RV34xシリーズルータでのユーザアカウントの設定と管理

目的

この記事の目的は、RV34xシリーズルータでローカルおよびリモートユーザアカウントを設定および管理する方法を説明することです。これには、ローカルユーザのパスワードの複雑度の設定方法、ローカルユーザの設定/編集/インポート、RADIUS、Active Directory、およびLDAPを使用したリモート認証サービスの設定方法が含まれます。

該当するデバイス |ファームウェアのバージョン

- RV34xシリーズ | 1.0.01.16 (最新のダウンロード)

概要

RV34xシリーズルータは、設定を表示および管理するためのユーザアカウントを提供します。ユーザは、異なるグループのユーザにすることも、認証ドメイン、ローカルエリアネットワーク(LAN)、サービスアクセスルール、およびアイドルタイムアウト設定を共有するSecure Sockets Layer(SSL)仮想プライベートネットワーク(VPN)の論理グループに属することもできます。ユーザ管理は、特定のタイプの機能を利用できるユーザのタイプと、その方法を定義します。

外部データベースの優先順位は、常にRemote Authentication Dial-In User Service(RADIUS)/Lightweight Directory Access Protocol(LDAP)/Active Directory(AD)/Localです。ルータにRADIUSサーバを追加すると、Webログインサービスやその他のサービスは、RADIUS外部データベースを使用してユーザを認証します。

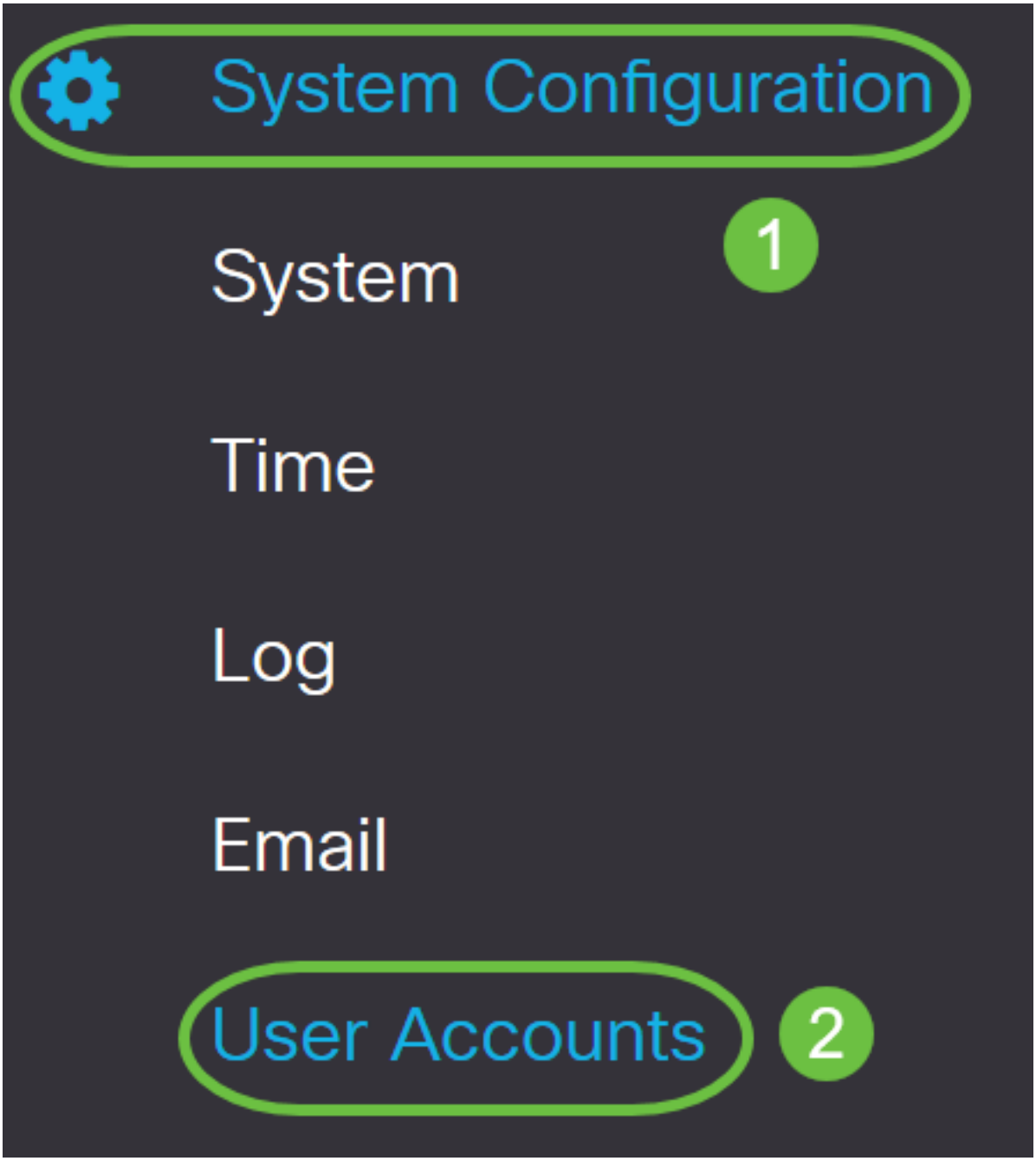
Webログインサービス専用の外部データベースを有効にし、別のサービス用に別のデータベースを設定するオプションはありません。ルータでRADIUSが作成され、有効になると、ルータはRADIUSサービスをWebログイン、サイト間VPN、EzVPN/3rd Party VPN、SSL VPN、Point-to-Point Transport Protocol(PPTP)/レイヤ2 Transport Protocol(L2TP) VPN)、および802.1x

目次

ローカルユーザアカウントの設定

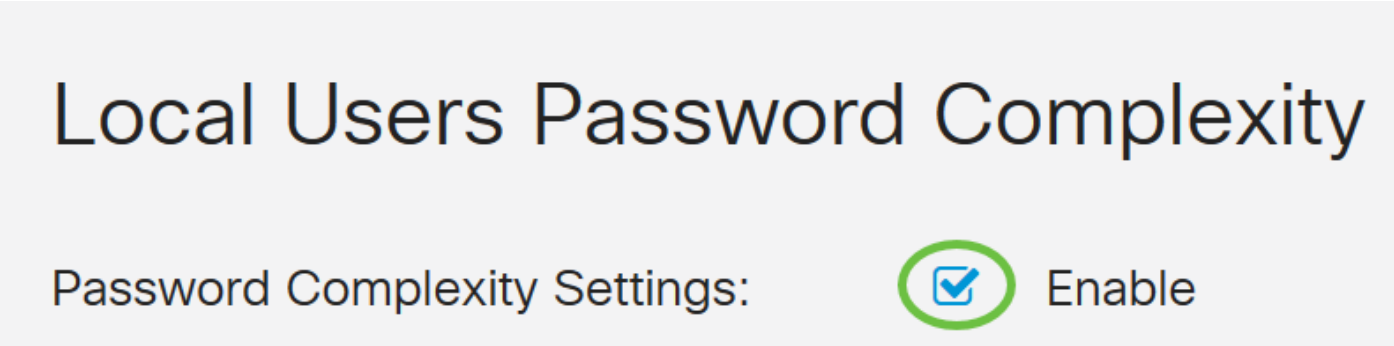
ローカルユーザのパスワードの複雑度

ステップ1：ルータのWebベースのユーティリティにログインし、[System Configuration] > [User Accounts]を選択します。



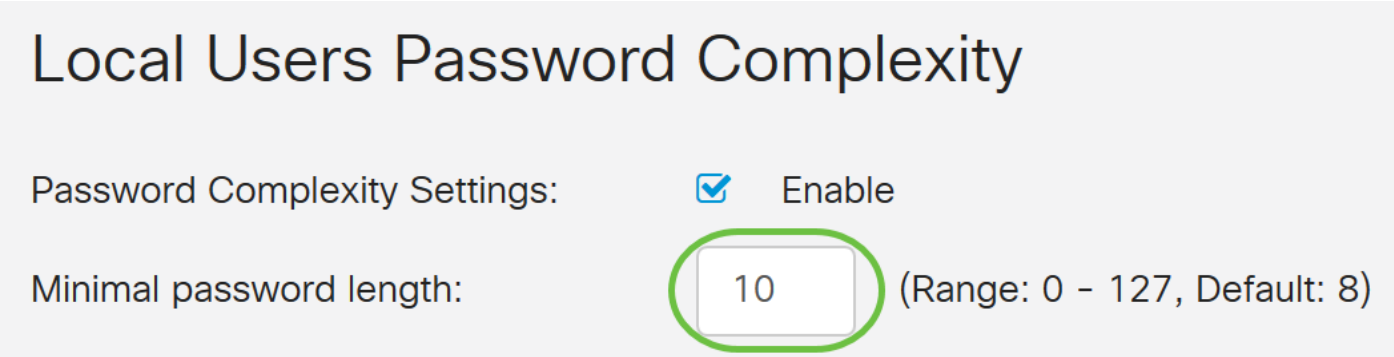
ステップ2：パスワードの複雑さパラメータを有効にするには、[パスワードの複雑さ設定を有効にする]チェックボックスをオンにします。

このチェックボックスをオフのままにした場合は、「ローカルユーザーの構成」に進みます。



ステップ3:[Minimal password length]*フィールド*に、0 ~ 127の範囲の数字を入力して、パスワードに含める必要がある最小文字数を設定します。デフォルト値は 8 です。

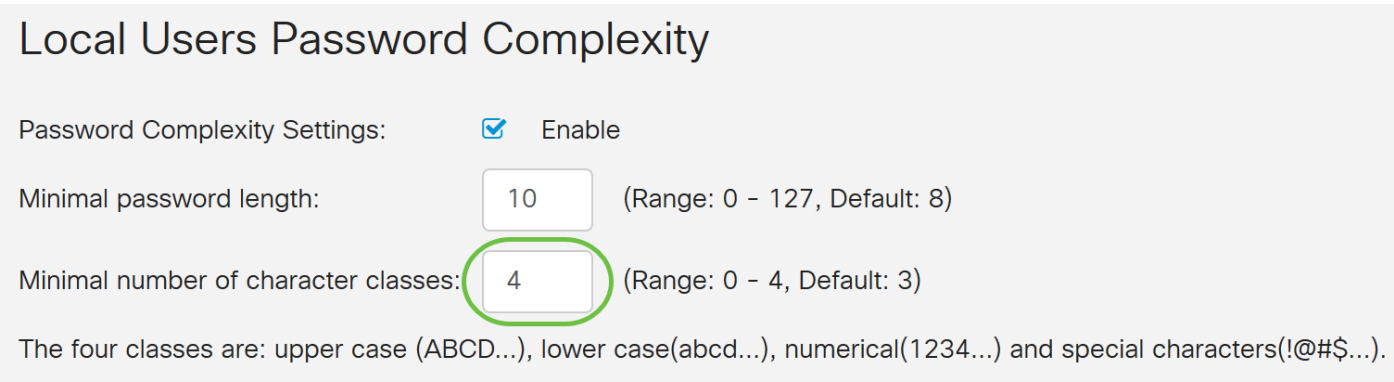
この例では、最小文字数を10に設定**します**。



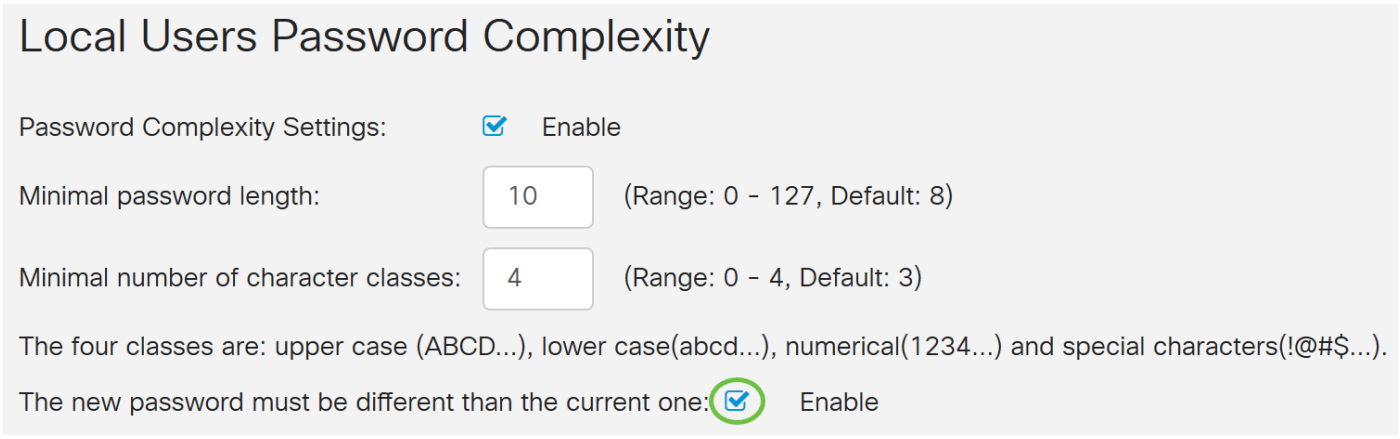
ステップ4:[Minimal number of character classes]*フィールドに、クラスを設定するために*0 ~ 4の数値を入力します。入力した数値は、異なるクラスの最小文字数または最大文字数を表します。

- パスワードは、大文字(ABCD)で構成されます。
- パスワードは、小文字(abcd)で構成されます。
- パスワードは数字で構成される(1234)。
- パスワードは特殊文字(!@#$)で構成されています。

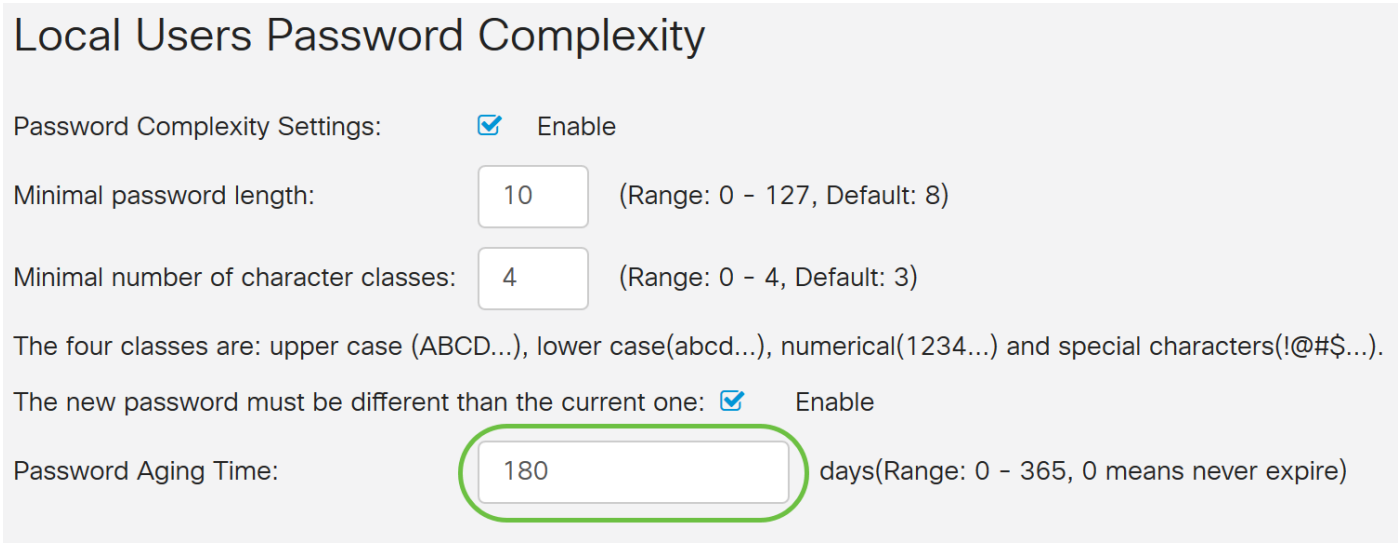
この例では、4 が使用されます。



ステップ5：新しいパスワードの[Enable] チェックボックスをオンにします。これは、現在のパスワードと異なるパスワードである必要があります。



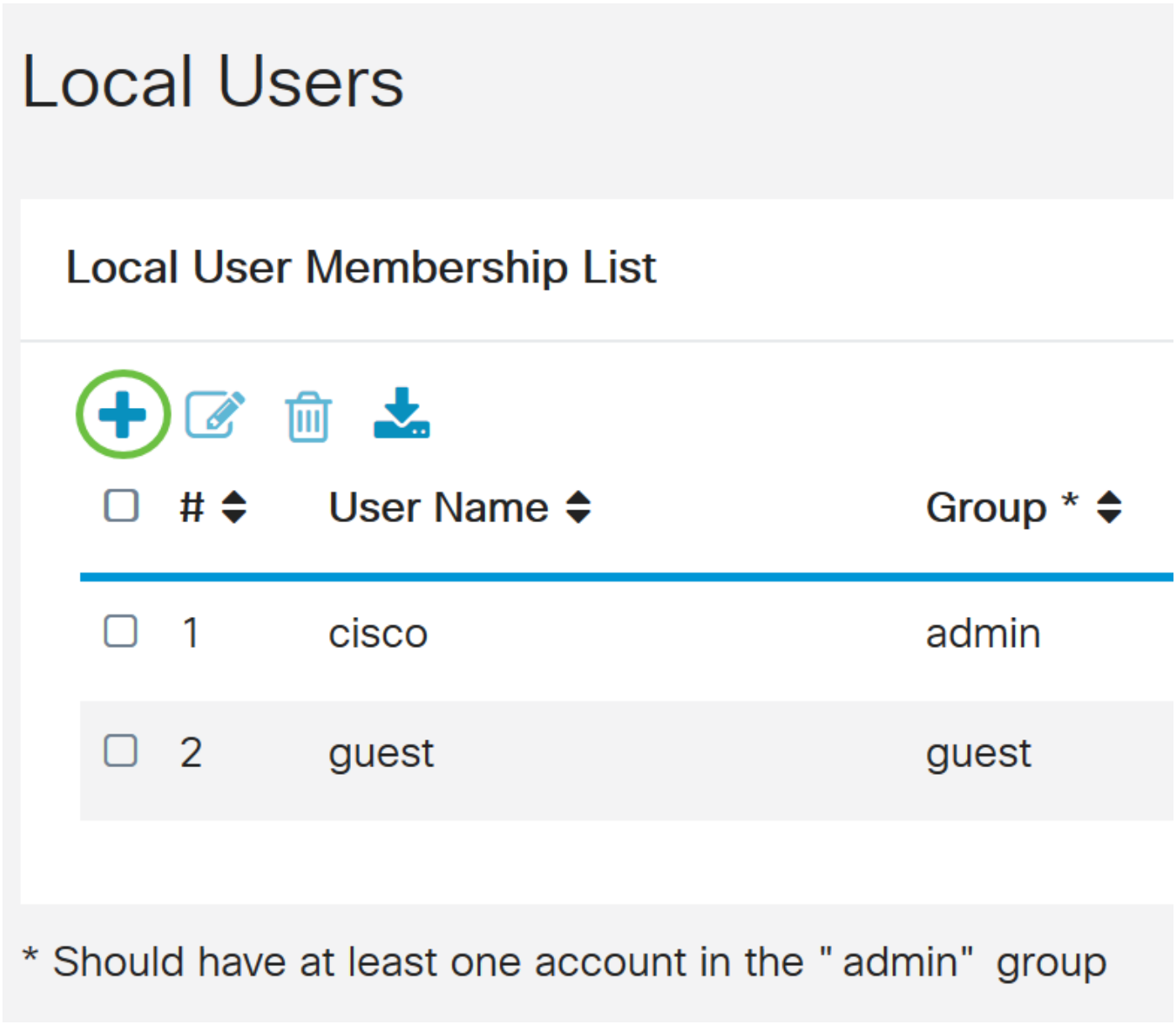
ステップ6:[パスワード・エージングタイム(Password Aging Time)]フィールドに、パスワード期限切れの日数(0 ~ 365)を入力します。この例では、180日が入力されています。



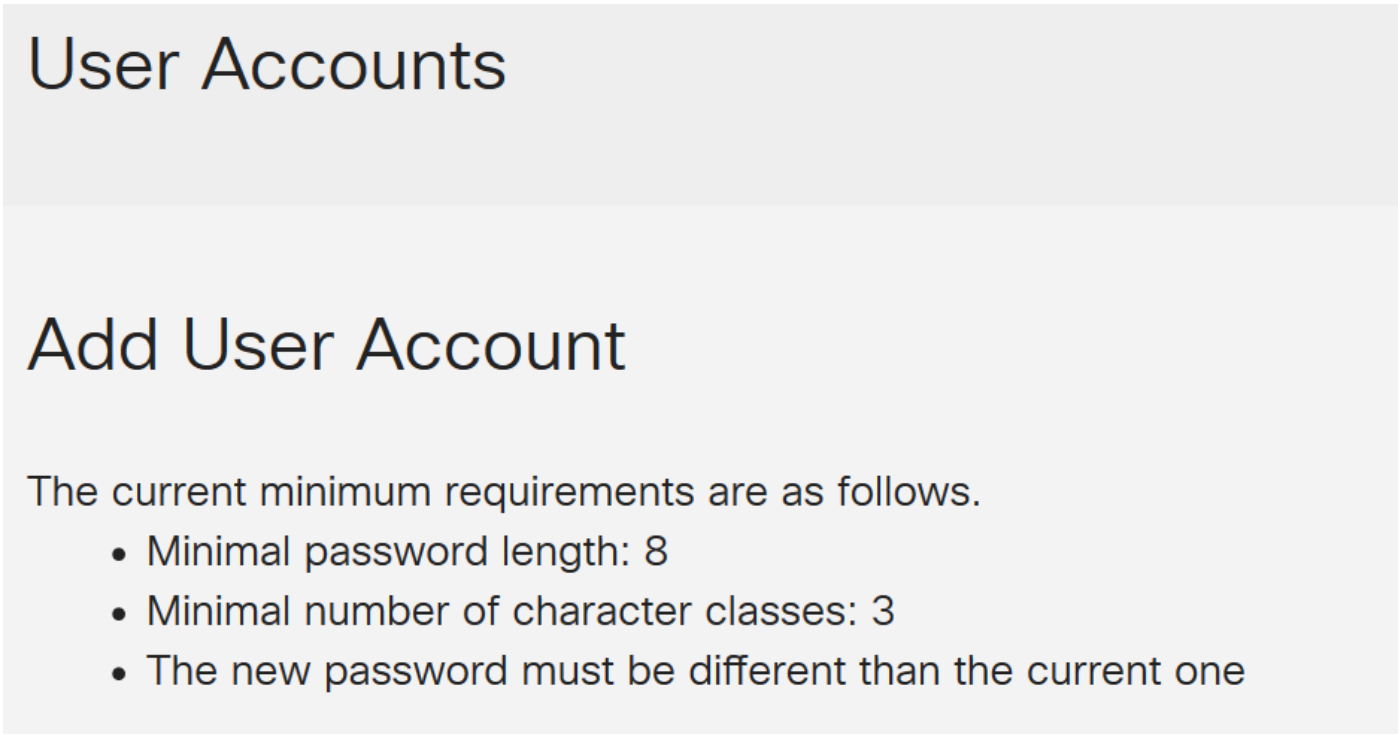
これで、ルータの[Local Users Password Complexity]設定が正常に設定されました。

ローカルユーザの設定

ステップ1:[Local User Membership List]テーブルで、[Add]をクリックして新しいユーザアカウントを作成します。[Add User Account]ページが表示されます。

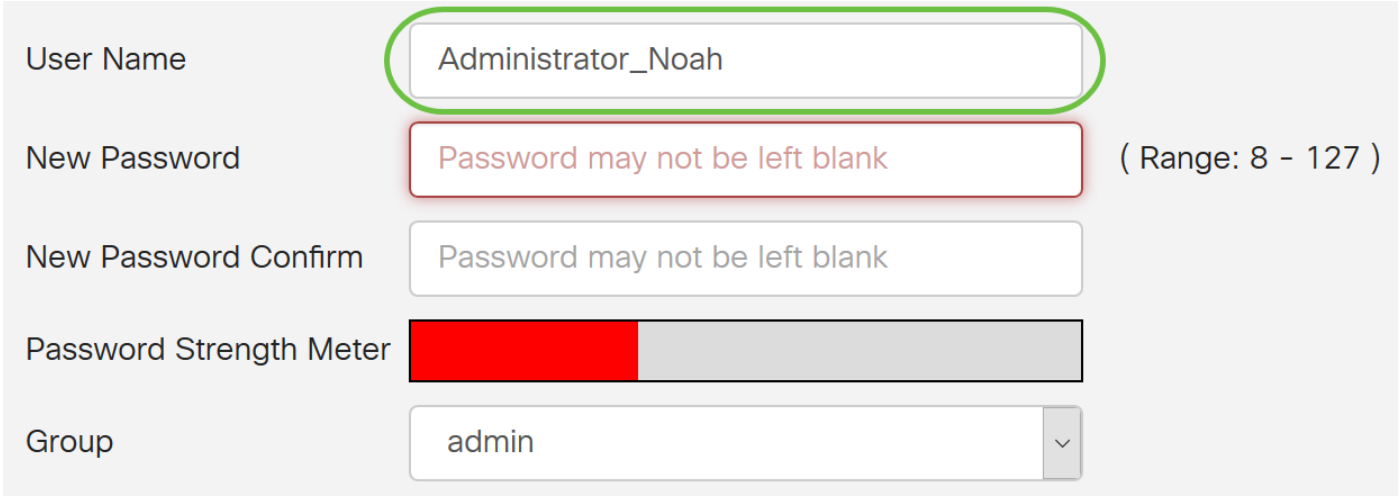


[Add User Account]ヘッダーの下に、[Local Password Complexity]ステップで定義したパラメータが表示されます。

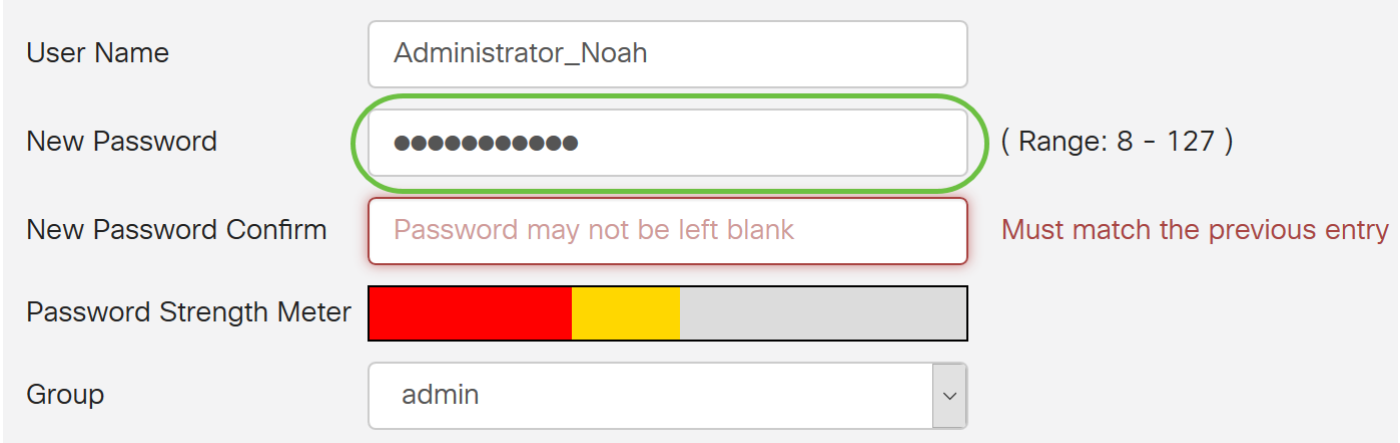


ステップ2:[ユーザー名]フィールドに、アカウントのユーザー名を入力します。

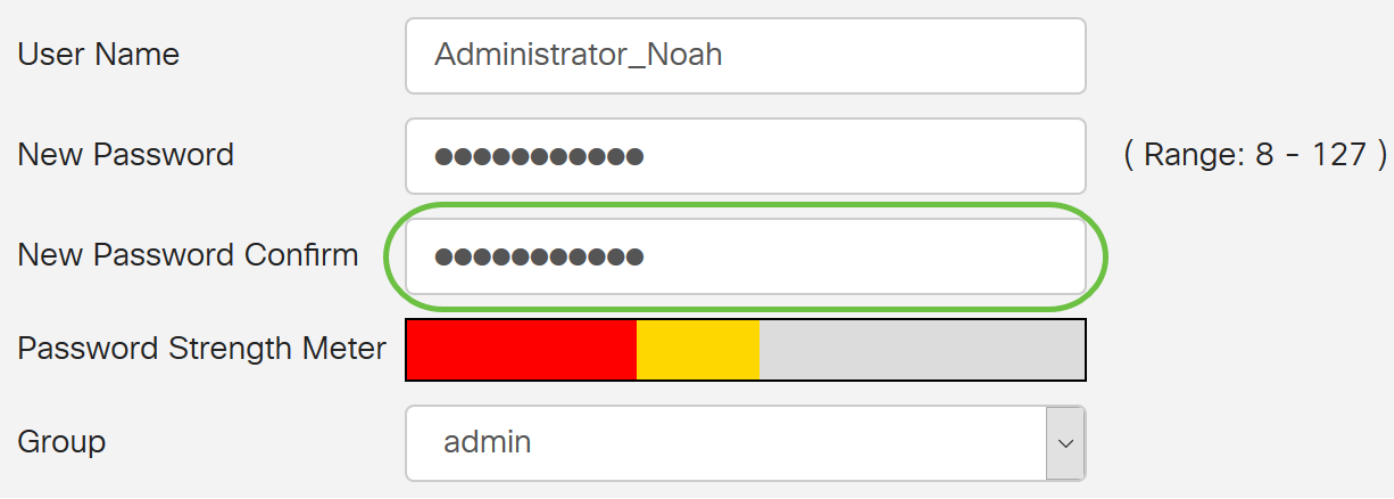
この例では、**Administrator_Noahが使**用されます。



ステップ3:[新しいパスワード]フィールドに、定義されたパラメータを持つパスワードを入力します。この例では、パスワードの最小長は10文字で構成され、大文字、小文字、数字、特殊文字が組み合わされている必要があります。



ステップ4:[新しいパスワードの確認(*New Password Confirm*)]フィールドで、確認するパスワードを再入力します。パスワードが一致しない場合は、フィールドの横にテキストが表示されます。

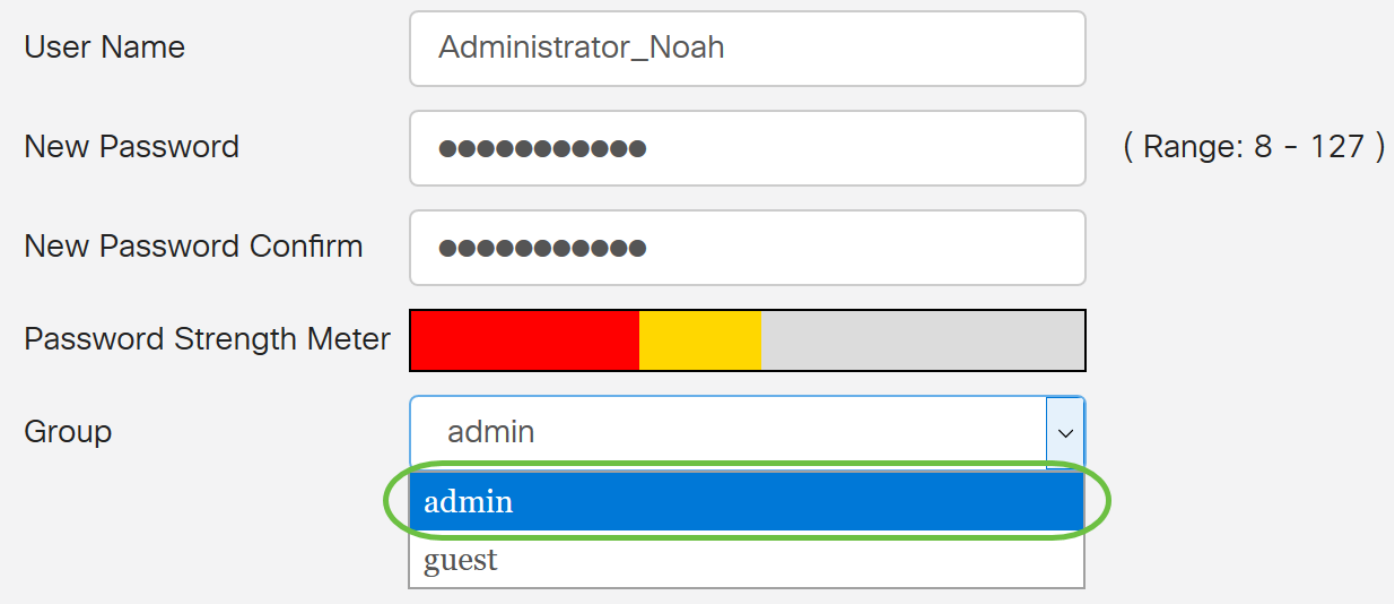


パスワード強度メーターは、パスワードの強度に応じて変化します。

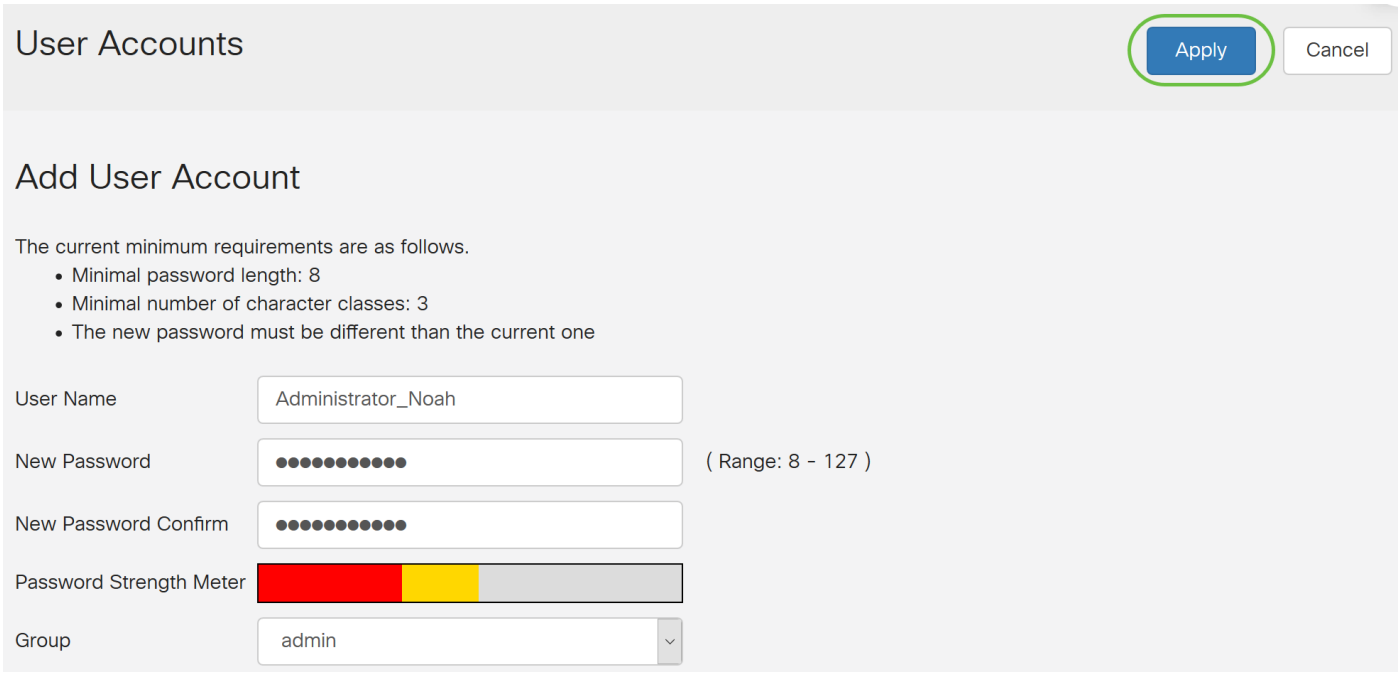
ステップ5:[グループ(*Group)]*ドロップダウンリストから、権限をユーザアカウントに割り当てるグループを選択します。次のオプションがあります。

- admin：読み取り/書き込み権限。
- guest：読み取り専用権限。

この例では、[admin]が選択されています。



ステップ6:[Apply]をクリックします。

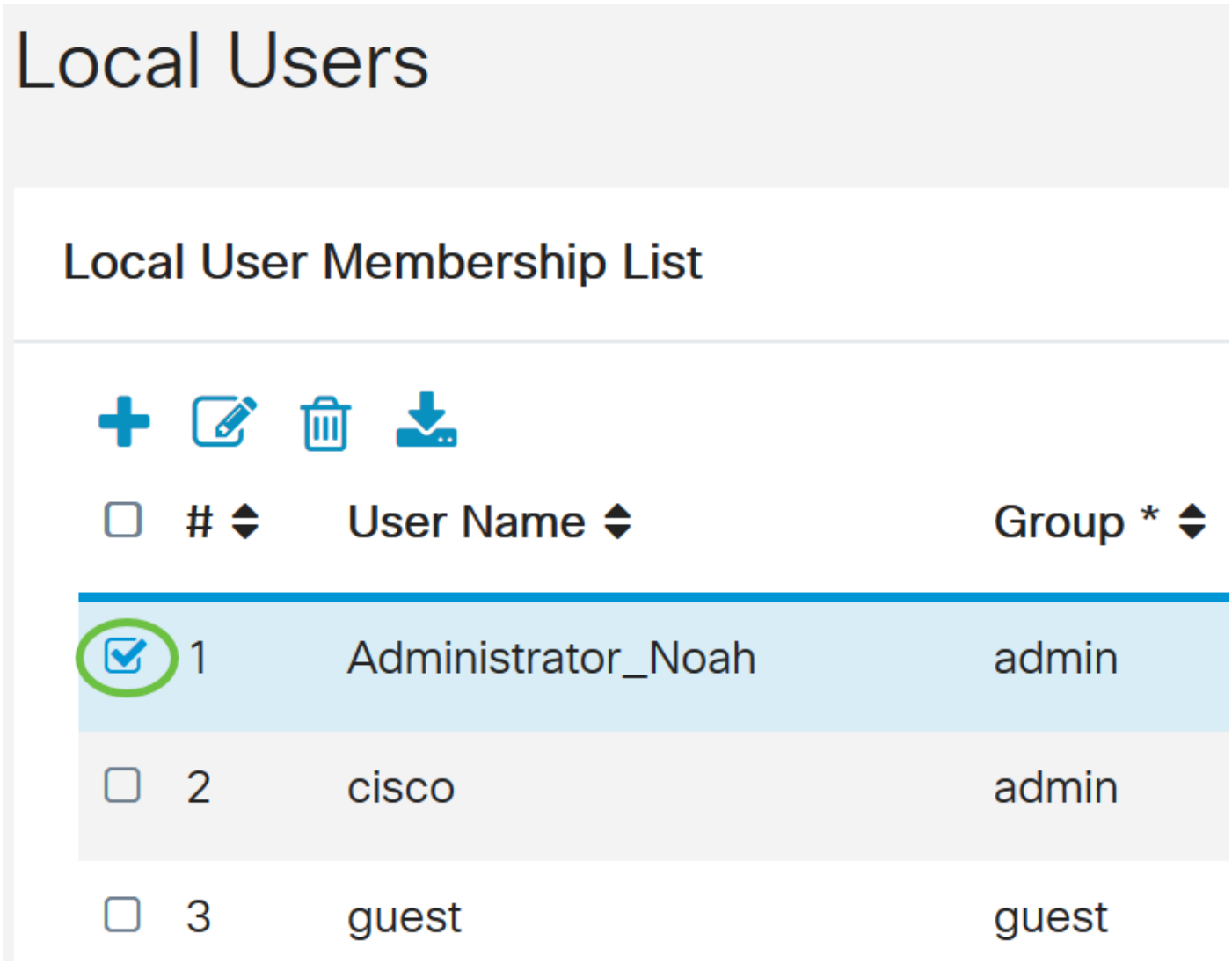


これで、RV34xシリーズルータのローカルユーザメンバーシップが正常に設定されました。

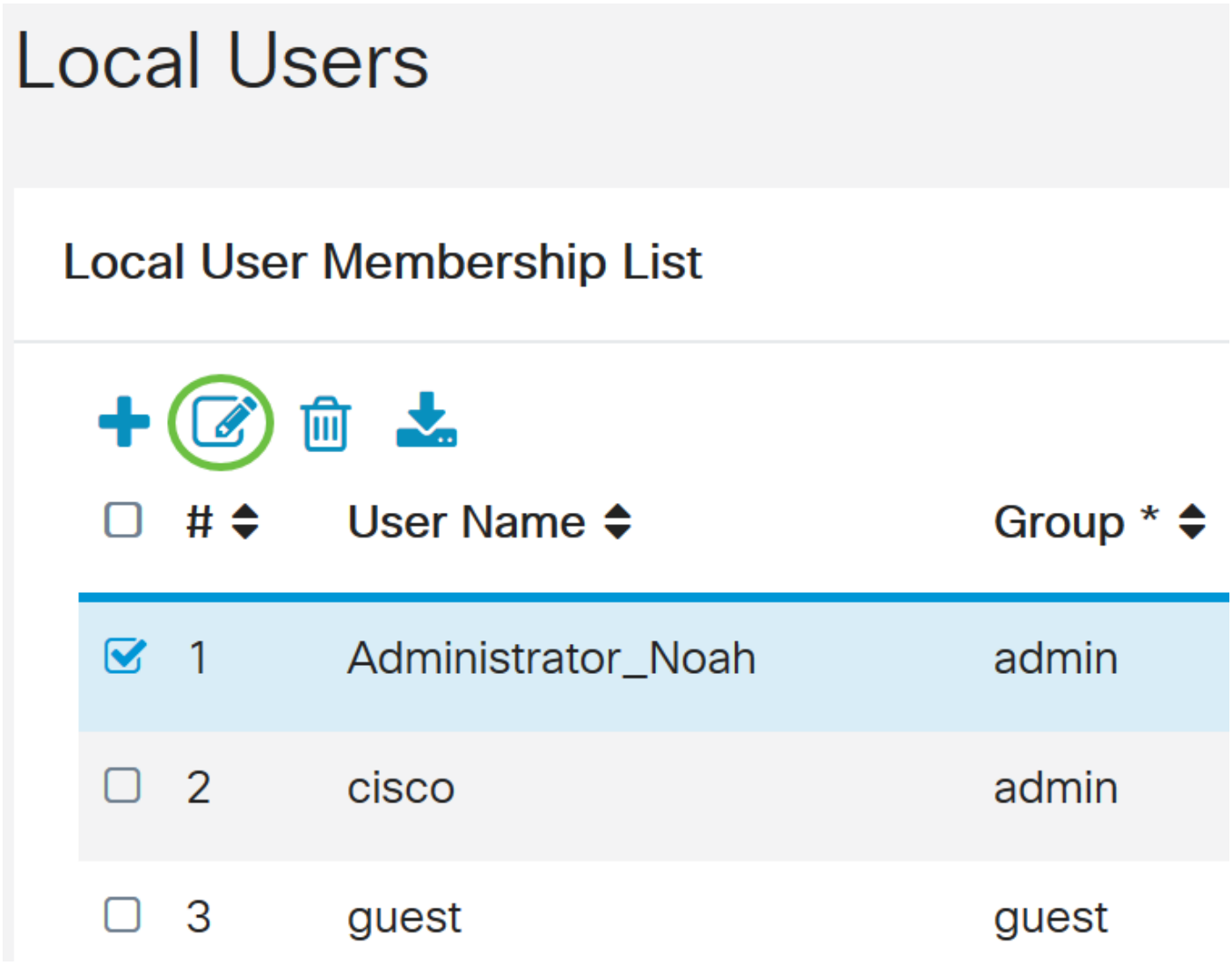
ローカルユーザの編集

ステップ1:[Local User Membership List]テーブルで、ローカルユーザのユーザ名の横にあるチェックボックスをオンにします。

この例では、**Administrator_Noahが選**択されます。

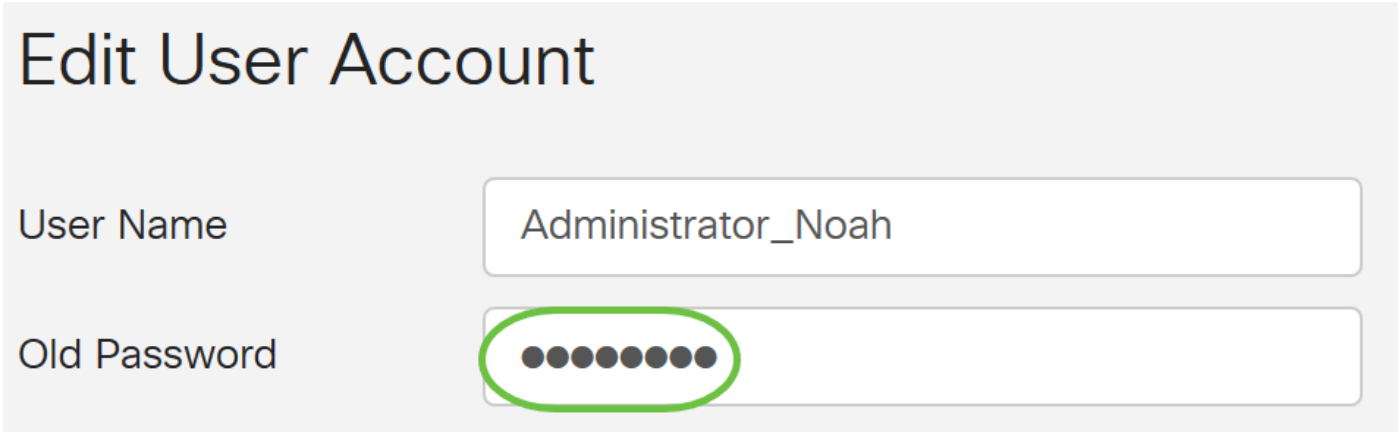


ステップ2:[Edit]をクリックします。

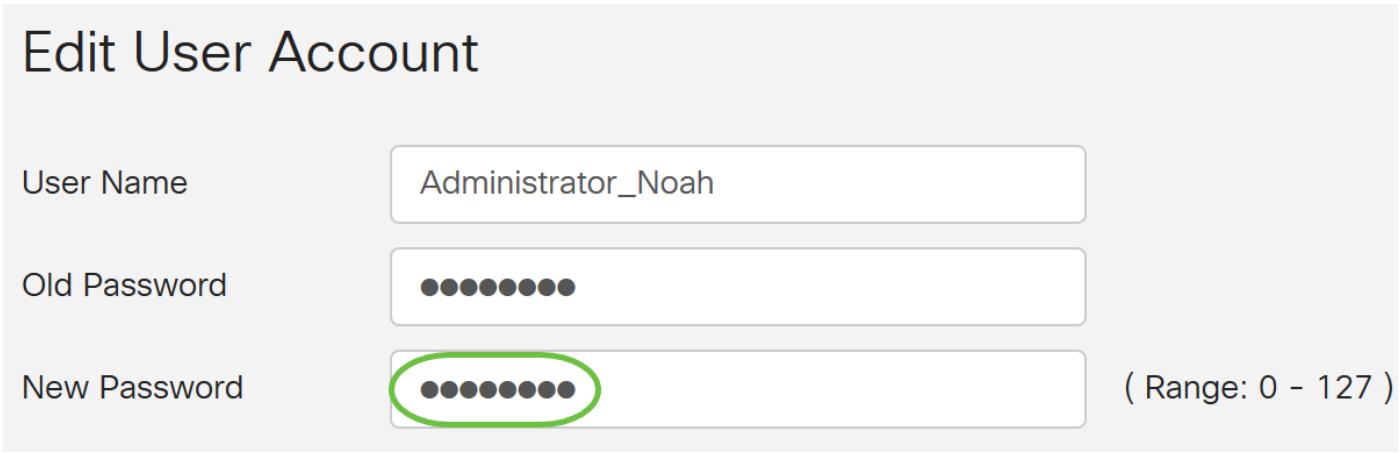


ユーザー名を編集できません。

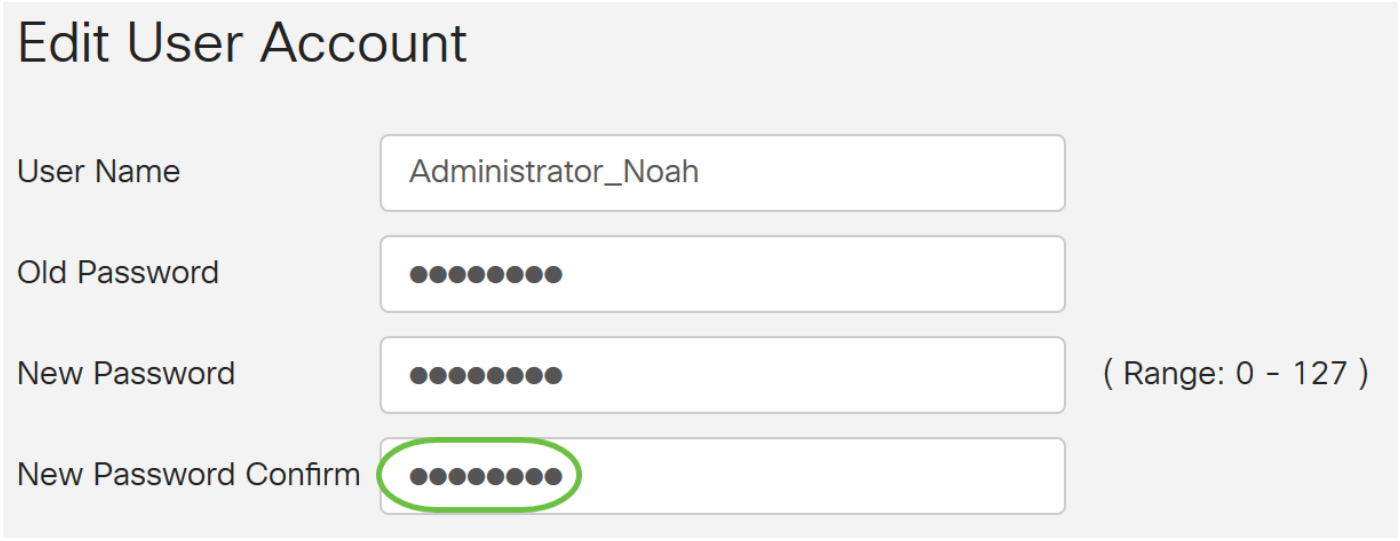
ステップ3:[*Old Password* (古いパスワード)]フィールドに、ローカルユーザアカウント用に以前に設定したパスワードを入力します。



ステップ4:[新しいパスワード*]フィールド*に、新しいパスワードを入力します。新しいパスワードは最小要件を満たしている必要があります。

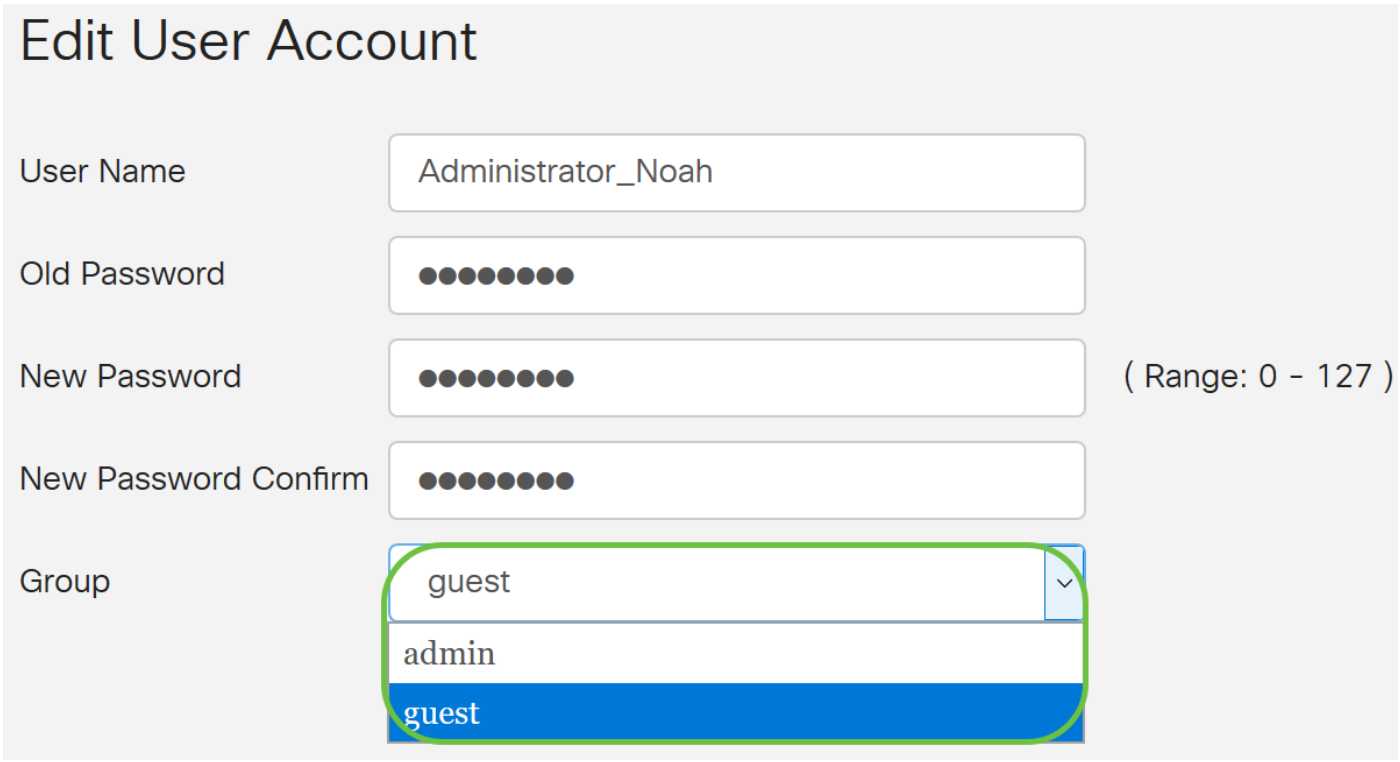


ステップ5:[New Password Confirm]フィールドにもう一度新しいパスワードを入力して確認します。これらのパスワードは一致している必要があります。

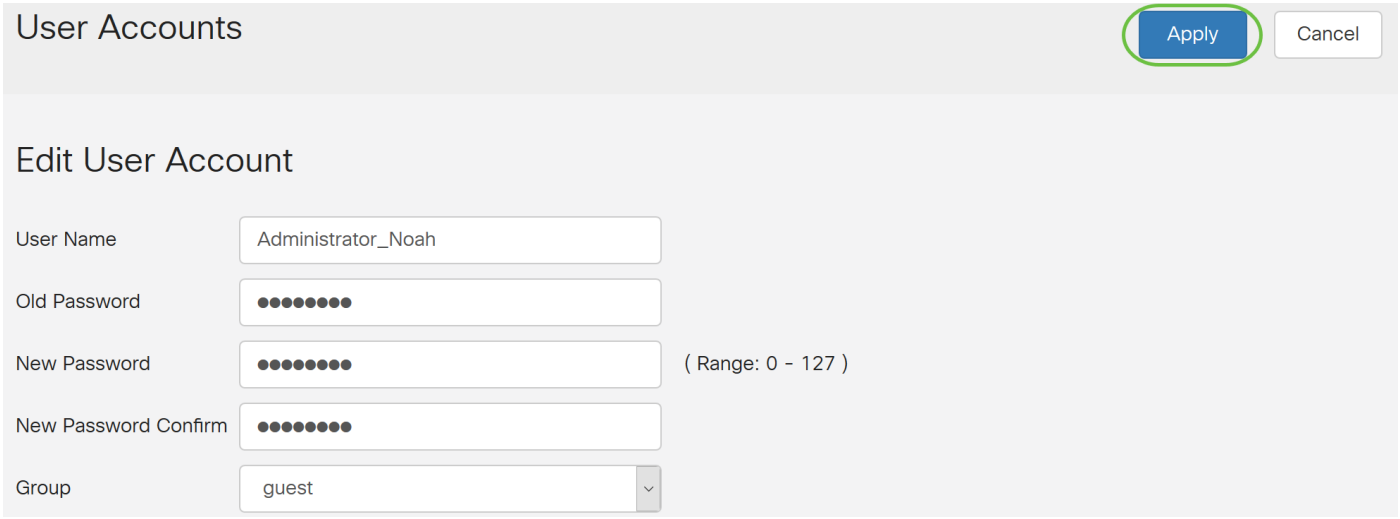


ステップ6: (オプション) [Group]ドロップダウンリストから、権限をユーザアカウントに割り当てるグループを選択します。

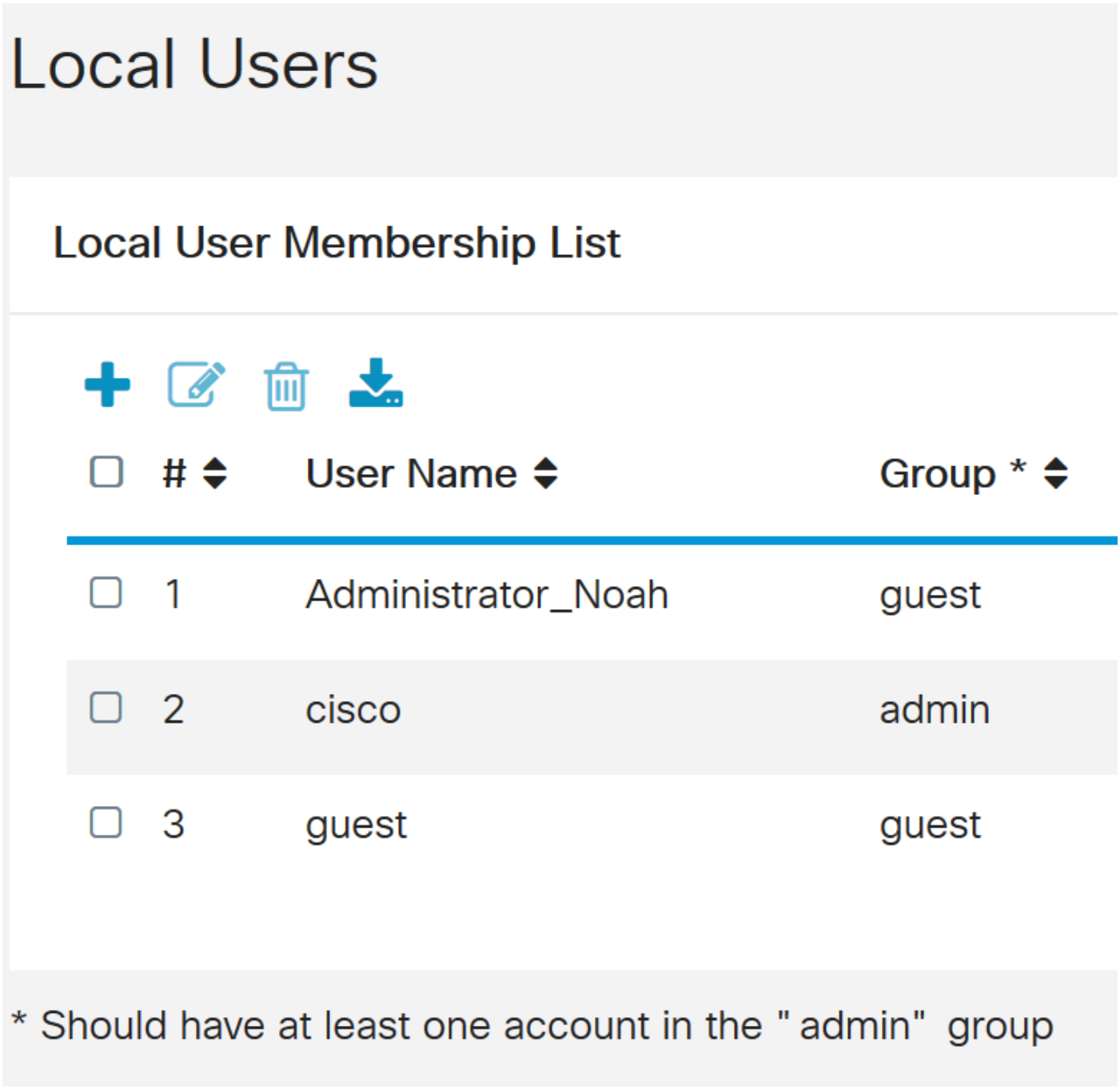
この例では、[guest]が選択されています。



ステップ7:[Apply]をクリックします。



これで、ローカルユーザアカウントが正常に編集されました。



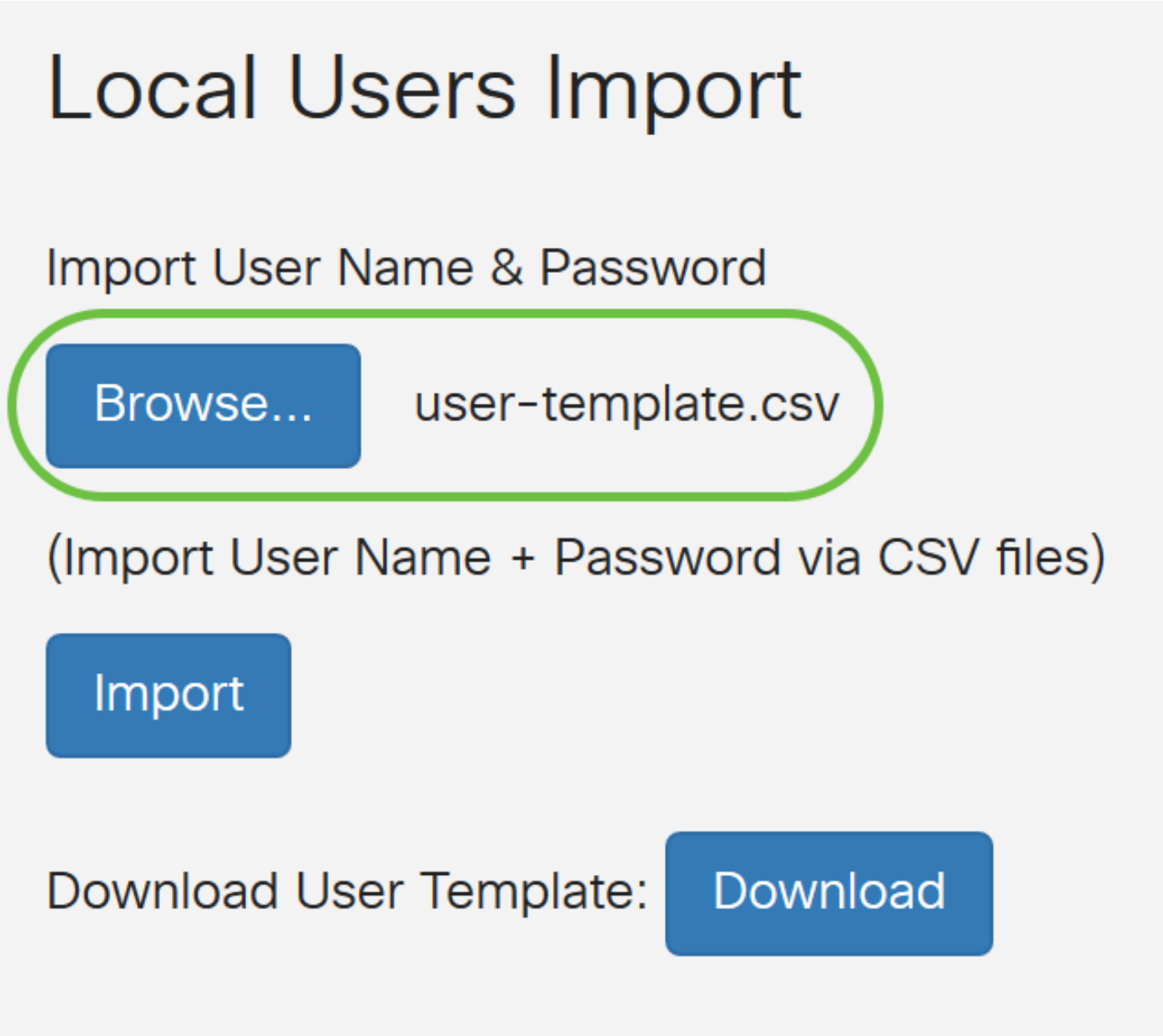
ローカルユーザのインポート

ステップ1:[Local Users Import (ローカルユーザのインポート)]領域で、をクリックします

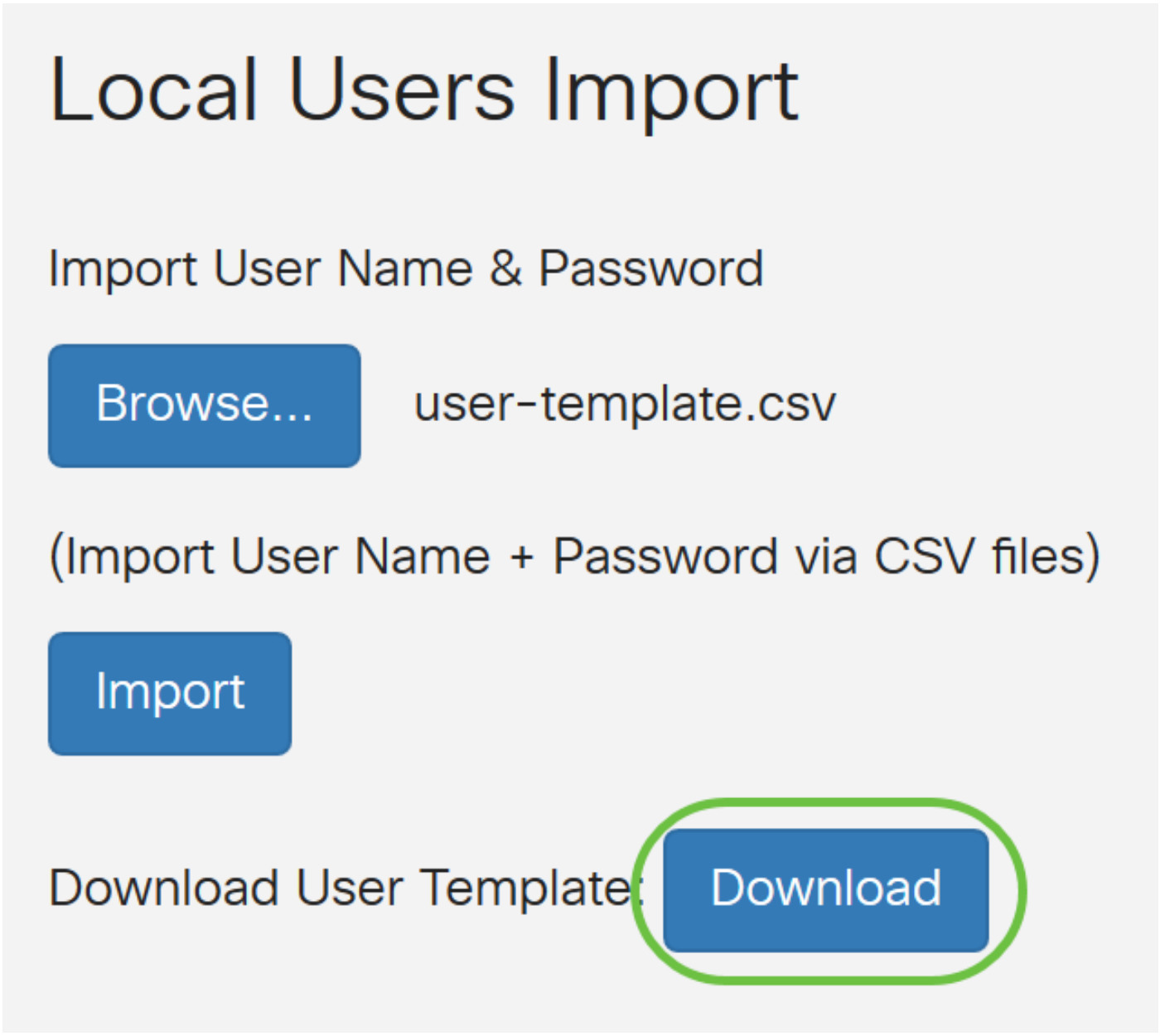
。

ステップ2:[Import User Name & Password]で**[Browse...]をクリックし**て、ユーザのリストをインポートします。このファイルは通常、カンマ区切り値(.CSV)形式で保存されたスプレッドシートです。

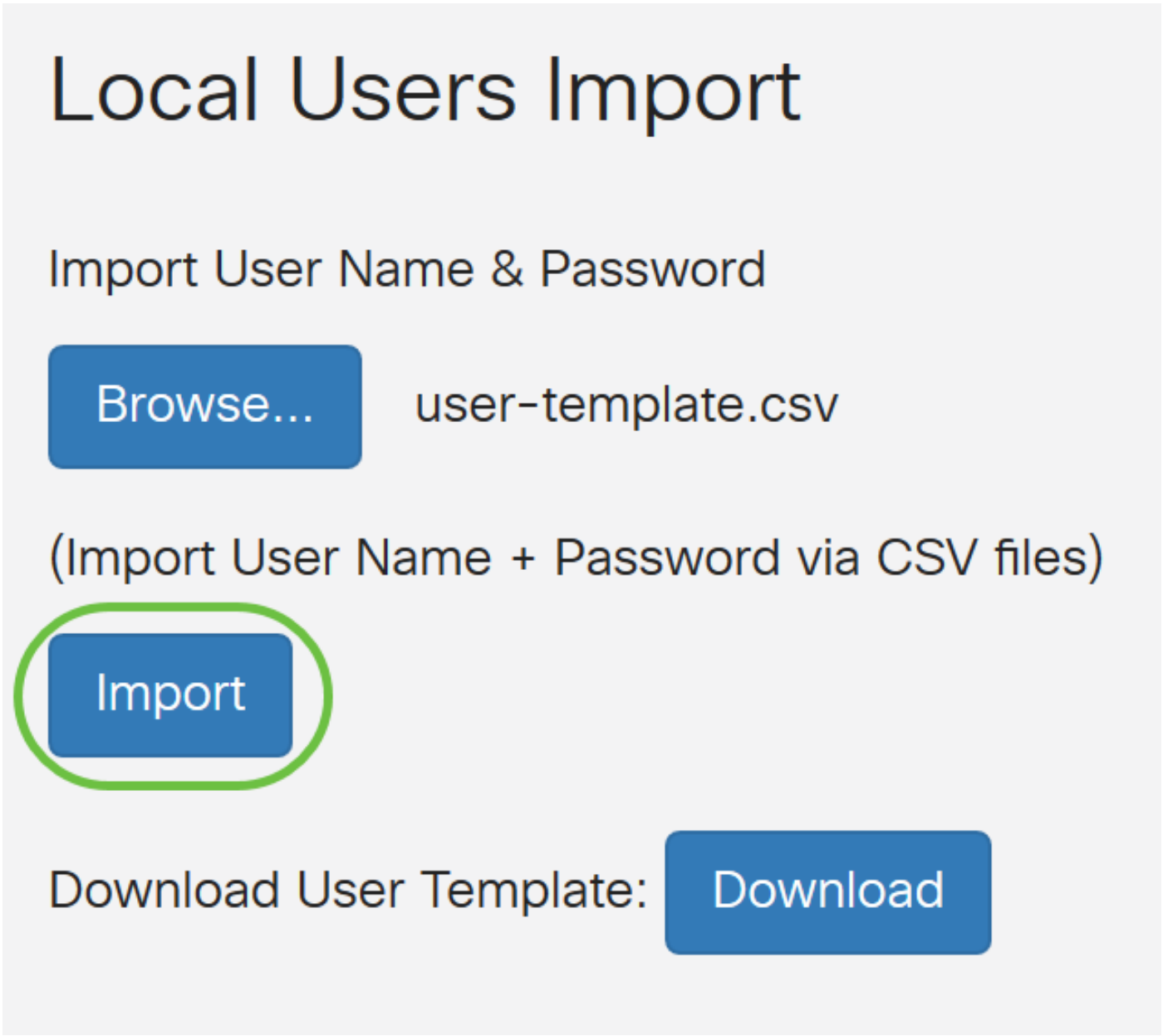
この例では、**user-template.csvが選択さ**れています。



ステップ3: (オプション) テンプレートがない場合は、[Download User Template]領域の[**Download**]をクリックします。



ステップ 4：[Import] をクリックします。



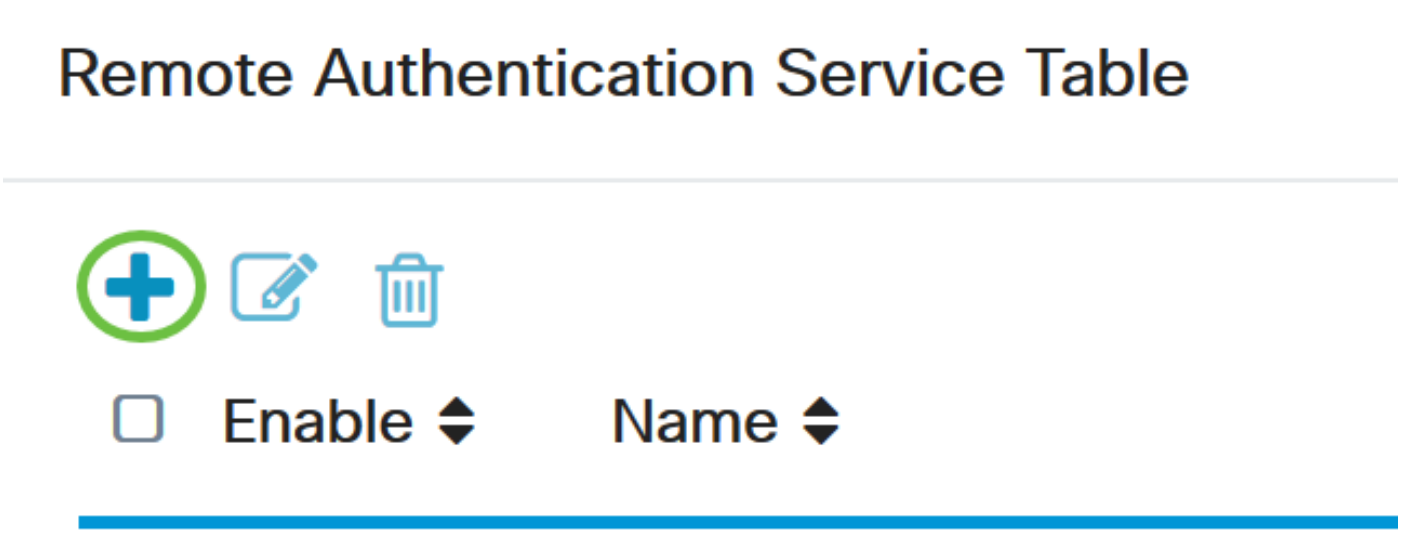
インポートが成功したことを示すメッセージがインポートボタンの横に表示されます。

これで、ローカルユーザのリストが正常にインポートされました。

リモート認証サービスの設定

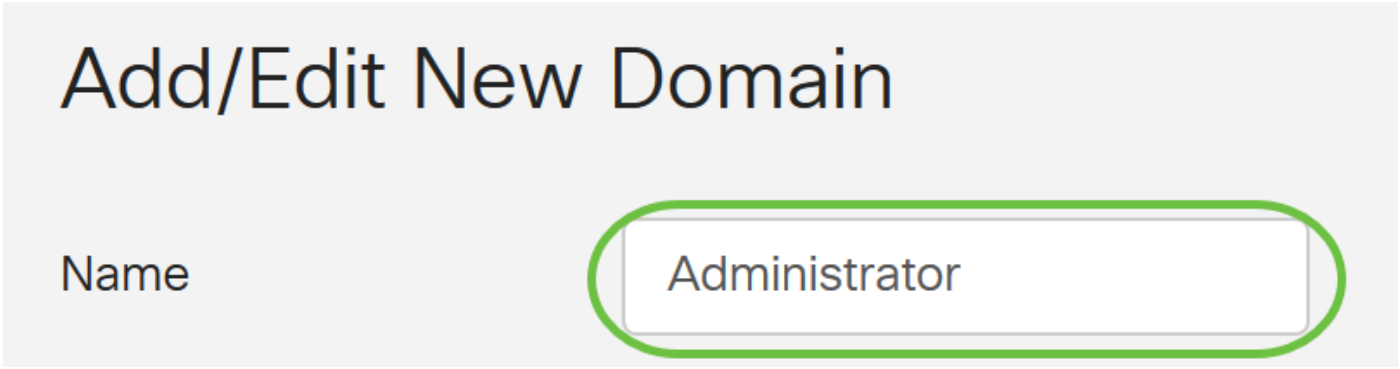
RADIUS

ステップ1:[Remote Authentication Service Table]で、[**Add**]をクリックして**エントリ**を作成します。



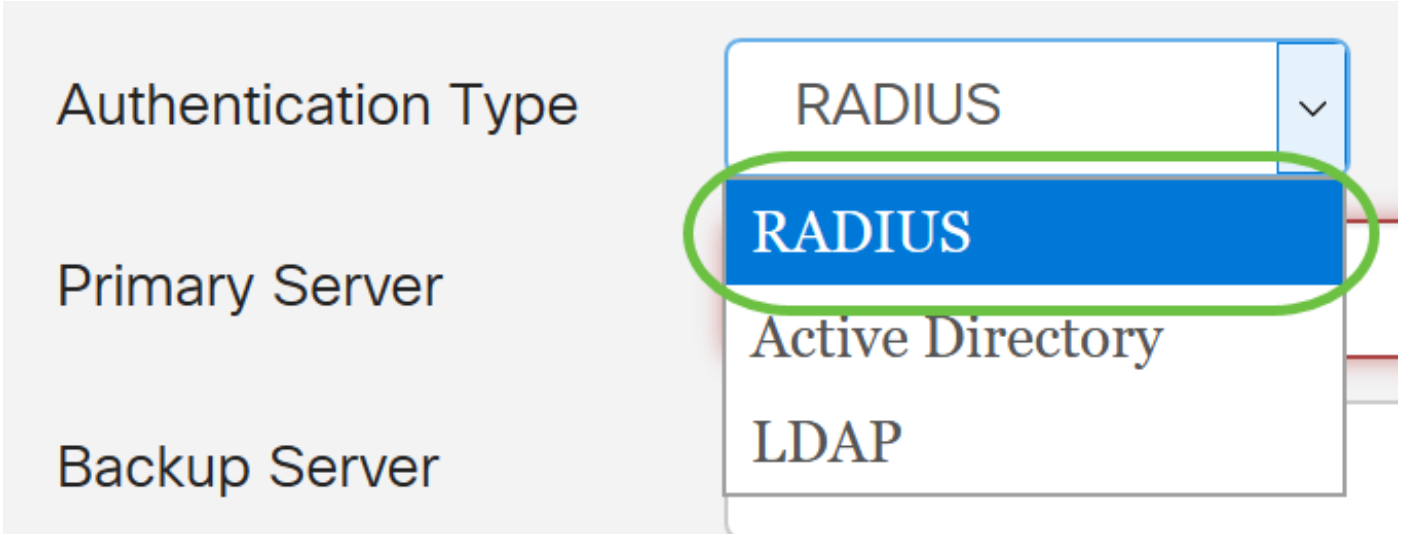
ステップ2:[*Name*]フィールドで、アカウントのユーザ名を作成します。

この例では、管理者**が使用**されます。



ステップ3:[Authentication Type]ドロップダウンメニューから[**Radius**]を選択**します**。つまり、ユーザ認証はRADIUSサーバを介して行われます。

RADIUSで設定できるリモートユーザアカウントは1つだけです。

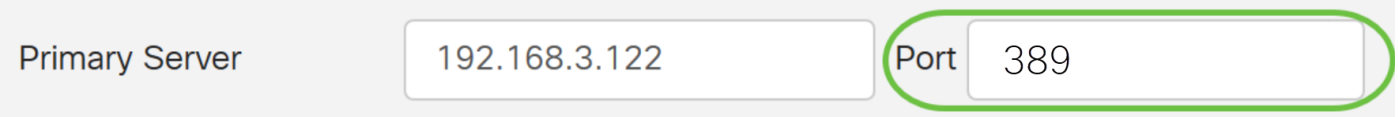


ステップ4:[プライマリ・サーバ]フィールドに、プライマリRADIUSサーバのIPアドレスを入力します。

この例では、プライマリサーバとして192.168.3.122が使用されています。

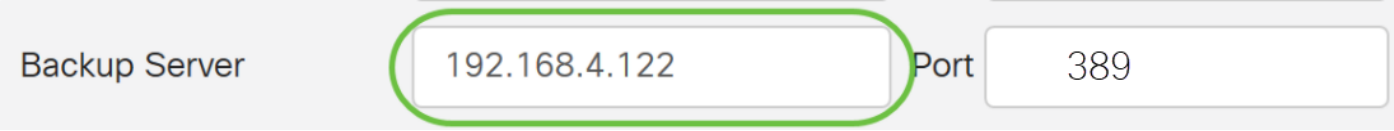
ステップ5:[Port] フィールドに、プライマリRADIUSサーバのポート番号を入力します。

この例では、ポート番号として1645が使用されます。



ステップ6:[*Backup Server*]フィールドに、バックアップRADIUSサーバのIPアドレスを入力します。これは、プライマリサーバがダウンした場合のフェールオーバーとして機能します。

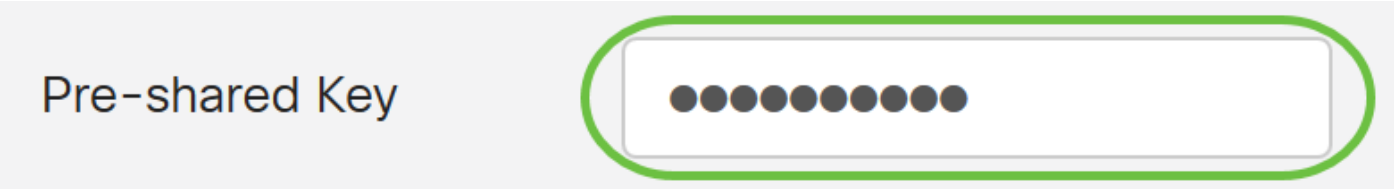
この例では、バックアップサーバのアドレスは192.168.4.122です。



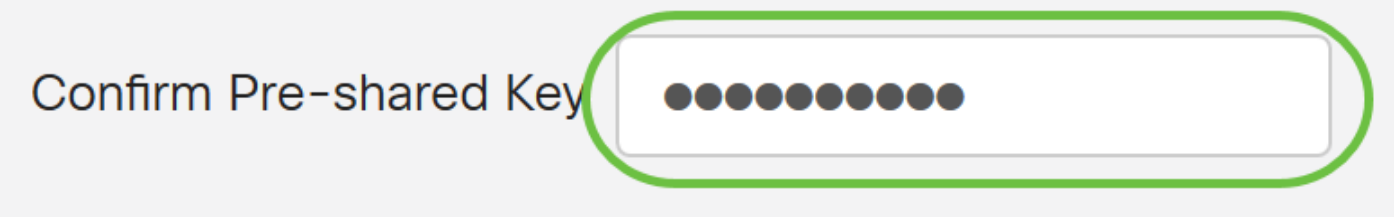
ステップ7:[*Port*]フィールドに、バックアップRADIUSサーバの数を入力します。

この例では、ポート番号として1646が使用されます。

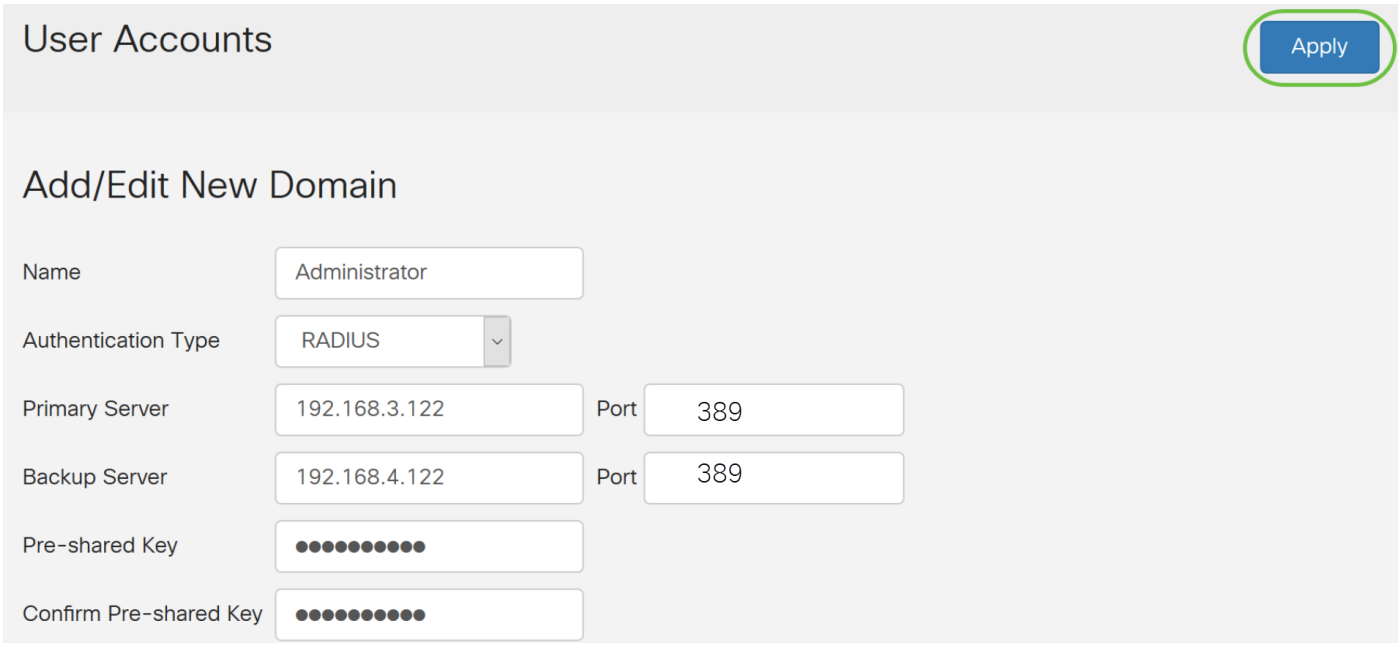
ステップ8:[Preshared-Key] フィールドに、RADIUSサーバで設定された事前共有キーを入力します。



ステップ9:[Confirm *Preshared-key*]フィールドで、事前共有キーを再入力して確認します。



ステップ10:[Apply]をクリックします。

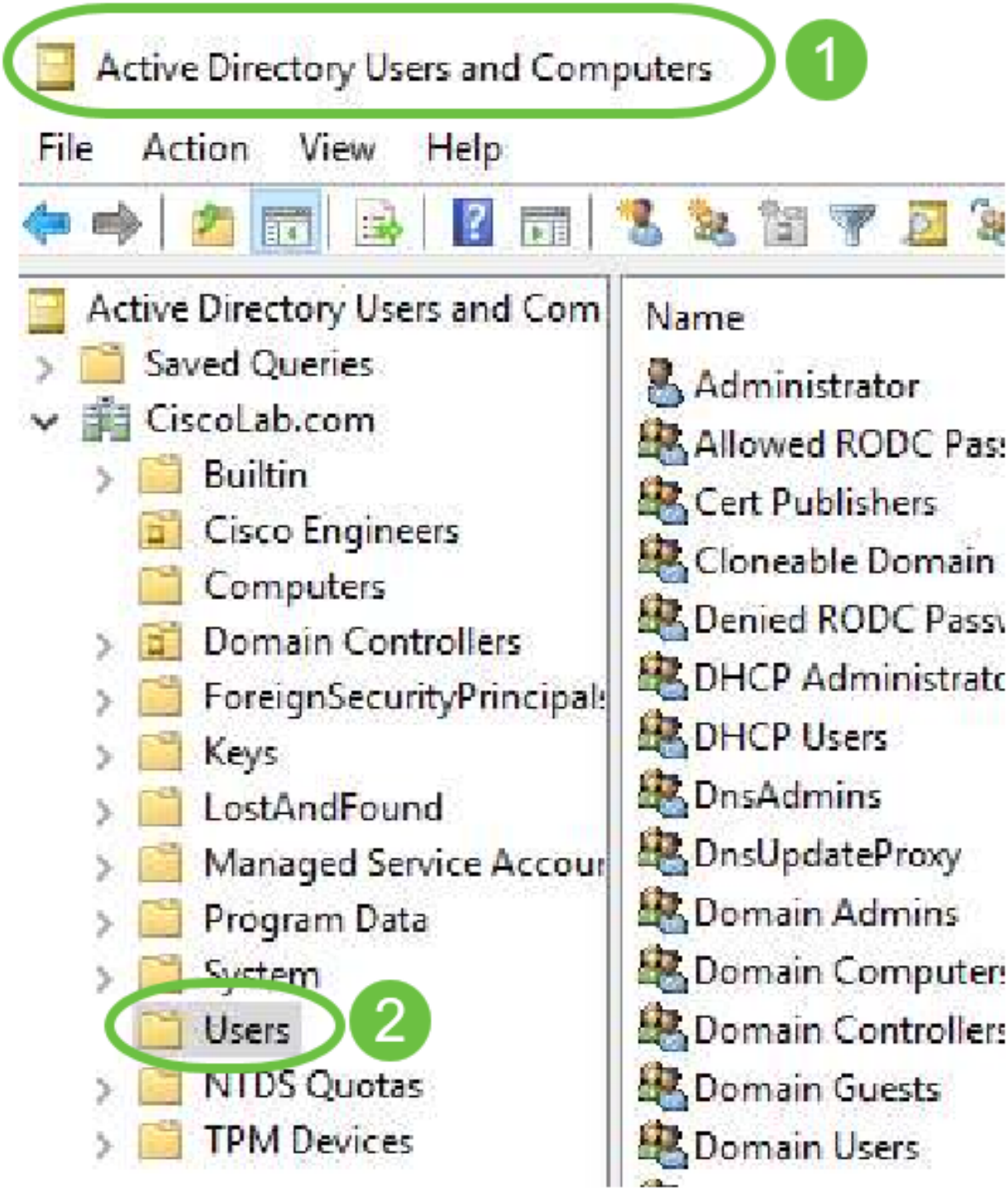


メインユーザアカウントのページが表示されます。最近設定したアカウントが[Remote Authentication Service]テーブルに表示されます。

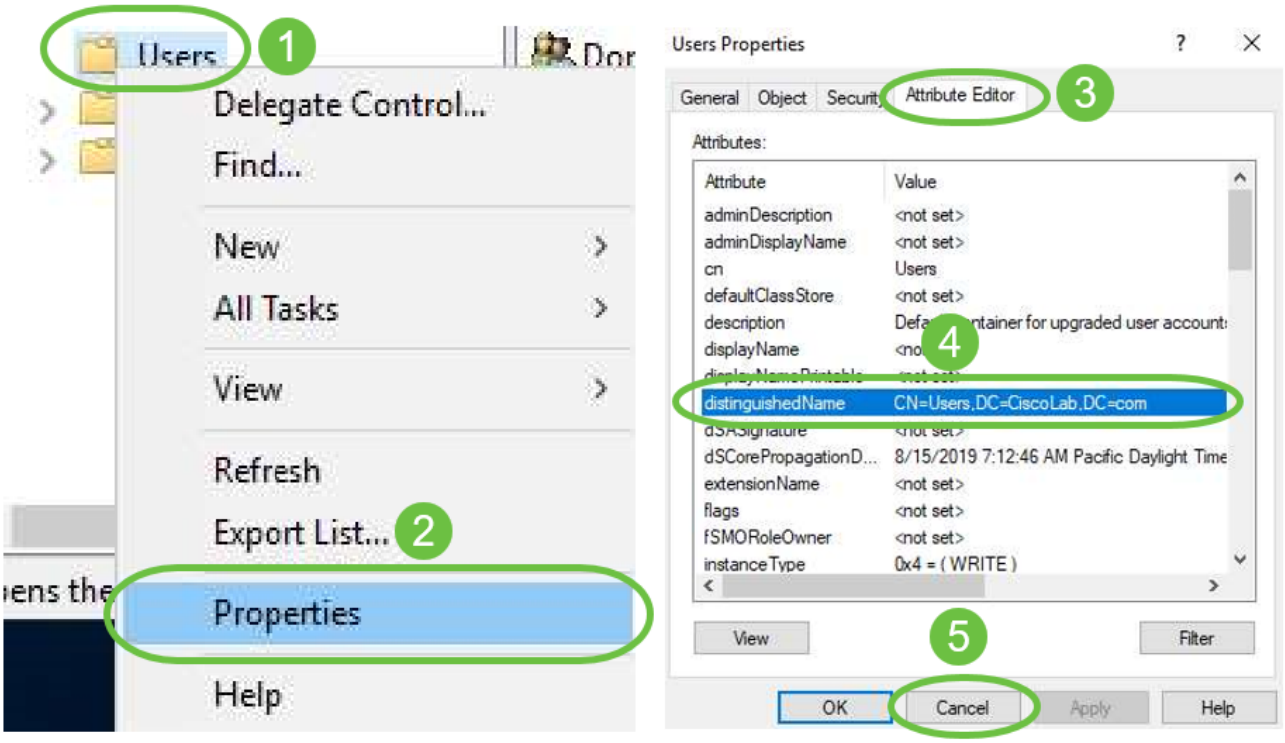
これで、RV34xシリーズルータでRADIUS認証が正常に設定されました。

Active Directoryの設定

ステップ1:Active Directoryの設定を完了するには、Active Directoryサーバにログインする必要があります。PCで**Active Directoryのユーザーとコンピュータを開**き、リモートでログインするために使用するユーザーアカウントがあるコンテナに移動します。この例では、Usersコンテナを使用します。



ステップ2：コンテナを右クリックし、[Properties]を選**択します**。[Attribute Editor]タブに*移動し*、[distinguishedName]フィールドを*探し*ます。このタブが表示されていない場合は、Active Directoryユーザーとコンピューターで拡張機能ビューを有効にし、やり直す必要があります。このフィールドをメモし、[キャンセル]をクリ**ックします**。これはユーザコンテナパスになります。このフィールドは、RV340を設定する際にも必要であり、正確に一致する必要があります。



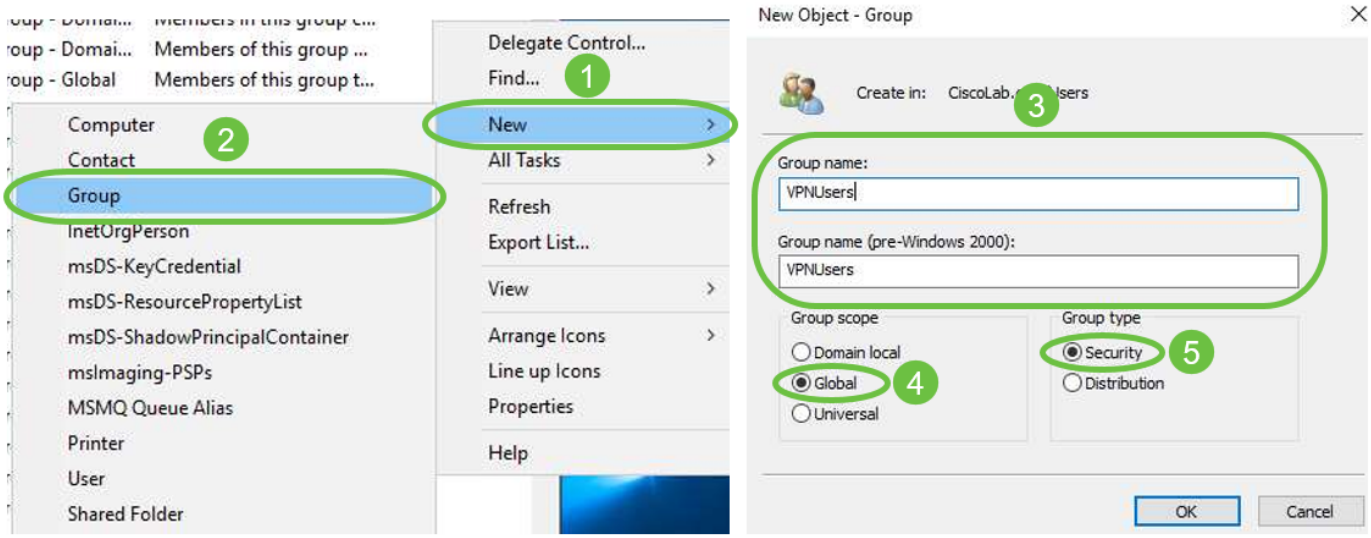
ステップ3：使用するユーザアカウントと同じコンテナにグローバルセキュリティグループを作成します。

選択したコンテナで、空白の領域を右クリックし、「新規」>「グループ」**を選択します。**

次の項目を選択してください。

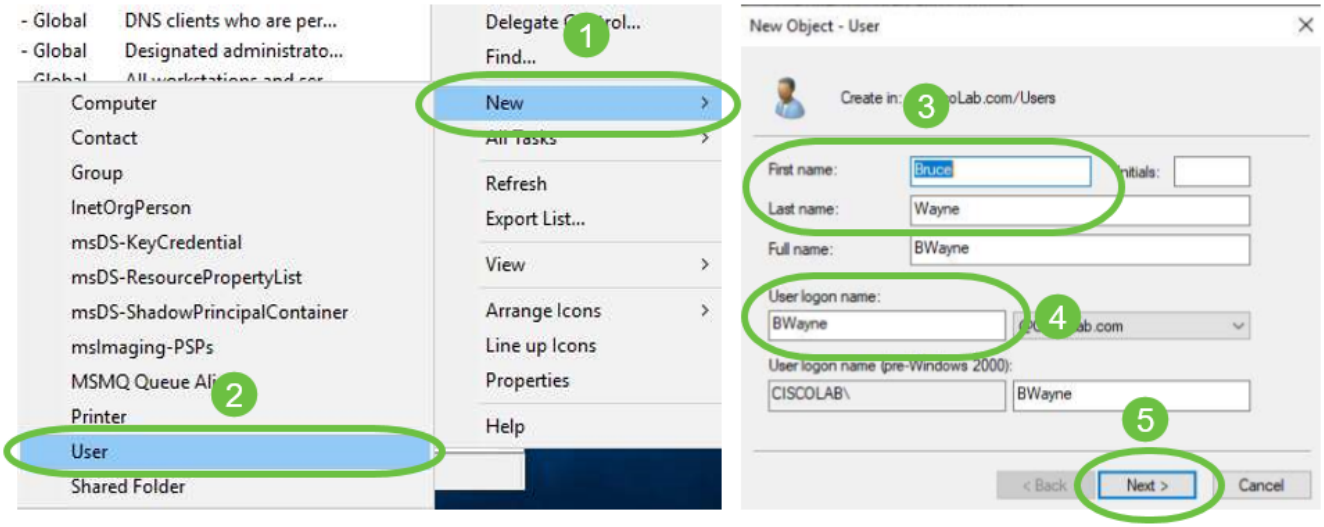
- グループ名：この名前は、RV340で作成されたユーザグループ名と完全に一致している必要があります。この例では、VPNUsersを使用**します。**
- グループスコープ – グローバル
- グループタイプ：セキュリティ

[OK] をクリックします。



ステップ4：新しいユーザアカウントを作成するには、次の手順を実行します。

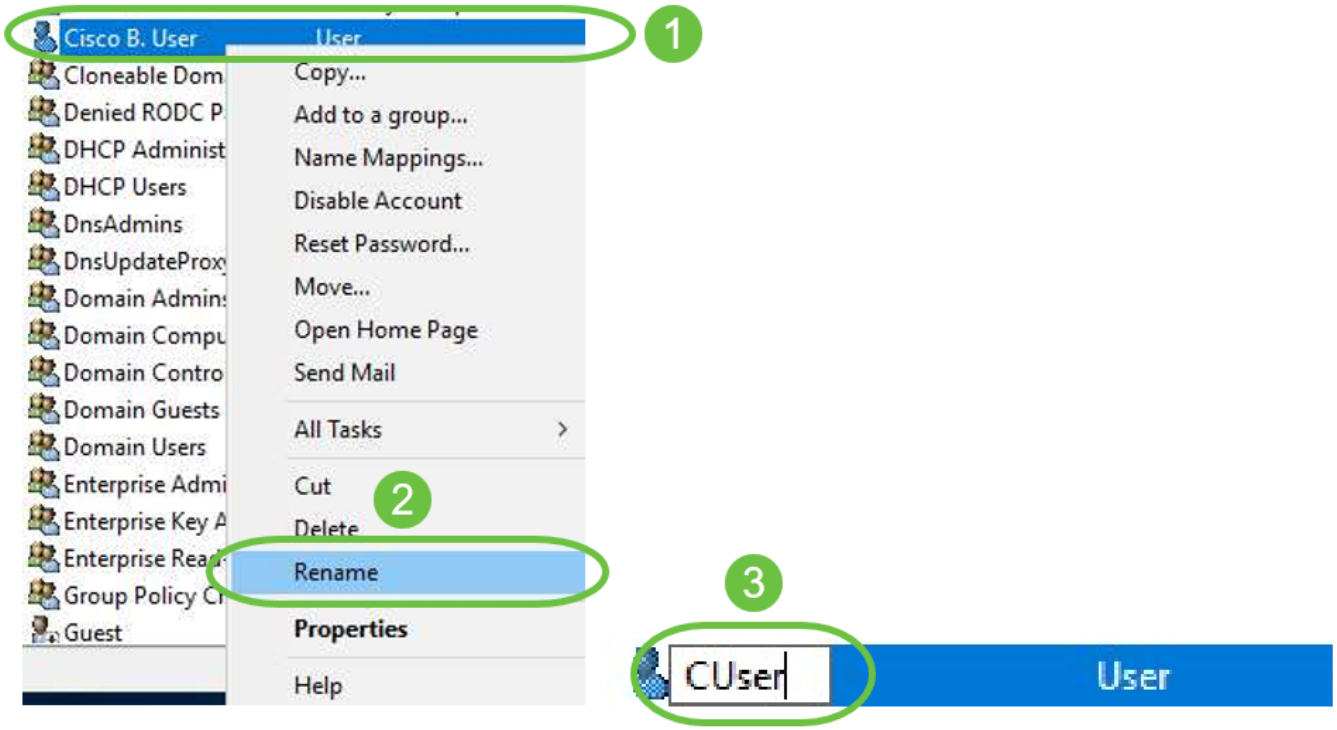
- コンテナ内の空のスペースを右クリックし、「新規」>「ユーザー」を選択します。
- [名 *前*]、*[名*前]を*入力*します。
- ユーザー・ログ*オン名を入力*します。
- [next] をクリックします。



ユーザのパスワードを入力するように求められます。[User must change password at *next logon]ボックスがオンになっている場合*は、リモートでログインする前に、ローカルでログインし、パスワードを変更する必要があります。

[Finish] をクリックします。

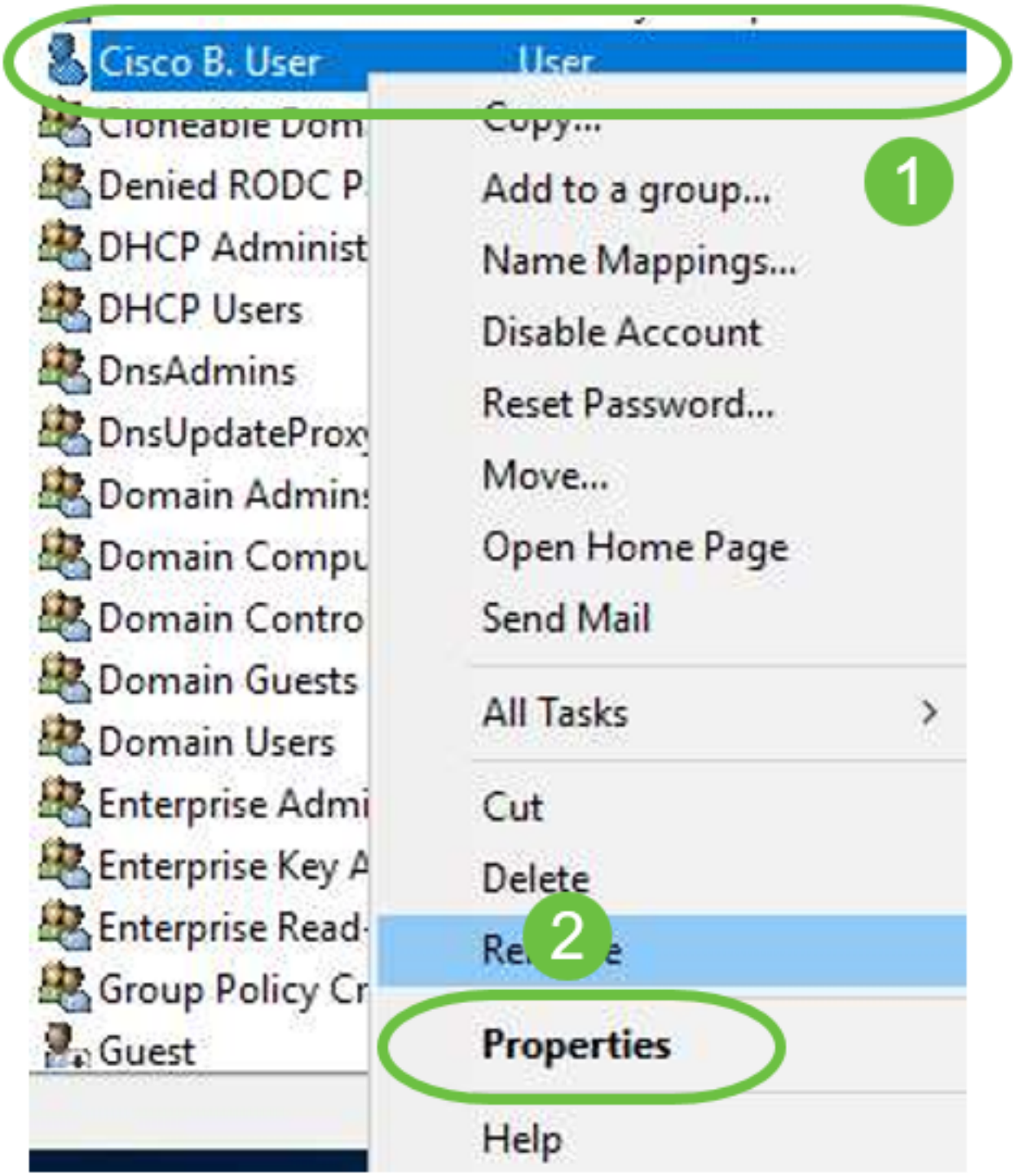
使用する必要のあるユーザーアカウントがすでに作成されている場合は、調整が必要な場合があります。ユーザーの正規名を調整するには、ユーザーを選択し、右クリックして「名前の変更」を**選択します**。すべてのスペースが削除され、ユーザのログオン名と一致していることを確認します。ユーザの表示名は変更されません。[OK] をクリックします。



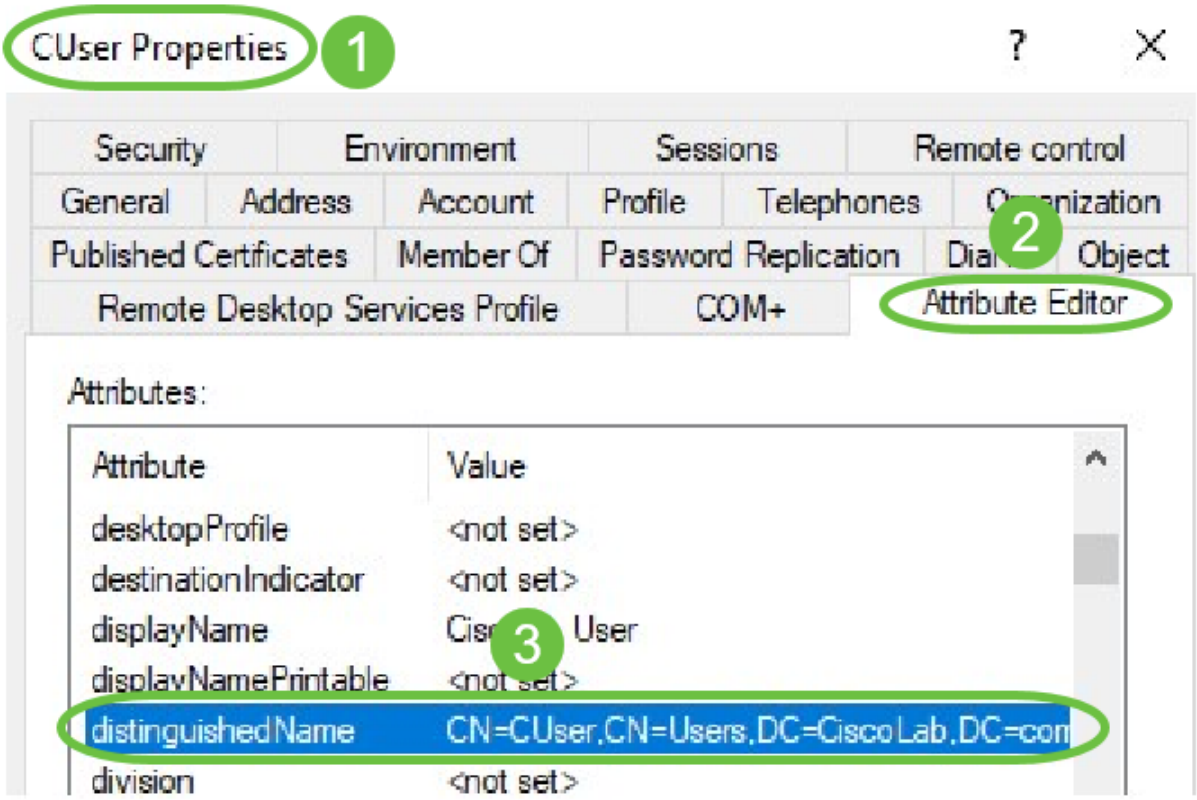
ステップ5：ユーザアカウントが正しく構成されたら、リモートでログインする権限を付与する必

要があります。

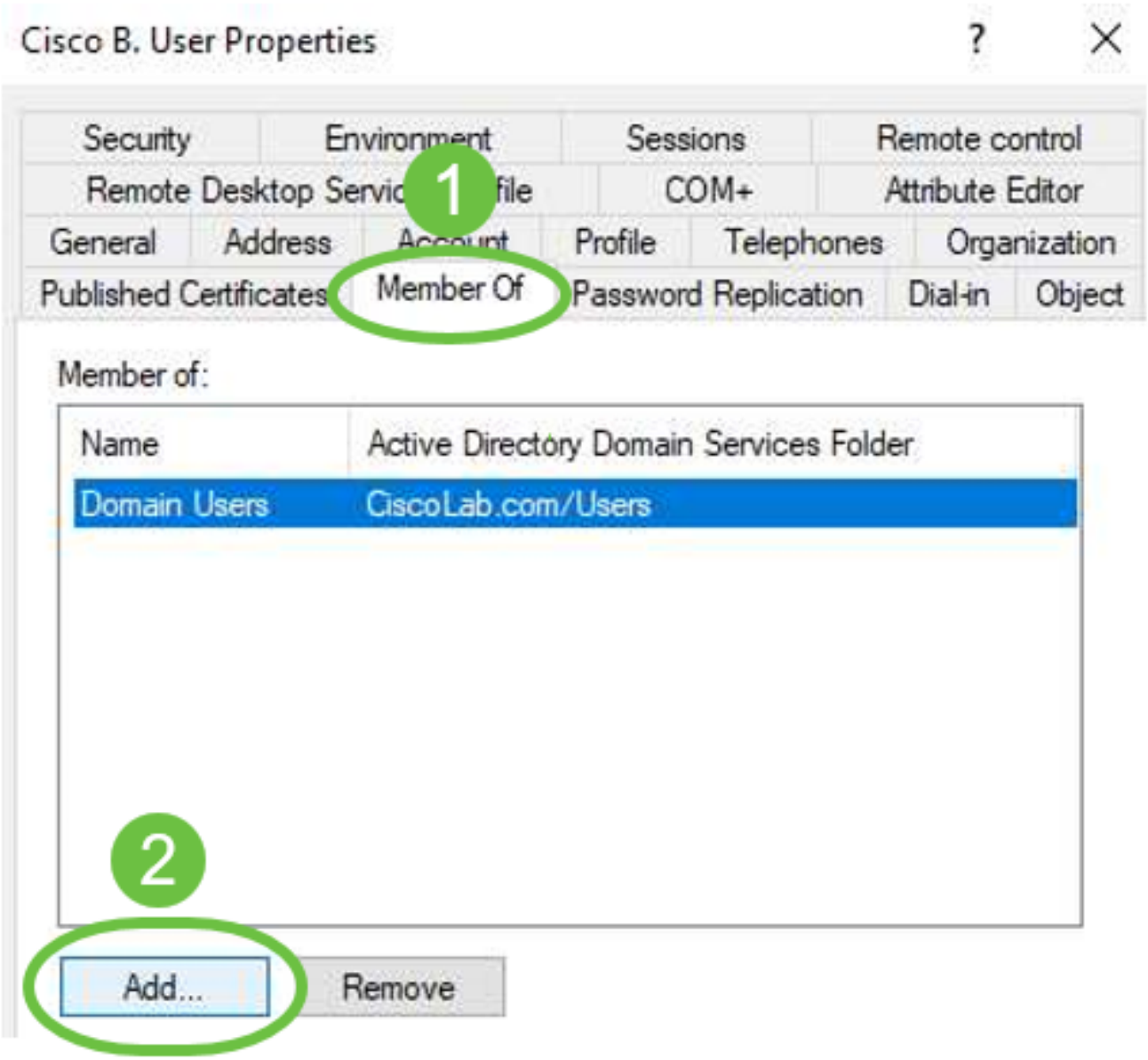
そのためには、ユーザーアカウントを選択し、右クリックして[プロパティ]を**選択します**。



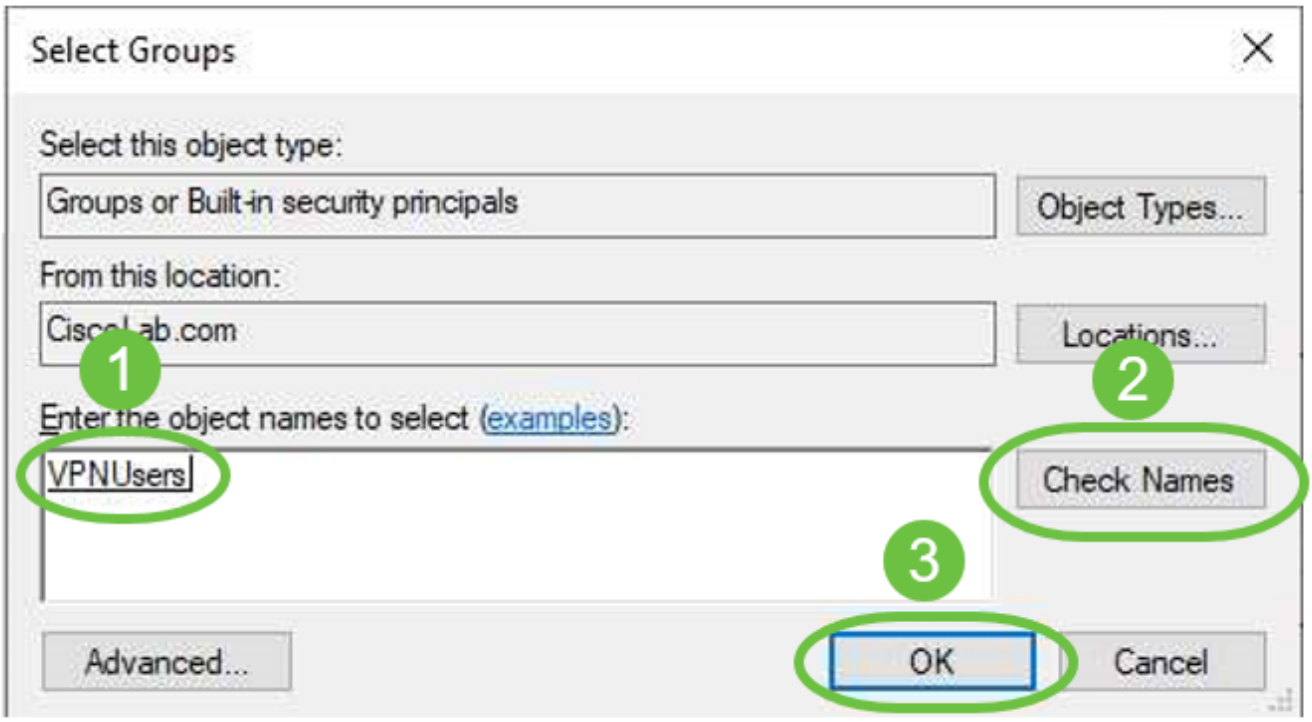
[ユーザプロパティ]で[属性**エディタ**]タブを選択し、[*distinguishedName*]までスクロールダウンします。最初の*CN=*にスペースを含まない*正しい*ユーザログオン名があることを確認してください。



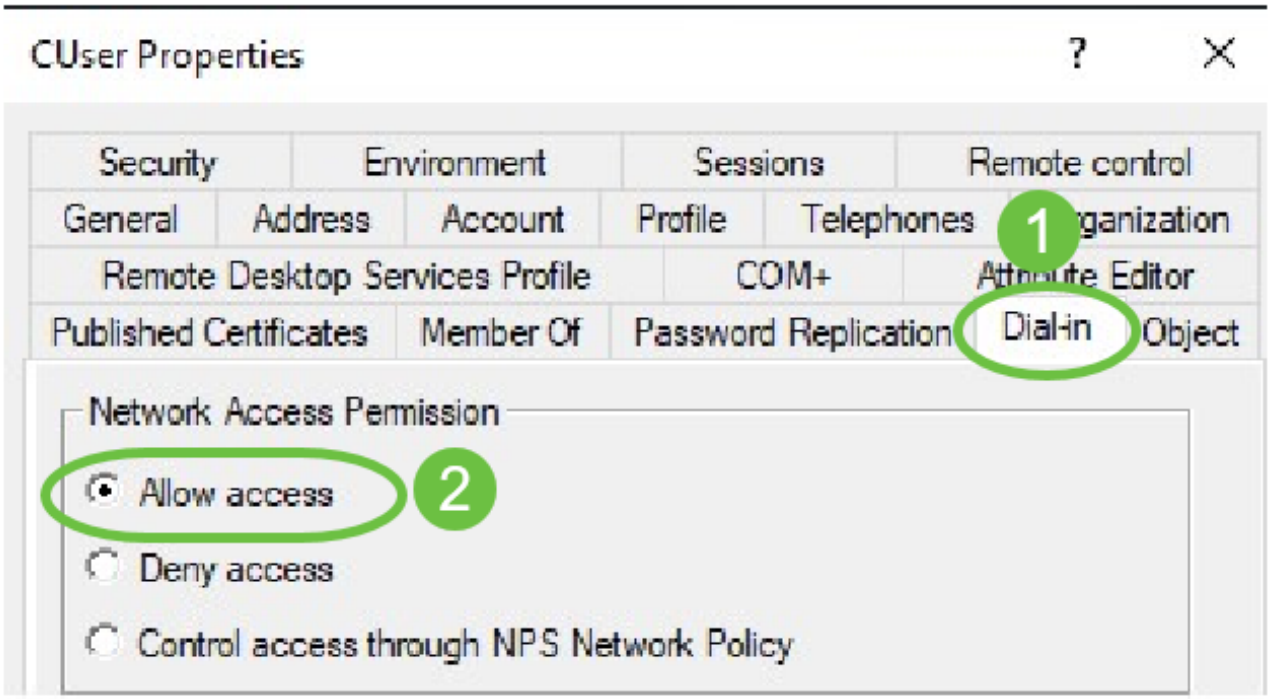
[メンバーの]タブを選択し、[追加]をクリックします。



グローバルセキュリティグループの名前を入力し、*[*Check **Name]*を**選択します**。エントリに下線が引かれている場合は、「**OK**」をクリ**ックします**。



[ダイヤルイン]**タブを選択**します。[ネットワークアクセス*許可*]セクションの[アクセスを許可]**を選択**し、残りの項目は既定のままにします。

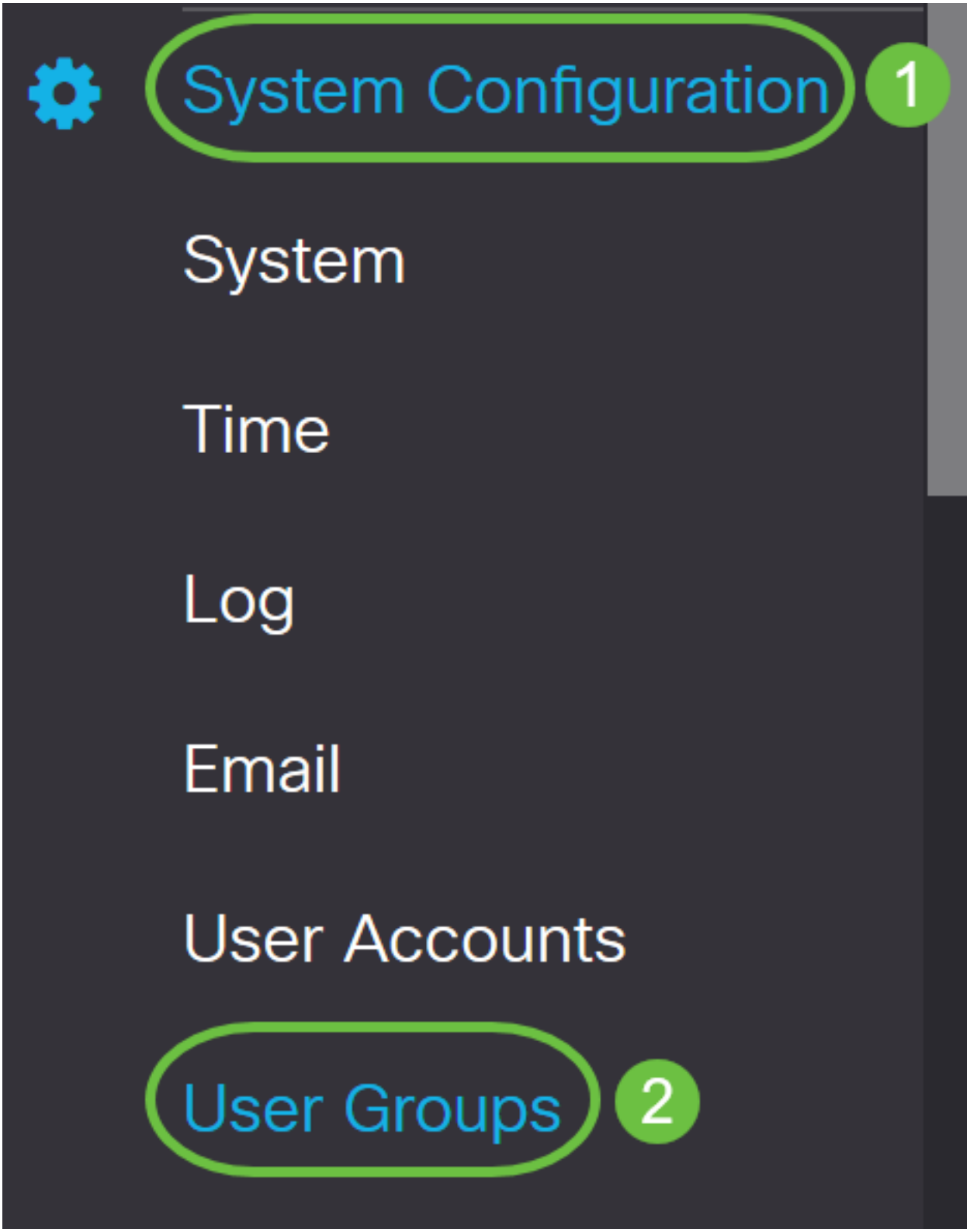


Active Directory統合

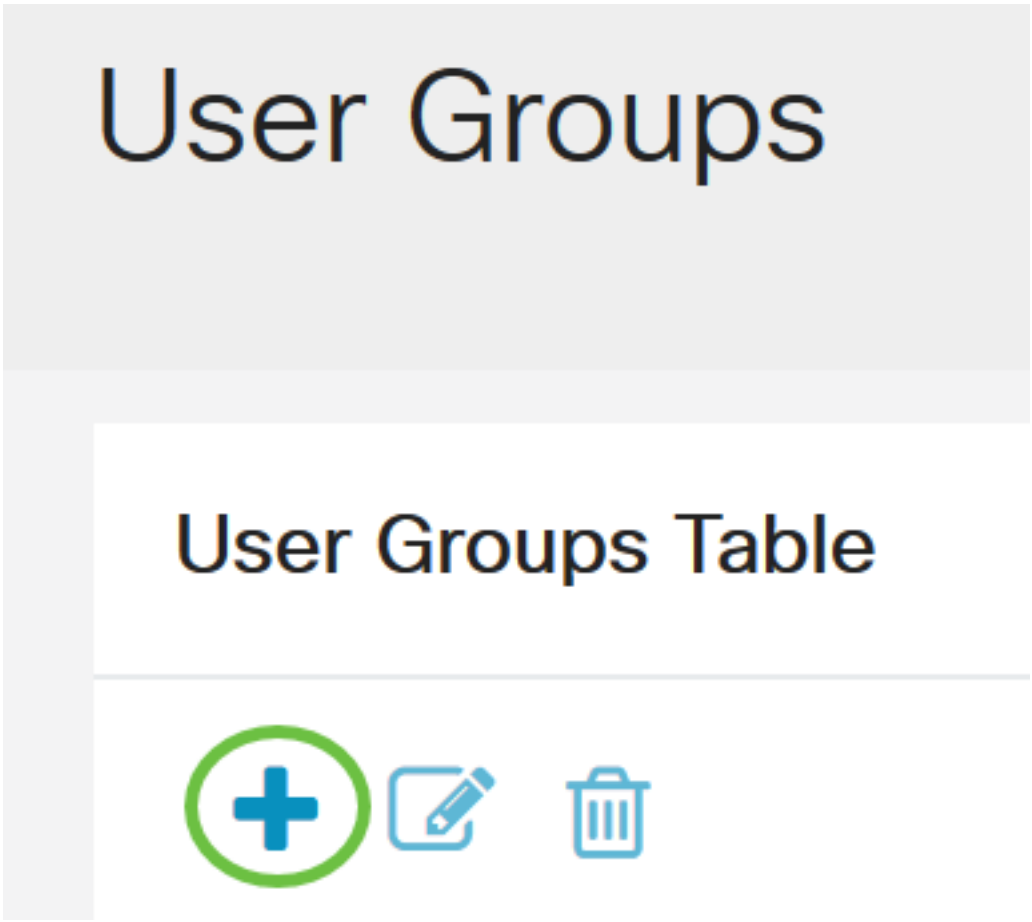
Active Directoryでは、RV34xルータの時刻がADサーバの時刻と一致している必要があります。RV34xシリーズルータの時刻設定の手順については、ここをクリックしてください。

ADでは、RV340にADグローバルセキュリティグループと一致するユーザグループが必要です。

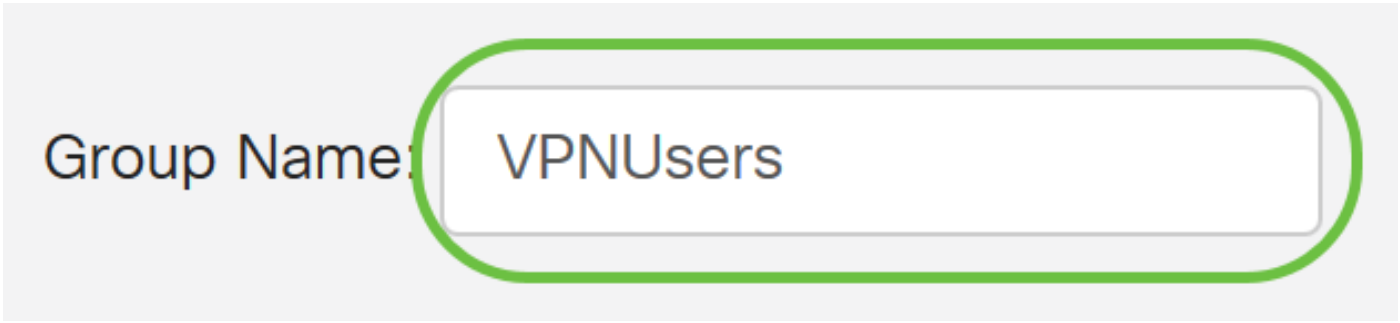
ステップ1:[System Configuration] > **[User Groups]に移動します。**



ステップ2:[+]アイコンをクリック**して**ユーザグループを追加します。

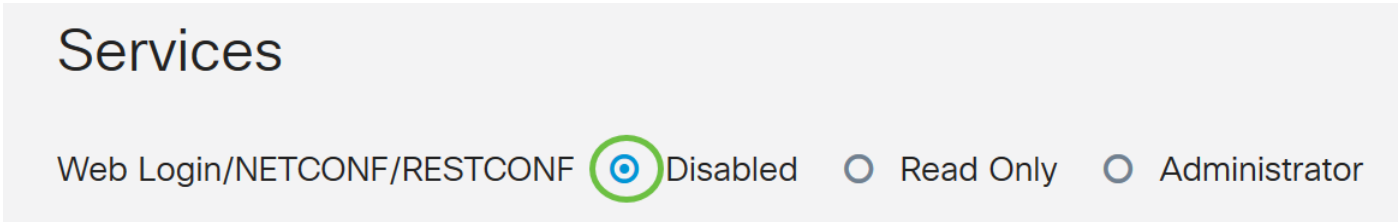


ステップ3：グループ名を*入力します*。この例では、VPNUsers**です**。



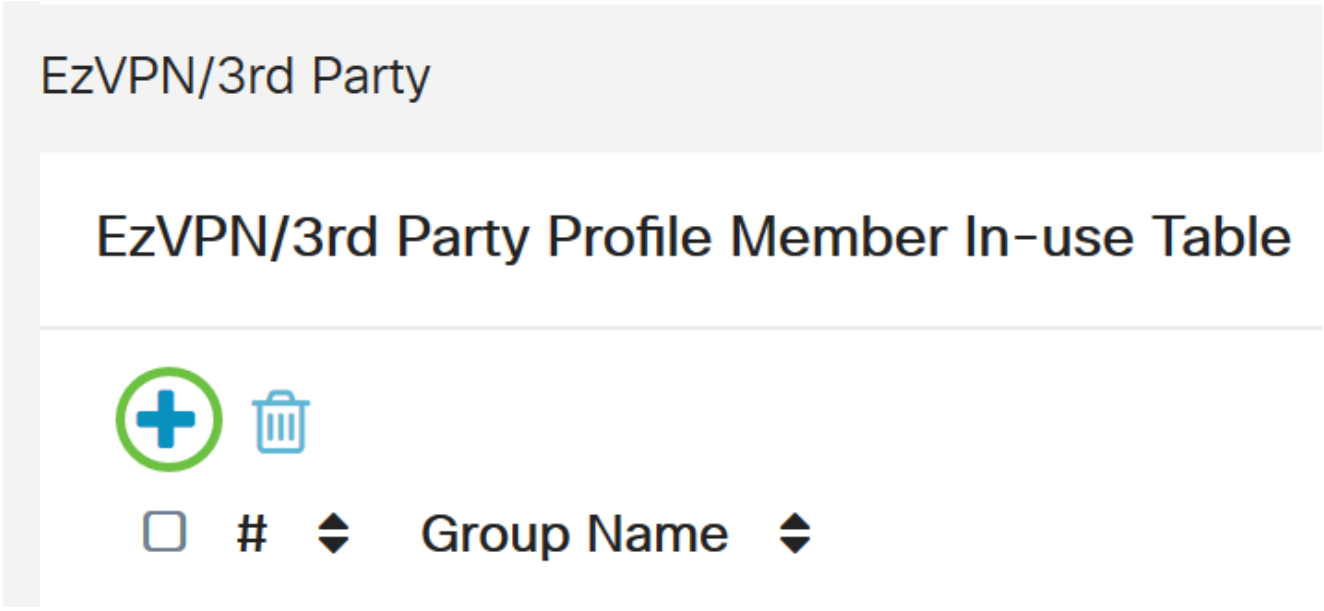
グループ名は、ADグローバルセキュリティグループとまったく同じでなければなりません。

ステップ4:[*Services*]の[*Web Login/NETCONF/RESTCONF*]を[**Disabled**]とマークする必要があります。AD統合がすぐに機能しない場合でも、RV34xにアクセスできます。

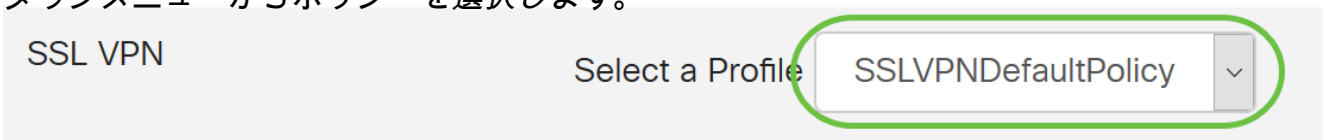


ステップ5:AD統合を使用してユーザをログインするVPNトンネルを追加できます。

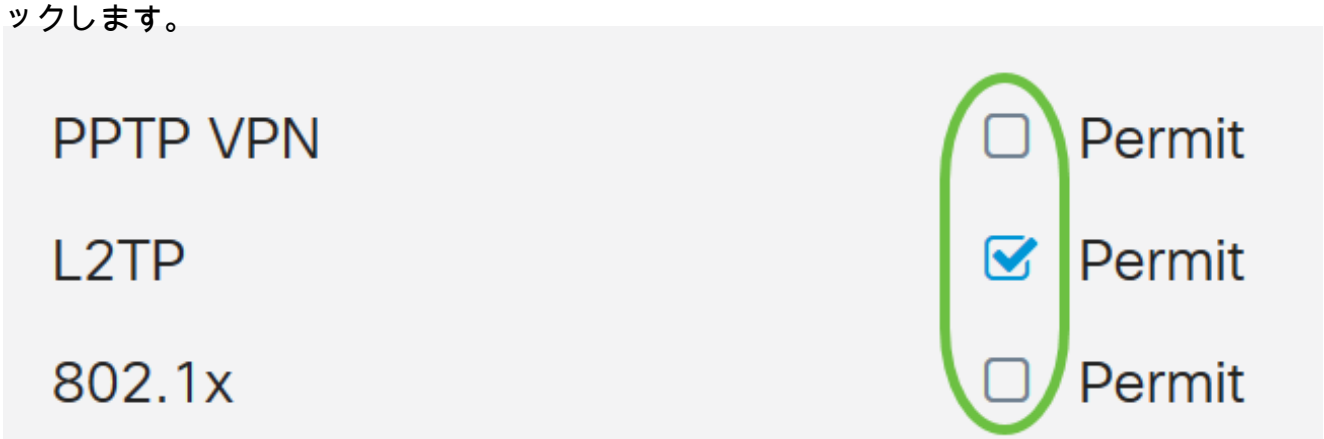
1. すでに設定されているクライアントからサイトへのVPNを追加するには、[*EZVPN/3rd Party*]*セクションに移動*し、プラスのアイコンを**クリック**します。ドロップダウンメニューからVPNプロファイルを選択し、[**Add**]をクリ**ックします**。



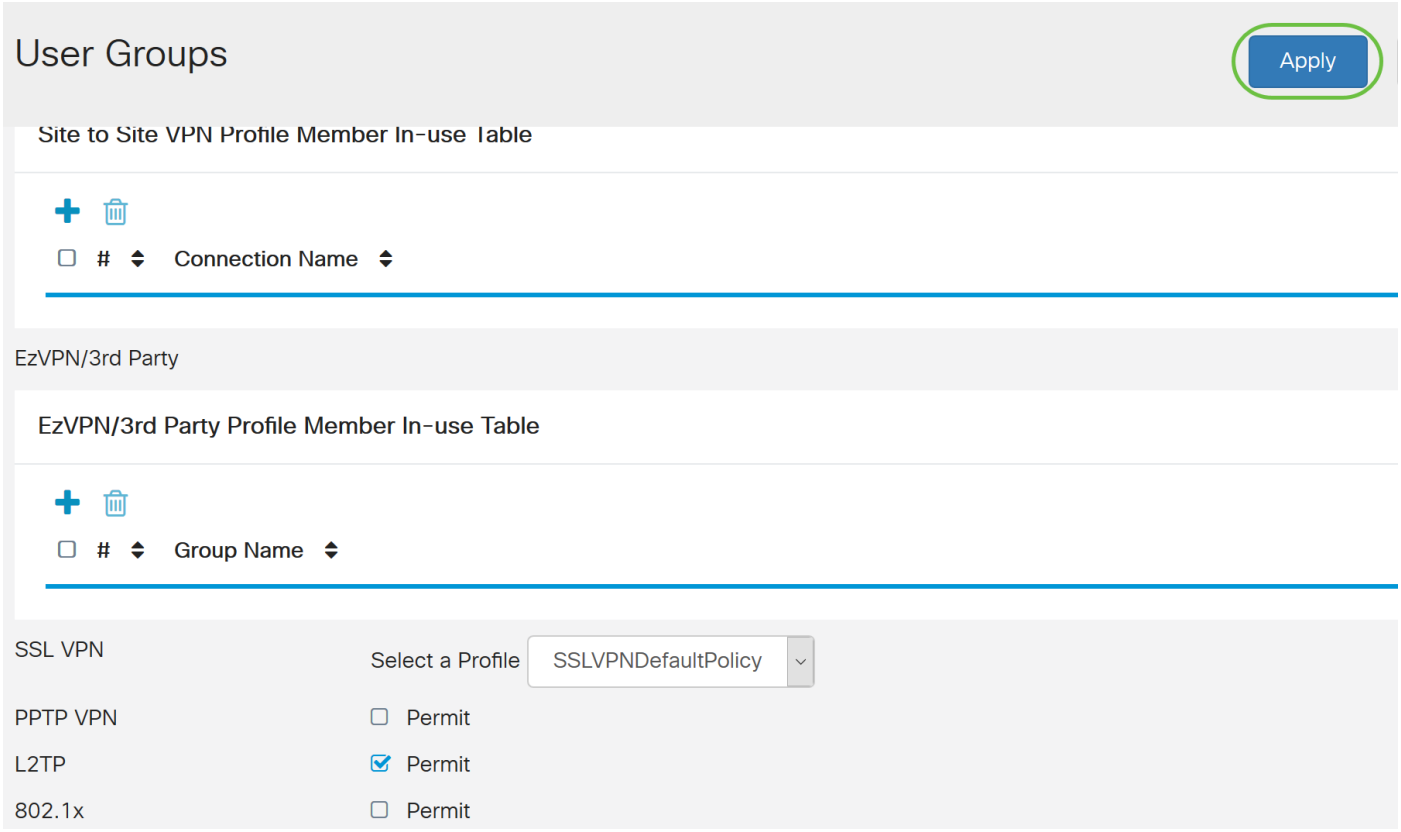
4. SSL VPN - SSL VPNトンネルを使用する場合は、[プロファイルの選択]の横にあるドロップダウンメニューからポリシーを*選択します*。



6. PPTP/L2TP/802.1x:ADの使用を許可するには、[*Permit*]の横にあるチェックボックスをクリックします。

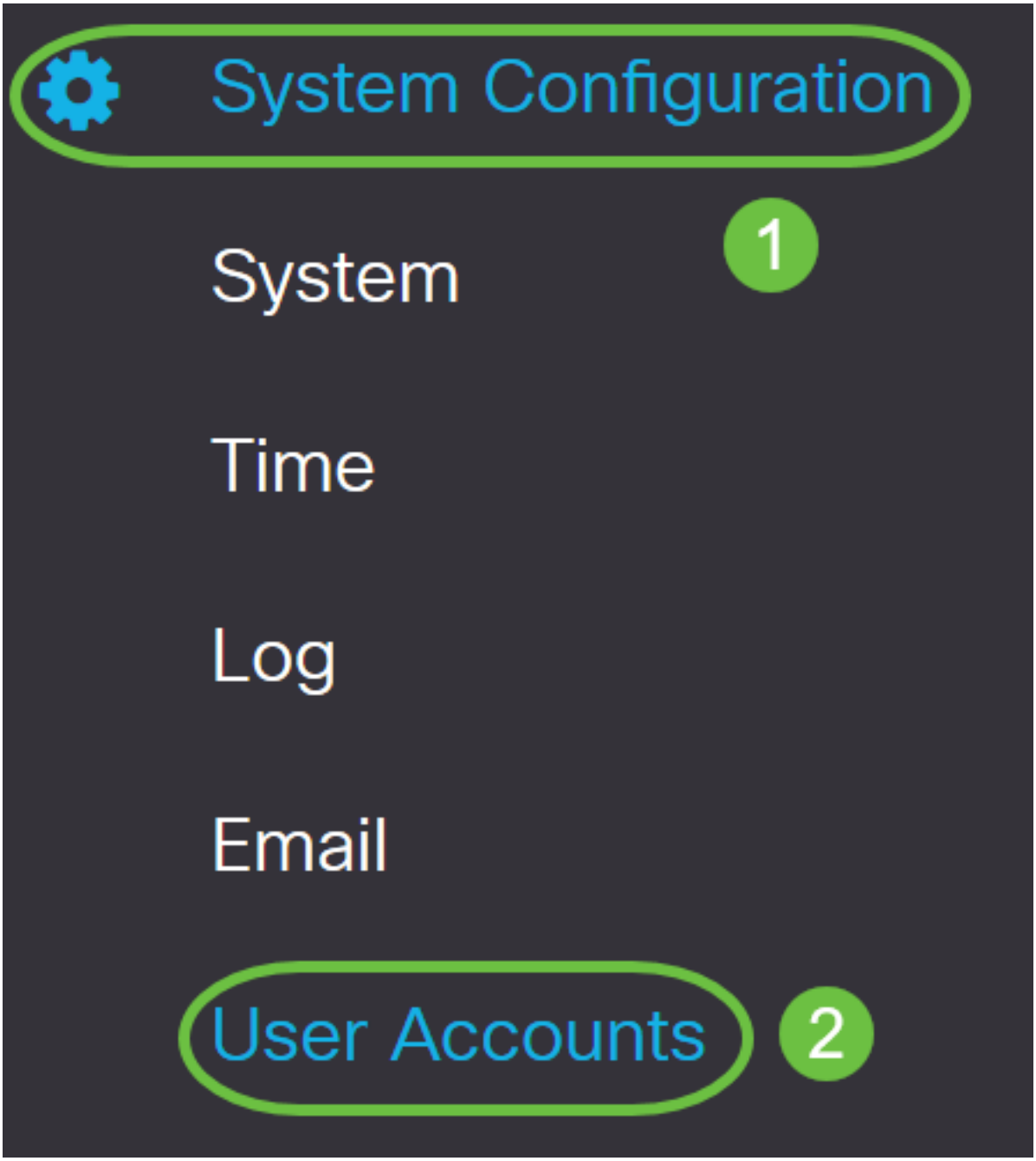


ステップ6:[Apply]をクリックして変更を保存します。

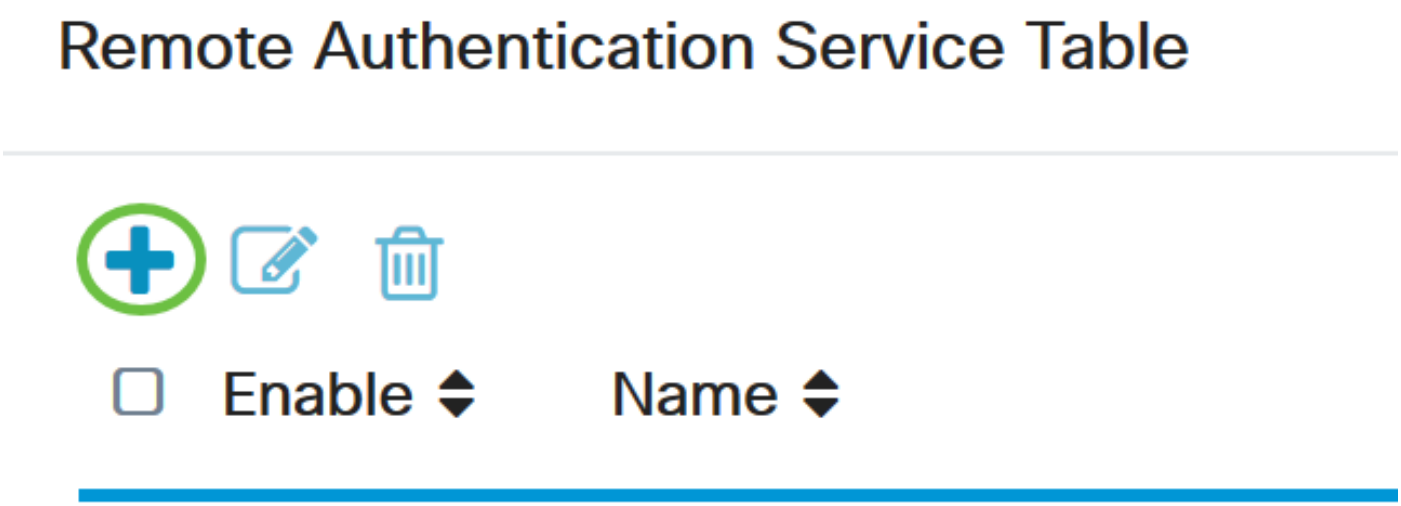


Active Directory統合設定

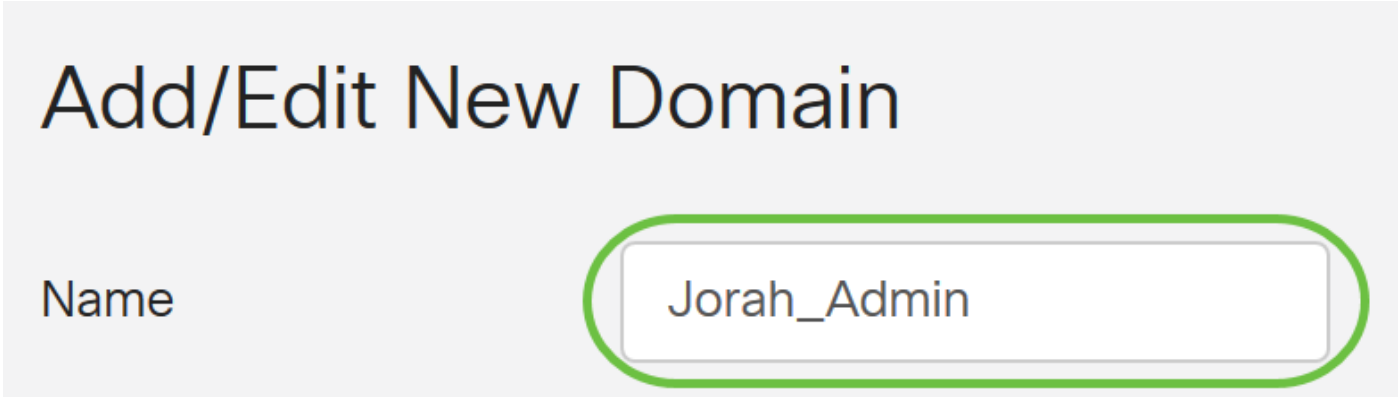
ステップ1:[System Configuration] > [User Accounts]に移動します。



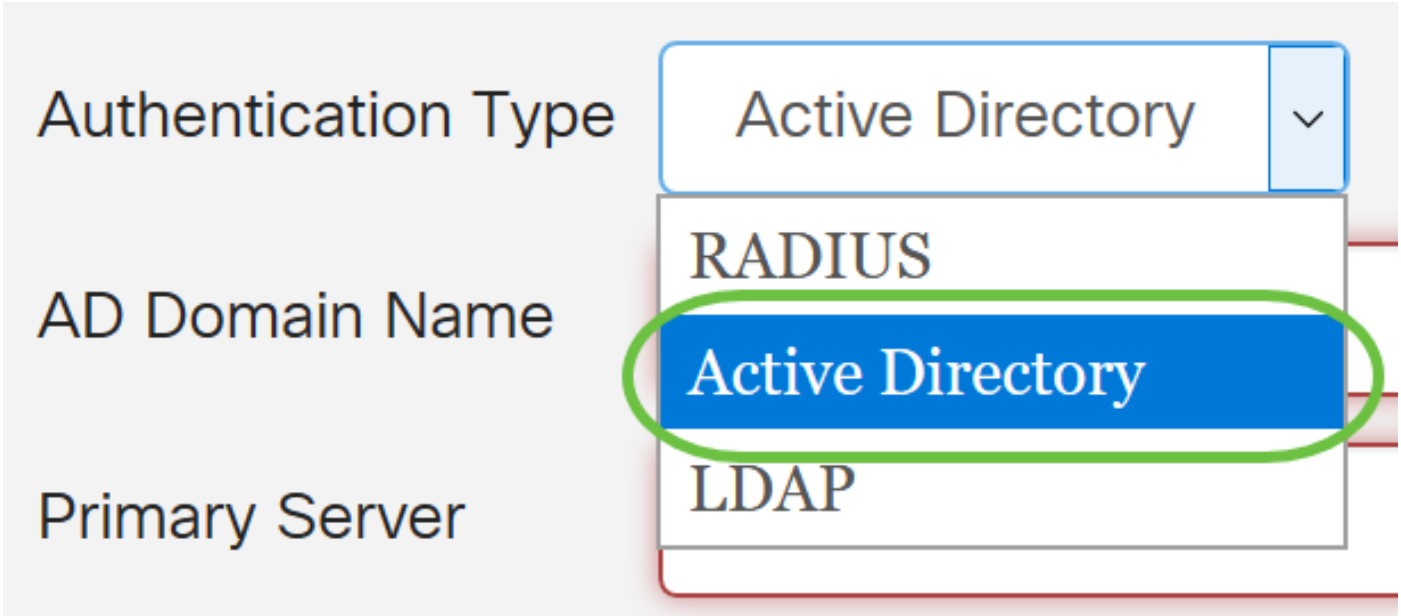
ステップ2:[Remote Authentication Service Table]で、[**Add**]をクリックして**エントリ**を作成します。



ステップ3:[*Name*]フィールドで、アカウントのユーザ名を作成します。この例では、**Jorah_Adminが使用**されています。

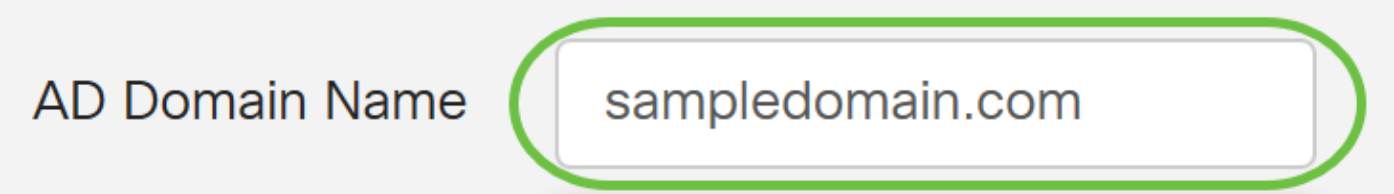


ステップ4:[*Authentication Type*]ドロップダウンメニューから、[**Active Directory**]を**選択します**。ADは、ネットワークのすべての要素に幅広いポリシーを割り当て、多くのコンピュータにプログラムを展開し、組織全体に重要な更新を適用するために使用されます。



ステップ5:[*AD Domain Name*]フィールドに、ADの完全修飾ドメイン名を入力します。

この例では、**sampledomain.comが使用**されます。

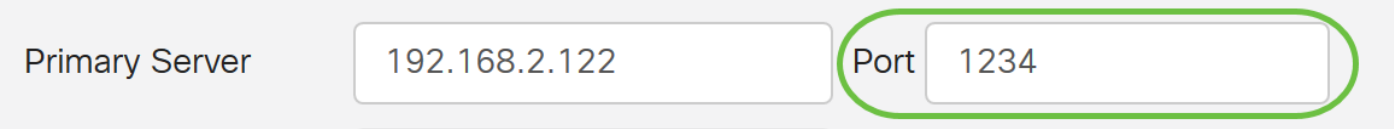


ステップ6:[プライマリ・サーバ]フィールドに、ADのアドレスを入力します。

この例では、**192.168.2.122が使用**されます。

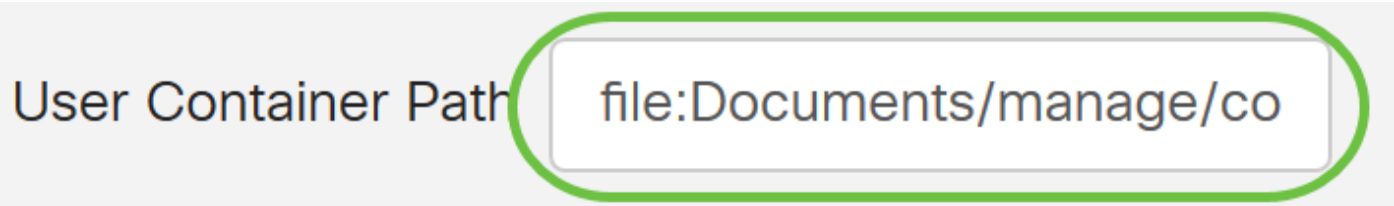
ステップ7:[ポート]フィールドに、プライマリサーバのポート番号を入力します。

この例では、ポート番号**として**1234が使用されています。

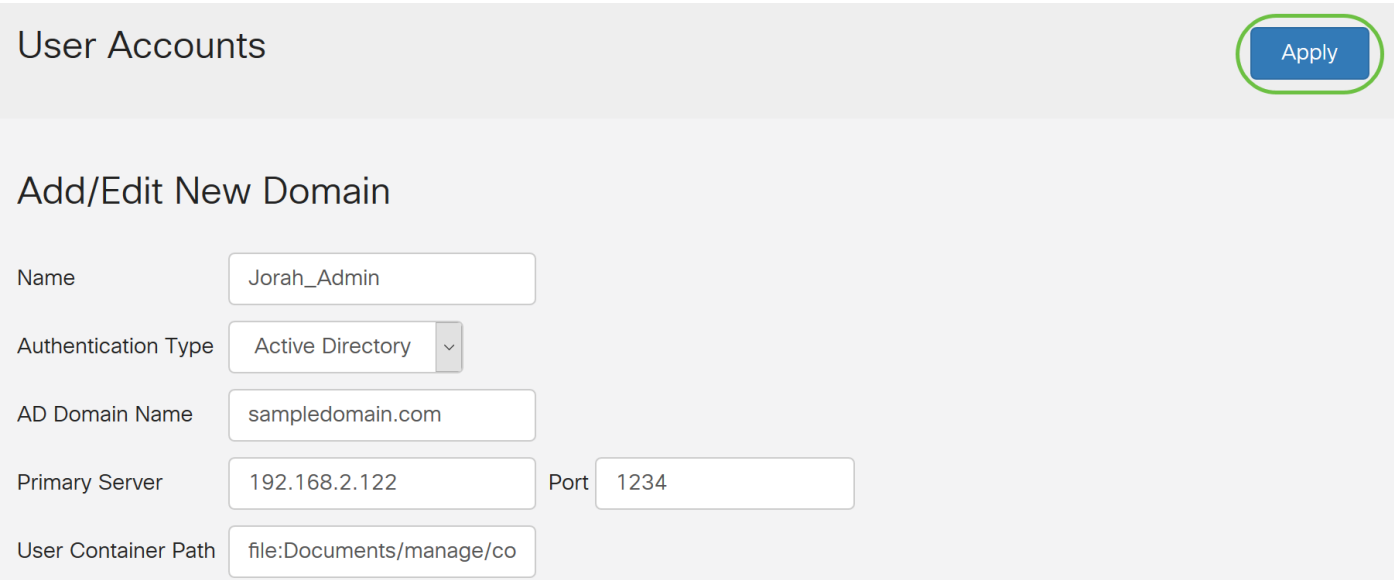


ステップ8:（オプション）[ユーザコンテナパス*(User Container Path)*]フィールドに、ユーザが含まれるルートパスを入力します。

注：この例では、file:Documents/manage/containersが使用されています。



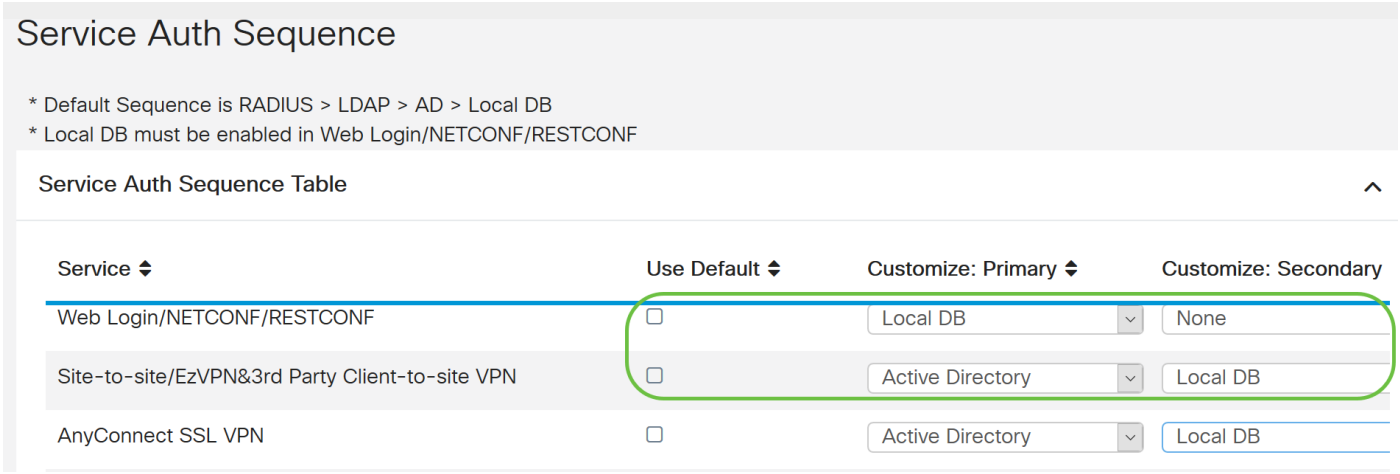
ステップ9:[Apply]をクリック**します。**



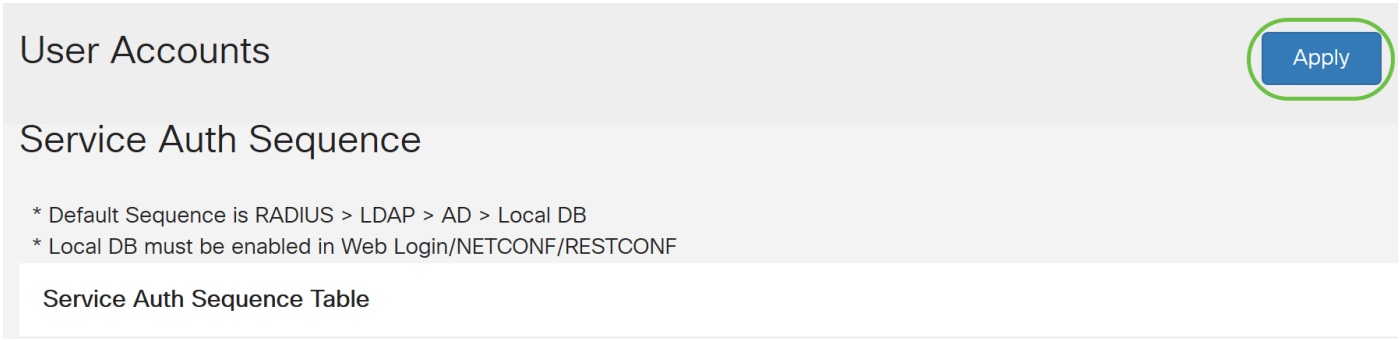
ステップ10:[Service Auth Sequence]までスクロールダウンして、さまざまなオプションのログイ

ン方式を設定します。

- Web Login/NETFCONF/RESTCONF:RV34xルータへのログイン方法です。[デフォルトを使用]チェックボックスをオフにし、[Primary method]を[**Local DB**]に**設定します**。これにより、Active Directory統合が失敗しても、ルータからログアウトされなくなります。
- Site-to-site/EzVPN&Rd Party Client-to-site VPN:ADを使用するようにClient-to-Site VPNトンネルを設定します。[Use Default]チェックボックスをオフにし、[Primary method]を[**Active Directory**]、[Secondary Method]を[**Local DB**]に設定**します**。



ステップ11:[Apply]をクリック**します**。

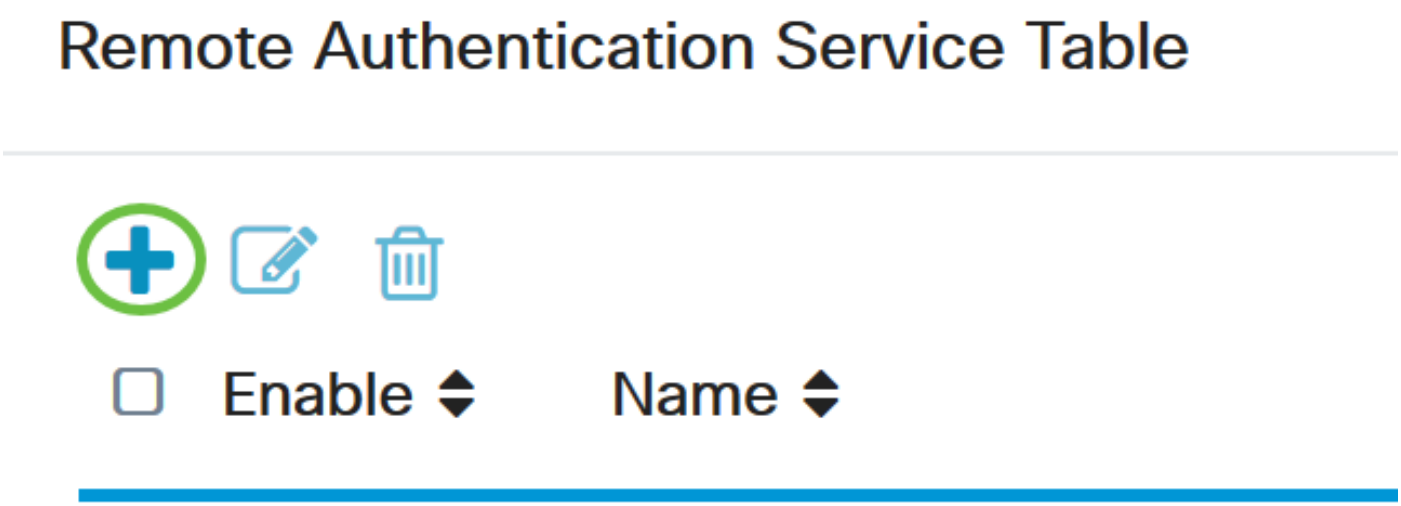


ステップ12：実行コンフィギュレーションをスタートアップコンフィギュレーションに保存します。

これで、RV34xシリーズルータのActive Directoryの設定が正常に完了しました。

[LDAP]

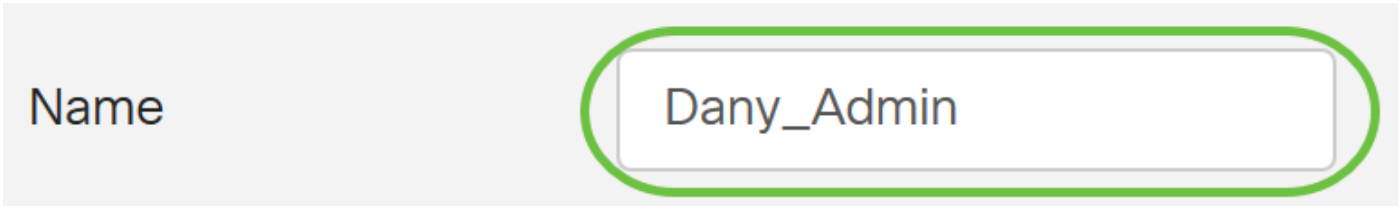
ステップ1:[Remote Authentication Service Table]で、[**Add**]をクリックして**エントリ**を作成します。



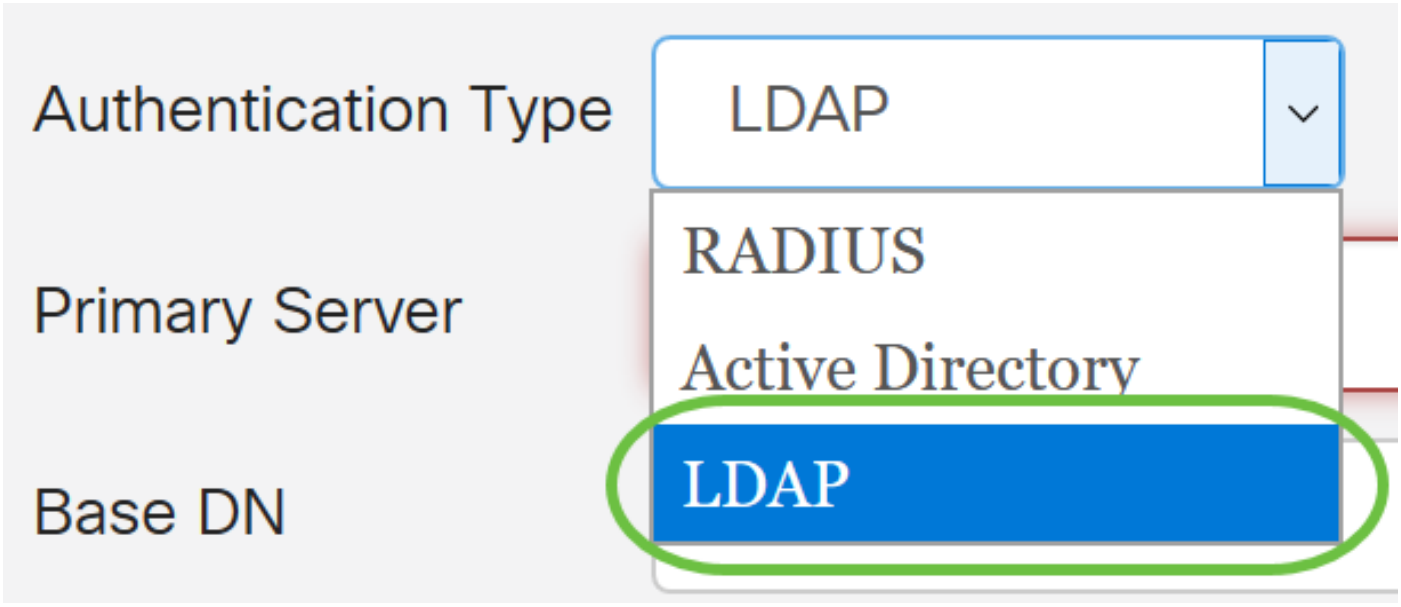
ステップ2:[*Name*]フィールドで、アカウントのユーザー名を作成します。

LDAPで設定できるリモートユーザアカウントは1つだけです。

この例では、Dany_Adminが使用されています。

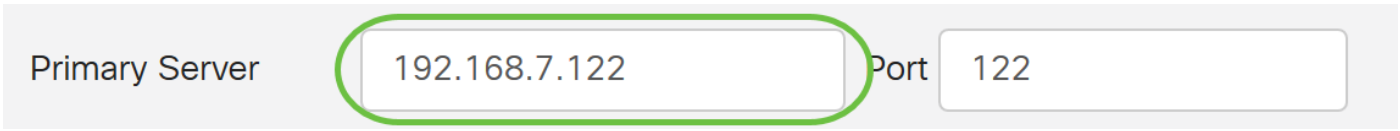


ステップ3:[Authentication Type]ドロップダウンメニューから、[**LDAP**]を選択**します**。Lightweight Directory Access Protocol(LDAP)は、ディレクトリサービスへのアクセスに使用されるアクセスプロトコルです。ドメインの認証を実行するためにディレクトリサーバを実行するリモートサーバです。



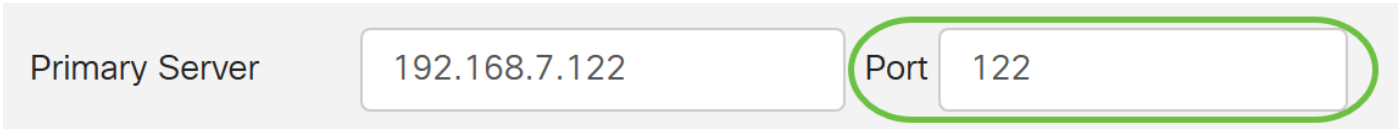
ステップ4:[プライマリ・サーバ]フィールドに、LDAPのサーバ・アドレスを入力します。

この例では、**192.168.7.122が使用**されます。



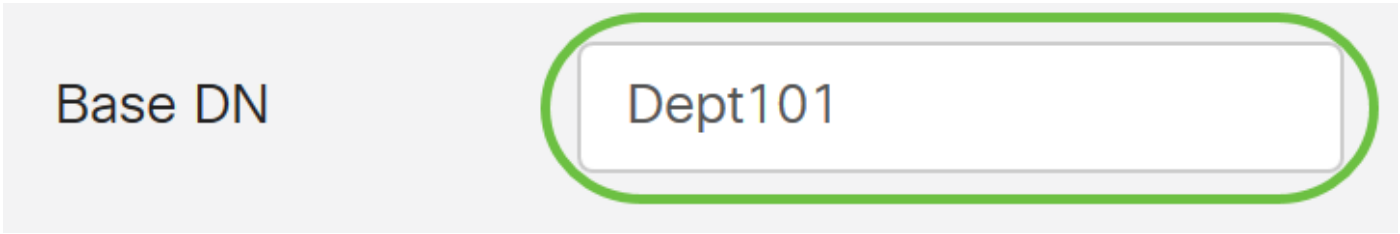
ステップ5:[*Port*]フィールドに、プライマリ・サーバのポート番号を入力します。

この例では、ポート番号**として**122が使用されています。



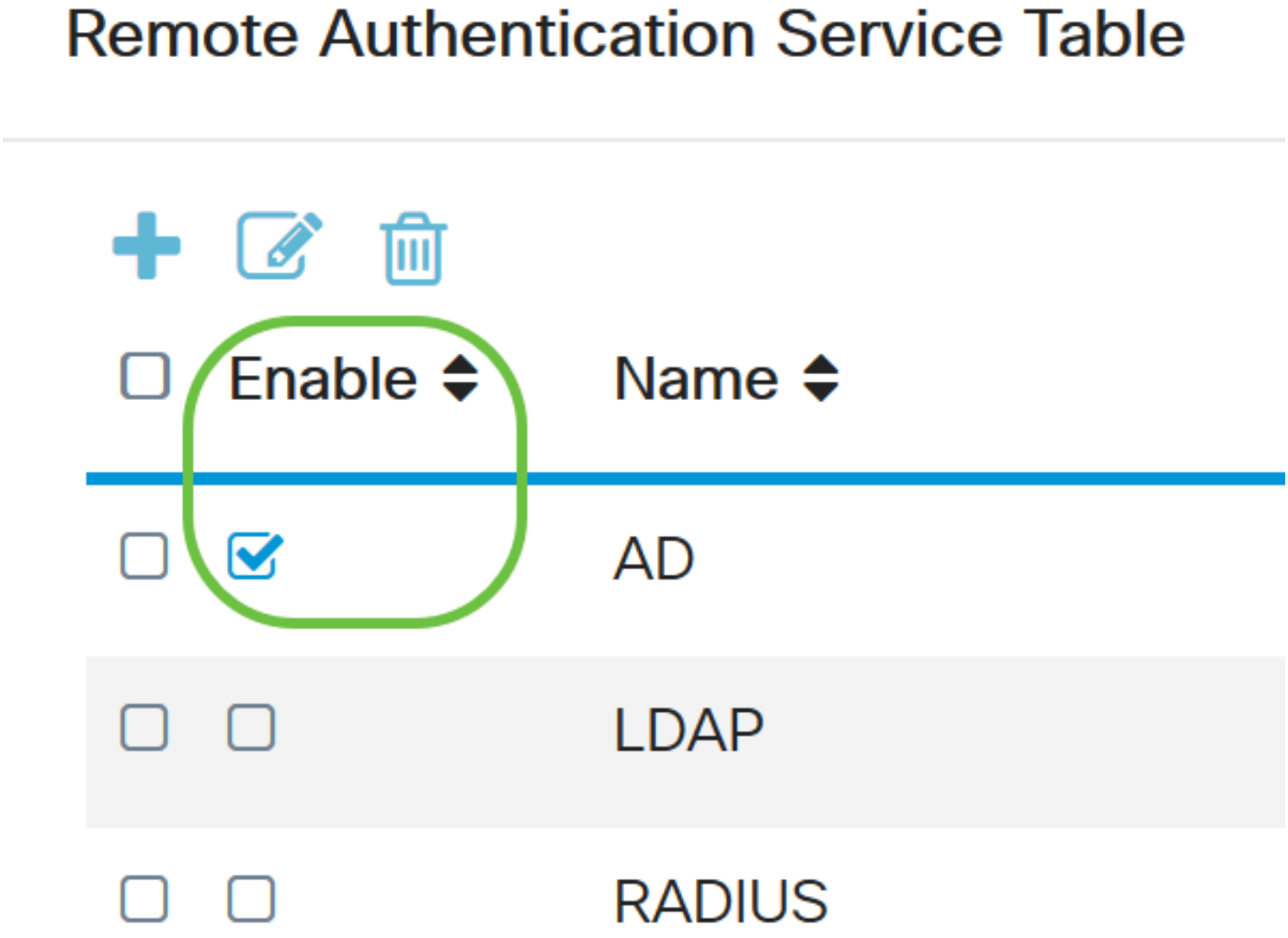
ステップ6:[Base DN]フィールドにLDAPサーバのベース識別名を入力します。ベースDNは、LDAPサーバが許可要求を受信したときにユーザを検索する場所です。このフィールドは、LDAPサーバに設定されているベースDNと一致している必要があります。

この例では、Dept101が**使用さ**れています。

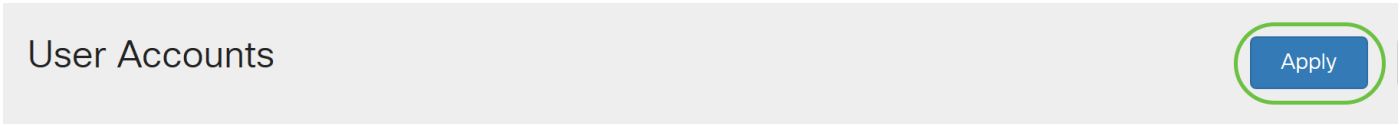


ステップ7:[Apply]をクリ**ックします**。リモート認証サービステーブルに移動します。

ステップ8:（オプション）リモート認証サービスを有効または無効にするには、有効または無効にするサービスの横にあるチェックボックスをオンまたはオフにします。



ステップ9:[Apply]をクリックします。



これで、RV34xシリーズルータでLDAPが正しく設定されました。

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