# スイッチでのMACベース認証の設定

## 目的

802.1Xは、リストデバイスを許可し、ネットワークへの不正アクセスを防止するための管理ツールです。このドキュメントでは、グラフィカルユーザインターフェイス(GUI)を使用してスイッチにMACベースの認証を設定する方法を説明します。 コマンドラインインターフェイス(CLI)を使用してMACベースの認証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。

**注：**このガイドは、ホストが認証されたことを確認するために、9つのセクションと1のセクションで長い時間を費やします。コーヒー、紅茶、または水を手に入れ、必要な手順を確認して実行するのに十分な時間があることを確認します。

詳細については、用語集を参照してください。

## RADIUS はどのように動作しますか。

802.1X認証には、サプリカント（クライアント）、オーセンティケータ（スイッチなどのネットワークデバイス）、および認証サーバ(RADIUS)の3つの主要コンポーネントがあります。Remote Authentication Dial-In User Service(RADIUS)は、ネットワークアクセスの管理に役立つ認証、許可、アカウンティング(AAA)プロトコルを使用するアクセスサーバです。RADIUSは、RADIUSサーバと1つ以上のRADIUSクライアント間でセキュアな認証情報が交換されるクライアントサーバモデルを使用します。クライアントのIDを検証し、クライアントがLANへのアクセスを許可されているかどうかをスイッチに通知します。

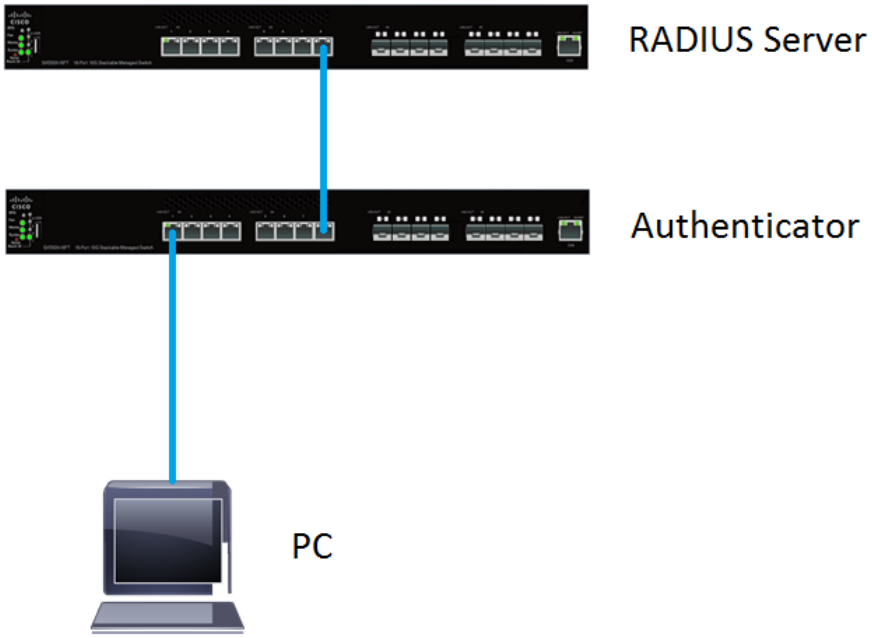
オーセンティケータは、クライアントと認証サーバの間で動作します。まず、クライアントからID情報を要求します。応答として、オーセンティケータは認証サーバで情報を確認します。最後に、クライアントに応答をリレーします。この記事では、オーセンティケータはRADIUSクライアントを含むスイッチです。スイッチは、Extensible Authentication Protocol(EAP)フレームをカプセル化およびカプセル化解除して、認証サーバと対話できます。

## MACベース認証について

MACベースの認証では、サプリカントがオーセンティケータと通信する方法を理解していない場合、またはオーセンティケータと通信できない場合は、ホストのMACアドレスを使用して認証します。MACベースのサプリカントは、純粋なRADIUSを使用して（EAPを使用せずに）認証されます。 RADIUSサーバには、許可されたMACアドレスだけを含む専用のホストデータベースがあります。MACベースの認証要求をPassword Authentication Protocol(PAP)認証として扱う代わりに、サーバは属性6 [Service-Type] = 10でこのような要求を認識します。これらの要求は、Calling-Station-Id属性のMACアドレスとホストデータベースに格納されているMACアドレスを比較します。

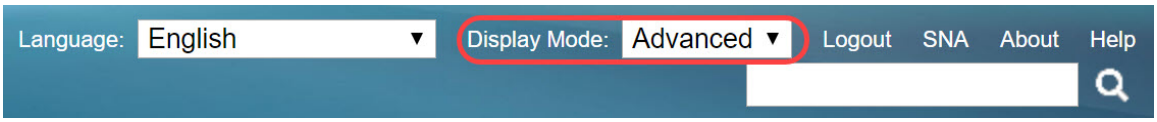
バージョン2.4リリースでは、MACベースのサプリカントに送信され、EAP認証方式または純粋なRADIUSのいずれかを定義するユーザ名の形式を設定する機能が追加されています。このバージョンでは、ユーザ名の形式を設定したり、MACベースのサプリカントに対してユーザ名とは異なる特定のパスワードを設定することもできます。

**トポロジ：**




**注**：この記事では、RADIUSサーバとオーセンティケータの両方にSG550X-24を使用します。RADIUSサーバのスタティックIPアドレスは192.168.1.100で、オーセンティケータのスタティックIPアドレスは192.168.1.101です。

このドキュメントの手順は、詳細表示モードで**実行**されます。モードを詳細モードに変更するには、右上隅の[表示モード(*Display Mode*)]ドロップダウン**リスト**の[詳細*(Advanced)]*を選択します。




# 目次



# 該当するデバイス

- Sx350Xシリーズ

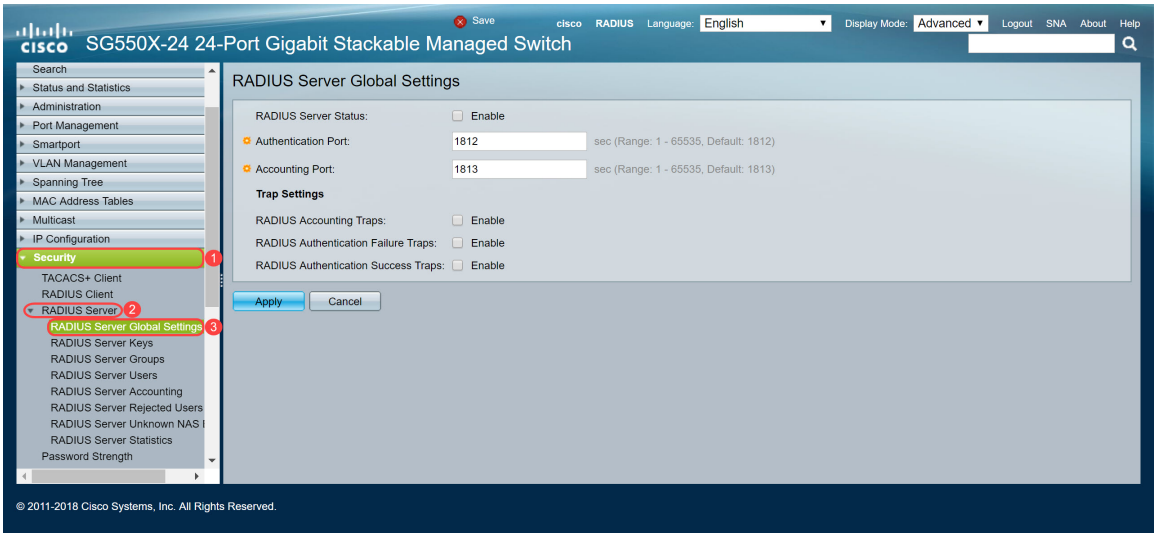
- SG350XGシリーズ
- Sx550Xシリーズ
- SG550XGシリーズ

# [Software Version]

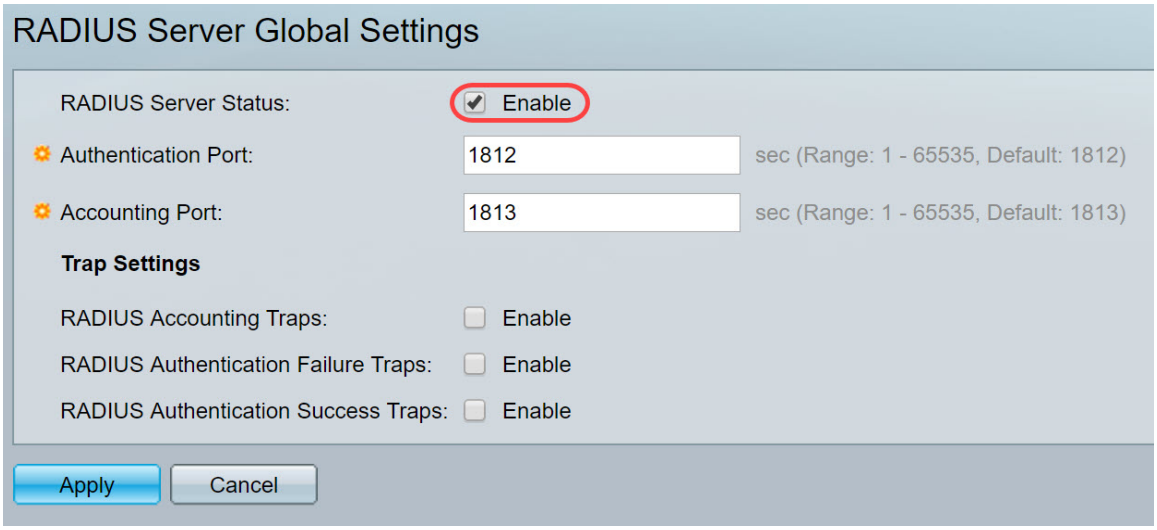
- 2.4.0.94

# RADIUSサーバのグローバル設定

ステップ1:RADIUSサーバとして設定するスイッチのWebベースユーティリティにログインし、[**Security] > [RADIUS Server] > [RADIUS Server Global Settings]に移動します。**



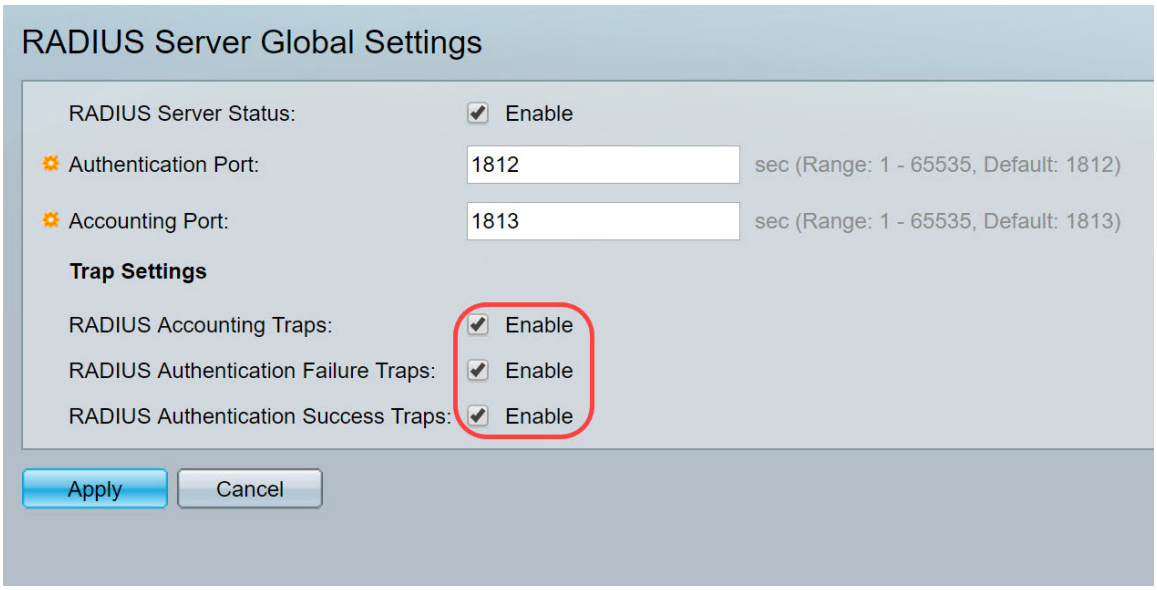

ステップ2:RADIUSサーバ機能のステータスを有効にするには、[RADIUS Server Status]フィールドの[**Enable**]チェックボックスをオンにします。




ステップ3:RADIUSアカウンティングイベント、失敗したログイン、成功したログインに対してトラップを生成するには、目的の[**Enable**]チェックボックスをオンにしてトラップを生成します。トラップは、Simple Network Management Protocol（SNMP；簡易ネットワーク管理プロトコル）によって生成されるシステムイベントメッセージです。違反が発生すると、トラップがスイッチのSNMPマネージャに送信されます。次のトラップ設定は次のとおりです。

- [RADIUS Accounting Traps]:RADIUSアカウンティングイベントのトラップを生成する場合にオンにします。

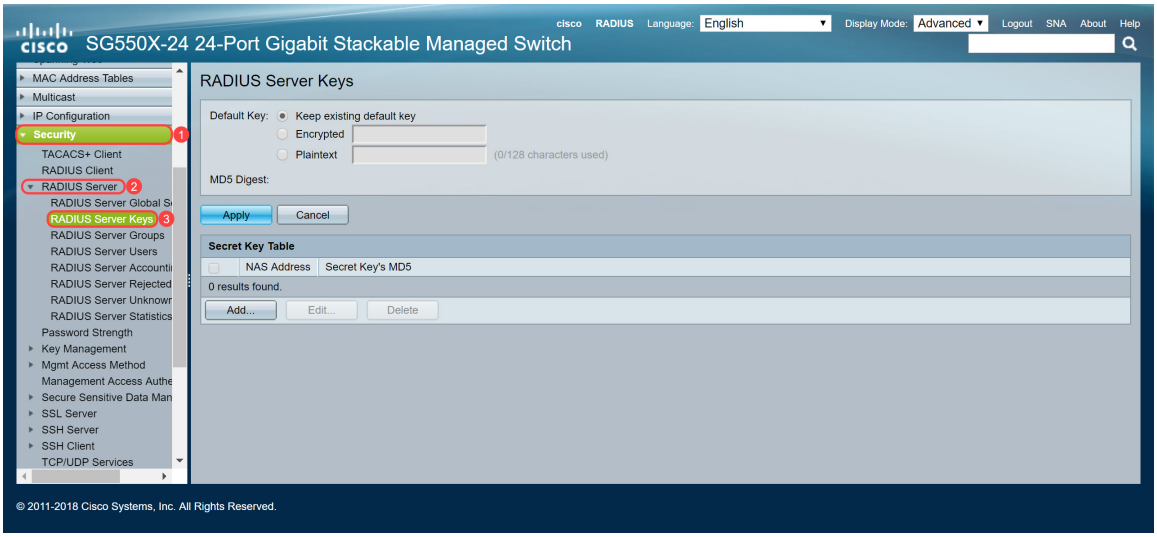
- [RADIUS Authentication Failure Traps]：失敗したログインのトラップを生成するには、このチェックボックスをオンにします。
- [RADIUS Authentication Success Traps]：成功したログインのトラップを生成するには、このチェックボックスをオンにします。



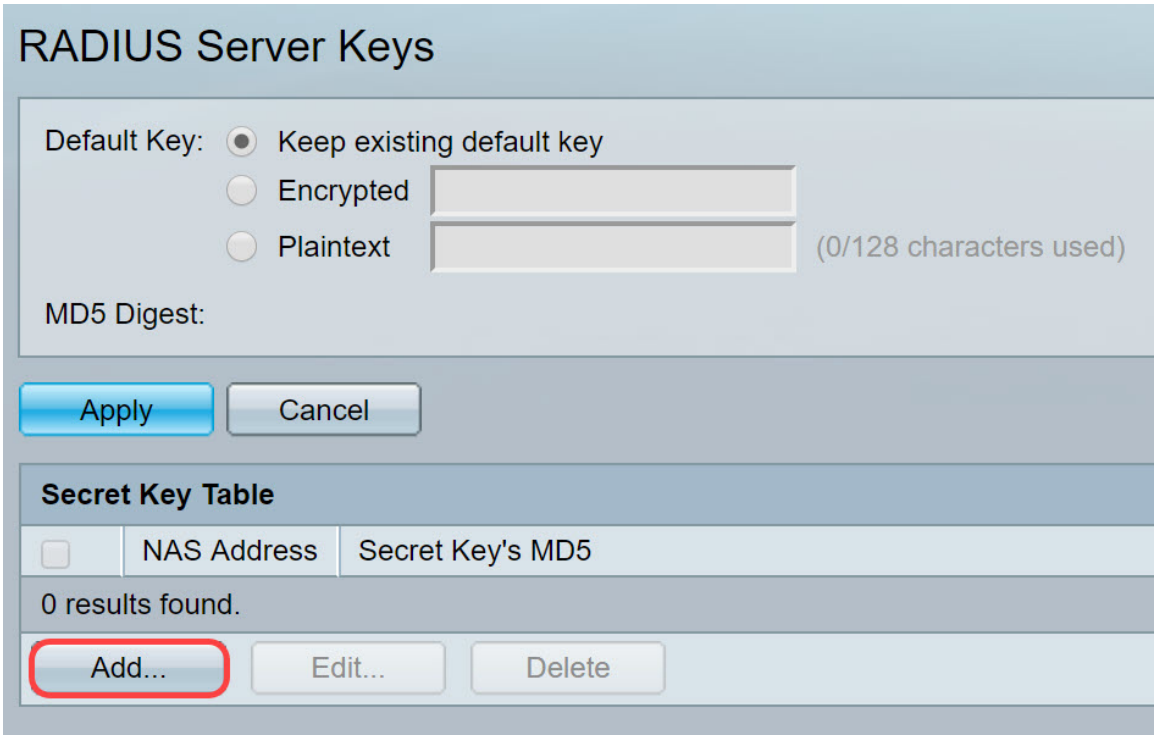

ステップ4:[Apply]をクリックして設定を保存します。

# RADIUSサーバキー

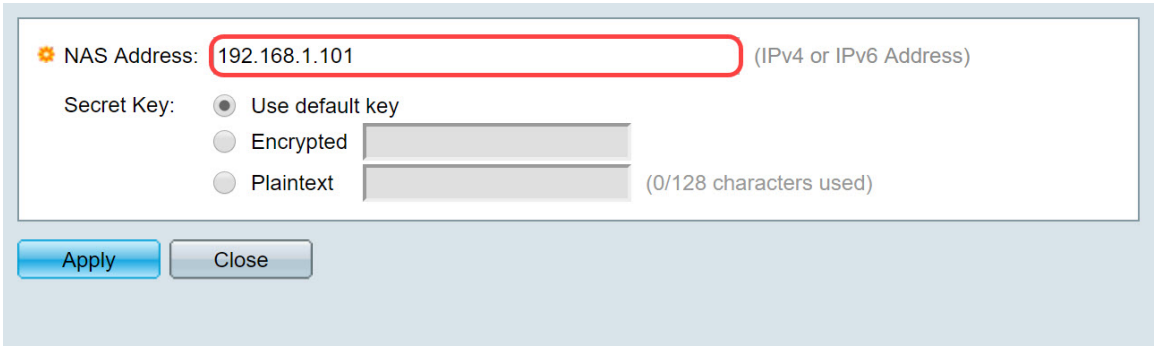
ステップ1:[Security] > [RADIUS Server] > [RADIUS Server Keys]に移動します。[*RADIUS Server Key*]ページが開きます。




ステップ2:[Secret Key Table]セクションで、[Add...]をクリックします。 秘密キーを追加します。




ステップ3:[秘密キーの追加*(Add Secret Key)]*ウィンドウが開きます。[*NAS Address*]フィールドに、RADIUSクライアントを含むスイッチのアドレスを入力します。この例では、IPアドレス192.168.1.101をRADIUSクライアントとして使用します。

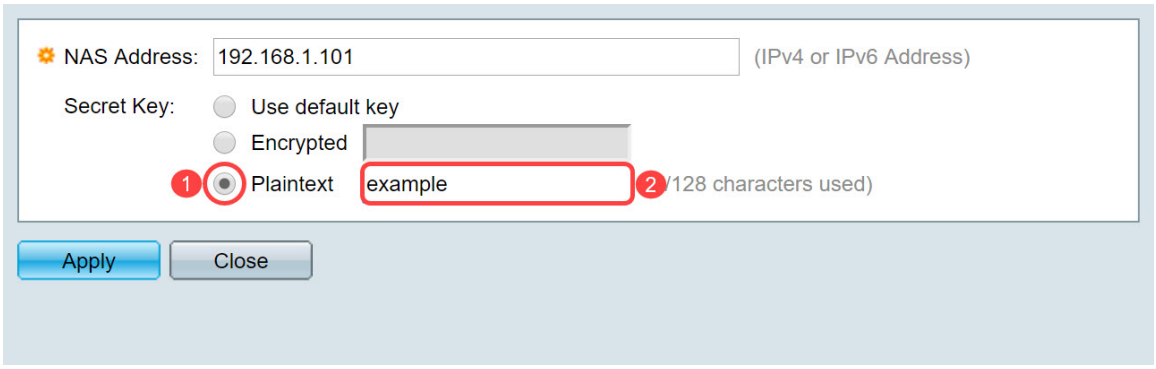



ステップ4：秘密キーとして使用するオプションボタンを1つ*選択します*。次のオプションがあります。

- 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)]:Message-Digest Algorithm 5(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。

この例では、[Plaintext]を選択し、[Secret Key]**に[example]**という語*を使用します*。[apply]を押すと、キーは暗号化された形式になります。

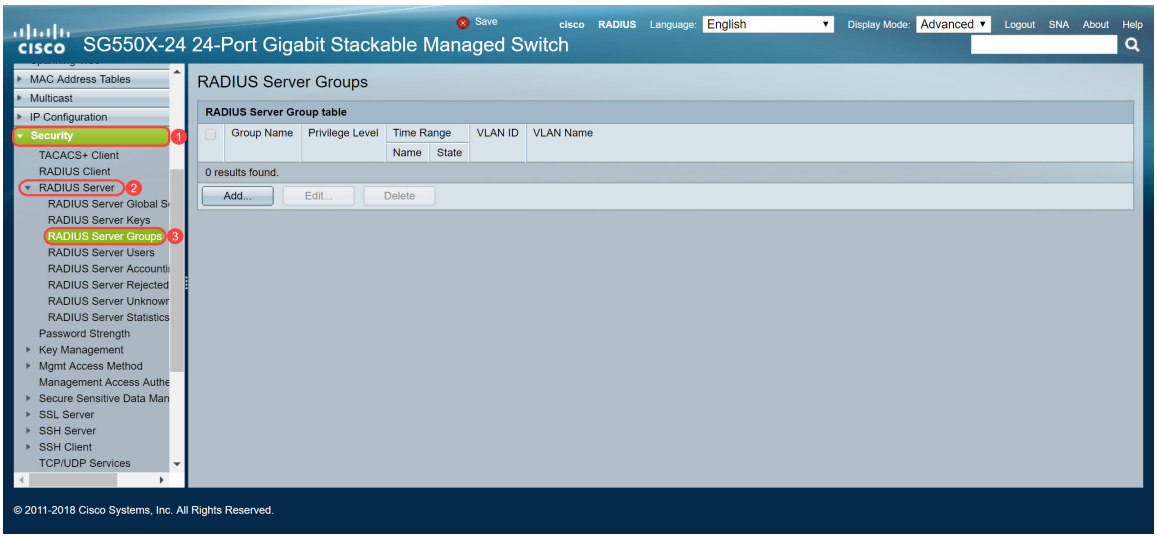
**注**：秘密キーとしてexampleという単語を使用**することは**お勧めしません。もっと強い鍵を使ってください。最大128文字を使用できます。パスワードが複雑すぎて覚えにくい場合は、パスワードは良いパスワードですが、パスワードを暗記可能なパスフレーズに変え、母音を置き換える特殊文字や数字を使う方が良いでしょう。 辞書に載っている単語を使わないのが一番です。フレーズを選択し、特殊文字や数字の一部の文字を入れ替えることをお勧めします。詳細については、このシスコのブログ記事を参照してください。



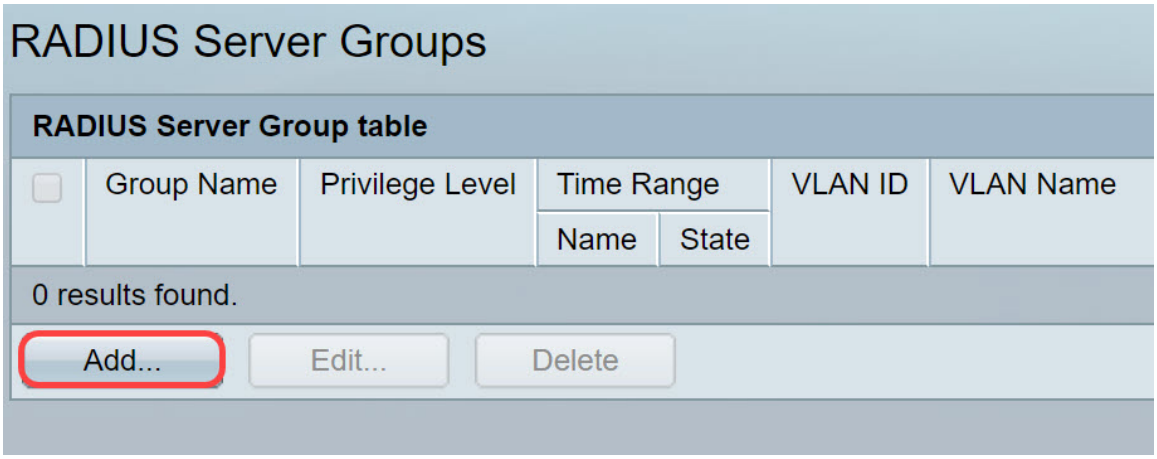

ステップ5:[**Apply**]をクリックして設定を保存します。秘密キーはMD5で暗号化されます。MD5は、データを取得し、通常は再生可能ではない一意の16進数出力を作成する暗号化ハッシュ関数です。MD5は128ビットハッシュ値を使用します。


# RADIUSサーバグループ

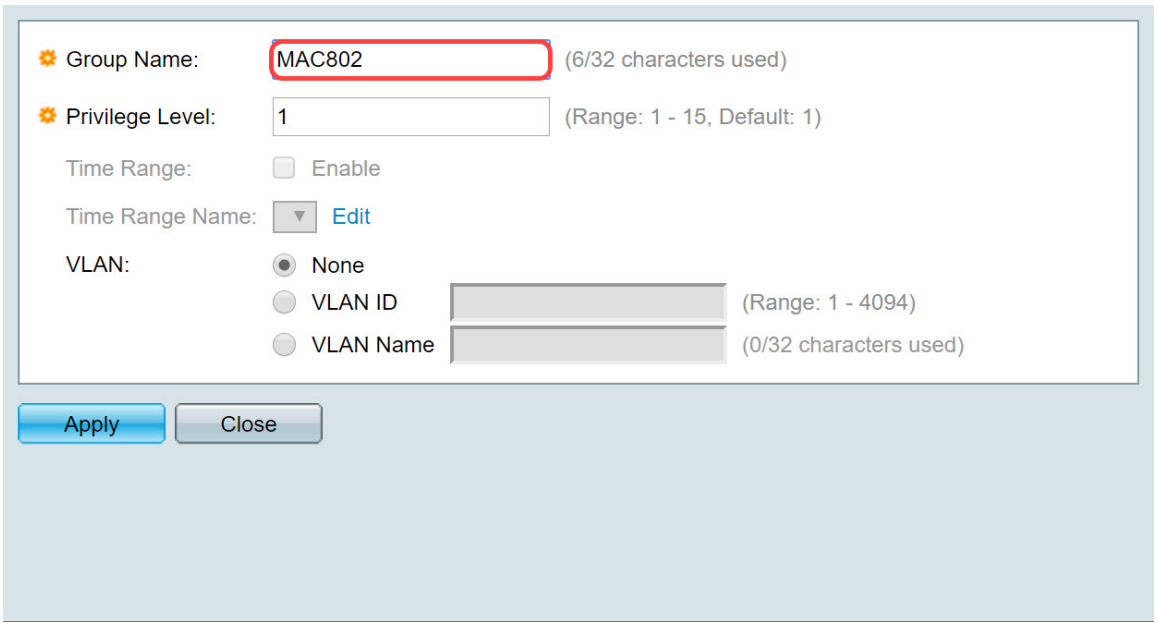
ステップ1:[Security] > [**RADIUS Server**] > [**RADIUS Server Groups**]に移動します。




ステップ2:[**Add...**]をクリックします。 新しいRADIUSサーバグループを追加します。

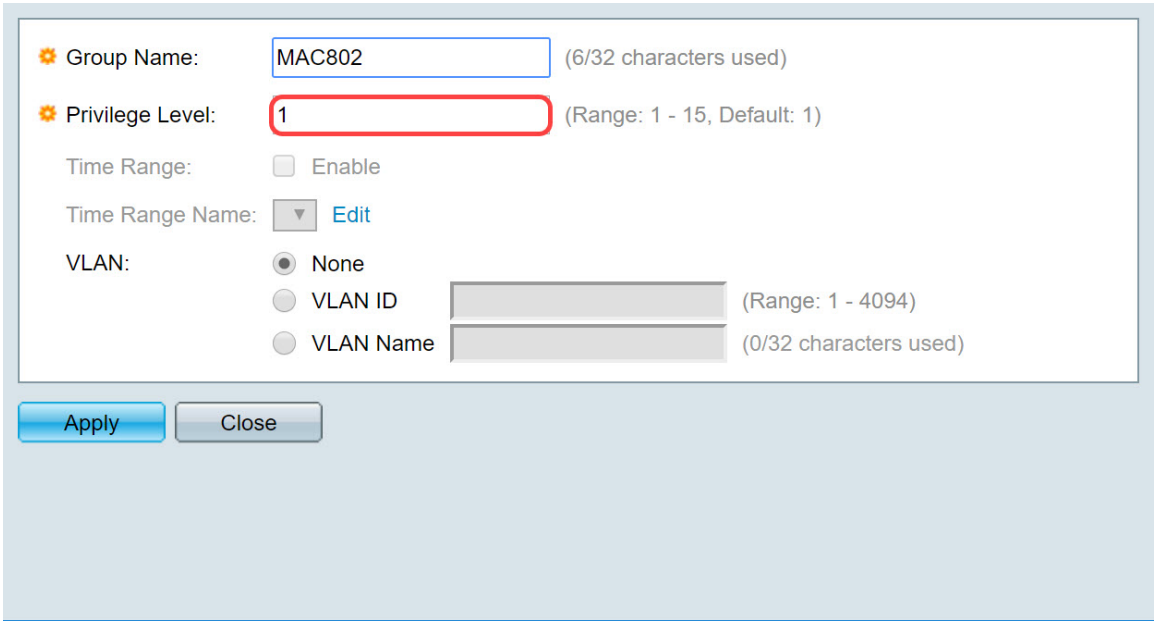



ステップ3:[*Add RADIUS Server Group*]ページが開きます。グループの名前を入力します。この例では、グループ名として**MAC802**を使用します。




ステップ4:[Privilege Level]フィールドにグループの管理アクセス特権レベルを入力します。範囲は1 ~ 15、15が最も特権で、デフォルト値は1です。この例では、特権レベルは1のままにします。

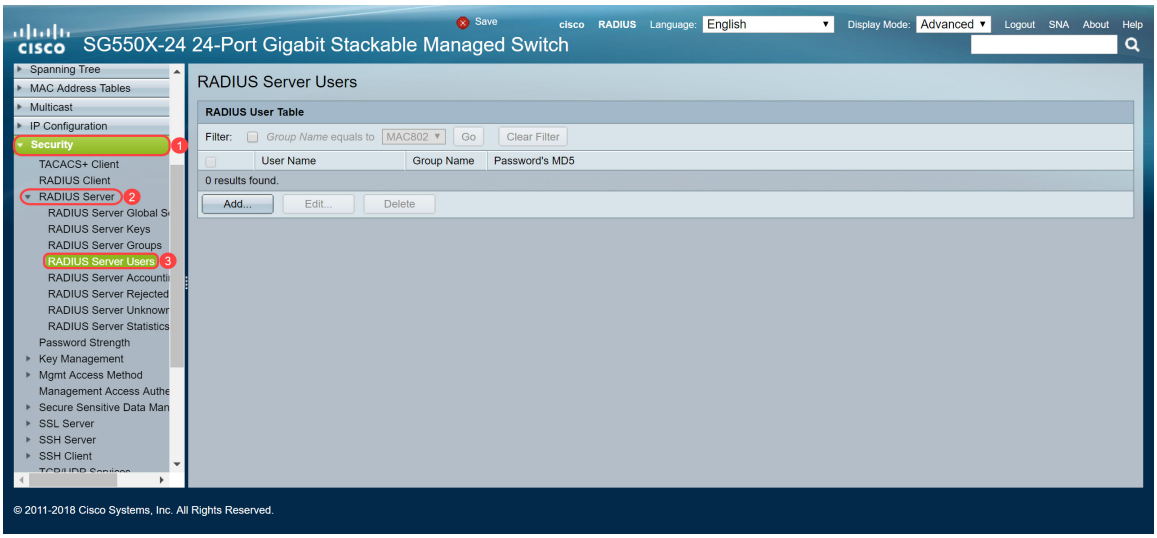
**注：この記事では、時間範囲やVLANを設定しません。**



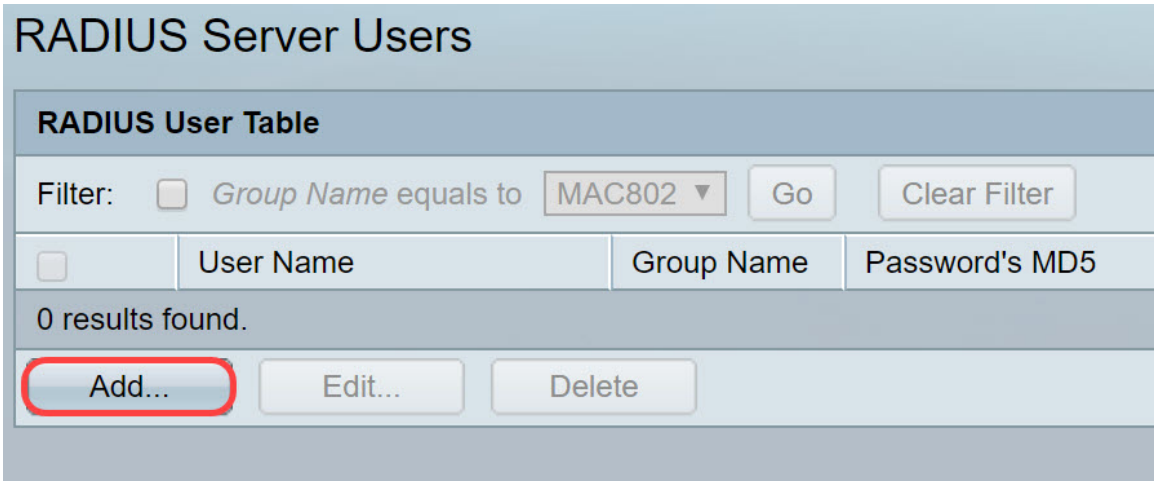

ステップ5:[Apply]をクリックして設定を保存します。

# RADIUSサーバユーザ

ステップ1:[Security] > [RADIUS Server] > [RADIUS Server Users]に移動し、RADIUSのユーザーを設定します。

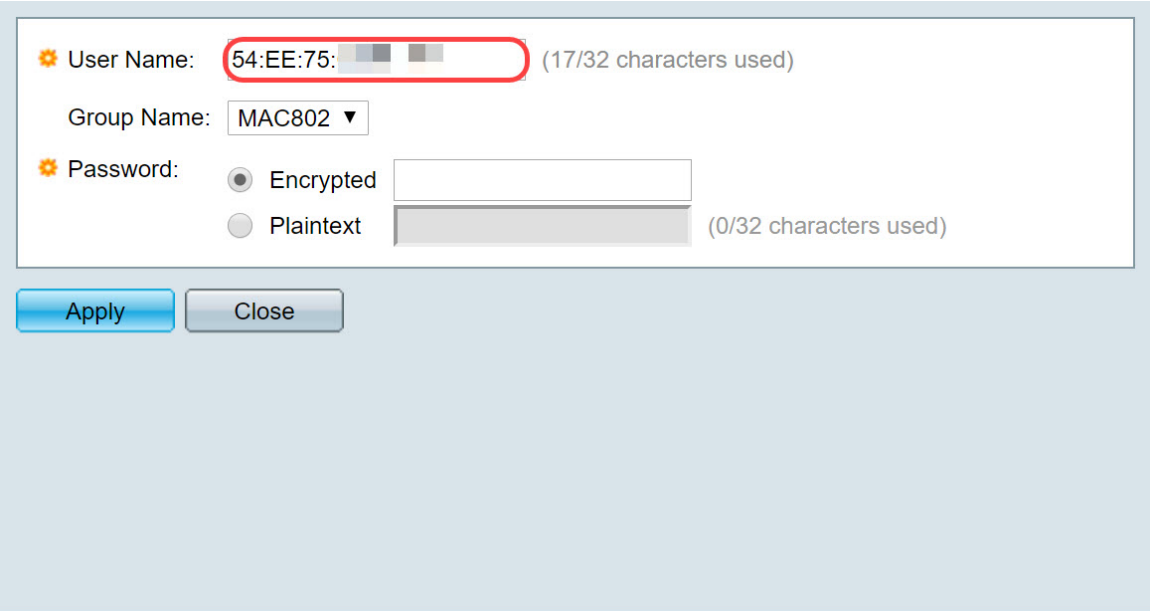



ステップ2:[Add...]をクリックします。 新しいユーザを追加します。

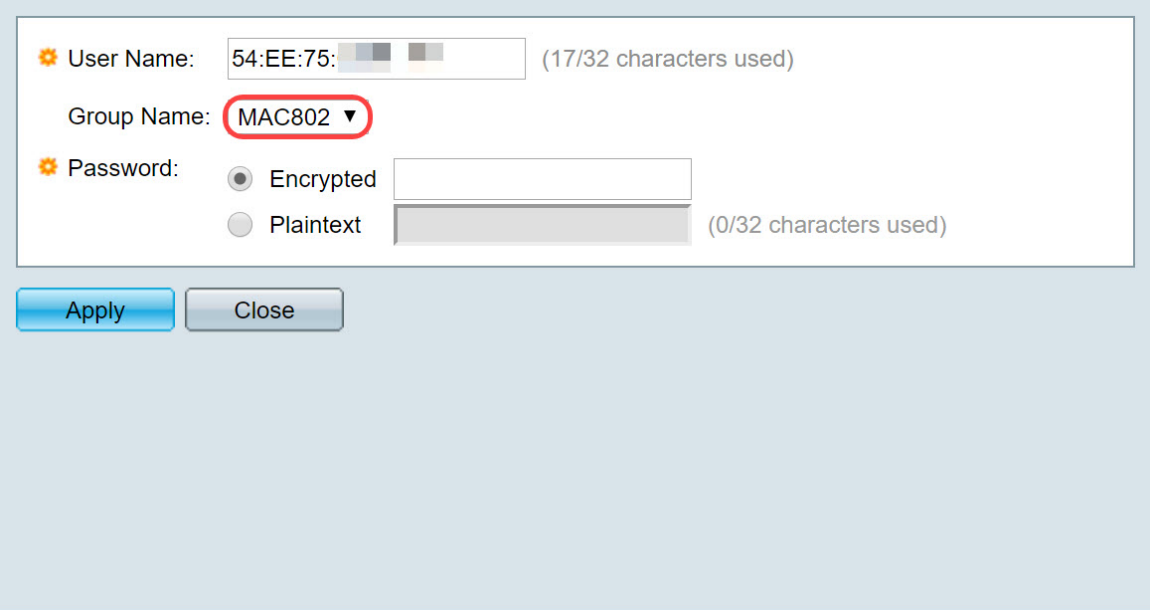



ステップ3:[*Add RADIUS Server User*]ページが開きます。[User Name]フィールドに、ユーザのMACアドレスを入力します。この例では、コンピュータのイーサネットMACアドレスを使用します。

**注**：MACアドレスの一部がぼやけている。




ステップ4:[グループ名]ドロップダウンリストで*グループ*を選択します。「RADIUS Server Group」セクションのステップ3で強調した通り、このユーザのグループ名として**MAC802**を選択します。

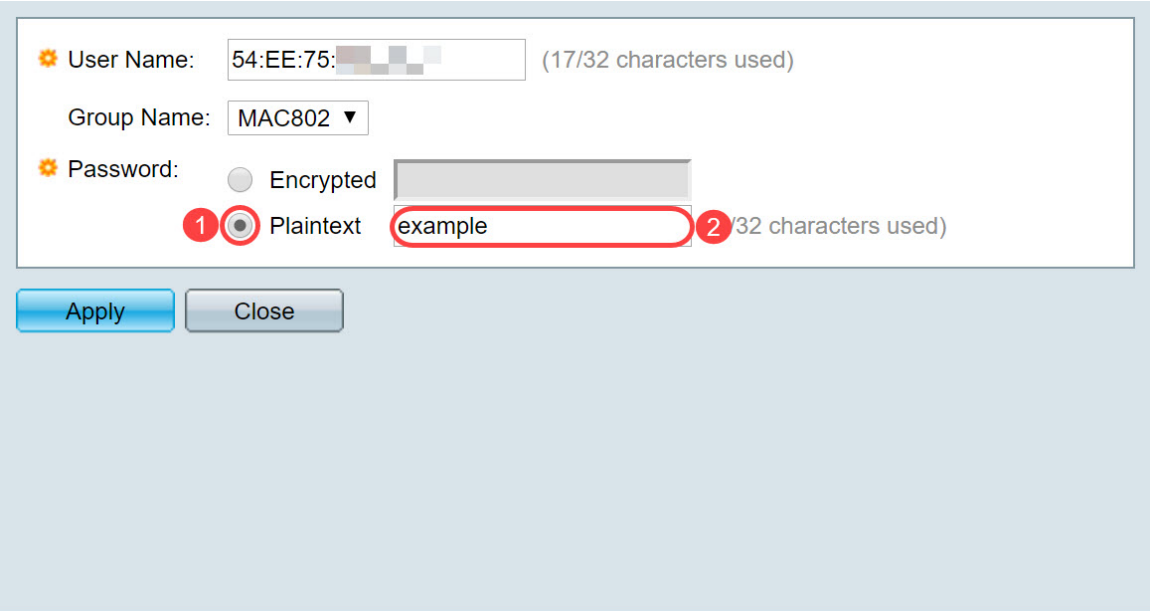



ステップ5：次のいずれかのオプションボタンを選択します。

- 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。

このユーザのパスワードとして*Plaintext*を選択し、プレーンテキストのパスワードとして**example**を入力します。

**注**：プレーンテキストのパスワードとしてexampleを**使用する**ことはお勧めしません。より強力なパスワードを使用することをお勧めします。

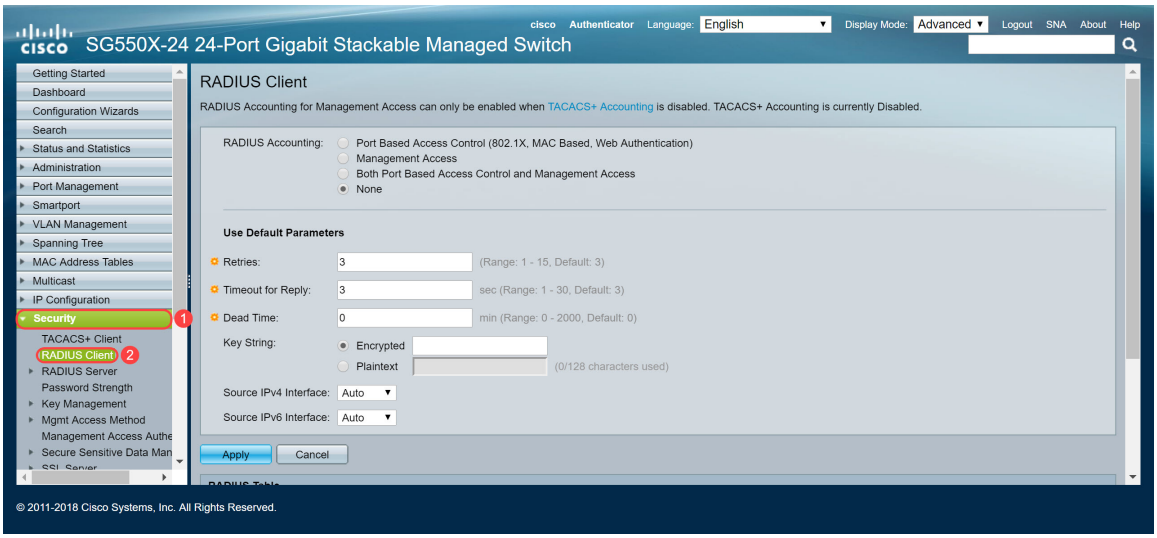



ステップ6：設定が完了したら、[**Apply**]をクリックします。

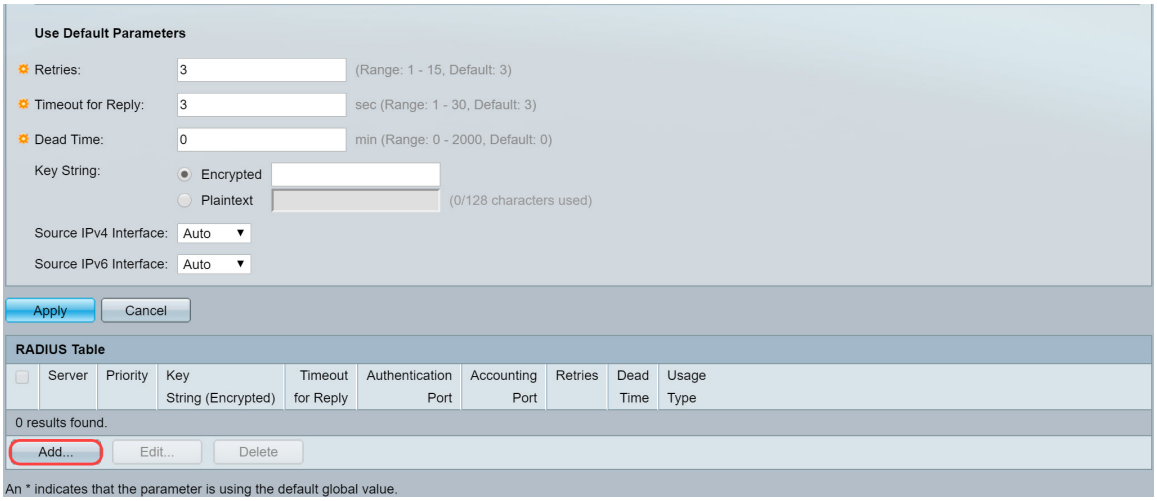
これで、RADIUSサーバの設定が完了しました。次のセクションでは、2番目のスイッチをオーセンティケータとして設定します。

# RADIUSクライアント

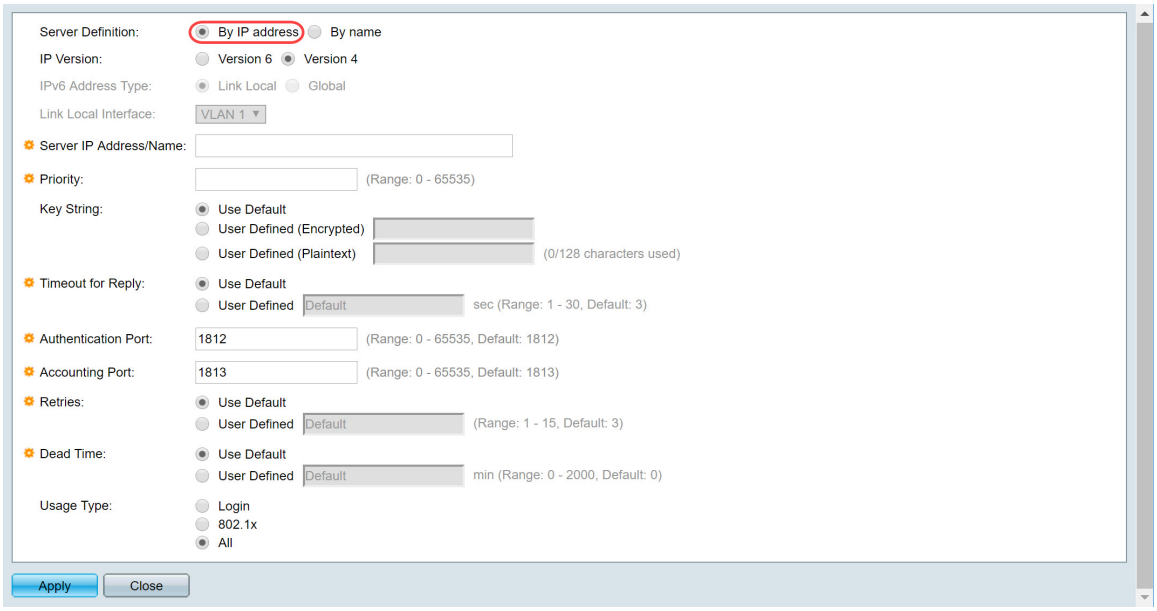
ステップ1：オーセンティケータとして設定するスイッチのWebベースのユーティリティにログインし、[**Security**] > [**RADIUS Client**]**に移動します。**



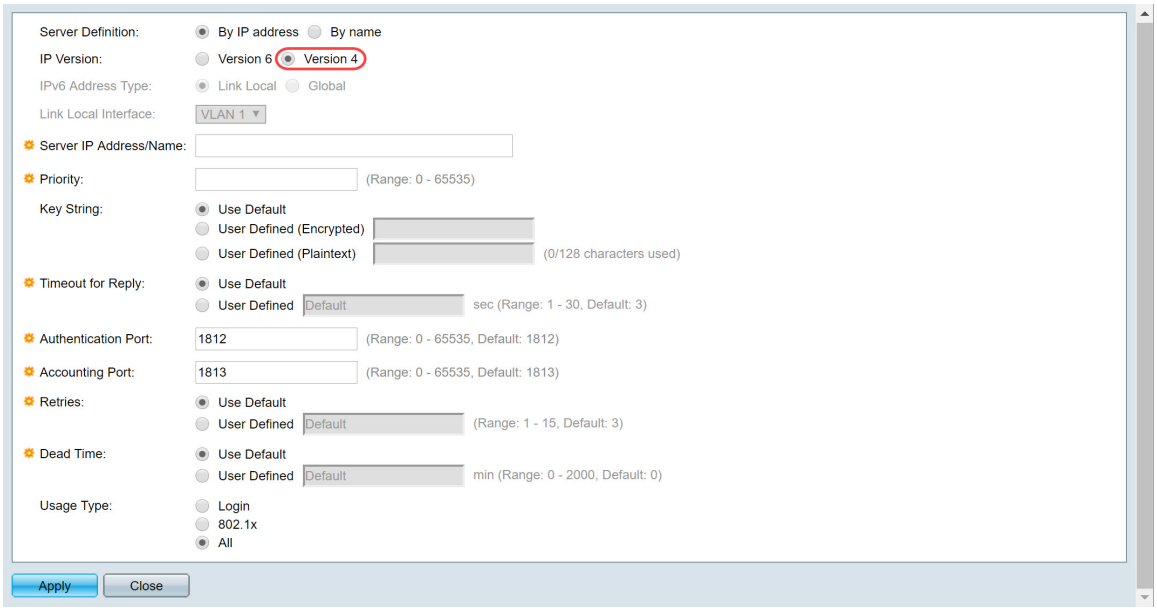

ステップ2:[*RADIUS Table*]セクションまで下にスクロールし、[**Add...**]**をクリックします。**
RADIUSサーバを追加します。



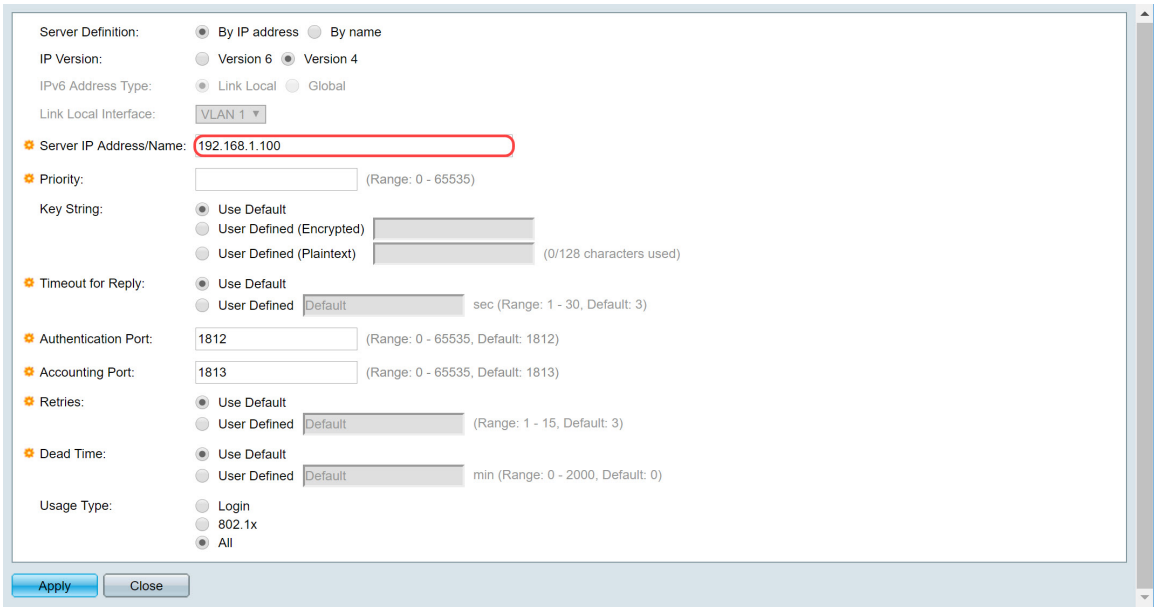

ステップ3: ( オプション ) [Server Definition]フィールドで、RADIUSサーバをIPアドレスまたは名前で指定するかどうかを*選択*します。この例では、[By IP address]のデフォルトの選択を**維持します**。



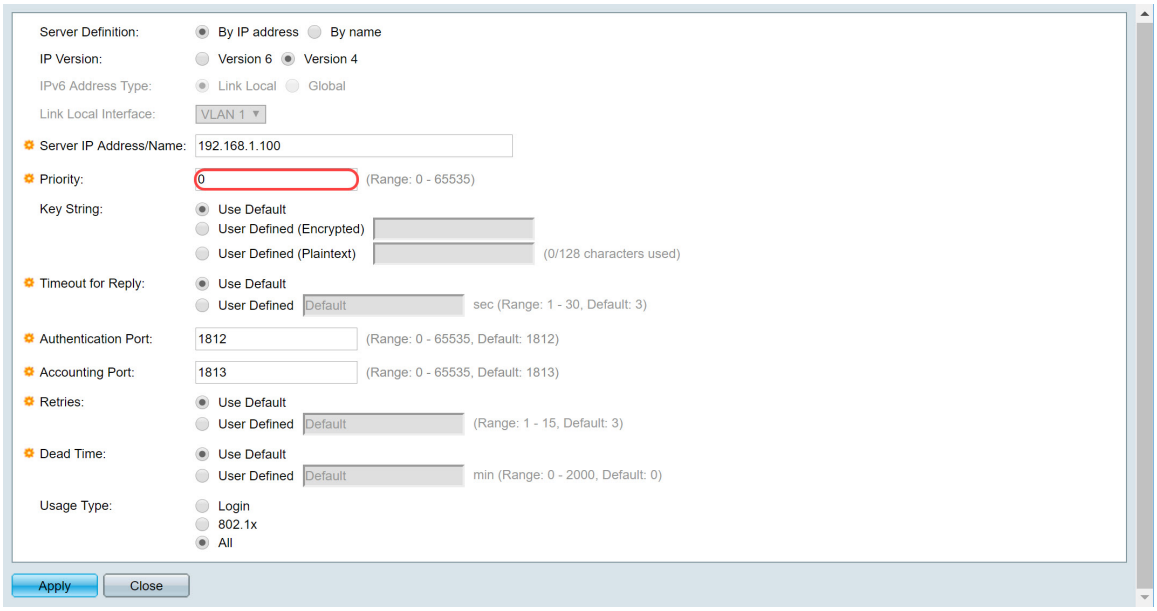

ステップ4: ( オプション ) [IP Version]フィールドで、RADIUSサーバのIPアドレスのバージョンを*選択*します。この例では、バージョン4のデフォルト**の選択を**維持します。




ステップ5:RADIUSサーバでIPアドレスまたは名前を入力します。[Server IP Address/Name]フィールドに**192.168.1.100のIPア**ドレスを*入力*します。

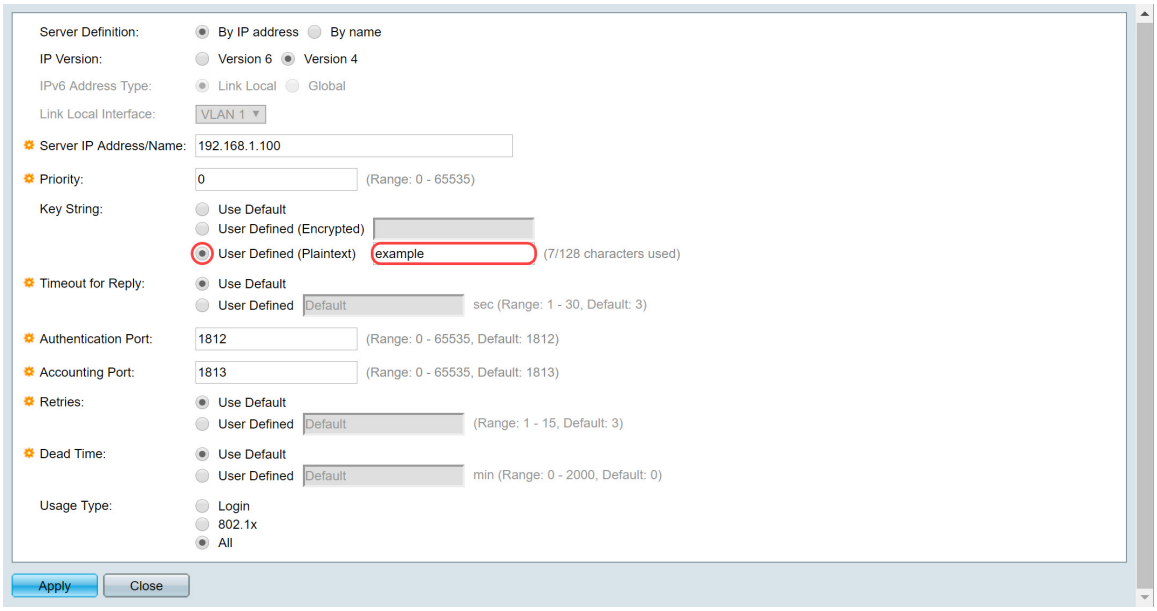



ステップ6：サーバの優先度を入力します。優先順位によって、デバイスがユーザを認証するためにサーバに接続する順序が決まります。デバイスは、最初に最も優先度の高いRADIUSサーバから開始します。ゼロが最も高い優先順位です。




ステップ7：デバイスとRADIUSサーバ間の通信の認証および暗号化に使用するキー文字列を入力します。このキーは、RADIUSサーバで設定されているキーと一致している必要があります。暗号化またはプレーンテキスト**形式**で入**力できます**。[Use **Default**]が選択されている場合、デバイスはデフォルトのキー文字列を使用してRADIUSサーバへの認証を試みます。ここでは、ユーザ定義(**Plaintext)を使用**し、キーの例を入力**します**。

**注**：残りの設定はデフォルトのままにします。必要に応じて設定できます。

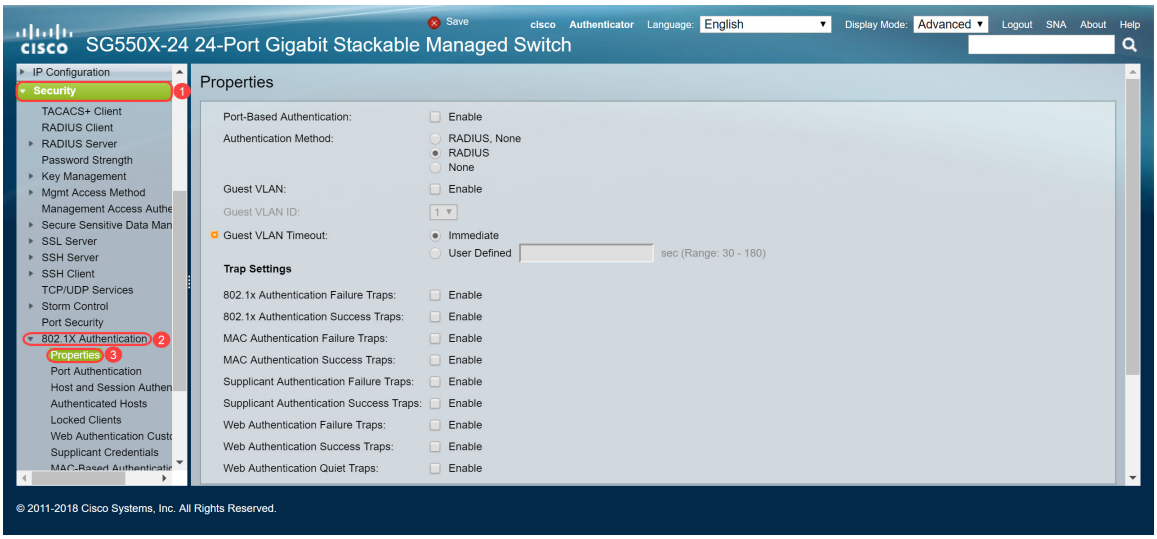



ステップ8:[Apply]をクリックして、設定を保存します。

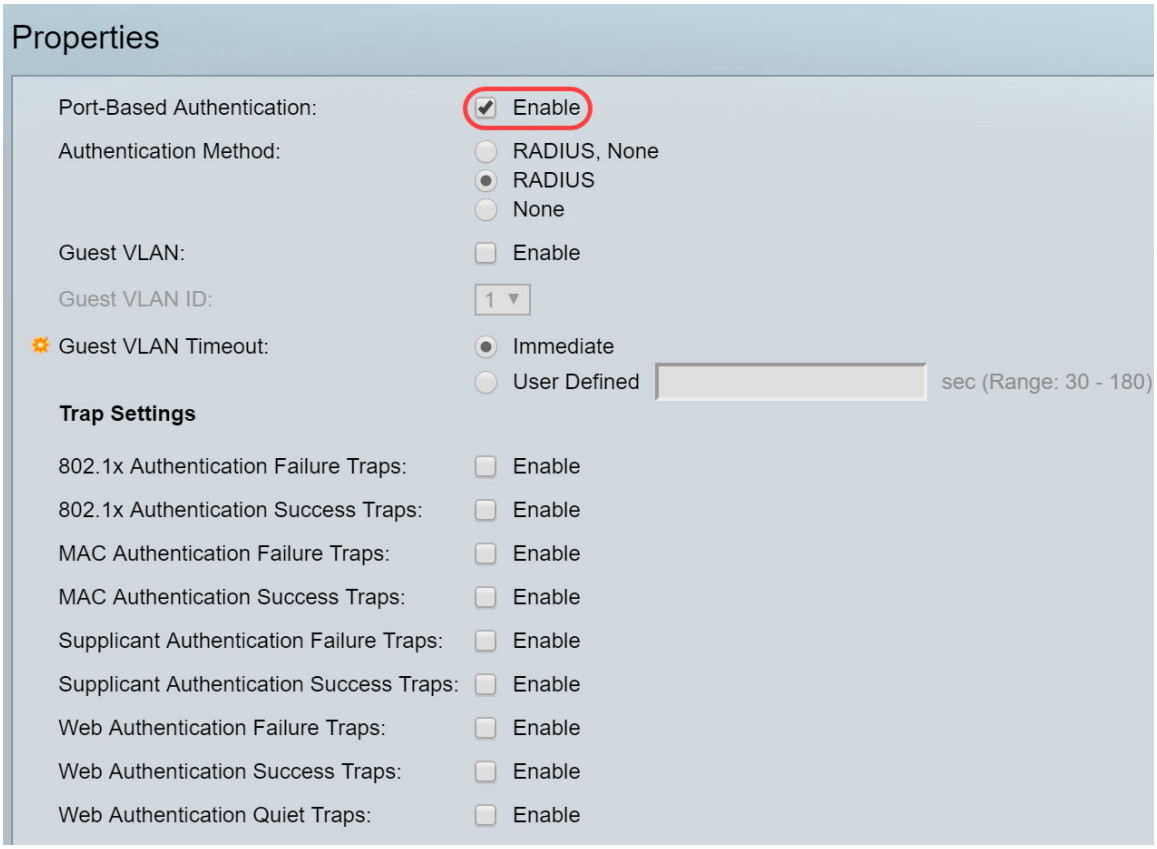
# 802.1X認証プロパティ

[Properties]ページは、ポート/デバイス認証をグローバルに有効にするために使用します。認証を機能させるには、各ポートでグローバルおよび個別にアクティブにする必要があります。

ステップ1:[Security] > [802.1X Authentication] > [Properties]に移動します。

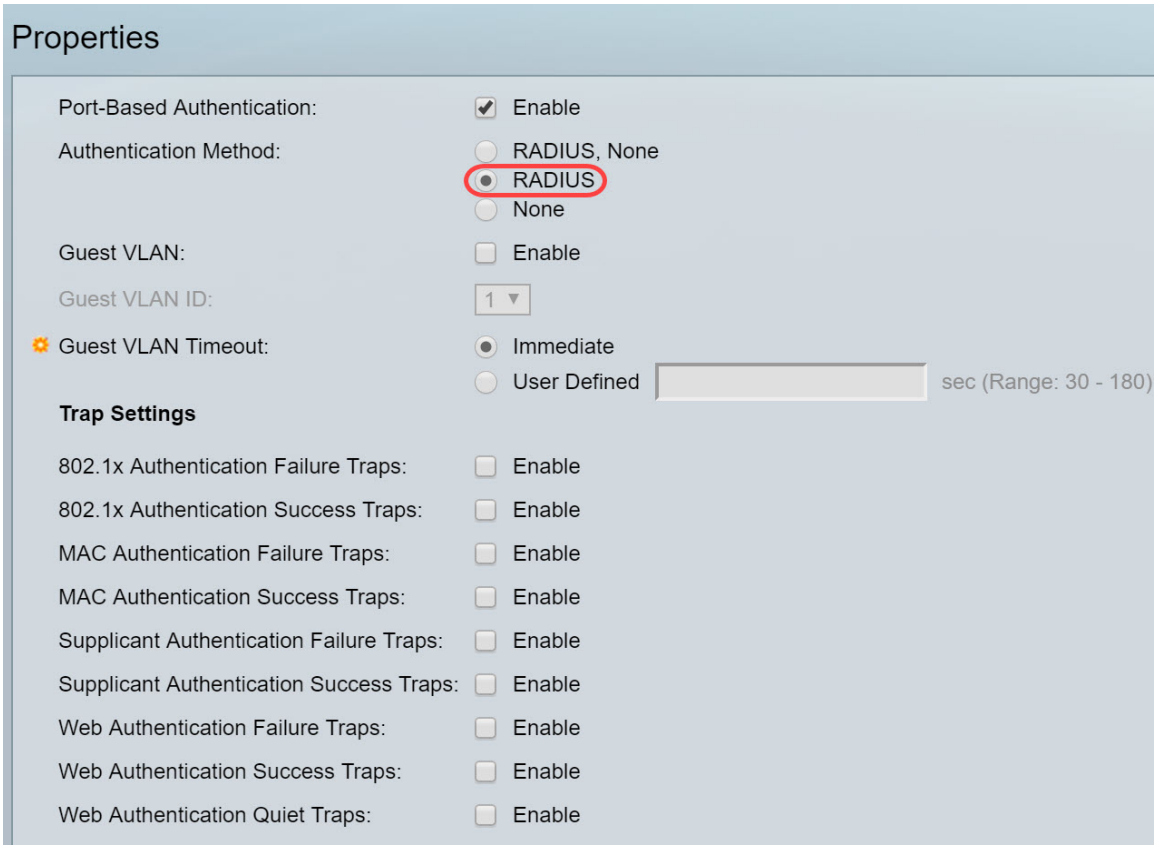



ステップ2:[Enable] チェックボックスをオンにして、ポートベース認証を有効にします。

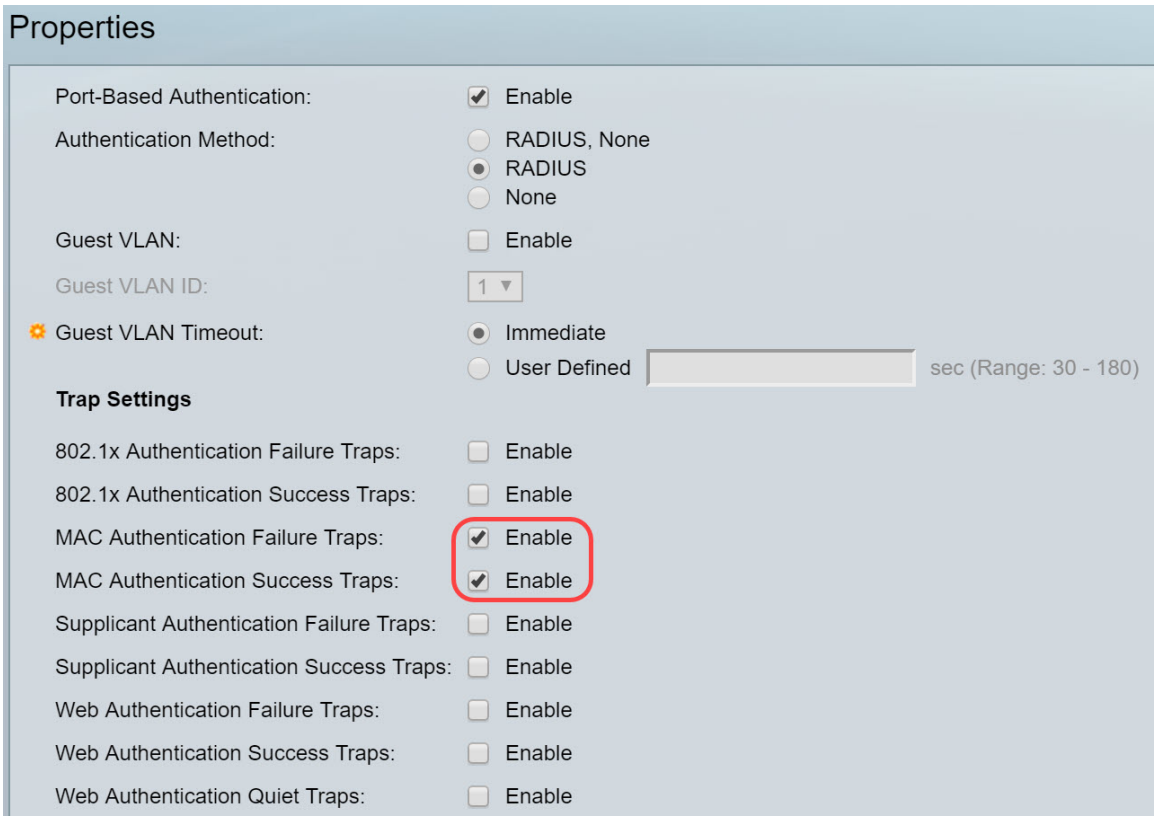



ステップ3：ユーザ認証方法を選択します。認証方式としてRADIUSを選択します。次のオプションがあります。

- RADIUS, None:RADIUSサーバを使用して、最初にポート認証を実行します。RADIUSから応答が受信されない場合（サーバがダウンしている場合など）、認証は実行されず、セッションは許可されます。サーバは使用可能であるが、ユーザのクレデンシャルが正しくない場合、アクセスは拒否され、セッションは終了します。
- RADIUS:RADIUSサーバでユーザを認証します。認証が実行されない場合、セッションは許可されません。
- [None]：ユーザを認証しません。セッションを許可します。




ステップ4: ( オプション ) *MAC* Authentication Failure Trapsおよび*MAC Authentication Success Traps*の**Enable**チェックボックスをオンにします。これにより、MAC認証が失敗または成功した場合にトラップが生成されます。この例では、*MAC* Authentication Failure TrapsとMAC Authentication Success Trapsの*両方*を有効にします。

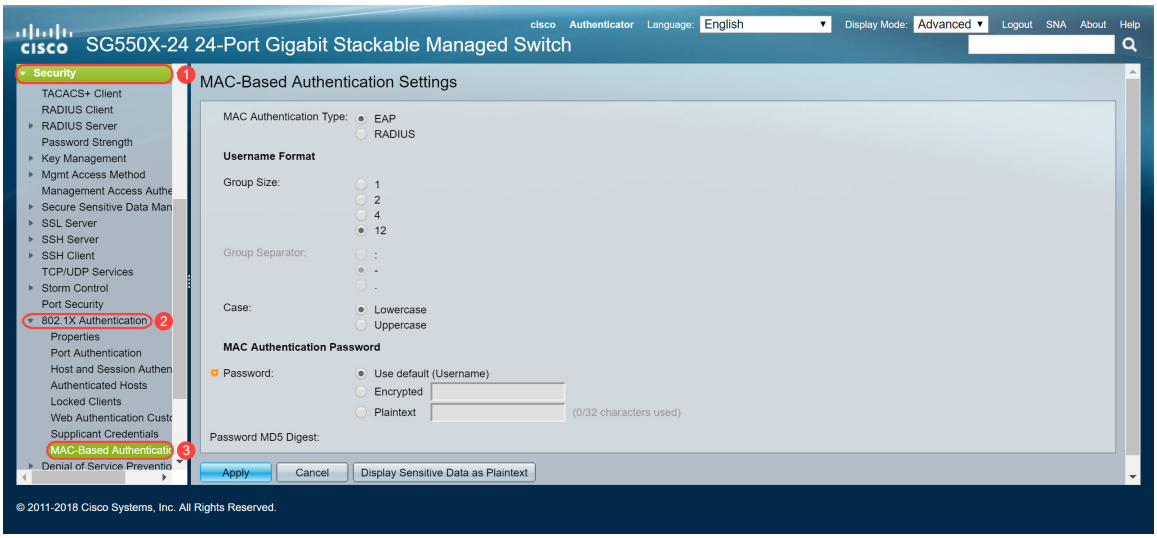



ステップ5:[Apply]をクリックします。

# 802.1X認証MACベースの認証設定

このページでは、MACベースの認証に適用できるさまざまな設定を設定できます。

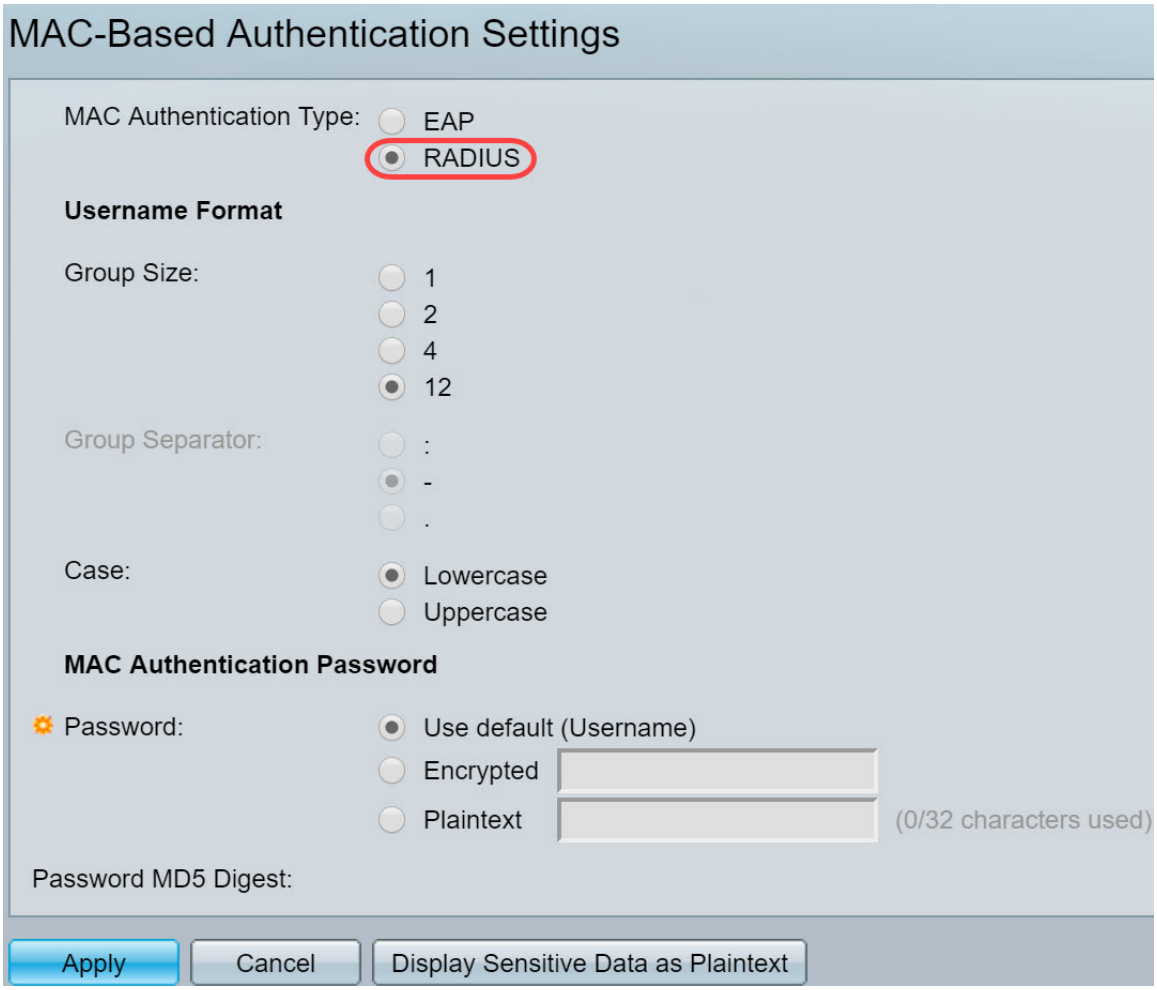
ステップ1:[Security] > [802.1X Authentication] > [MAC-Based Authentication Settings]に移動します。




ステップ2:[*MAC Authentication Type*]で、*次のいずれか*を選択します。

- EAP：スイッチ（RADIUSクライアント）とRADIUSサーバ間のトラフィックにEAPカプセル化されたRADIUSを使用します。RADIUSサーバはMACベースのサプリカントを認証します。
- RADIUS:MACベースのサプリカントを認証するスイッチ（RADIUSクライアント）とRADIUSサーバ間のトラフィックに対して、EAPカプセル化なしでRADIUSを使用します。

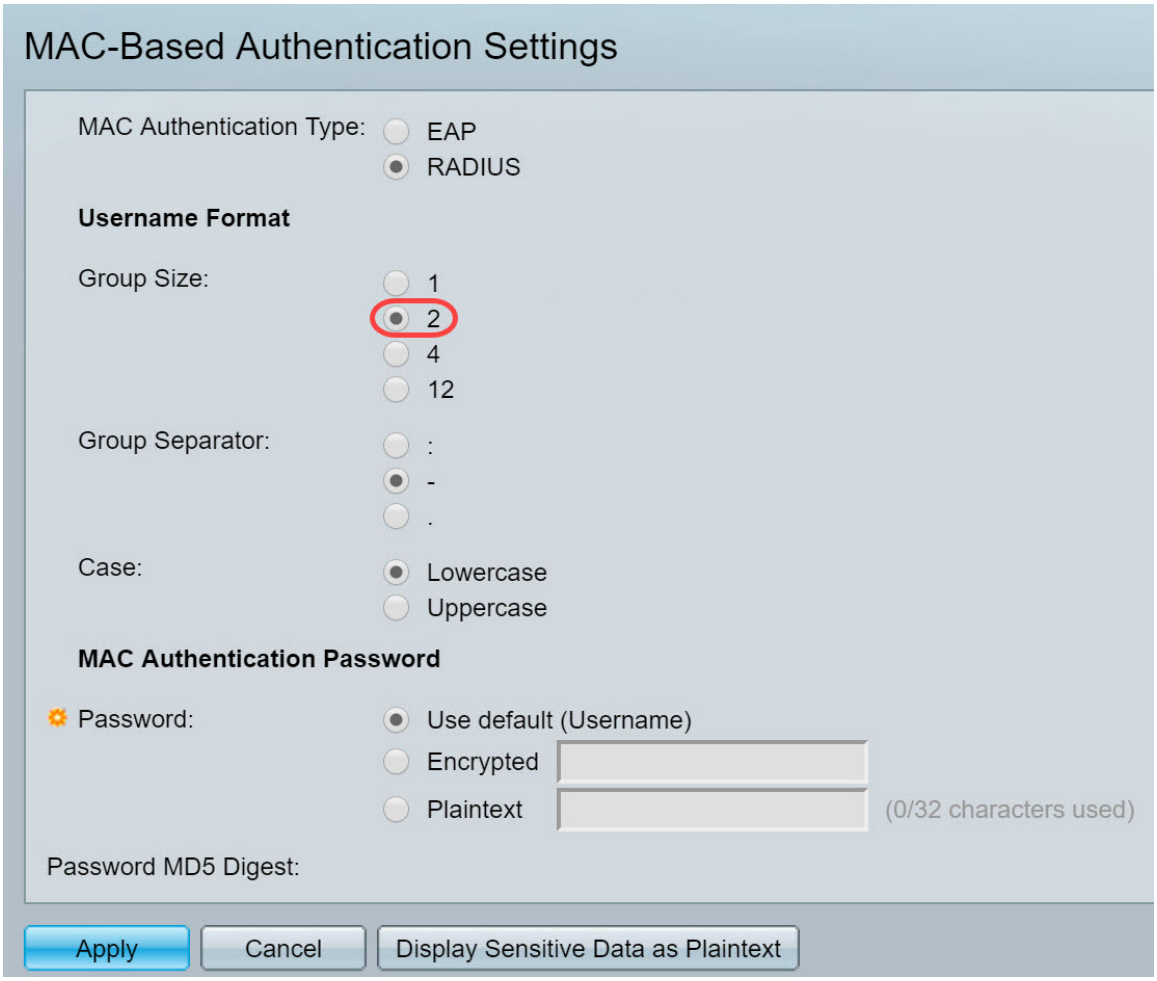
この例では、MAC認証タイプとしてRADIUSを選択します。



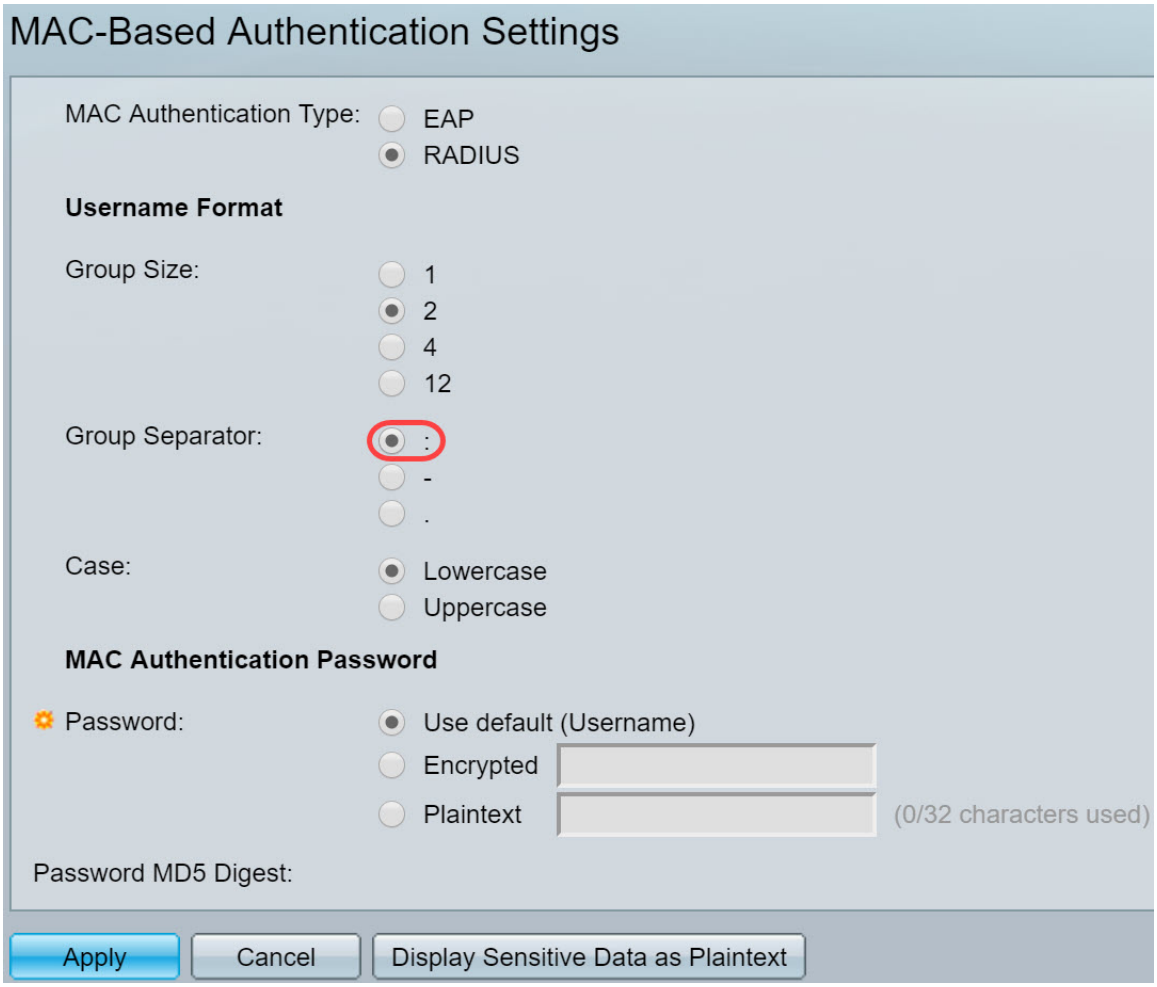

ステップ3:[ユーザ*名の形式*]で、ユーザ名として送信されるMACアドレスの区切り記号の間の

ASCII文字の数を選択します。この場合、グループサイズとして2を選択します。

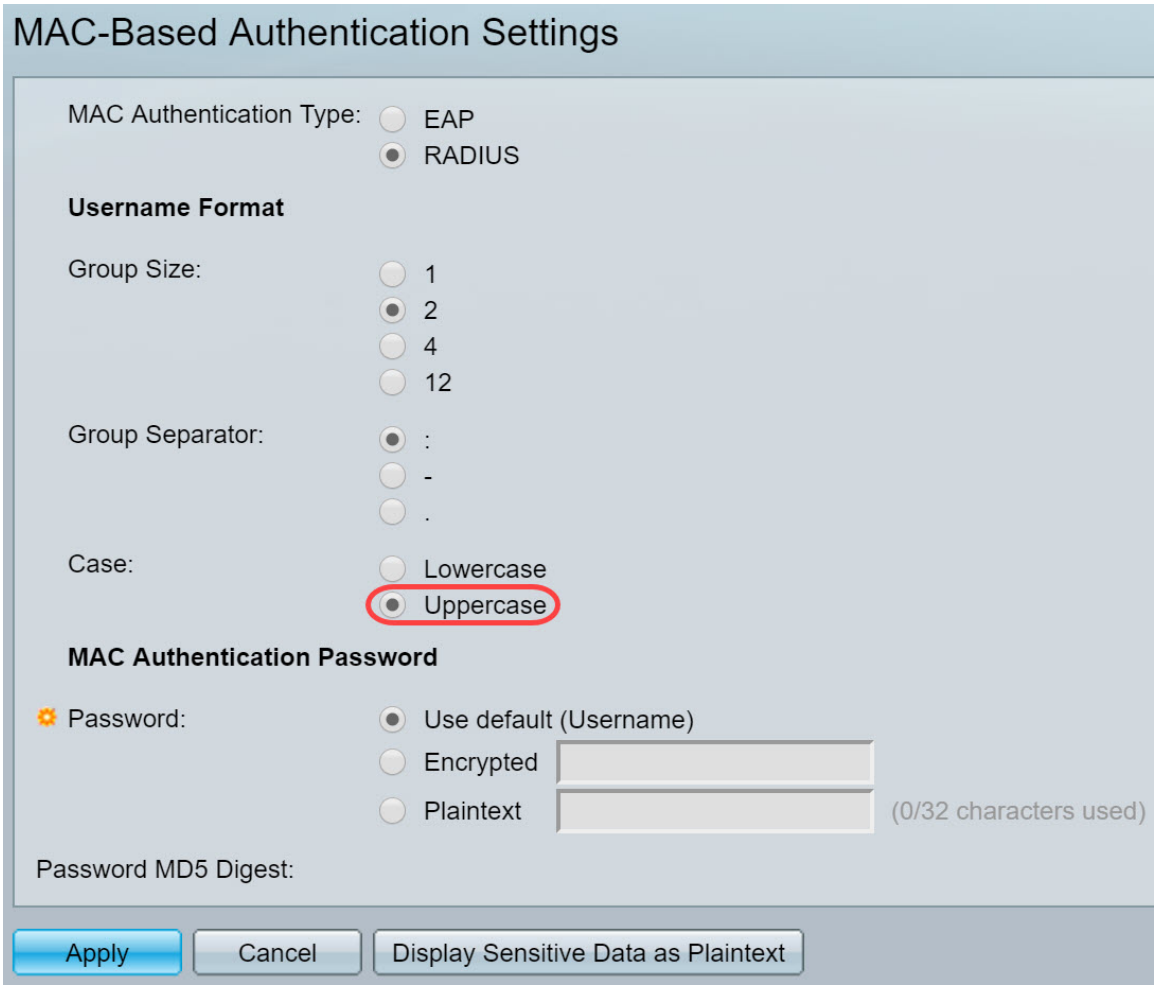
**注**：ユーザ名の形式が、[*Radius Server Users*]セクションでMACアドレスを入力する方法と同じであることを確認します。




ステップ4:MACアドレスで定義された文字グループ間の区切り文字として使用する文字を選択します。この例では、次の項目を選択します。グループ区切り記号として使用します

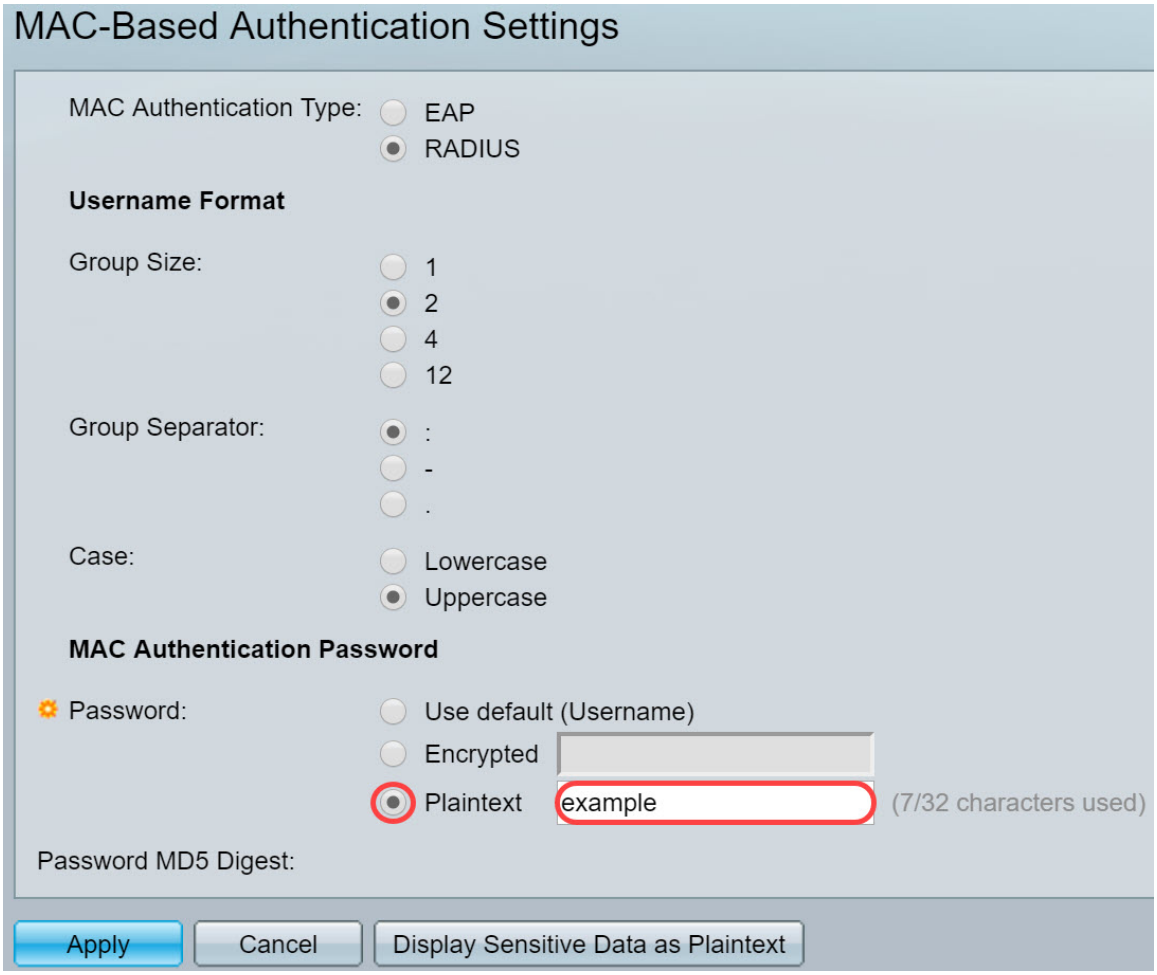



ステップ5:[大文字]フィールドで、[小文]または[大文]を選択し、ユーザー名を小文字または大文字で送信します。




ステップ6：パスワードは、スイッチがRADIUSサーバを介して認証に使用する方法を定義します。次のオプションのいずれかを選択します。

- [デフォルトを使用（ユーザ名）(Use default (Username))]：定義されたユーザ名をパスワードとして使用する場合に選択します。
- [Encrypted]：暗号化された形式でパスワードを定義します。
- プレーンテキスト：プレーンテキスト形式でパスワードを定義します。



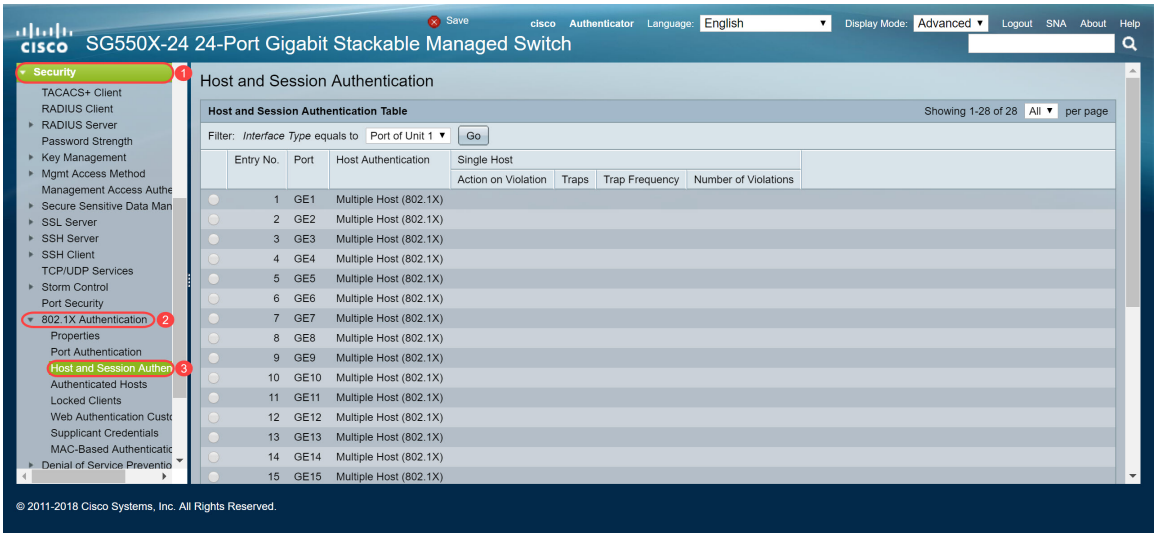

注：*Password Message-Digest Algorithm 5 (MD5) Digest*は、MD5ダイジェストパスワードを表示します。MD5は暗号化ハッシュ関数で、データの一部を取得し、通常は再生可能ではない一意の16進数出力を作成します。MD5は128ビットハッシュ値を使用します。

ステップ7:[Apply]をクリックし、設定が実行コンフィギュレーションファイルに保存されます。

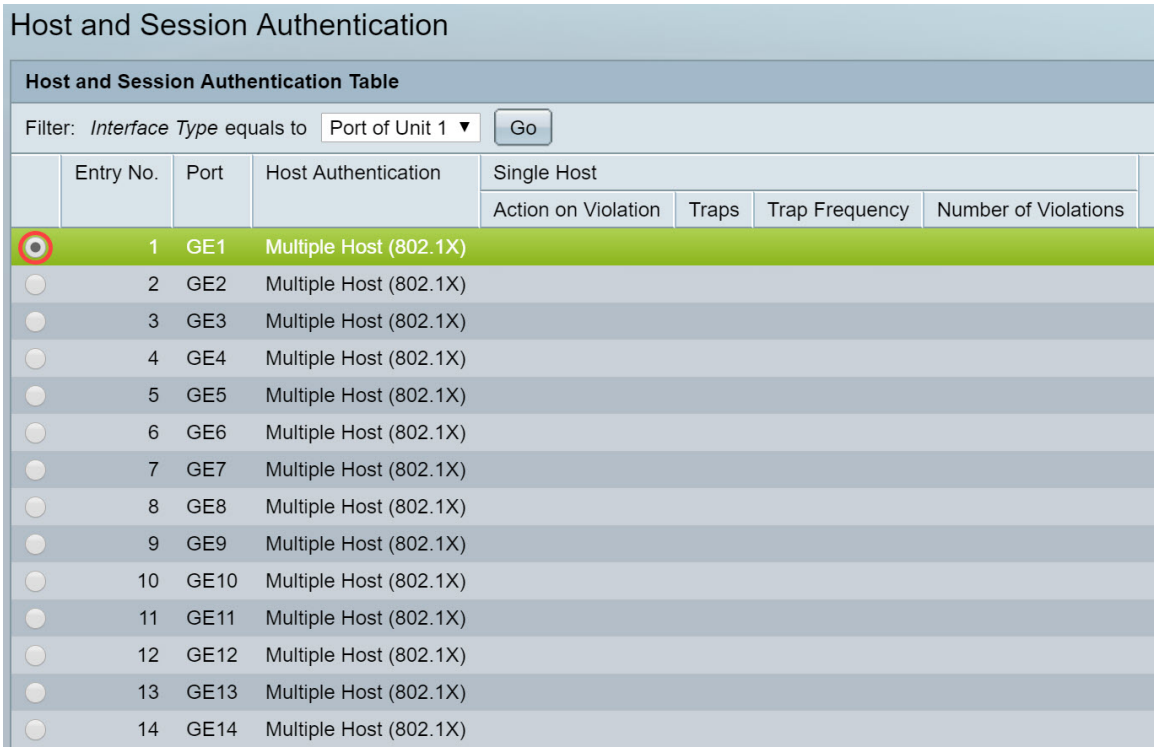
# 802.1X認証ホストおよびセッション認証

[*Host and Session Authentication*]ページでは、802.1Xがポートで動作するモードと、違反が検出された場合に実行するアクションを定義できます。

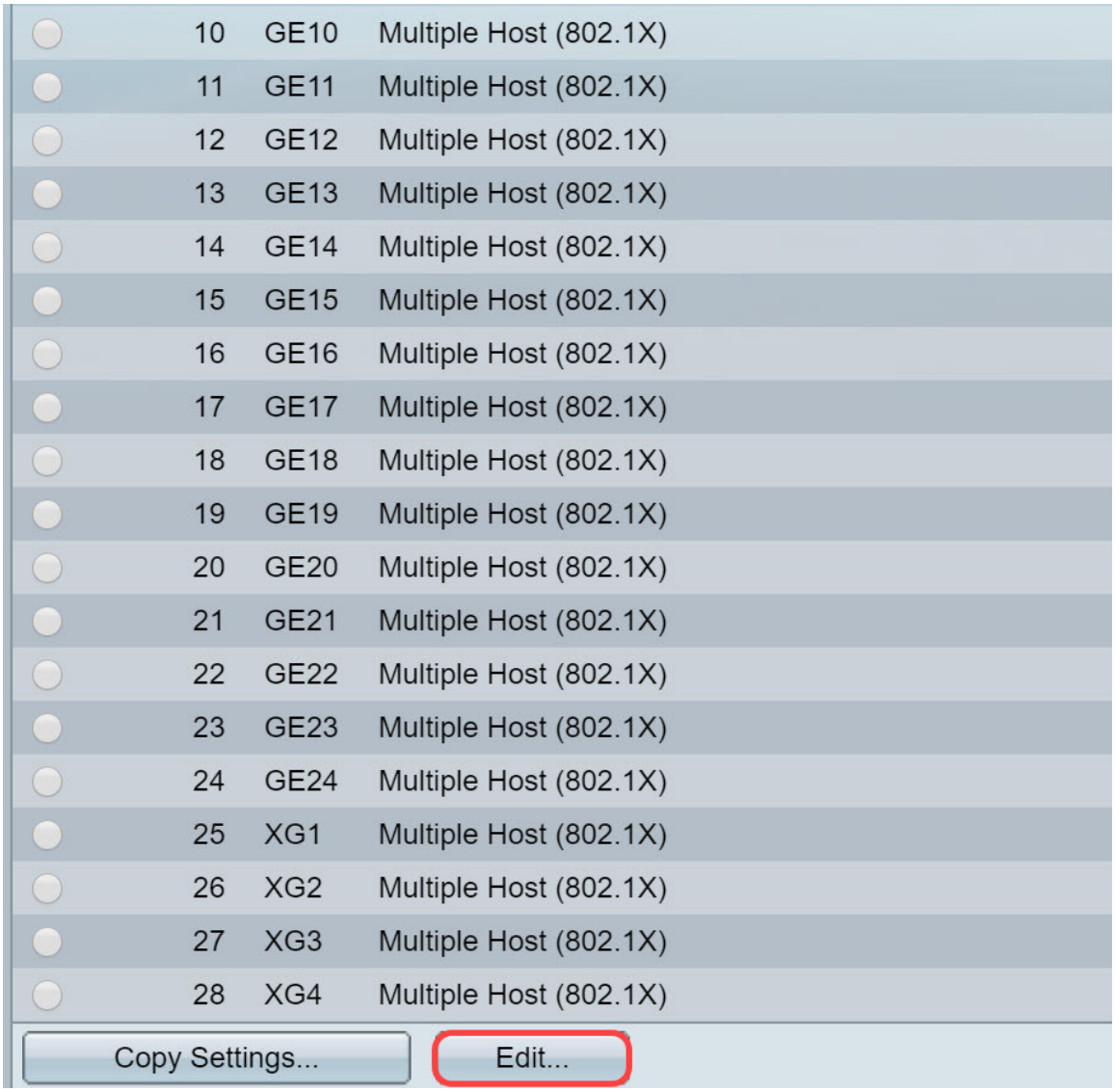
ステップ1:[Security] > [802.1X Authentication] > [Host and Session Authentication]に移動します。




ステップ2：ホスト認証を設定するポートを選択します。この例では、GE1をエンドホストに接続するように設定します。




ステップ3:**[Edit...]をクリックします。** ポートを設定します。

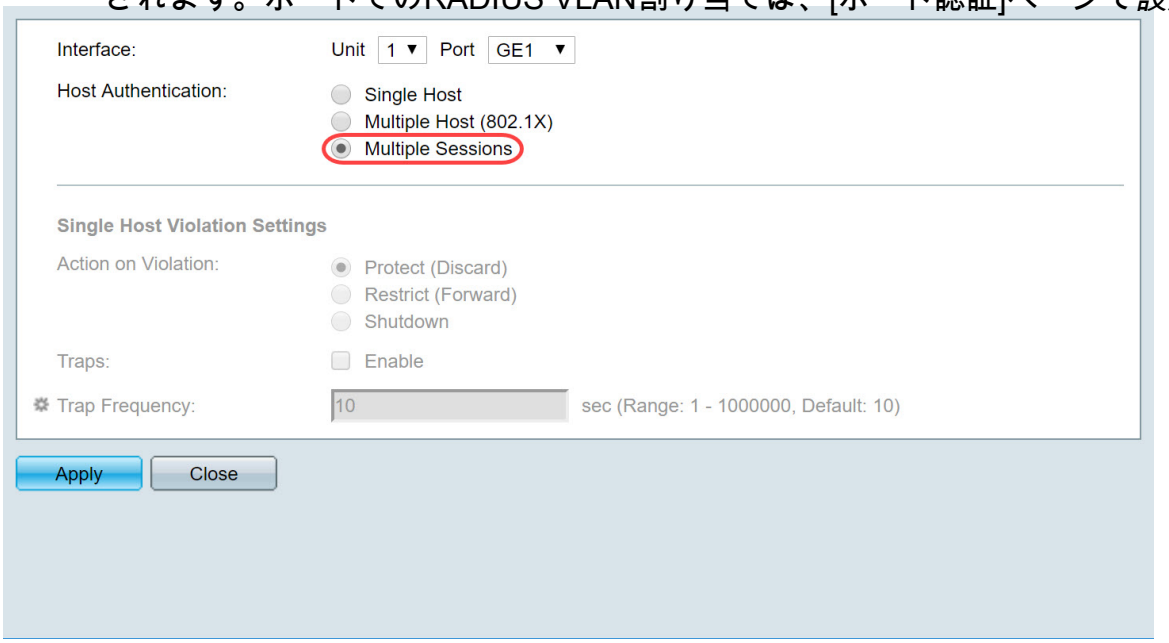



ステップ4:[*Host Authentication* ( ホスト認証 ) ]フィールドで、次のいずれかのオプションを選択します。

1. シングルホストモード
   - 許可されたクライアントがある場合、ポートは許可されます。1つのポートで許可できるホストは1つだけです。
   - ポートが不正で、ゲストVLANが有効になっている場合、タグなしトラフィックはゲストVLANに再マップされます。タグ付きトラフィックは、ゲストVLANまたは認証されていないVLANに属していない限り、ドロップされます。ゲストVLANがポートで有効になっていない場合、非認証VLANに属するタグ付きトラフィックだけがブリッジされます。
   - ポートが承認されると、承認されたホストからのタグなしトラフィックおよびタグ付きトラフィックは、スタティックVLANメンバーシップポート設定に基づいてブリッジされます。他のホストからのトラフィックはドロップされます。
   - ユーザは、認証プロセス中にRADIUSサーバによって割り当てられたVLANに、許可されたホストからのタグなしトラフィックが再マッピングされるように指定できます。タグ付きトラフィックは、RADIUSによって割り当てられたVLANまたは認証されていないVLANに属していない限り、ドロップされます。ポートでのRADIUS VLAN割り当ては、[ポート認証]ページで*設定*されます。
2. マルチホストモード
   - 許可されたクライアントが少なくとも1つ存在する場合、ポートは許可されます。
   - ポートが不正で、ゲストVLANが有効になっている場合、タグなしトラフィックはゲストVLANに再マップされます。タグ付きトラフィックは、ゲストVLANまたは認証されていな

いVLANに属していない限り、ドロップされます。ゲストVLANがポートで有効になっていない場合、非認証VLANに属するタグ付きトラフィックだけがブリッジされます。
- ポートが承認されると、スタティックVLANメンバーシップポート設定に基づいて、ポートに接続されているすべてのホストからのタグなしトラフィックとタグ付きトラフィックがブリッジされます。
- 認証プロセス中に、RADIUSサーバによって割り当てられたVLANに、認可ポートからのタグなしトラフィックが再マップされるように指定できます。タグ付きトラフィックは、RADIUSが割り当てたVLANまたは認証されていないVLANに属していない限り、ドロップされます。ポートでのRADIUS VLAN割り当ては、[ポート認証]ページで設定されます。

3. マルチセッションモード
- シングルホストモードとマルチホストモードとは異なり、マルチセッションモードのポートには認証ステータスはありません。このステータスは、ポートに接続された各クライアントに割り当てられます。
- 認証されていないVLANに属するタグ付きトラフィックは、ホストが許可されているかどうかにかかわらず、常にブリッジされます。
- 非認証VLANに属していない不正ホストからのタグ付きトラフィックおよびタグなしトラフィックは、VLANで定義および有効になっている場合はゲストVLANに再マップされ、ポートでゲストVLANが有効になっていない場合はドロップされます。
- 認証プロセス中に、RADIUSサーバによって割り当てられたVLANに、認可ポートからのタグなしトラフィックが再マップされるように指定できます。タグ付きトラフィックは、RADIUSが割り当てたVLANまたは認証されていないVLANに属していない限り、ドロップされます。ポートでのRADIUS VLAN割り当ては、[ポート認証]ページで設定します。




ステップ5:[Apply]をクリックして設定を保存します。

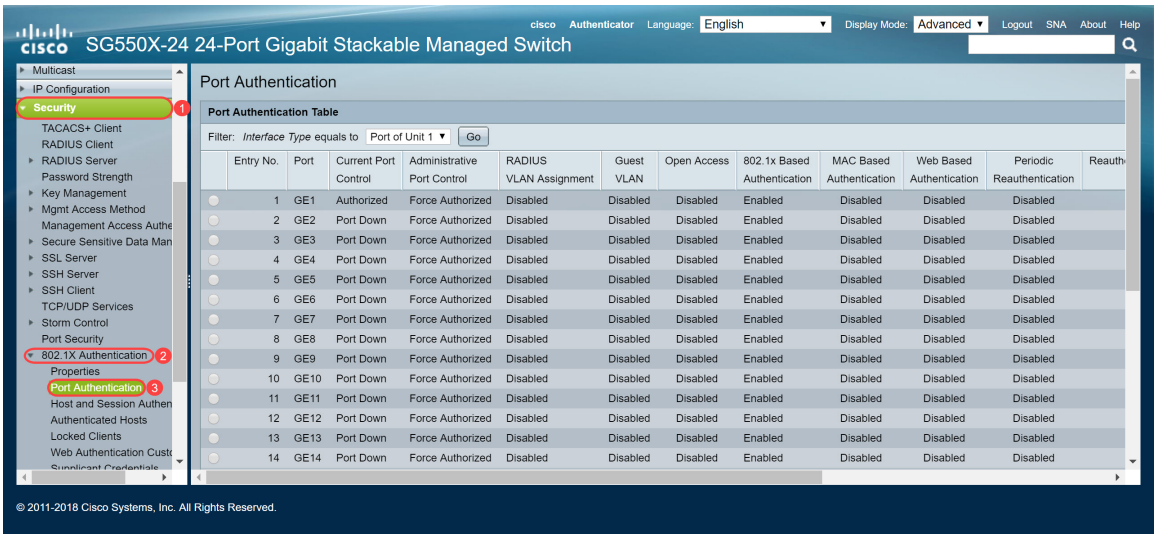
**注：**設定の*コピー*を*使用*... GE1の同じ設定を複数のポートに適用します。RADIUSサーバに接続されているポートは*Multiple Host (802.1X)*のままにします。

# 802.1X認証ポート認証

「ポート*認証*」ページでは、各ポートのパラメータを設定できます。設定の変更の一部は、ホスト認証など、ポートが強制承認済み状態である場合にのみ可能であるため、変更を行う前にポート制御を[強制承認済み(Force Authorized)]に変更することをお勧めします。設定が完了したら、ポート制御を以前の状態に戻します。

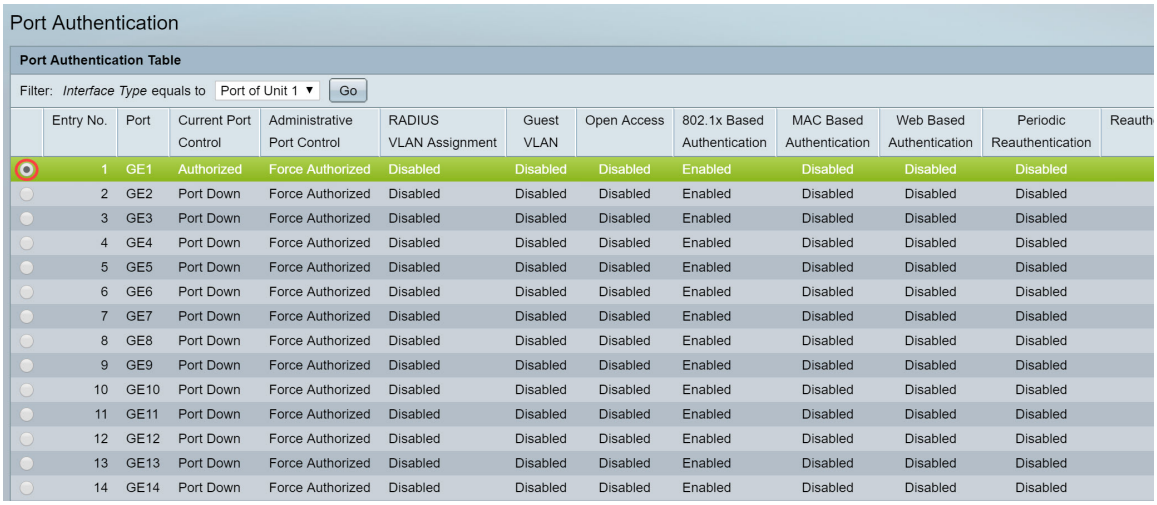
**注：ここでは、MACベースの認証に必要な設定だけを設定します。残りの設定はデフォルトのままになります。**

ステップ1:**[Security] > [802.1X Authentication] > [Port Authentication]に移動します。**

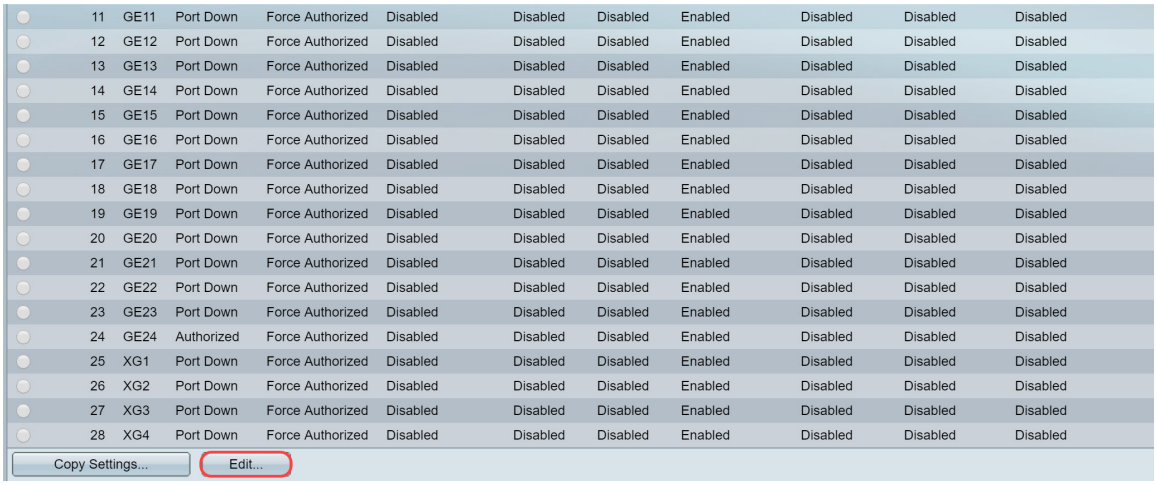



ステップ2：ポート許可を設定するポートを選択します。

**注：スイッチが接続されているポートは設定しないでください。スイッチは信頼できるデバイスであるため、そのポートは[強制*承認*]*のままにします。***




ステップ3：下にスクロールし、**[Edit...]をクリックします。** ポートを設定します。



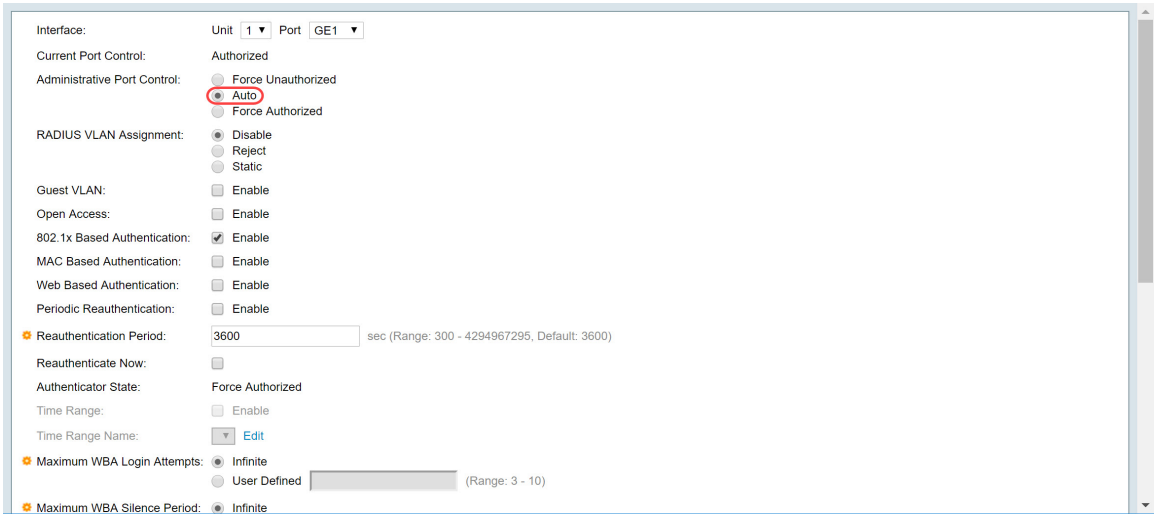

[ポート認証の*編集*]ページで、[現在のポート*制御*]*フィールド*に現在のポート認証状態が表示されます。状態がAuthorizedの場合は、ポートが認証されるか、管理ポート制御が*Force Authorized*になります。逆に、状態が*Unauthorized*の場合、ポートは認証されていないか、管理ポート制御は

*Force Unauthorized*になります。サプリカントがインターフェイスで有効になっている場合、現在のポート制御はサプリカントになります。

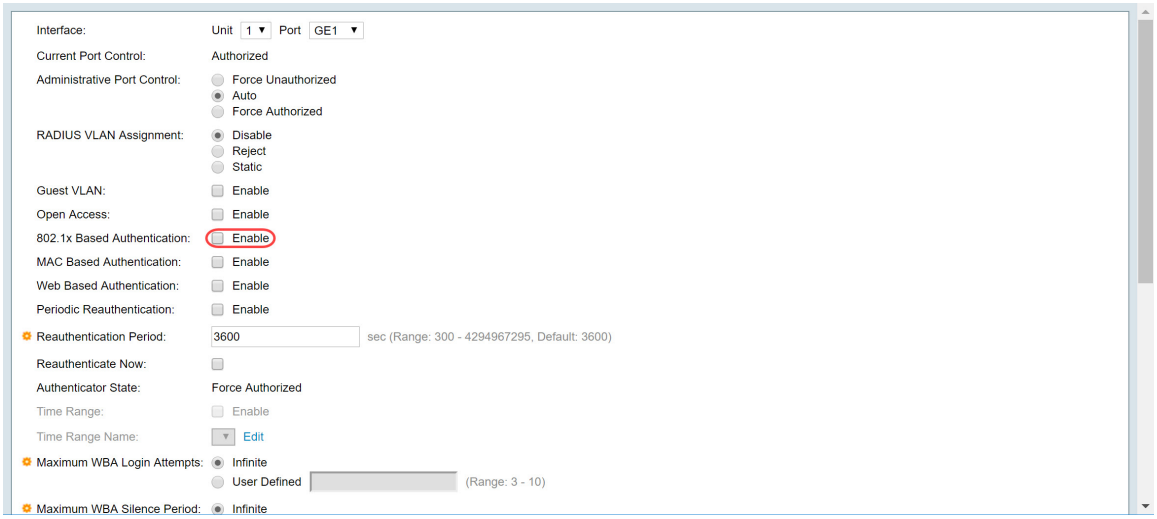
ステップ4：管理ポートの許可状態を選択します。ポートを自動に設定**します**。使用可能なオプションは次のとおりです。

- Forced Unauthorized：インターフェイスを不正な状態に移行することによって、インターフェイスアクセスを拒否します。デバイスは、インターフェイスを介してクライアントに認証サービスを提供しません。
- [Auto]：デバイスでポートベースの認証と許可を有効にします。インターフェイスは、デバイスとクライアント間の認証交換に基づいて、許可された状態または不正な状態の間を移動します。
- Forced Authorized：認証なしでインターフェイスを承認します。

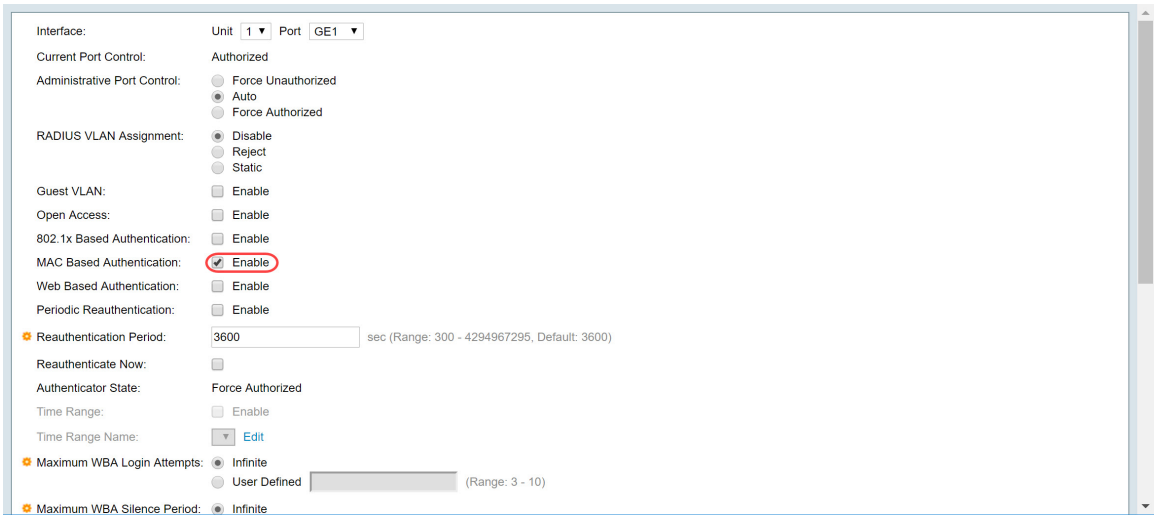
**注：[強制*承認]*は**既定値です。




ステップ5:[*802.1X Based Authentication]フィールド*で、[**Enable**]チェックボックスをオフにします。これは、認証に802.1Xを使用しないためです。802.1x Based Authenticationのデフォルト*値は有効*です。




ステップ6：サプリカントのMACアドレスに基づいてポート認証を有効にする場合は、[MAC Based Authentication] の[Enable]チェックボックスをオンにします。ポートで使用できるMACベースの認証は8つだけです。



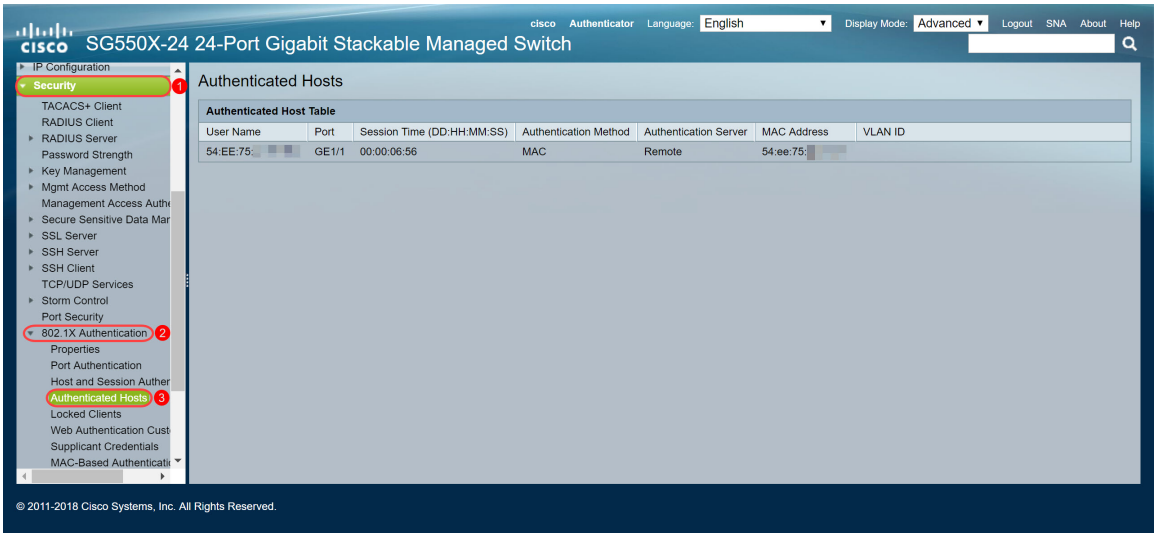

ステップ7:[Apply]をクリックして、変更を保存します。

設定を保存する場合は、画面の上部にある[保存]ボタンを押します。


# 結論

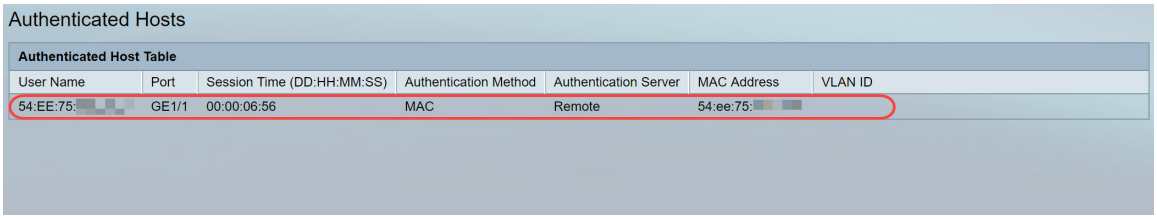
これで、スイッチでMACベースの認証が正常に設定されました。MACベースの認証が機能していることを確認するには、次の手順を実行します。

ステップ1:[Security] > [802.1X Authentication] > [Authenticated Hosts]に移動し、認証されたユーザに関する詳細を表示します。

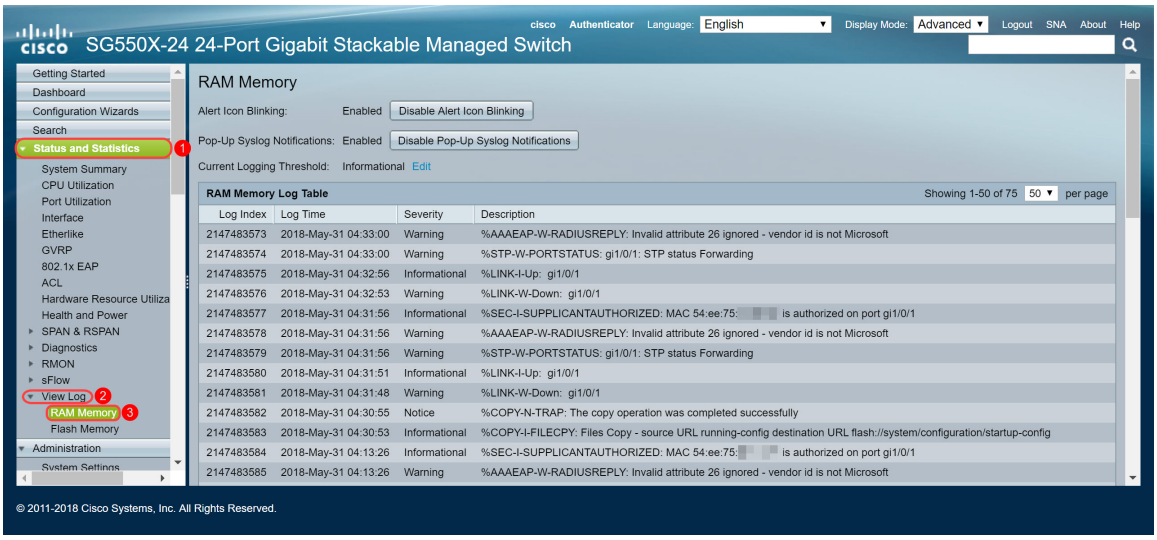



ステップ2：この例では、イーサネットMACアドレスが認証済みホストテーブルで認証されたことを*確認*できます。次のフィールドは次のように定義されます。

- [User Name]：各ポートで認証されたサプリカント名。
- Port：ポートの番号。
- Session Time(DD:HH:MM:SS)：サプリカントが認証され、ポートでアクセスが許可された時間。
- [Authentication Method]：最後のセッションが認証された方式。
- [Authenticated Server]:RADIUSサーバ。
- [MAC Address]：サプリカントのMACアドレスを表示します。
- VLAN ID：ポートのVLAN。




ステップ3: ( オプション ) [Status and **Statistics] > [View Log] > [RAM Memory]に移動します。** [RAMメモリ]ページには、RAM ( キャッシュ ) に保存されたすべてのメッセージが時系列で表示されます。エントリは、[ログの設定]ページの設定に従ってRAMログに*保存*されます。




ステップ4:*RAMメモリログテーブル*に、ポートgi1/0/1でMACアドレスが許可されていることを示す情報ログメッセージが表示されます。

**注**：MACアドレスの一部がぼやけている。


## この記事のビデオ版を表示...

[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]