スイッチでの802.1xポート認証設定の設定

目的

IEEE 802.1xは、クライアントとサーバ間のアクセス制御を容易にする標準です。ローカルエリアネットワーク(LAN)またはスイッチによってクライアントにサービスを提供するには、スイッチポートに接続されたクライアントが、リモート認証ダイヤルインユーザサービス(RADIUS)を実行する認証サーバによって認証される必要があります。

802.1x認証では、許可されていないクライアントがパブリケーションアクセス可能なポートを介してLANに接続することを制限します。802.1x認証は、クライアントサーバモデルです。このモデルでは、ネットワークデバイスには次の役割があります。

クライアントまたはサプリカント：クライアントまたはサプリカントは、LANへのアクセスを要求するネットワークデバイスです。クライアントはオーセンティケータに接続されています。

オーセンティケータ：オーセンティケータは、ネットワークサービスを提供し、サプリカントポートが接続されているネットワークデバイスです。次の認証方式がサポートされています。

802.1xベース：すべての認証モードでサポートされます。802.1xベースの認証では、オーセンティケータは802.1xメッセージまたはEAP over LAN(EAPoL)パケットからExtensible Authentication Protocol(EAP)メッセージを抽出し、RADIUSプロトコルを使用して認証サーバに渡します。

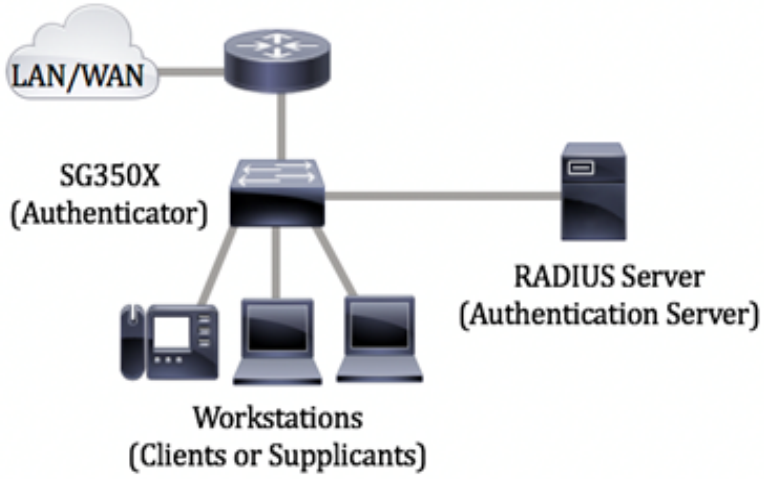
MACベース：すべての認証モードでサポートされます。メディアアクセス制御(MAC)ベースでは、オーセンティケータ自体が、ネットワークアクセスを求めるクライアントに代わってソフトウェアのEAPクライアント部分を実行します。

Webベース：マルチセッションモードでのみサポートされます。Webベース認証では、オーセンティケータ自体が、ネットワークアクセスを求めるクライアントに代わってソフトウェアのEAPクライアント部分を実行します。

認証サーバ：認証サーバは、クライアントの実際の認証を実行します。デバイスの認証サーバは、EAP拡張を備えたRADIUS認証サーバです。

注：ネットワークデバイスは、クライアントまたはサプリカント、オーセンティケータ、または両方のポートを使用できます。

次の図は、特定のロールに従ってデバイスを設定したネットワークを示しています。この例では、SG350Xスイッチが使用されています。



802.1x設定のガイドライン：

仮想アクセスネットワーク(VLAN)を作成します。 スイッチのWebベースのユーティリティを使用してVLANを作成するには、ここをクリックします。CLIベースの手順については、ここをクリックします。

スイッチのポートからVLANへの設定を行います。Webベースのユーティリティを使用して設定するには、ここをクリックします。CLIを使用するには、ここをクリックします。

スイッチで802.1xプロパティを設定します。802.1xポートベース認証を有効にするには、スイッチで802.1xをグローバルに有効にする必要があります。手順についてはここをクリックしてください。

（オプション）スイッチで時間範囲を設定します。スイッチで時間範囲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。

802.1xポート認証を設定します。この記事では、スイッチの802.1xポート認証設定の設定方法について説明します。

スイッチで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。

該当するデバイス

Sx300シリーズ

Sx350シリーズ

SG350Xシリーズ

Sx500シリーズ

Sx550Xシリーズ

[Software Version]

1.4.7.06 — Sx300、Sx500

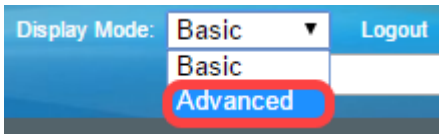
2.2.8.04 — Sx350、SG350X、Sx550X

スイッチでの802.1xポート認証設定の設定

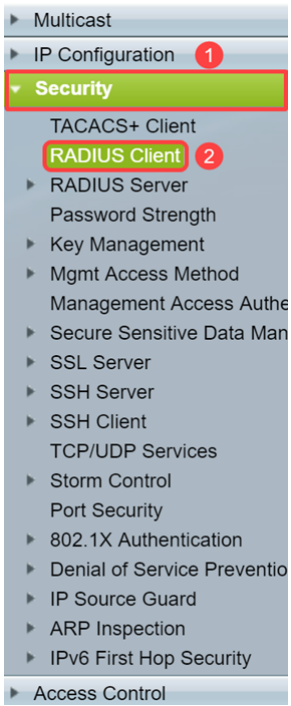
RADIUSクライアントの設定

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で[**Advanced**]を選択します。

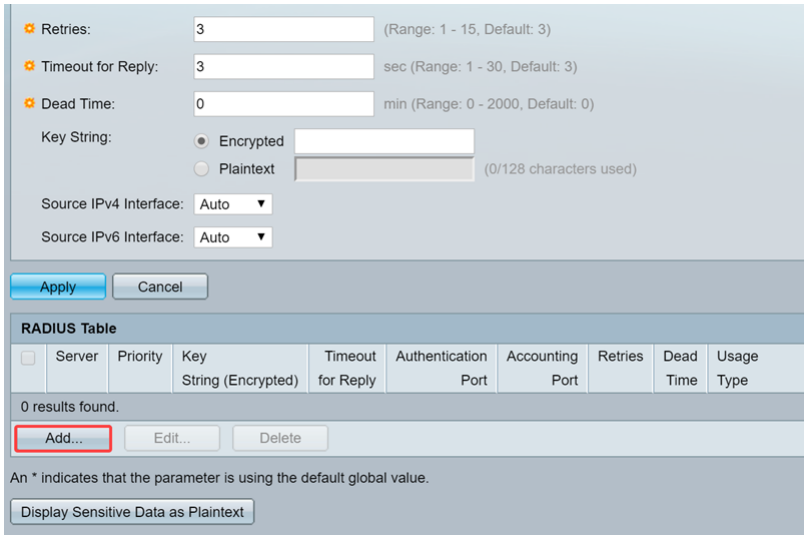
注：使用できるメニューオプションは、デバイスのモデルによって異なります。この例では、SG550X-24が使用されています。



ステップ2:[Security] > [**RADIUS Client**]**に移動します。**

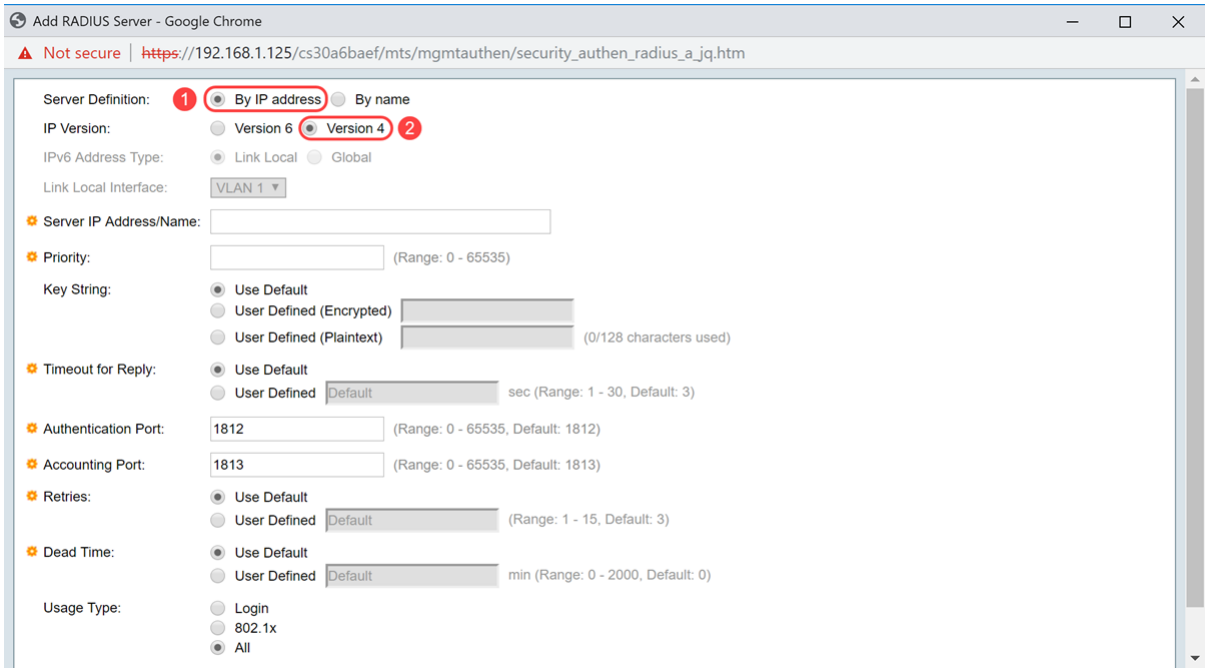


ステップ3:[*RADIUS Table*]セクションまで下にスクロールし、[**Add...]をクリック**してRADIUSサーバを追加します。



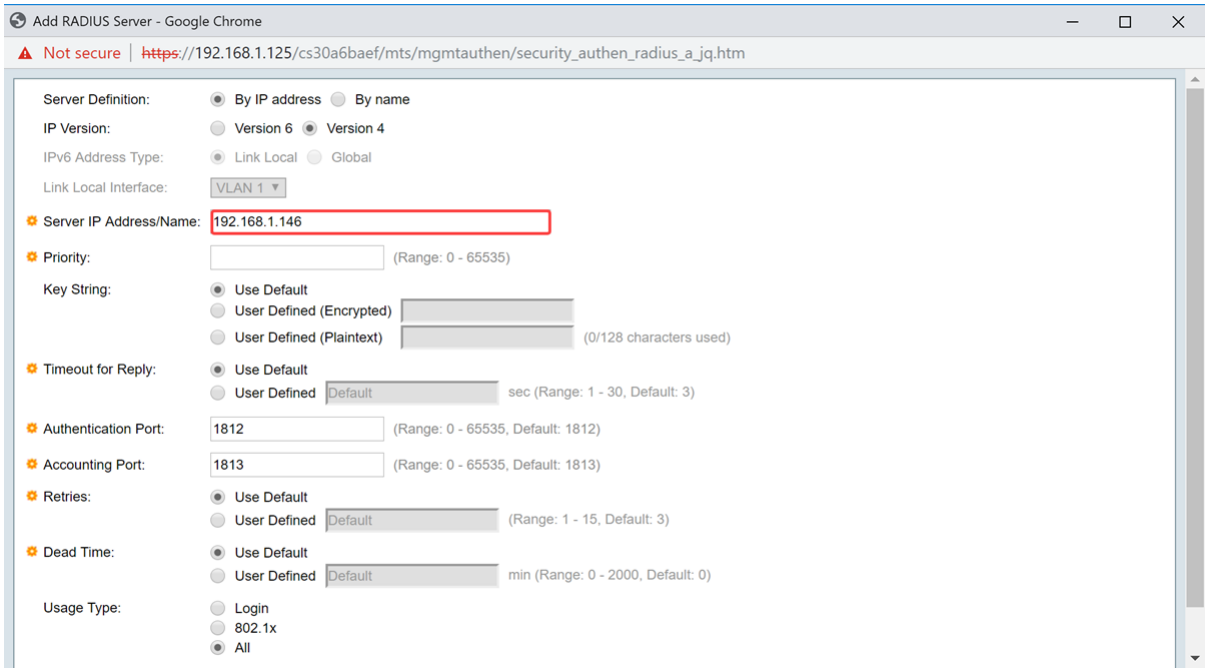
ステップ4:[Server Definition]フィールドで、RADIUSサーバをIPアドレスまたは名前で指定するかどうかを選択します。[IP Version]フィールドで、RADIUSサーバのIPアドレスのバージョンを選択します。

注：この例では、By IP addressとVersion 4を使用します。

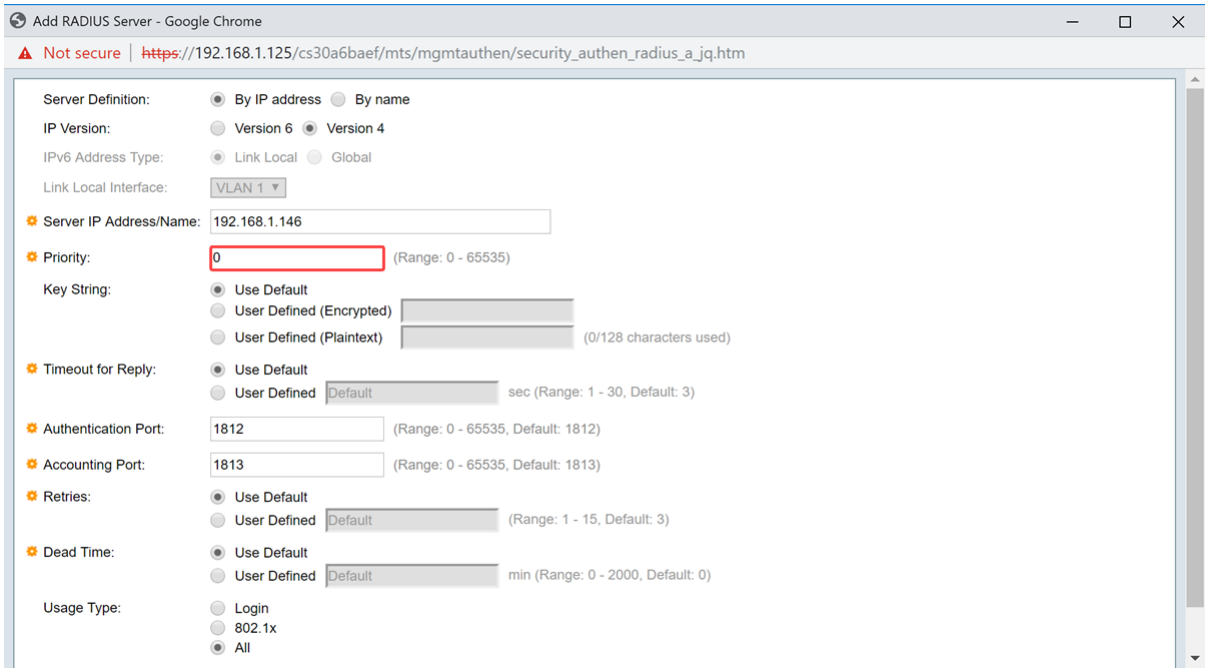


ステップ5:RADIUSサーバでIPアドレスまたは名前を入力します。

注：[Server IP Address/Name]フィールドに**192.168.1.146のIPア**ドレスを入力します。



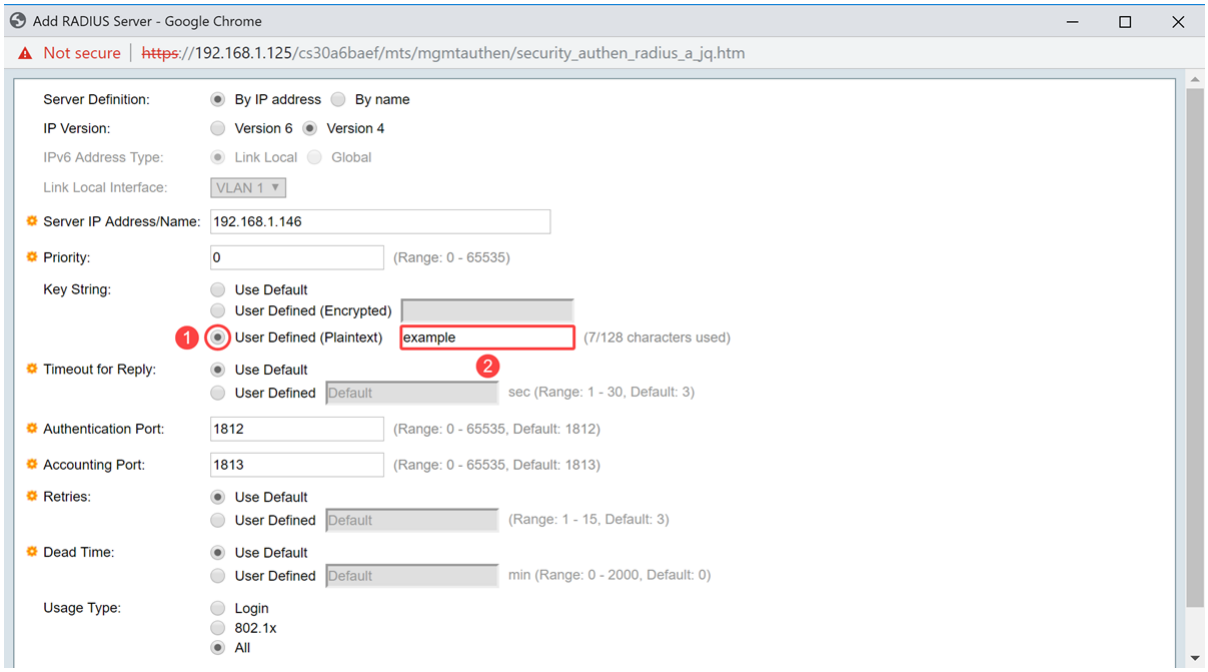
ステップ6：サーバの優先度を入力します。優先順位によって、デバイスがユーザを認証するためにサーバに接続する順序が決まります。デバイスは、最初に最も優先度の高いRADIUSサーバから開始します。0が最も高い優先順位です。



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。

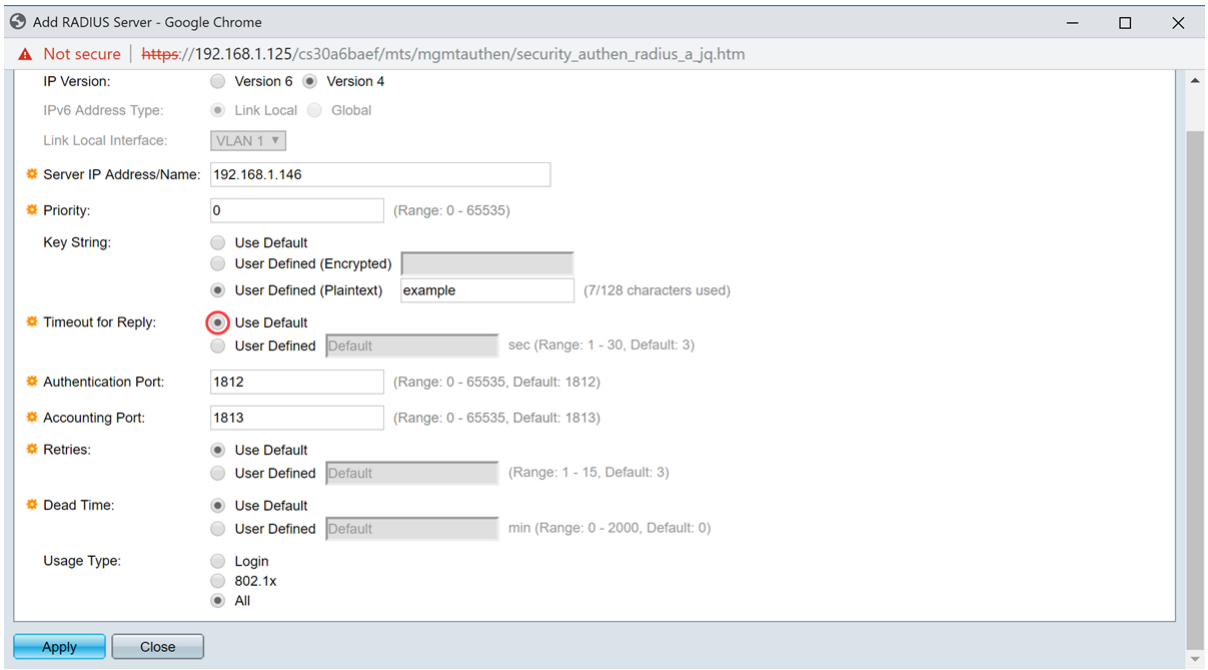
注：ここでは、ユーザ定義(Plaintext)を使用し、キーの例を入力します。

スイッチのRADIUSサーバーの設定方法については、ここをクリックしてください。



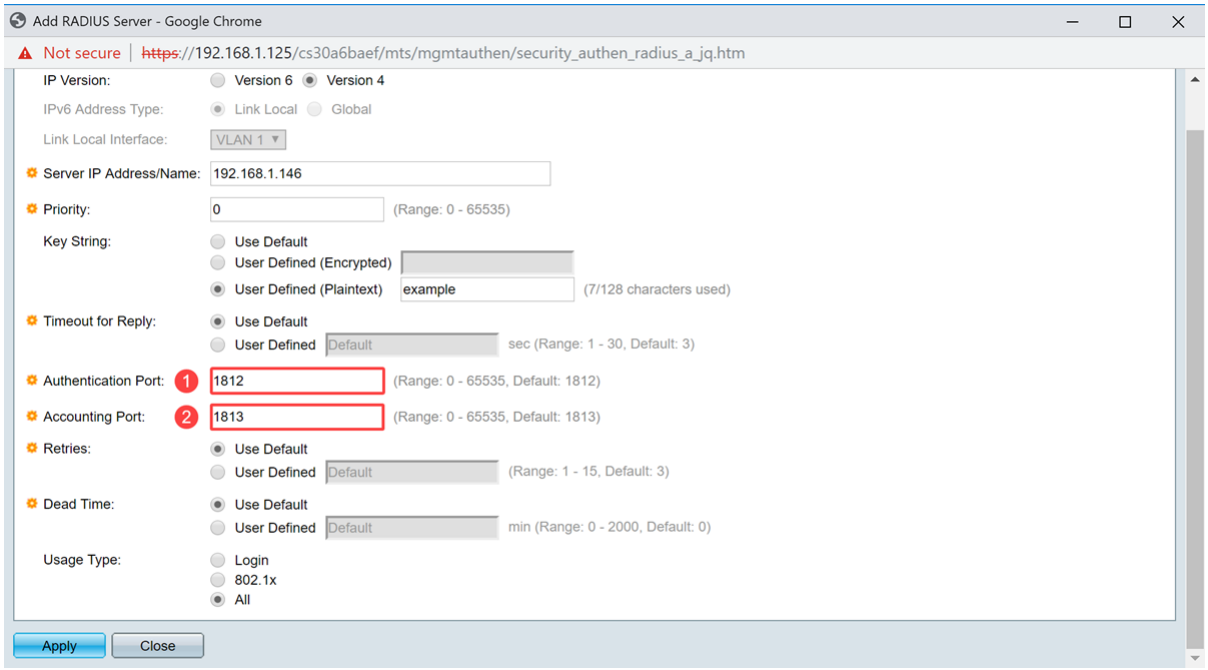
ステップ8:[応答のタイムアウト*]フィールド*で、[既定を使**用]または[ユ**ーザ定**義]を選択しま**す。[User Defined] を選択した場合は、クエリーを再試行する前にデバイスがRADIUSサーバからの応答を待機する秒数を入力するか、再試行の最大回数が設定されている場合は次のサーバに切り替えます。[Use **Default**]が**選択され**ている場合、デバイスはデフォルトのタイムアウト値を使用します。

注：この例では、[既定を使**用]が選択**されています。



ステップ9:[Authentication Port]フィールドに、認証要求に使用するRADIUSサーバポートのUDPポート番号を入力します。[Accounting Port]フィールドに、アカウンティング要求用のRADIUSサーバポートのUDPポート番号を入力します。

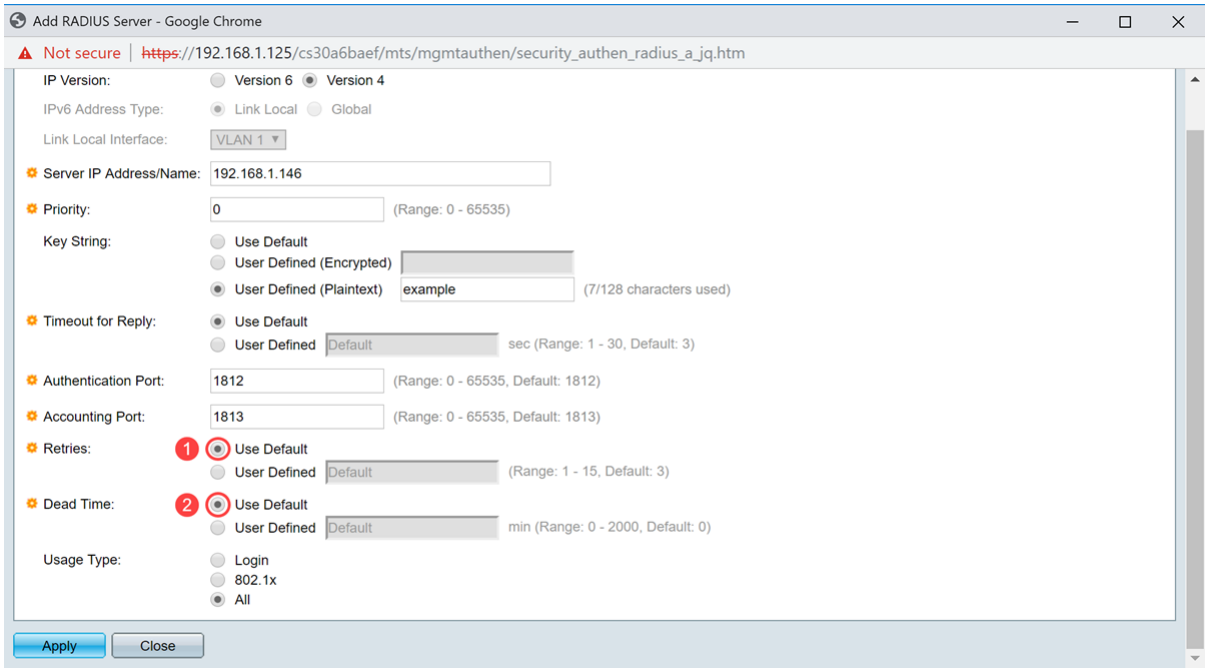
注：この例では、認証ポートとアカウンティングポートの両方にデフォルト値を使用します。



ステップ10:[Retries]フィールドで[**User Defined**]を選択した場合は、障害が発生したと見なされる前にRADIUSサーバに送信された要求の数を入力します。[Use **Default**]を**選択した**場合、デバイスは再試行の回数にデフォルト値を使用します。

[Dead Time] に[User Defined] を選択した場合は、応答しないRADIUSサーバがサービス要求にバイパスされるまでに経過する必要がある時間（分）を入力します。[Use **Default**]を**選択した**場合、デバイスはデッドタイムのデフォルト値を使用します。0分と入力すると、デッドタイムはありません。

注：この例では、これらのフィールドの両方に対して[**デフォルト**を使用]を選択します。

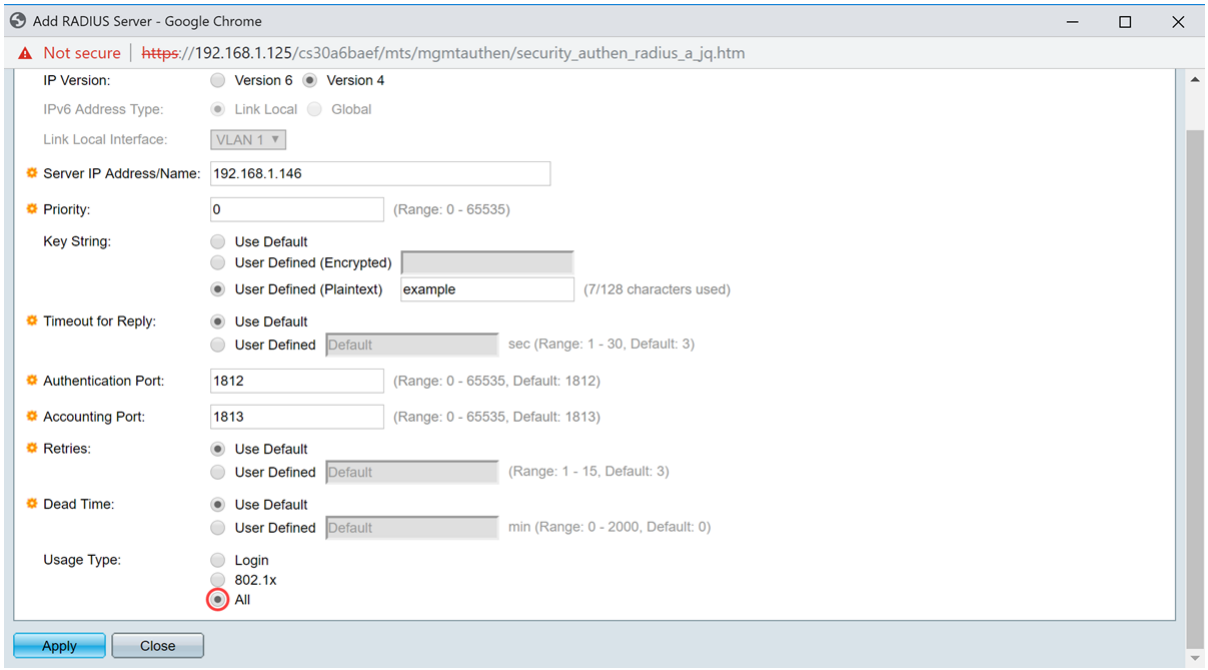


ステップ11:[Usage Type]フィールドに、*RADIUS*サーバーの認証タイプを入力します。次のオプションがあります。

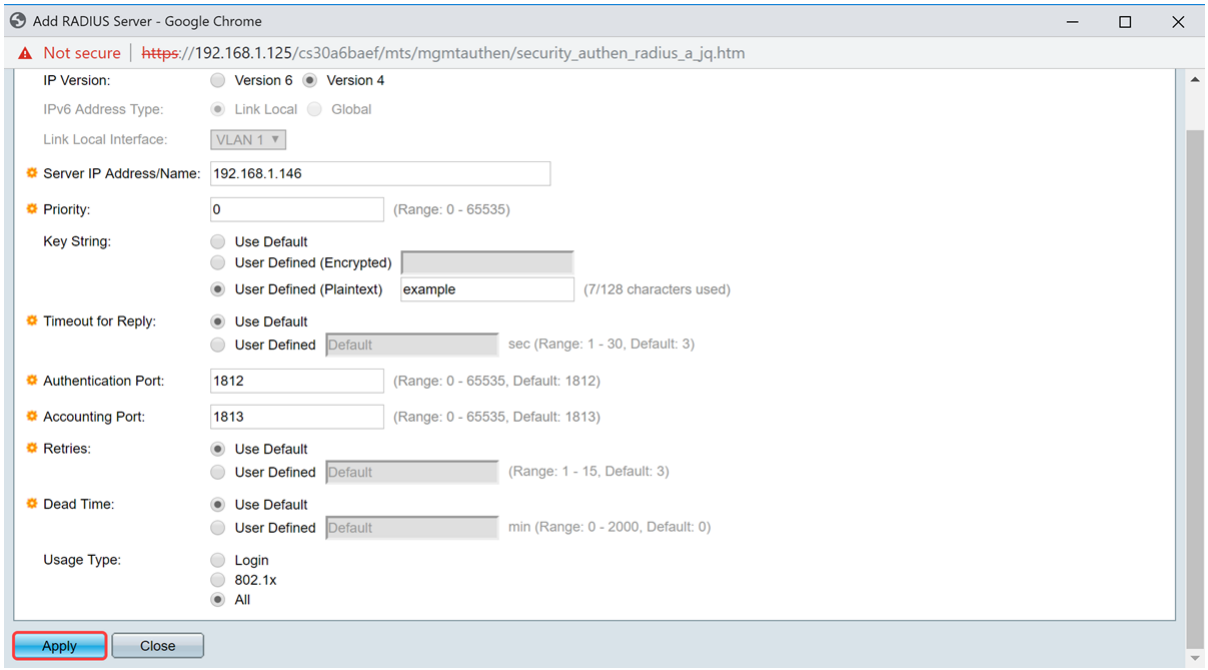
Login:RADIUSサーバは、デバイスの管理を要求するユーザの認証に使用されます。

802.1x:802.1x認証にはRADIUSサーバが使用されます。

All:RADIUSサーバは、デバイスの管理と802.1x認証を要求するユーザの認証に使用されます。



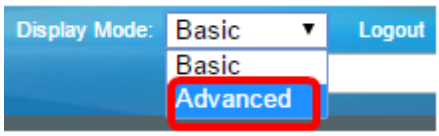
ステップ12:[Apply]をクリックします。



802.1xポート認証設定の設定

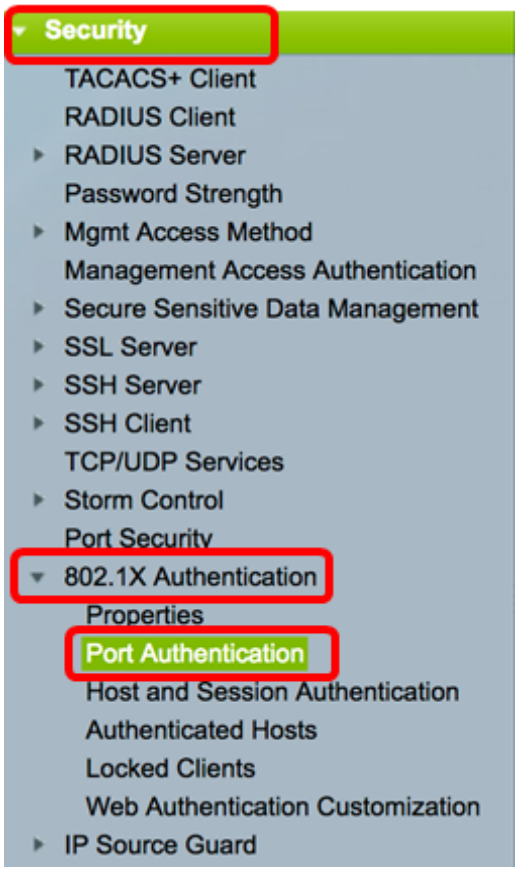
ステップ1：スイッチのWebベースのユーティリティにログインし、[Display Mode]ドロップダウンリストで[**Advanced**]を選択します。

注：使用できるメニューオプションは、デバイスのモデルによって異なります。この例では、SG350X-48MPが使用されています。



注：Sx300またはSx500シリーズスイッチを使用している場合は、ステップ2に進みます。

ステップ2:[Security] > [802.1X Authentication] > [Port Authentication]を選択します。

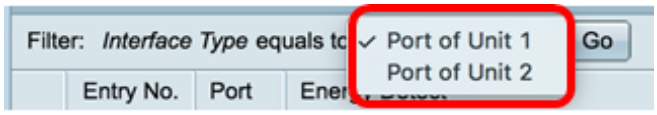


ステップ3:[インターフェイスタイプ]ドロップダウンリストからインターフェイスを選択します。

[ポート]:[インターフェイスタイプ]ドロップダウンリストから、1つのポートだけを選択する必要がある場合、[ポート]を選択します。

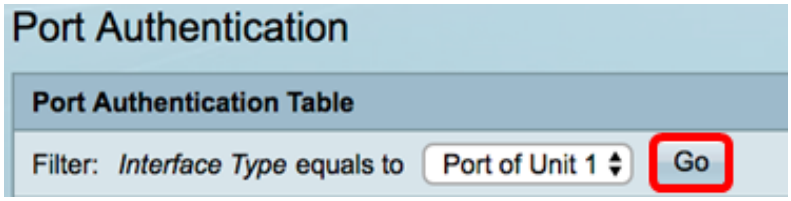
LAG:[インターフェイスタイプ]ドロップダウンリストから、設定するLAGを選択します。これは、LAG設定で定義されたポートのグループに影響します。

注：この例では、ユニット1のポートが選択されています。

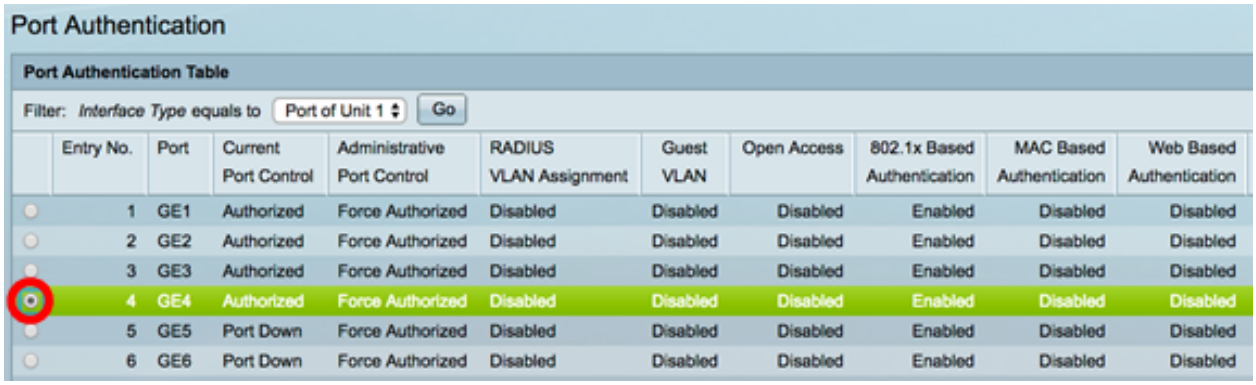


注：Sx300シリーズスイッチなど、スタック可能ではないスイッチがある場合は、ステップ5に進みます。

ステップ4:[Go]をクリックして、インターフェイス上のポートまたはLAGのリストを表示します。



ステップ5：設定するポートをクリックします。



注：この例では、GE4が選択されています。

ステップ6：ページを下にスクロールし、**[Edit]をクリックします。**

ステップ7:（オプション）別のインターフェイスを編集する場合は、[Unit and Port]ドロップダウンリストから選択します。

注：この例では、ユニット1のポートGE4が選択されています。

ステップ8:[Administrative Port Control]エリアで、目的のポート制御に対応する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。

Force Unauthorized：ポート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。ポートはトラフィックを廃棄します。

[Auto]：サプリカントの認証に基づいて、ポートが許可された状態または許可されていない状態の間で移動します。

Force Authorized：認証なしでポートを承認します。ポートはトラフィックを転送します。

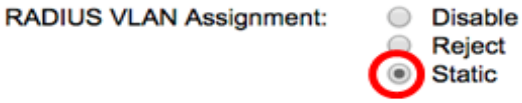
注：この例では、[Auto]が選択されています。

ステップ9:[RADIUS VLAN Assignment]オプションボタンをクリックして、選択したポートにダイナミックVLAN割り当てを設定します。次のオプションがあります。

Disable：機能が有効になっていません。

Reject:RADIUSサーバがサプリカントを承認したが、サプリカントVLANを提供しなかった場合、サプリカントは拒否されます。

[Static]:RADIUSサーバがサプリカントを承認したが、サプリカントVLANを提供しなかった場合、サプリカントは受け入れられます。



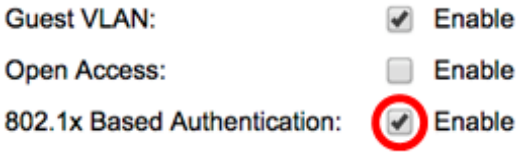
注：この例では、[Static]が選択されています。

ステップ10:[Guest VLAN]チェックボックスの[Enable] をオンにして、権限のないポートのゲストVLANを有効にします。ゲストVLANは、802.1プロパティのゲストVLAN ID領域で選択されたVLANに、許可されていないポートを自動的に参加させます。

ステップ11:（オプション）オープン・アクセスを有効にするには、「オープン・アクセスを有効にする」チェックボックスをオンにします。Open Accessを使用すると、ネットワークに接続するホストの設定の問題を理解し、問題の状況を監視し、これらの問題を解決できます。

注：インターフェイスでOpen Accessが有効な場合、スイッチはRADIUSサーバから受信したすべての障害を成功として扱い、認証結果に関係なく、インターフェイスに接続されているステーションのネットワークへのアクセスを許可します。この例では、[Open Access]は無効になっています。

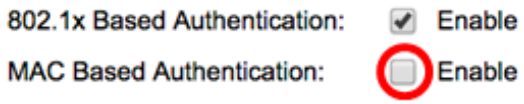
ステップ12：ポートで802.1X認証を有効にするには、[**Enable** 802.1x Based Authentication]チェックボックスをオンにします。



ステップ13：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には、

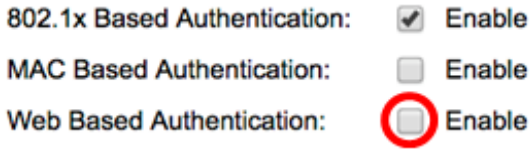
[Enable MAC Based Authentication]チェックボックスをオンにします。ポートで使用できるMACベースの認証は8つだけです。

注：MAC認証が成功するには、RADIUSサーバサプリカントユーザ名とパスワードがサプリカントのMACアドレスである必要があります。MACアドレスは、小文字で入力する必要があり、を使用せずに入力する必要があります。または – 区切り文字（0020aa00bbccなど）。



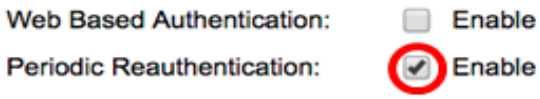
注：この例では、MACベースの認証が無効になっています。

ステップ14：スイッチでWebベースの認証を有効にするには、[Webベースの認証を有効にする(Enable Web Based Authentication)]チェックボックスをオンにします。この例では、Webベースの認証が無効になっています。



注：この例では、Webベースの認証が無効になっています。

ステップ15:（オプション）[Enable Periodic Reauthentication]チェックボックスをオンにして、特定の時間が経過した後にポートが再認証されるようにします。この時間は、[再認証期間]フィールドで定義されます。

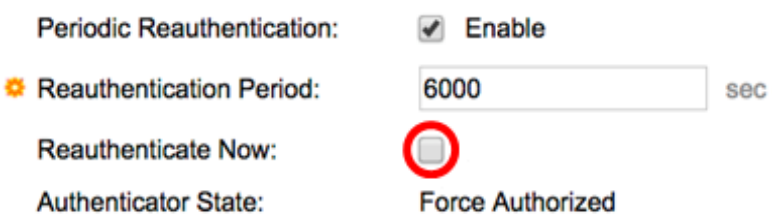


注：この例では、期間再認証が有効になっています。

ステップ16:（オプション）[再認証期間]フィールドに*値*を入力します。この値は、インターフェイスがポートを再認証するまでの秒数を表します。デフォルト値は3600秒で、範囲は300 ～ 4294967295秒です。

注：この例では、6000秒が設定されています。

ステップ17:（オプション）[Enable Reauthenticate Now]チェックボックスをオンにして、即時のポート再認証を強制的に行います。この例では、即時再認証が無効になっています。



[Authenticator State]領域には、ポートの認証状態が表示されます。

ステップ18:（オプション）ポートが許可される時間の制限を有効にするには、[Enable Time Range]チェックボックスをオンにします。

注：この例では、[Time Range]が有効になっています。この機能をスキップする場合は、ステップ20に進んでください。

ステップ19:（オプション）[Time Range Name]ドロップダウンリストから、使用する時間範囲を選択します。

注：この例では、[Dayshift]が選択されています。

ステップ20:[Maximum WBA Login Attempts]領域で、[Infinite for no limit]または[User Defined]をクリックして制限を設定します。[ユーザ定義(User Defined)]を選択した場合は、Webベースの認証で許可されるログインの最大試行回数を入力します。

注：この例では、[Infinite]が選択されています。

ステップ21:[Maximum WBA Silence Period（WBAサイレントの最大期間）]領域で、[Infinite for no limit（無制限）]または[User Defined（ユーザ定義）]をクリックして制限を設定します。[ユーザ定義(User Defined)]を選択した場合は、インターフェイスで許可されるWebベース認証のサイレント期間の最大長を入力します。

注：この例では、[Infinite]が選択されています。

ステップ22:[Max Hosts（最大ホスト）]領域で、[Infinite（無制限）]または[User Defined（ユーザ定義）]をクリックして制限を設定します。[User Defined]を選択した場合は、インターフェイスで許可される許可ホストの最大数を入力します。

注：この値を1に設定すると、マルチセッションモードでWebベース認証のシングルホストモードをシミュレートできます。この例では、[Infinite]が選択されています。

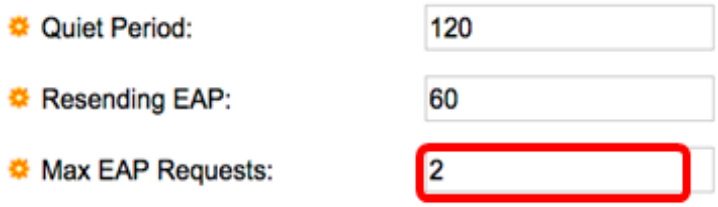
ステップ23:[Quiet Period]フィールドに、認証交換の失敗後にスイッチがQuiet状態のままになる時間を入力します。スイッチがquiet状態の場合、スイッチはクライアントからの新しい認証要求をリッスンしていないことを意味します。デフォルト値は60秒で、範囲は1 ~ 65535秒です。

注：この例では、Quiet期間は120秒に設定されています。

ステップ24:[*Reending EAP*]フィールドに、スイッチが要求を再送信する前にサプリカントからの応答メッセージを待機する時間を入力します。デフォルト値は30秒で、範囲は1 ~ 65535秒です。

注：この例では、EAPの再送信は60秒に設定されています。

ステップ25:[*Max EAP Requests*]フィールドに、送信可能なEAP要求の最大数を入力します。EAPは、802.1Xで使用される認証方式で、スイッチとクライアント間の認証情報の交換を提供します。この場合、EAP要求は認証のためにクライアントに送信されます。クライアントは応答し、認証情報を照合する必要があります。クライアントが応答しない場合、別のEAP要求が再送EAP値に基づいて設定され、認証プロセスが再起動されます。デフォルト値は2で、範囲は1 ~ 10です。

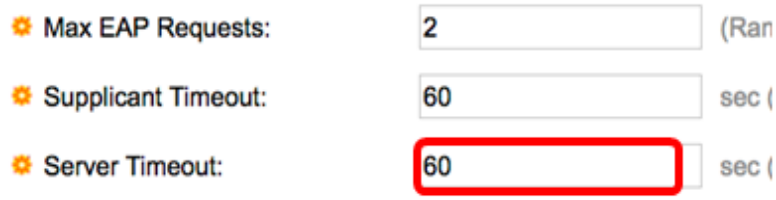


注：この例では、デフォルト値2が使用されます。

ステップ26:[*Supplicant Timeout*]フィールドに、EAP要求がサプリカントに再送信されるまでの時間を入力します。デフォルト値は30秒で、範囲は1 ~ 65535秒です。

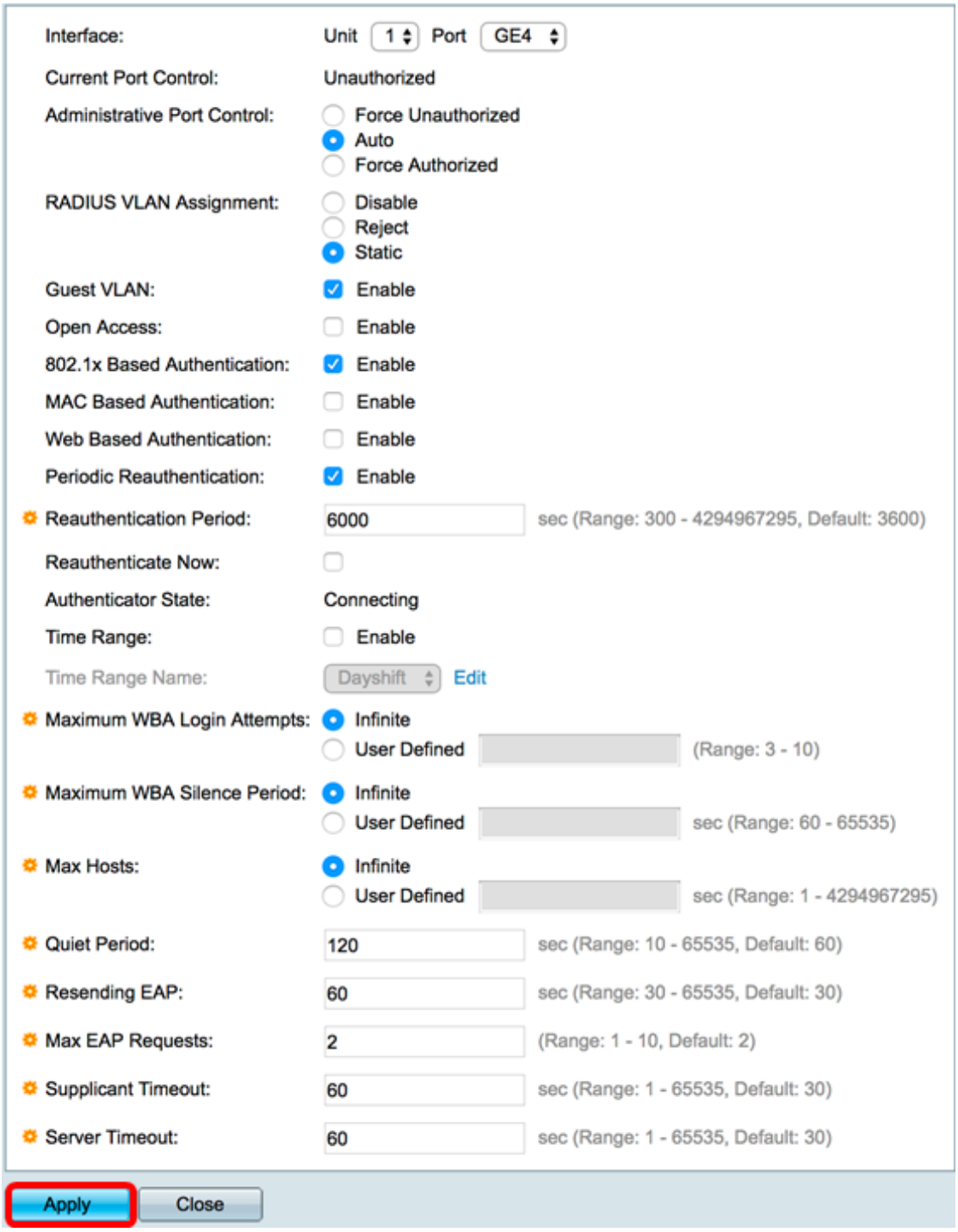
注：この例では、サプリカントタイムアウトは60秒に設定されています。

ステップ27:[*Server Timeout*]フィールドに、スイッチがRADIUSサーバに要求を再送信するまでの時間を入力します。デフォルト値は30秒で、範囲は1 ~ 65535秒です。

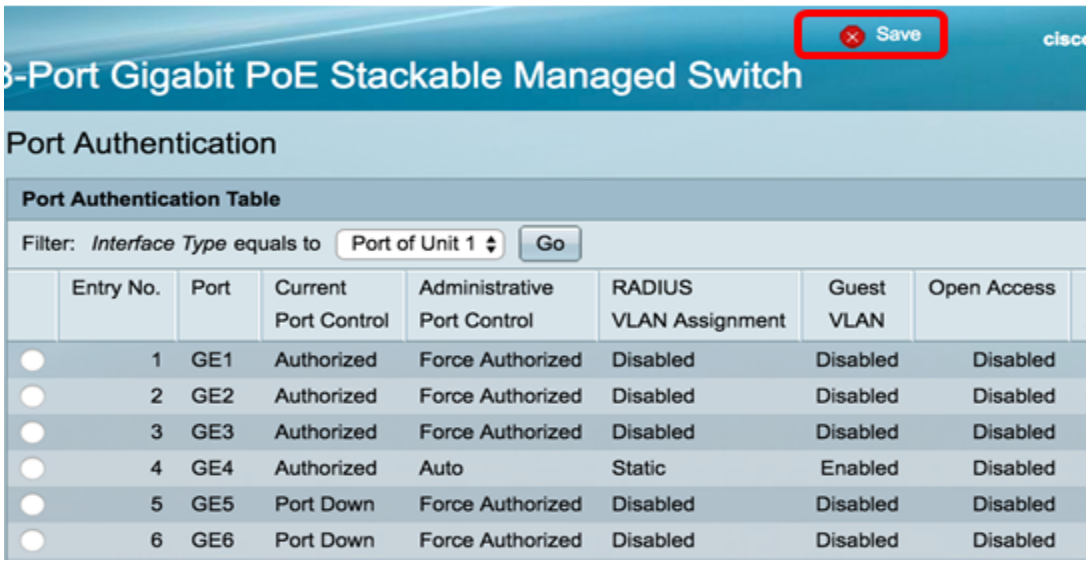


注：この例では、サーバタイムアウトは60秒に設定されています。

ステップ28:[Apply]をクリックし、[Close]をクリックします。



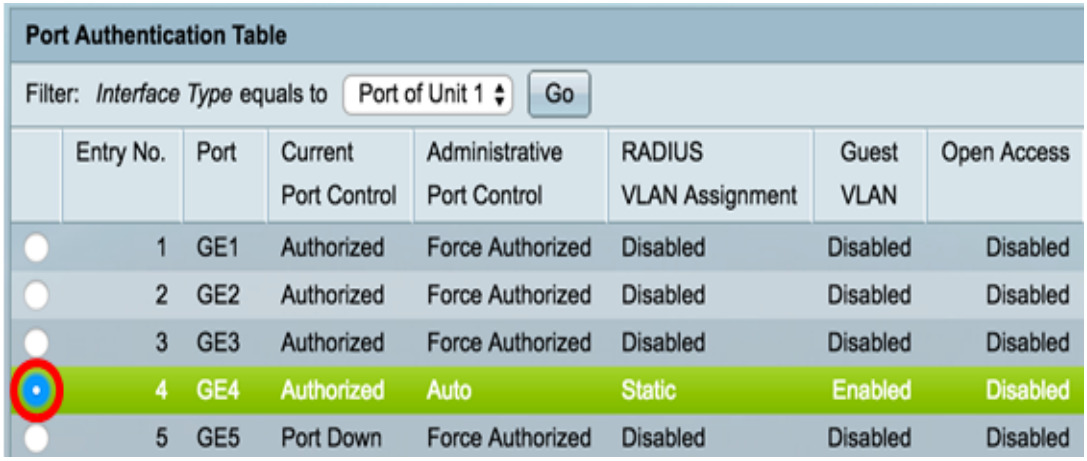
ステップ29:（オプション）[Save]をクリックし、設定をスタートアップコンフィギュレーションファイルに保存します。



これで、スイッチの802.1xポート認証設定が正常に設定されたはずです。

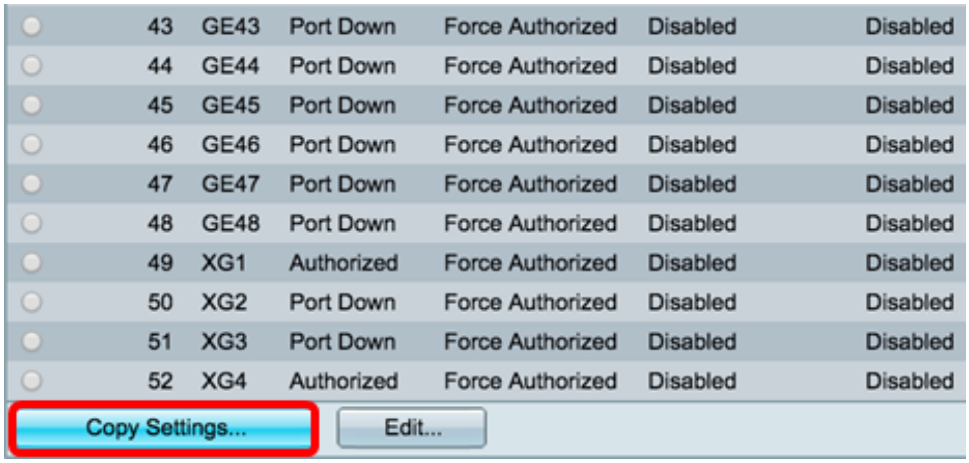
複数のインターフェイスへのインターフェイス設定の適用

ステップ1：複数のインターフェイスに認証設定を適用するインターフェイスのオプションボタンをクリックします。



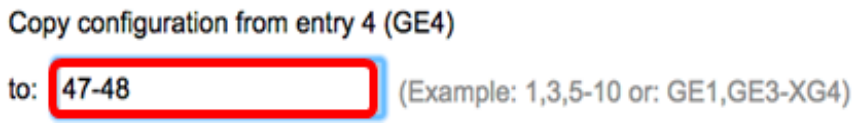
注：この例では、GE4が選択されています。

ステップ2：下にスクロールし、[設定のコピー]をクリックします。



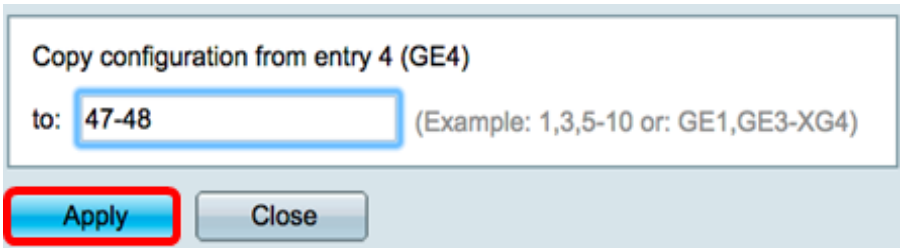
ステップ3:[*to*]フィールドに、*選択*したインターフェイスの設定を適用するインターフェイスの範囲を入力します。インターフェイス番号またはインターフェイス名を入力として使用

できます。各インターフェイスをカンマで区切って入力するか（1、3、5、GE1、GE3、GE5など）、またはインターフェイスの範囲（1 ~ 5またはGE1 ~ GE5など）を入力できます。

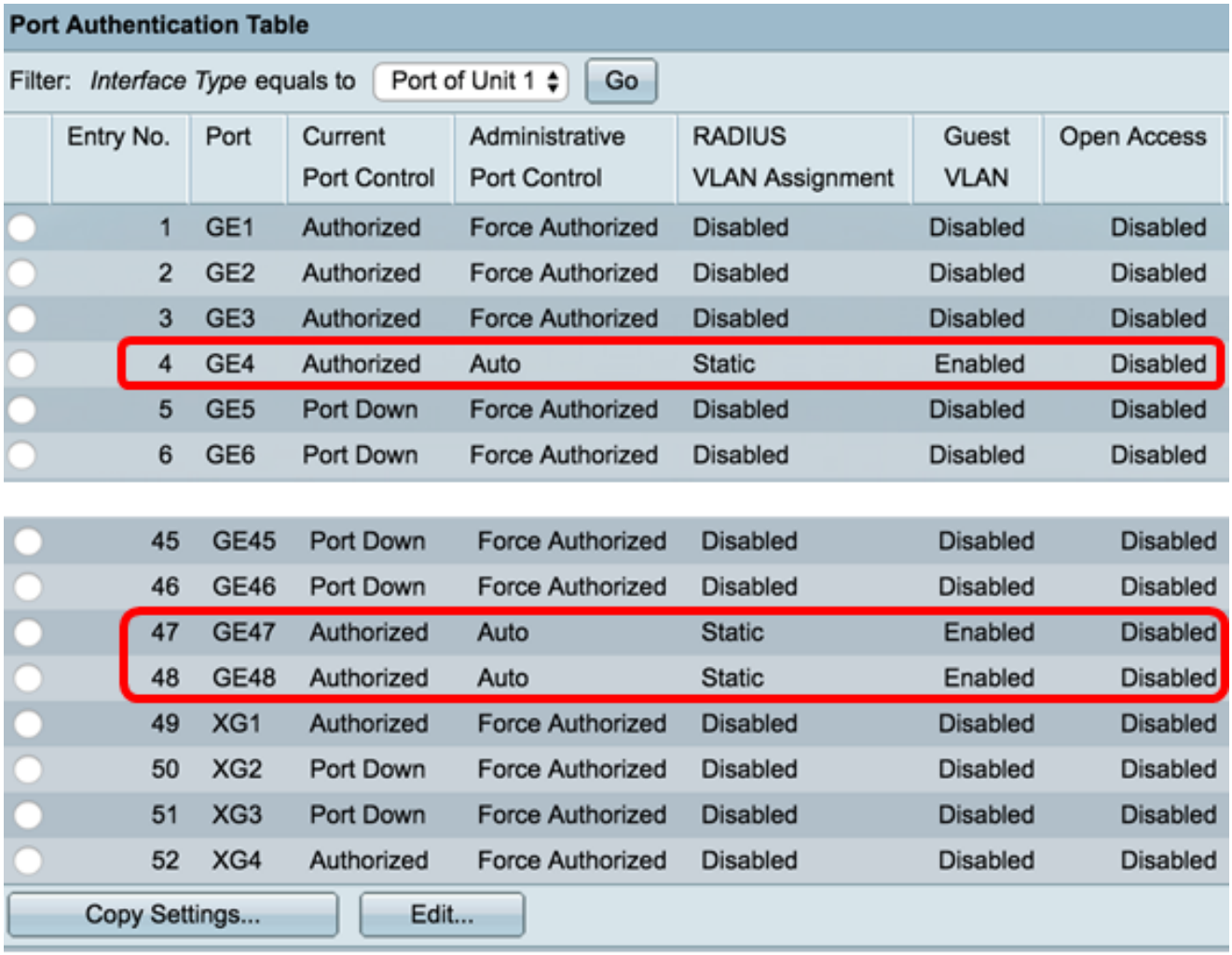


注：この例では、ポート47 ~ 48に設定値が適用されます。

ステップ4:[Apply]をクリックし、[Close]をクリックします。



次の図は、設定後の変更を示しています。



これで、1つのポートの802.1x認証設定が正常にコピーされ、スイッチの他のポートに適用されます。