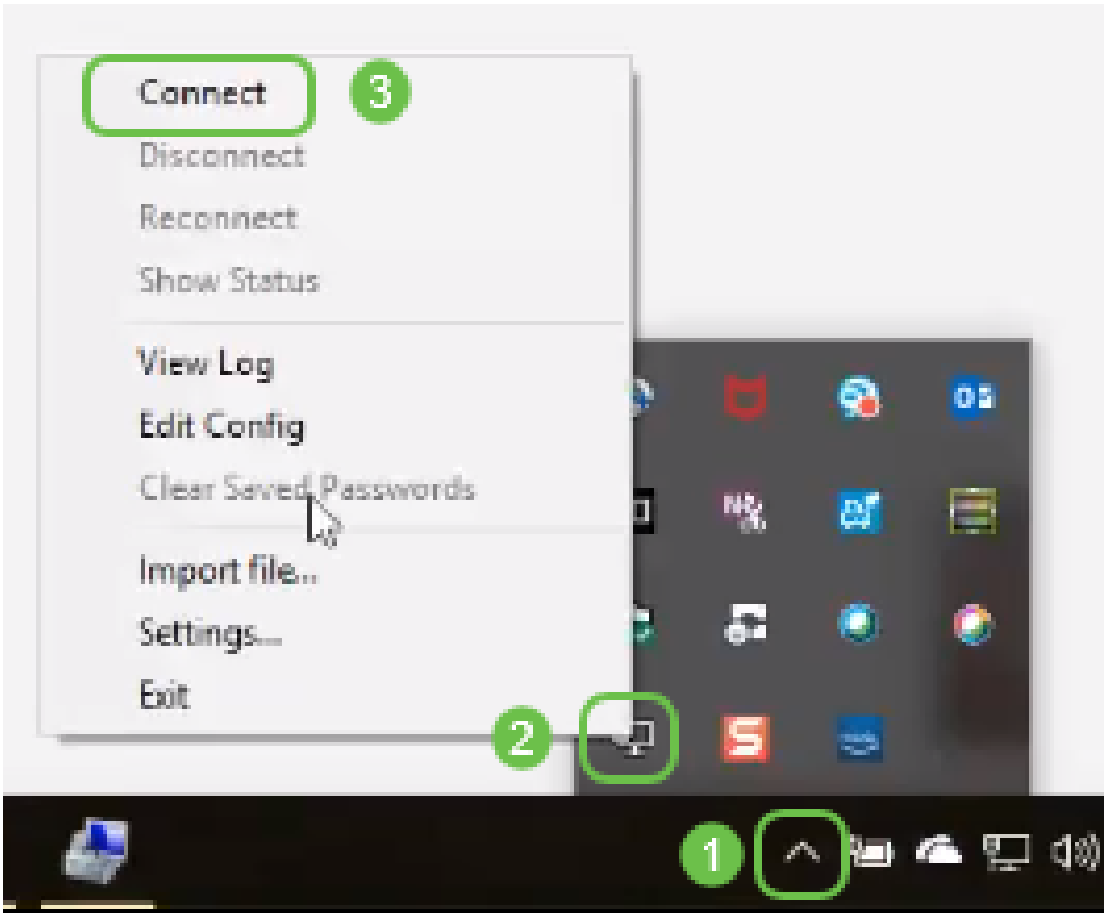
注：このセットアップは、Windows 10専用です。

ステップ1：デスクトップの右下にある矢印アイコンに移動し、クリックして[OpenVPN]アイコンを開きます。右クリックして、*[ファイルのインポート]を選択します。*

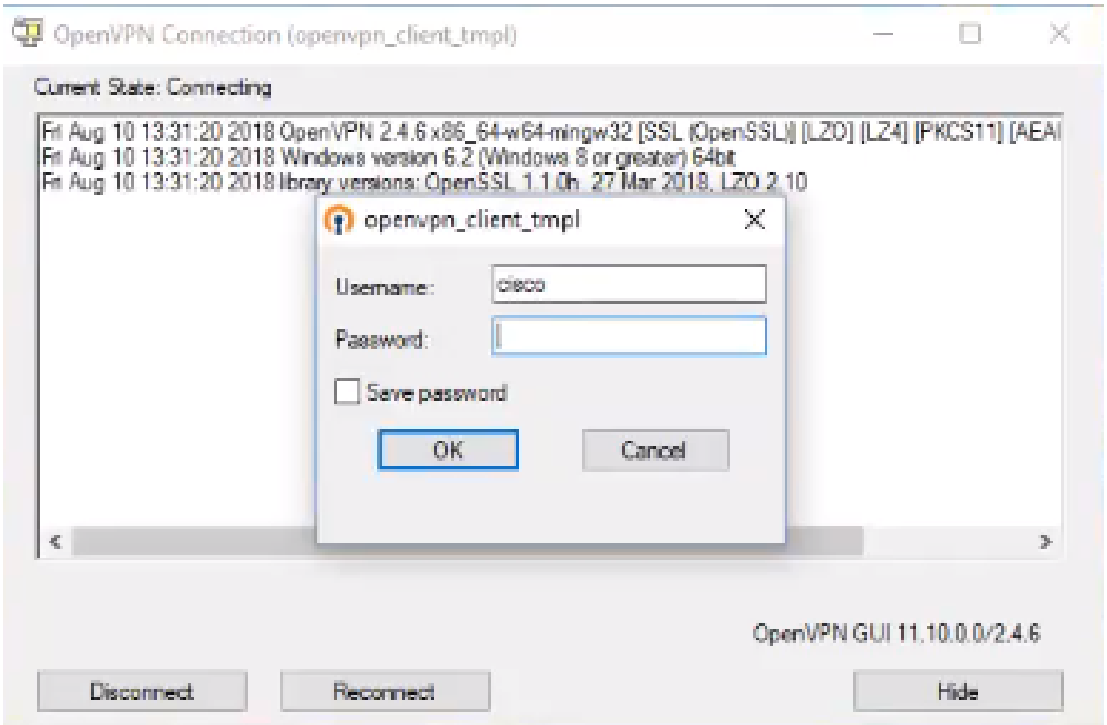


注：アイコンは白黒で、現在実行されていないことを示します。実行すると、アイコンがカラーで表示されます。

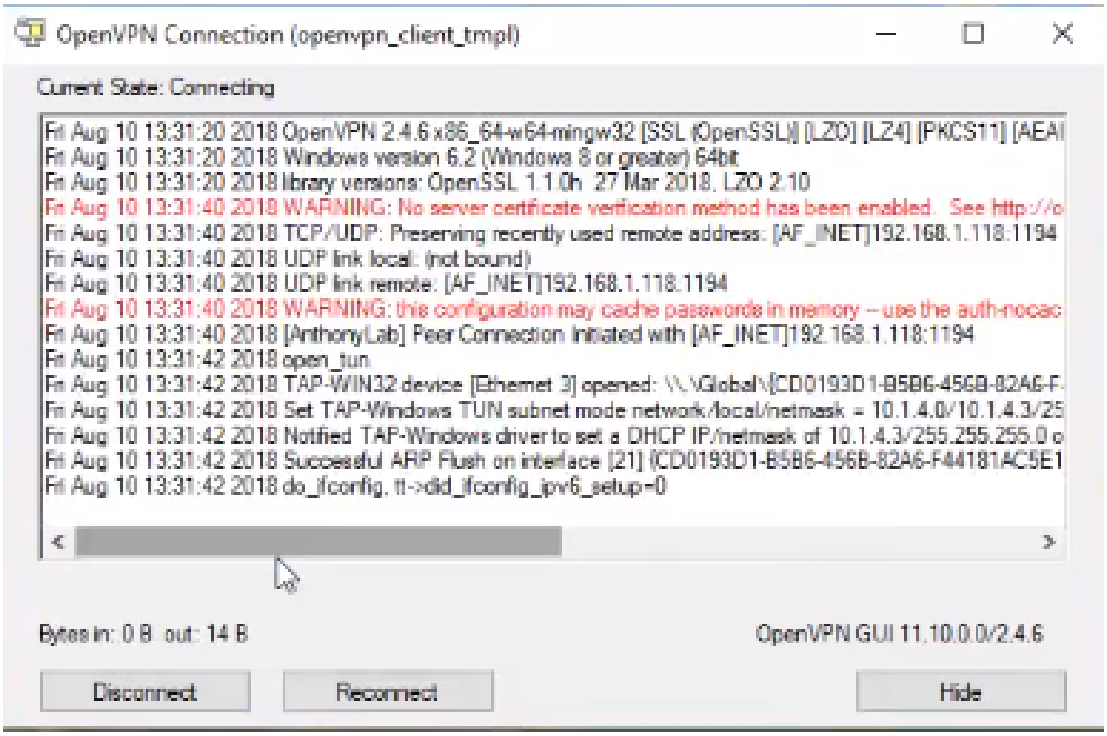
ステップ2：上矢印をクリックします。[OpenVPN]アイコンをクリックします。右クリックして、ドロップダウンメニューから[接続]を選択します。



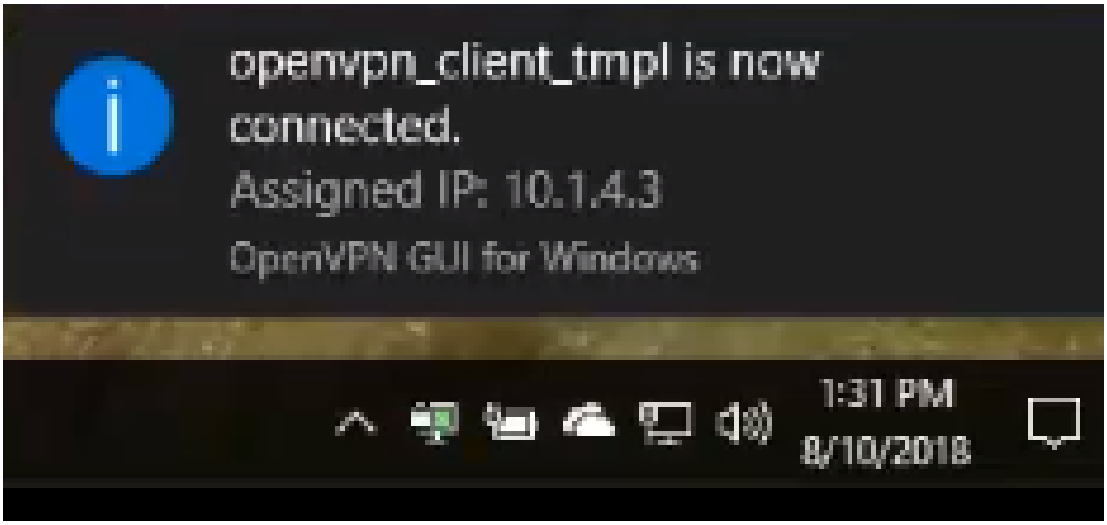
ステップ3：ユーザ名とパスワードを入力します。



ステップ4：ウィンドウに、ログデータとともにOpenVPN接続が表示されます。

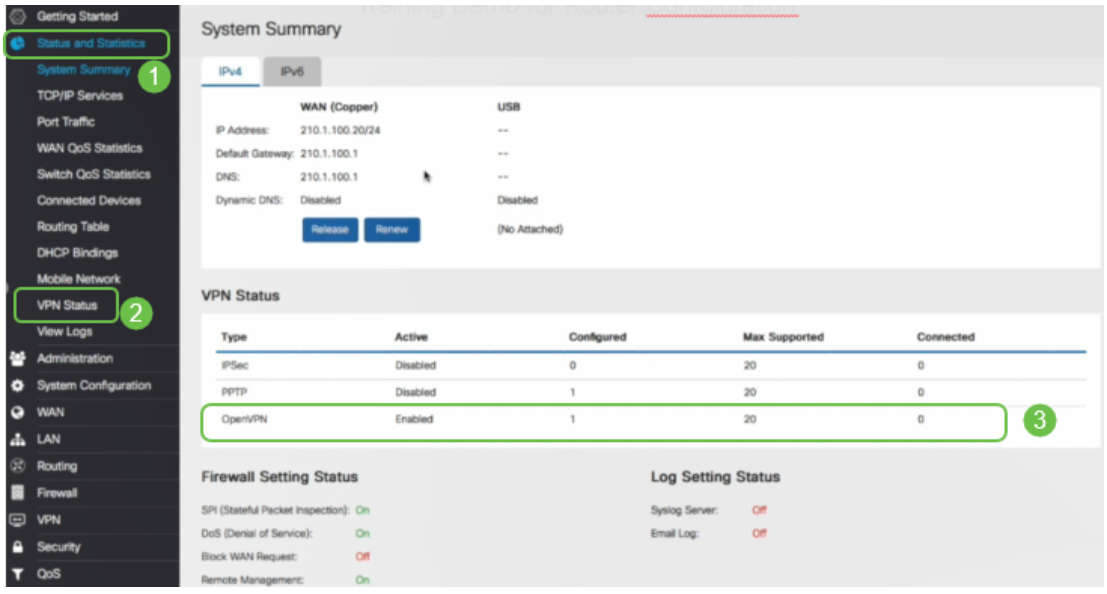


ステップ5：システムログは、接続があることを警告します。



ステップ6:VPNクライアントは、OpenVPNを介して着信および発信情報を安全にトンネルできます。これは、OpenVPN設定で自動的に接続するように設定できます。

ステップ7：管理者は、ルータの[Status and **Statistics**] > [**VPN Status**]に移動して、**VPN Statusを確認**できます。



結論

これで、RV160またはRV260ルータとVPNクライアントサイトにOpenVPNが正常にインストールされました。

OpenVPNに関するコミュニティのディスカッションを行う場合は、ここをクリックしてOpenVPNを検索してください。

この記事に関連するビデオを表示...

シスコのその他のテクニカルトークを表示するには、ここをクリックしてください