スイッチでのリモート認証ダイヤルインユーザサービス(RADIUS)サーバの設定

目的

Remote Authentication Dial-In User Service(RADIUS)は、ネットワークサービスに接続して使用するユーザに対して、一元化された認証、許可、アカウンティング（AAAまたはトリプルA）管理を提供するネットワークプロトコルです。RADIUSサーバは、入力されたログインクレデンシャルを使用してユーザのIDを確認することにより、ネットワークへのアクセスを規制します。たとえば、公共のWi-Fiネットワークは大学のキャンパスに設置されます。これらのネットワークにアクセスできるのは、パスワードを持つ受講者だけです。RADIUSサーバは、ユーザが入力したパスワードをチェックし、必要に応じてアクセスを許可または拒否します。

RADIUSサーバをセットアップすると、クライアントまたはユーザにネットワークへのアクセスを許可する前に認証が行われるため、セキュリティを強化するのに役立ちます。RADIUSサーバは、サーバの可用性、再送信、およびタイムアウトに関連するクライアントの問題に対応します。また、RADIUSサーバは、ユーザの接続要求を処理し、ユーザを認証し、ユーザにサービスを提供するために必要な設定情報をクライアントに送信します。

RADIUSサーバは、RADIUS対応デバイスで構成されるネットワークの制御を一元化するサーバです。RADIUSサーバは、802.1Xまたはメディアアクセスコントロール(MAC)アドレスに基づいて転送を決定します。

この記事では、Sx350、SG350X、およびSx550Xシリーズスイッチの RADIUS設定の設定方法について説明します。

該当するデバイス

- Sx350シリーズ
- SG350Xシリーズ
- Sx550Xシリーズ

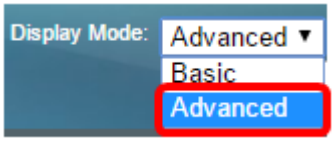
[Software Version]

- 2.2.5.68

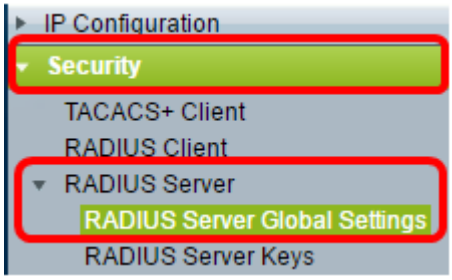
RADIUSサーバの設定

RADIUSサーバのグローバル設定

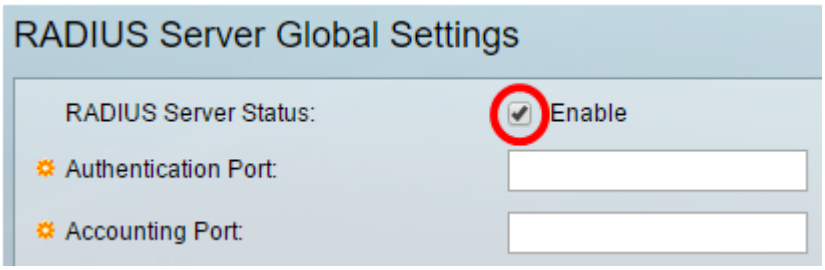
ステップ1：スイッチのWebベースのユーティリティにログインし、[Display Mode]ドロップダウンリストから[Advanced]を選択します。



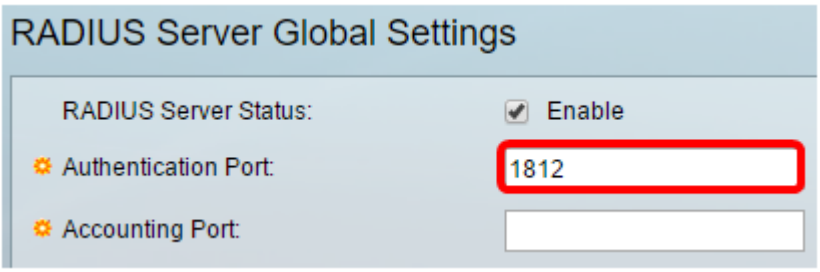
ステップ2:[Security] > [RADIUS Server] > [RADIUS Server Global Settings]を選択します。



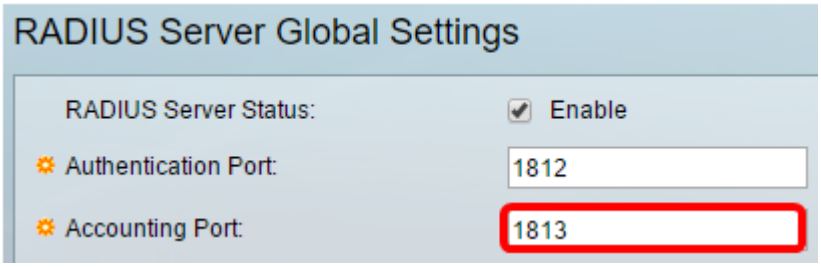
ステップ3:[RADIUS Server Status]の[**Enable**]チェックボックスをオンにします。



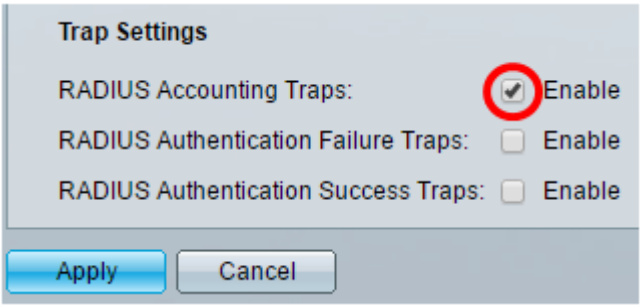
ステップ4：認証要求のRADIUSサーバポートのUser Datagram Protocol(UDP)ポート番号を入力します。範囲は1 ~ 65535で、デフォルトは1812です。



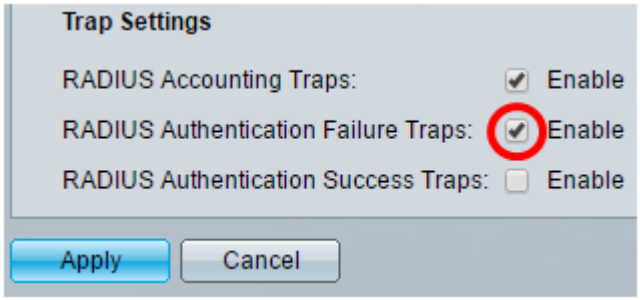
ステップ5：アカウンティング要求のRADIUSサーバポートのUDPポート番号を入力します。範囲は1 ~ 65535で、デフォルトは1813です。



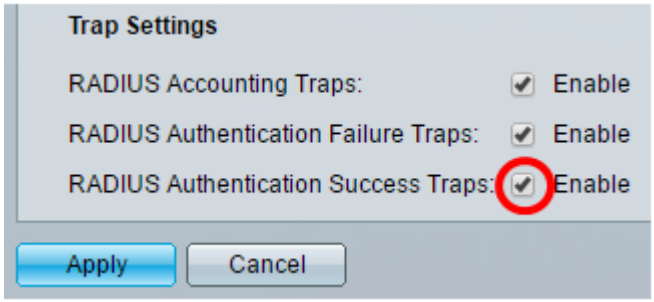
ステップ6:（オプション）RADIUSアカウンティングイベントのトラップを生成するには、[Trap Settings]の[RADIUS Accounting Traps]の[**Enable**]チェックボックスをオンにします。



ステップ7:（オプション）失敗したログインのトラップを生成するには、RADIUS認証失敗トラップの[**Enable**]チェックボックスをオンにします。



ステップ8:（オプション）成功したログインのトラップを生成するには、RADIUS認証成功トラップの**[Enable]**チェックボックスをオンにします。



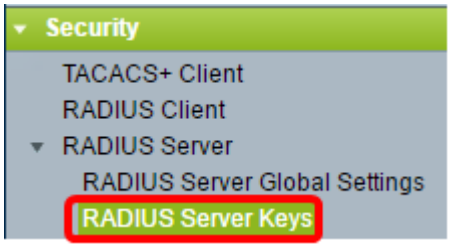
ステップ9:[Apply]をクリ**ックします。**

ステップ10：構成が正常に保存され  たことを示すアイコンが表示されます。構成を永続的に保存するには、[ファイル操作]ページに移動するか、ページ上部のアイコンをクリックします 

。それ以外の場合は、[閉じる]を**クリックします。**

RADIUSサーバキーの設定

ステップ1:[RADIUS Server]の下の**[RADIUS Server Keys]**を選択します。



ステップ2:（オプション）必要に応じて、デフォルトのRADIUSキーを入力します。[Default Key]に入力した値は、[Add RADIUS Server]ページで設定したすべてのサーバに適用され、デフォルトキーが使用されます。

デフォルトキー：デバイスとRADIUSクライアントの間の認証および暗号化に使用するデフ

ォルトキー文字列を選択します。次のオプションがあります。

- Keep existing default key：指定されたサーバの場合、デバイスは既存のデフォルトのキー文字列を使用してRADIUSクライアントの認証を試みます。
- [暗号化(Encrypted)]:Message Digest 5(MD5)アルゴリズムを使用して通信を暗号化するには、暗号化された形式でキーを入力します。
- 「プレーンテキスト」 – プレーンテキストモードでキー文字列を入力します。

MD5 Digest：ユーザが入力したパスワードのMD5ダイジェストを表示します。

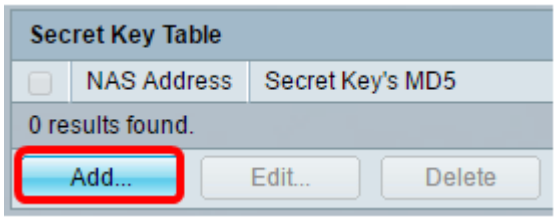
注：この例では、[Default Key]で[Keep existing default key]が選択されています。

ステップ3:[Apply]をクリックします。

ステップ4：アイコン  は、構成が正常に保存されたことを示します。構成を永続的に保存するには、[ファイル操作]ページに移動するか、ページ上部のアイコンをクリックします 

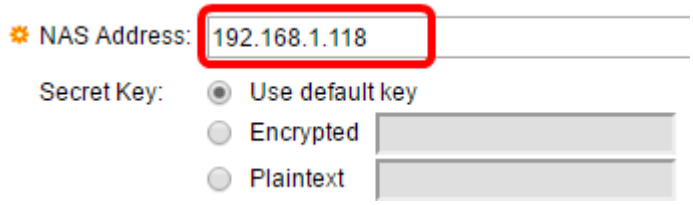
。

ステップ5:（オプション）[Secret Key Table]領域で、[Add]ボタンをクリックして、秘密キーを追加します。



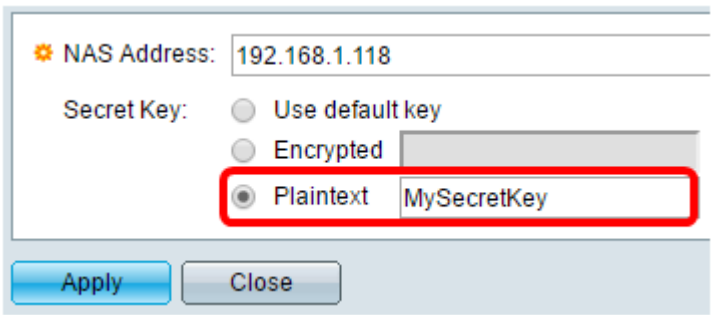
ステップ6:[NAS Address]フィールドに、NASまたはRADIUSクライアントを含むスイッチのIPアドレスを入力します。

注：次の図では、192.168.1.118がIPアドレスの例として使用されています。



ステップ7：優先する秘密キーを選択します。

注：次の図では、例としてプレーンテキストが選択されています。



次のオプションがあります。

- Use default key：指定されたサーバでは、デバイスは既存のデフォルトのキー文字列を使用してRADIUSクライアントの認証を試みます。
- [暗号化(Encrypted)]:MD5を使用して通信を暗号化するには、暗号化された形式でキーを入力します。
- 「プレーンテキスト」 – プレーンテキストモードでキー文字列を入力します。最大 128 文字入力できます。

ステップ8:[Apply]をクリックします。

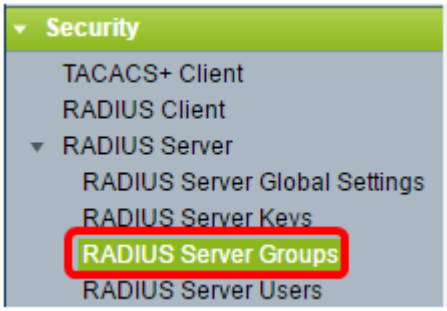
ステップ9：アイコン  は、構成が正常に保存されたことを示します。構成を永続的に保存するには、[ファイル操作]ページに移動するか、ページ上部のアイコンをクリックします 

。それ以外の場合は、[閉じる]をクリックします。

RADIUSサーバグループの設定

RADIUSサーバグループは、デバイスをRADIUSサーバとして使用するユーザグループです。グループを設定するには、次の手順に従います。

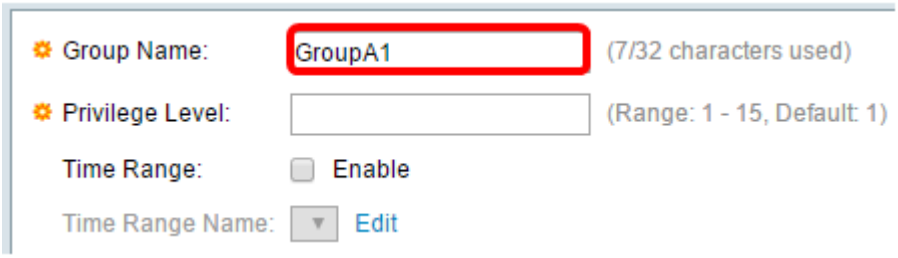
ステップ1:[RADIUS Server]で[RADIUS Server Groups]を選択します。



ステップ2:[RADIUS Server Group]テーブルの下の[Add]ボタンをクリックします。

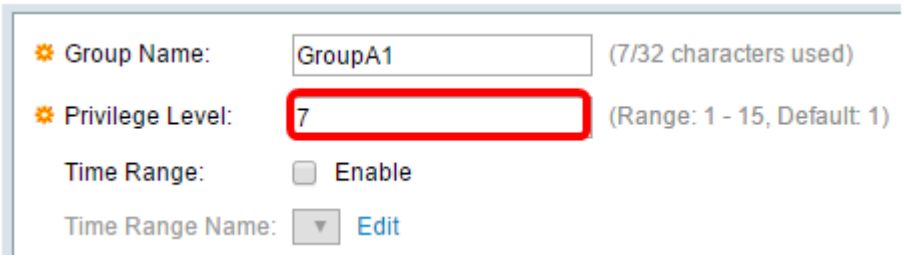
ステップ3：ポップアップウィンドウで、[グループ名]フィールドにグループの名前を入力します。最大 32 文字入力できます。

注：次の図では、例としてGroupA1が使用されています。



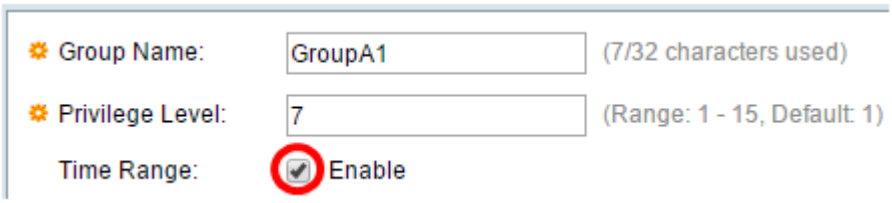
ステップ4：グループに割り当てる権限レベルを入力します。特権レベルは、作成した各グループに割り当てるアクセスレベルを決定します。レベルは1 ~ 15の範囲で設定できます。デフォルト値は1です。

注：この例では、7 が使用されます。

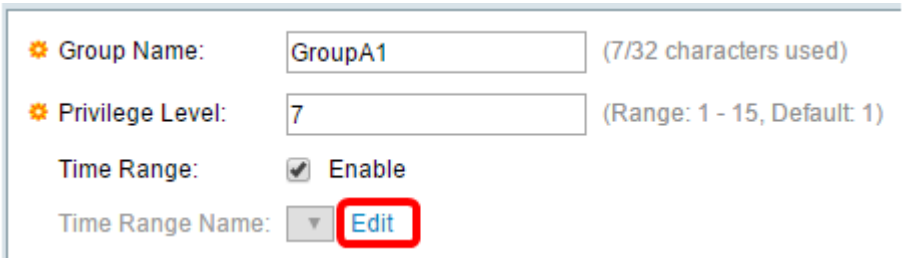


- 1（読み取り専用CLIアクセス）：グループのユーザはGUIにアクセスできず、デバイス設定を変更しないCLIコマンドにのみアクセスできます。
- 7（読み取り/制限付き書き込みCLIアクセス）：グループのユーザはGUIにアクセスできず、デバイス設定を変更する一部のCLIコマンドにのみアクセスできます。詳細については、CLIリファレンスガイドを参照してください。
- 15（読み取り/書き込み管理アクセス）：グループのユーザはGUIにアクセスでき、デバイスを設定できます。

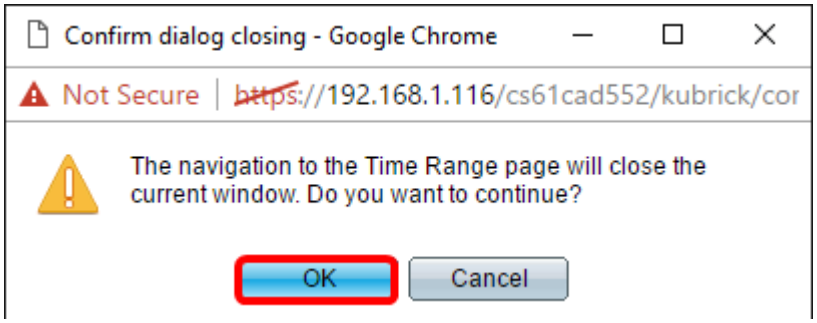
ステップ5:（オプション）このグループに時間範囲を適用する場合は、[時間範囲]の[有効]チェックボックスをオンにします。それ以外の場合は、ステップ 15 に進みます。



ステップ6:[Time Range Name]の横にある[**Edit**]リンクをクリックして、時刻設定を行います。

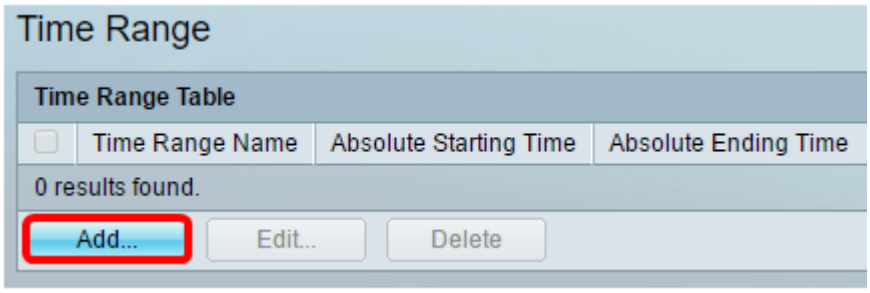


ステップ7：現在のウィンドウが閉じられることを示すポップアップウィンドウが表示され、時間範囲の設定を続行できます。[OK] をクリックします。



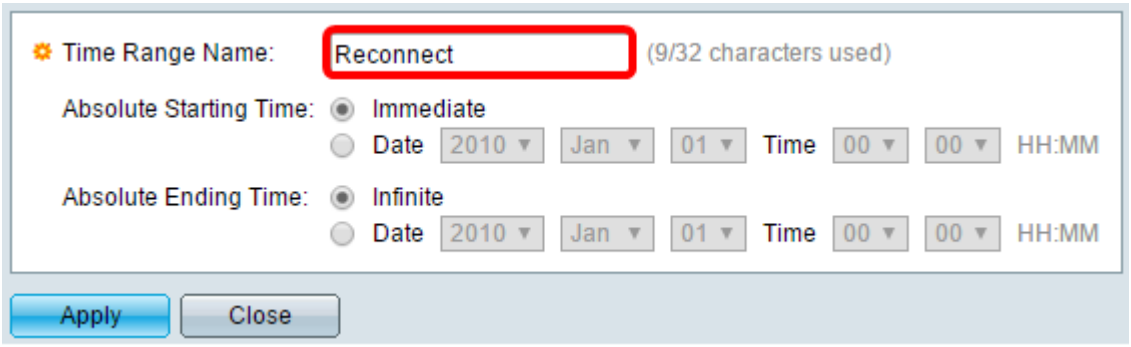
[Time Range]ページが表示されます。

ステップ8:[Time Range]テーブルの下の[Add]ボタンをクリックします。

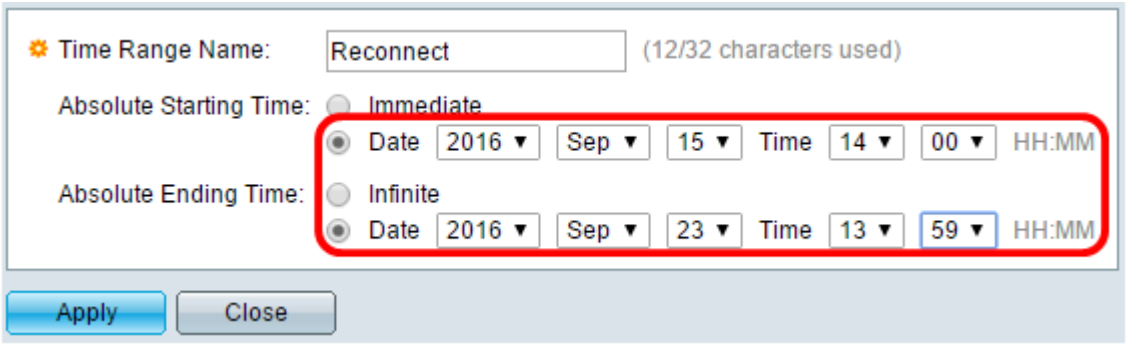


ステップ9:[Time Range Name]フィールドに時間範囲の名前を入力します。

注：次の図では、例として[Reconnect]を使用しています。



ステップ10：オプションボタンをクリックして、希望する絶対開始時間と終了時間を選択します。



- 「絶対開始時間」(Absolute Starting Time) – 開始時間を定義するには、次のいずれかを選択します。
- [即時(Immediate)]：時間範囲をすぐに開始する場合に、このオプションを選択します。
- 「日付、時刻」(Date, Time) - 「時間範囲」(Time Range)の開始日時を指定する場合に選択します。
- 「絶対終了時間」(Absolute Ending Time) – 開始時間を定義するには、次のいずれかを選択します。
- [無限]：時間範囲を終了させない場合に選択します。
- 「日付、時刻」(Date, Time) - 「時間範囲」(Time Range)の終了日時を指定する場合に選択します。

注：この例では、[Date and Time]が選択されています。

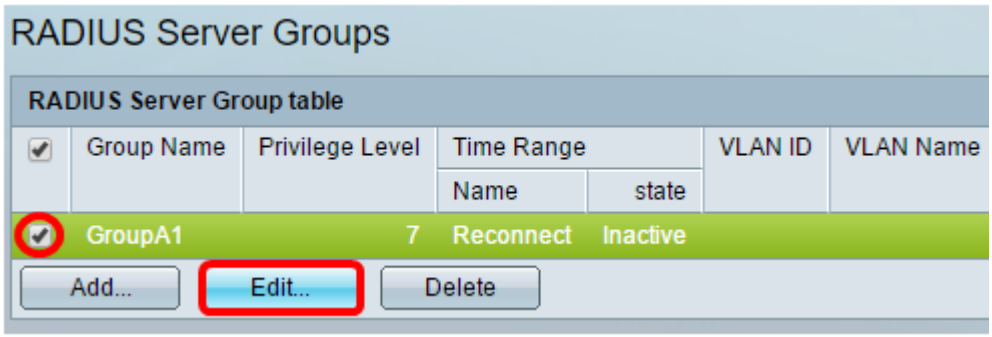
ステップ11:[Apply]をクリックします。

ステップ12：構成が正常に保存され たことを示すアイコンが表示されます。構成を永続的に保存するには、[ファイル操作]ページに移動するか、ページ上部のアイコンをクリックします Save 。それ以外の場合は、[閉じる]をクリックします。

その後、メインページに移動します。

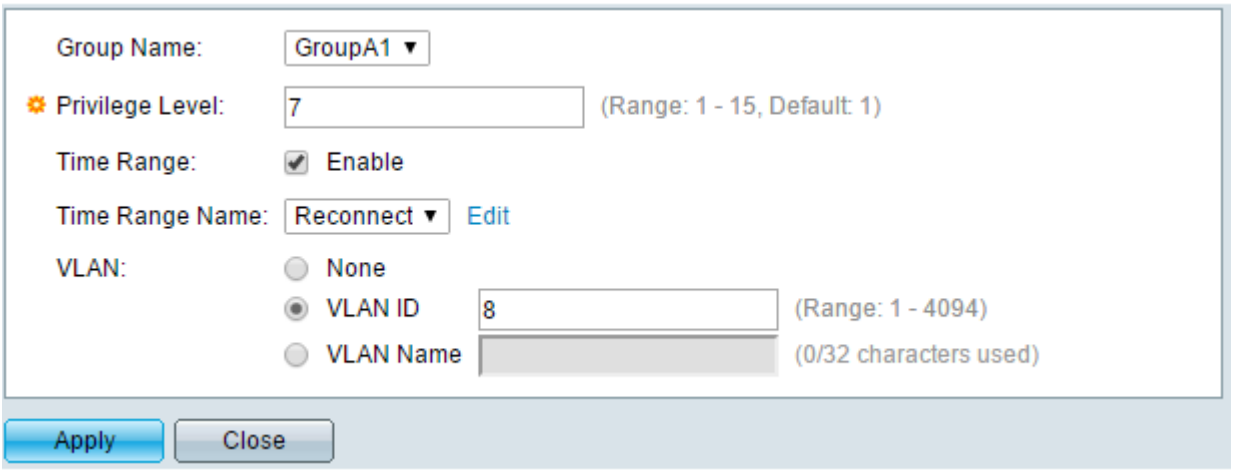
ステップ13:[RADIUS Server]の下の[RADIUS Server Groups]を再度クリックします。

ステップ14：新しく作成されたグループが[RADIUS Server Group]テーブルの下に表示されます。グループの名前の横にあるチェックボックスをオンにし、[Edit]をクリックします。



ステップ15:（オプション）グループのVLANを選択します。次のオプションがあります。

- None:VLANが指定されていません。
- [VLAN ID]:VLAN IDを指定します。
- [VLAN名]:VLAN名を指定します。



注：この例では、VLAN ID 8が使用されています。

ステップ16:[Apply]をクリックします。

ステップ17：アイコン  は、構成が正常に保存されたことを示します。構成を永続的に保存するには、[ファイル操作]ページに移動するか、ページ上部のアイコンをクリックします 

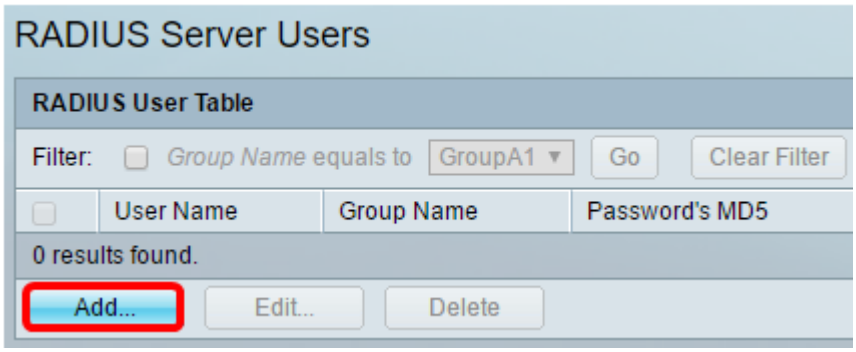
。それ以外の場合は、[閉じる]をクリックします。

RADIUSサーバユーザの設定

以前に作成したグループにユーザを追加するには、次の手順に従います。

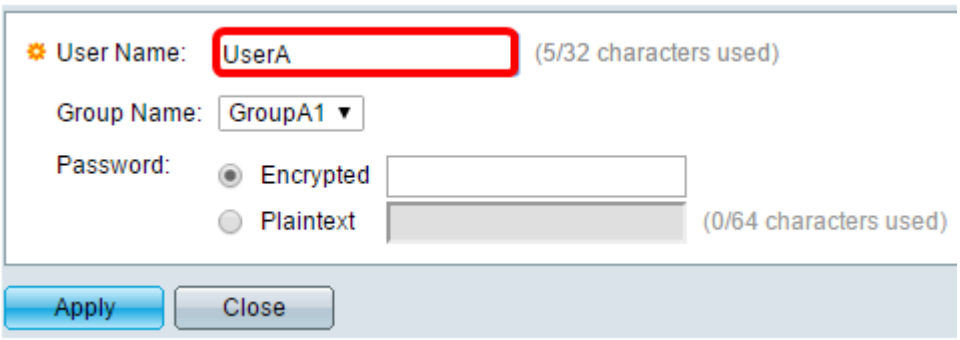
ステップ1:[RADIUS Server]の下の[RADIUS Server Users]をクリックします。

ステップ2:[RADIUS User Table]の下の[Add]ボタンをクリックします。

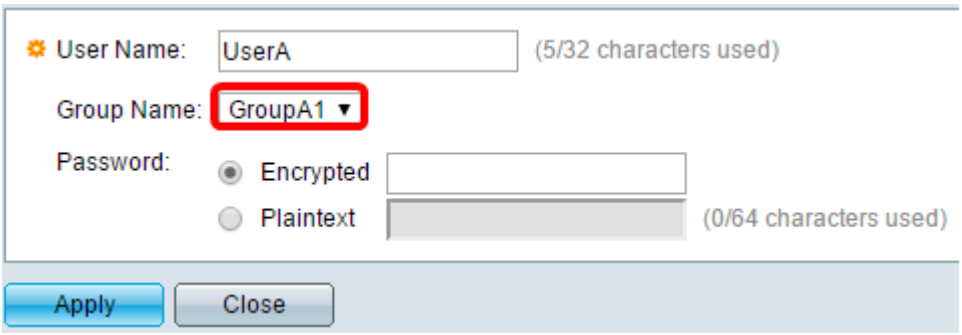


ステップ3:[User Name]フィールドにユーザの名前を入力します。

注：この例では、UserAが使用されています。

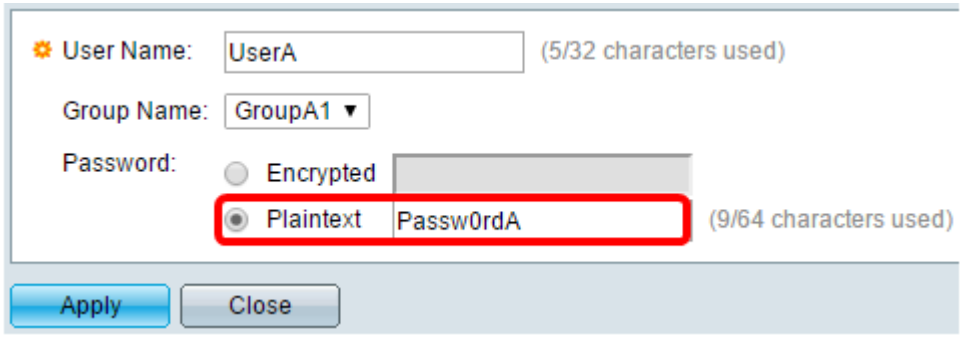


ステップ4:[Group Name]ドロップダウンリストから、ユーザが属するグループを選択します。



ステップ5:[Password]領域のオプションボタンをクリックします。

ステップ6：優先パスワードを入力します。



- 暗号化：MD5を使用して通信を暗号化するためにキー文字列が使用されます。暗号化を使用するには、暗号化された形式でキーを入力します。
- プレーンテキスト：暗号化されたキー文字列（別のデバイスから）がない場合は、プレーンテキストモードでキー文字列を入力します。暗号化されたキー文字列が生成され、表示されます。

注：この例では、[Plaintext]が選択されています。

ステップ6:[Apply]をクリックします。

ステップ7：構成が正常に保存され  たことを示すアイコンが表示されます。構成を永続的に保存するには、[ファイル操作]ページに移動するか、ページ上部のアイコンをクリックします 

。それ以外の場合は、[閉じる]をクリックします。

これで、スイッチのRADIUSサーバの設定が正常に完了したはずです。