Sx500シリーズスタッカブルスイッチの802.1xプロパティの設定

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。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前に、スイッチポートに接続されたクライアントは、この場合Remote Authentication Dial-In User Service(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ポートベース認証を有効にするには、802.1xをスイッチでグローバルに有効にする必要があります。

802.1xを完全に設定するには、次の設定を行う必要があります。

1. VLANを作成します。ここをクリックします。
2.ポートをVLANに割り当て、上記の記事を続けます。CLIで設定するには、ここをクリックしてください。
3.ポート認証を構成します。ここをクリックします。

この記事では、802.1xプロパティ（認証およびゲストVLANプロパティを含む）の設定方法について説明します。その他の設定については、上記の記事を参照してください。ゲストVLANは、加入しているデバイスやポートを802.1xまたはMACベースの認証によって認証および許可する必要のないサービスにアクセスできるようにします。

該当するデバイス

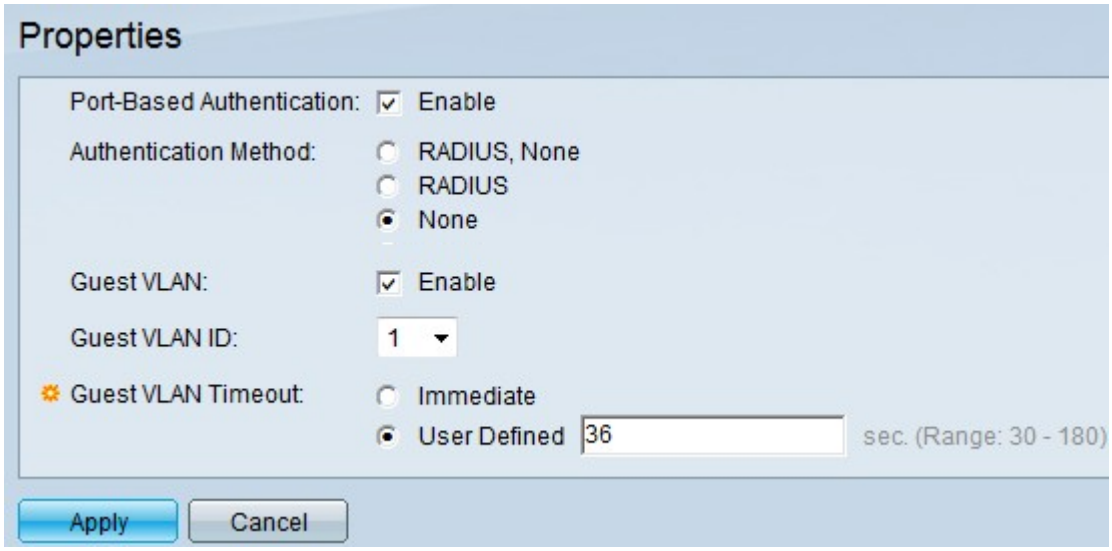
- Sx500シリーズスタッカブルスイッチ

[Software Version]

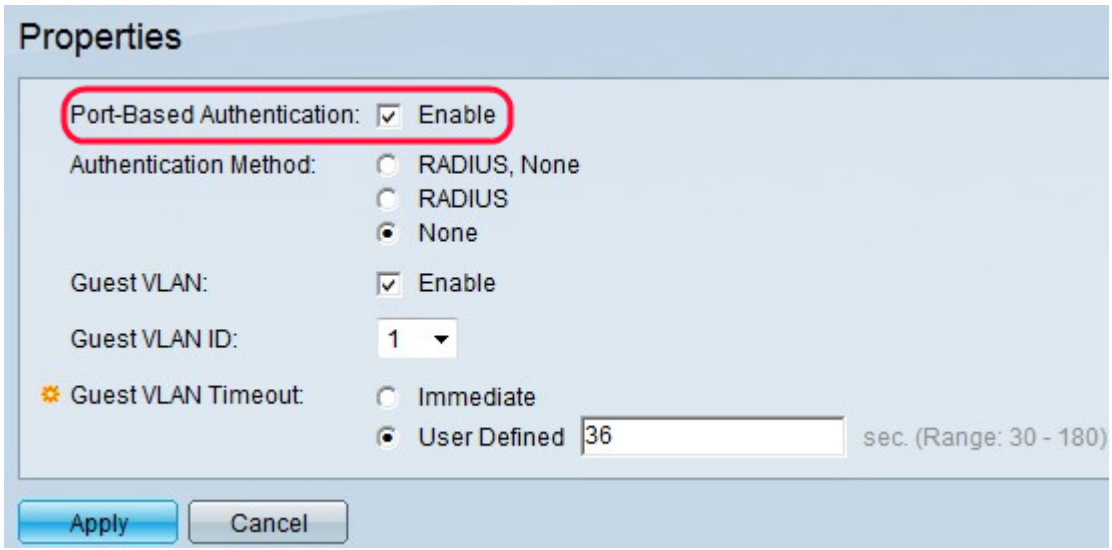
•1.3.0.62

802.1xプロパティでポートベース認証とゲストVLANを有効にする

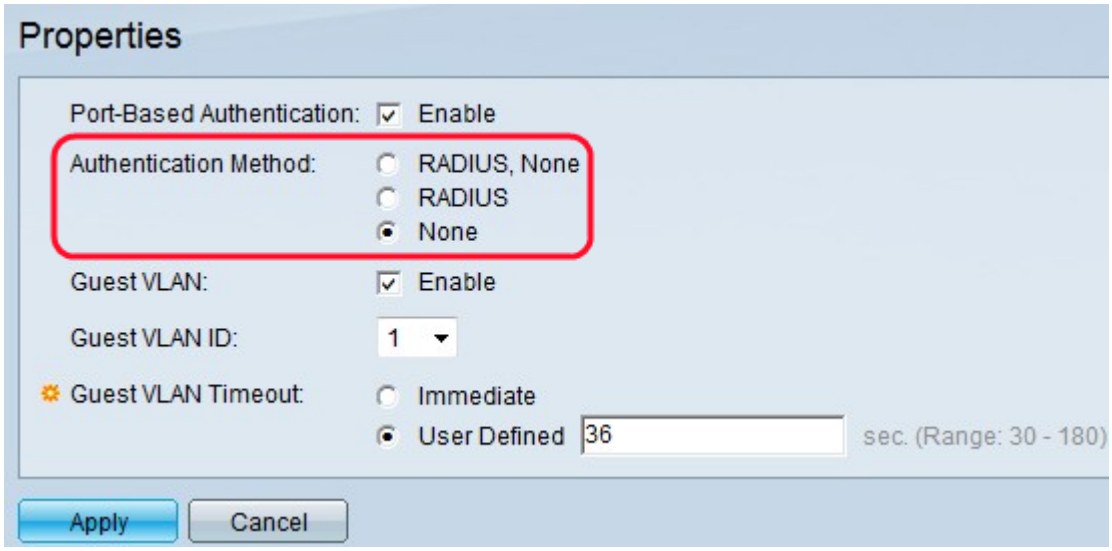
ステップ1:Web構成ユーティリティにログインし、**[Security] > [802.1X] > [Properties]を選択します。**[*Properties*]*ページが開*きます。



ステップ2:[Port-Based Authentication]フィールドの[Enable] をオンにして、ポートベースの802.1x認証を有効にします。



ステップ3:[Authentication Method]フィールドから目的のオプションボタンをクリックします。RADIUSサーバはクライアントの認証を実行します。このサーバは、ユーザが認証されているかどうかを検証し、クライアントがLANおよび他のスイッチサービス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。スイッチはプロキシとして機能し、サーバはクライアントに対して透過的です。

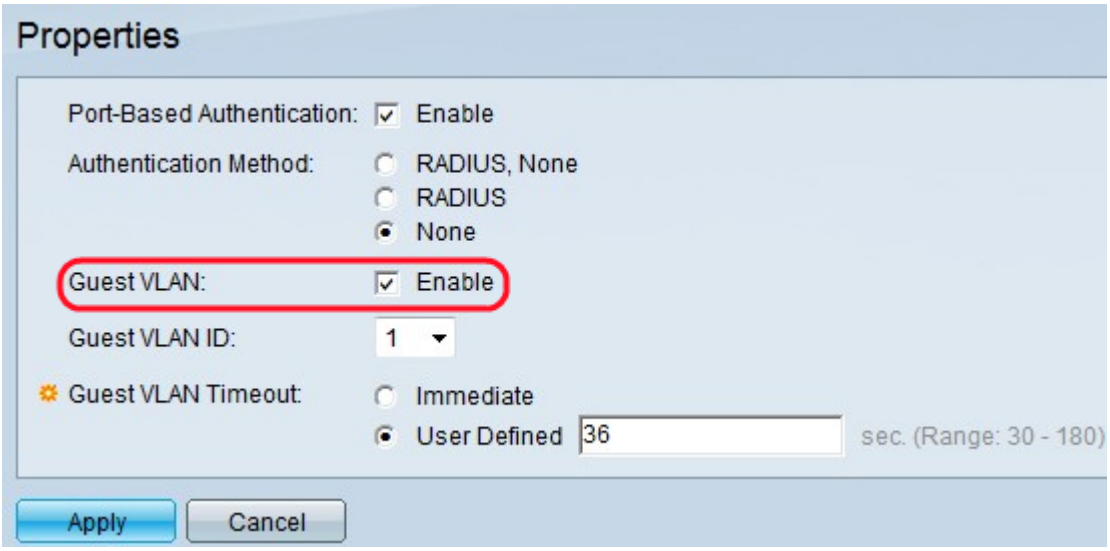


・ RADIUS, None:RADIUSサーバを使用して、最初にポート認証を実行します。サーバがダウンしたときなど、サーバからの応答がない場合、認証は行われず、セッションは許可されます。サーバが使用可能で、ユーザクレデンシャルが正しくない場合、アクセスは拒否され、セッションは終了します。

・ RADIUS:RADIUSサーバに基づいてポート認証を実行します。 認証が実行されない場合、セッションは終了します。

・ None：ユーザを認証せず、セッションを許可します。

ステップ4: (オプション) [Enable] をオンにして、[Guest VLAN]フィールドの権限のないポートに対してゲストVLANを使用できるようにします。ゲストVLANが有効になっている場合、すべての不正なポートが[ゲストVLAN ID(Guest VLAN ID)]フィールドで選択したVLANに自動的に参加します。ポートが後で承認されると、ゲストVLANから削除されます。



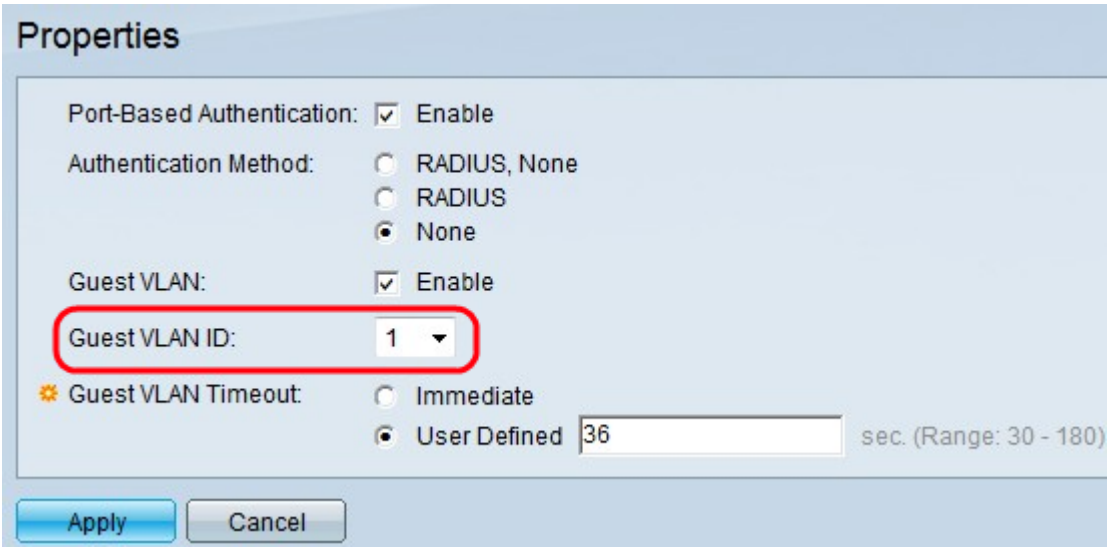
MAC認証モードを使用する前に、ゲストVLANモードを設定する必要があります。802.1xフレームワークを使用すると、デバイス (サプリカント) は、接続先のリモートデバイス (オーセンティケータ) からポートアクセスを要求できます。ポートアクセスを要求するサプリカントが認証され、許可されている場合にのみ、ポートへのデータ送信が許可されます。そうしないと、オーセンティケータは、データがゲストVLANまたは認証されていないVLANに送信されない限り、サプリカントデータを廃棄します。

注：ゲストVLANが設定されている場合は、次の特性を持つスタティックVLANです。

・ 既存のスタティックVLANから手動で定義する必要があります。
・ 接続され、ゲストVLAN対応のデバイスの不正なデバイスまたはポートにのみ自動的に使用可能
・ ポートがゲストVLAN対応の場合、スイッチはポートが認可されていない場合にゲストVLANのタグなしメンバーとしてポートを自動的に追加し、ポートの最初のサプリカントが認可された場合にゲストVLANからポートを削除します。
・ ゲストVLANを音声VLANと非認証VLANの両方として使用することはできません。

タイムセバー：ゲストVLANが無効になっている場合は、ステップ7に進みます。

ステップ5:[Guest VLAN ID]ドロップダウンリストで、VLANのリストからゲストVLAN IDを選択します。



ステップ6:[Guest VLAN Timeout]フィールドで、目的のオプションボタンをクリックします。使用できるオプションは次のとおりです。

- Immediate：ゲストVLANは10秒後に期限切れになります。
- 「ユーザー定義」 –「ユーザー定義」フィールドに期間を手動で入力します。

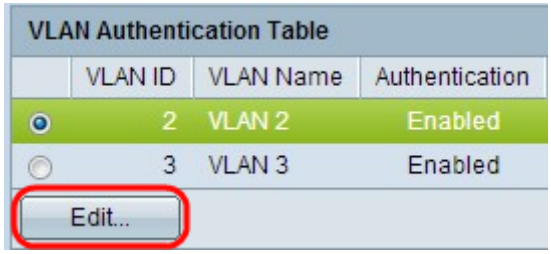
注：リンクアップ後、ソフトウェアが802.1xサプリカントを検出しない場合、またはポート認証が失敗した場合、そのポートはゲストVLANタイムアウト期間が経過した後にのみゲストVLANに追加されます。ポートが[Authorized]から[Not Authorized]に変更された場合、そのポートは[Guest VLAN Timeout]期間が経過した後にのみゲストVLANに追加されます。VLAN認証テーブルには、すべてのVLANが表示され、認証が有効になっているかどうかが表示されます。

ステップ7:[Apply]をクリックして設定を保存します。

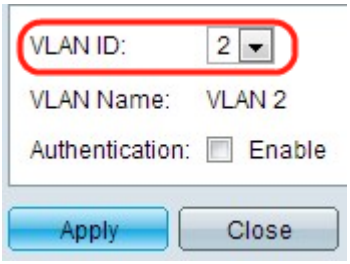
非認証VLANの設定

802.1xを有効にすると、不正なポートまたはデバイスがゲストVLANまたは非認証VLANの一部でない限り、VLANへのアクセスが許可されません。[ポートからVLAN]ページを使用して、ポートをVLANに手動で追加する*必要があります*。

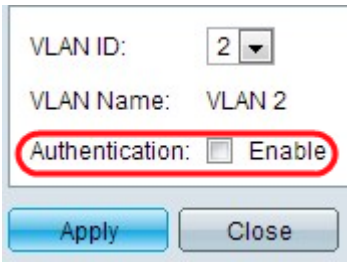
ステップ1:Web構成ユーティリティにログインし、**[Security] > [802.1X] > [Properties]を選択します。**[Properties]*ページが開*きます。



ステップ2:[VLAN Authentication Table]までページを下にスクロールし、認証を無効にするVLANのオプションボタンをクリックして、[Edit]をクリックします。[Edit VLAN *Authentication]ページ*が開きます。



ステップ3:（オプション）[VLAN ID]ドロップダウンリストからVLAN IDを選択します。



ステップ4:[Enable] をオフにして認証を無効にし、VLANを非認証VLANにします。

ステップ5:[Apply]をクリックして設定を適用します。VLAN認証テーブルが変更されます。