スイッチでのセキュアシェル(SSH)サーバ認証設定の設定

目的

この記事では、スイッチへの接続方法ではなく、管理対象スイッチでサーバ認証を設定する方法について説明します。SSH + Putty経由でスイッチに接続する方法については、ここをクリックして記事を参照してください。

セキュアシェル(SSH)は、特定のネットワークデバイスへのセキュアなリモート接続を提供するプロトコルです。この接続は、暗号化されている点を除き、Telnet接続に似た機能を提供します。SSHを使用すると、管理者はコマンドラインインターフェイス(CLI)からサードパーティプログラムを使用してスイッチを設定できます。スイッチは、ネットワーク内のユーザにSSH機能を提供するSSHクライアントとして機能します。スイッチはSSHサーバを使用してSSHサービスを提供します。SSHサーバ認証が無効になっている場合、スイッチは任意のSSHサーバを信頼できるものと見なすため、ネットワーク上のセキュリティが低下します。スイッチでSSHサービスが有効になっていると、セキュリティが強化されます。

適用可能なデバイス

- Sx200シリーズ
- 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]

- 1.4.5.02 - Sx200シリーズ、Sx300シリーズ、Sx500シリーズ
- 2.2.0.66 - Sx350シリーズ、SG350Xシリーズ、Sx550Xシリーズ

SSHサーバ認証の設定

SSHサービスの有効化

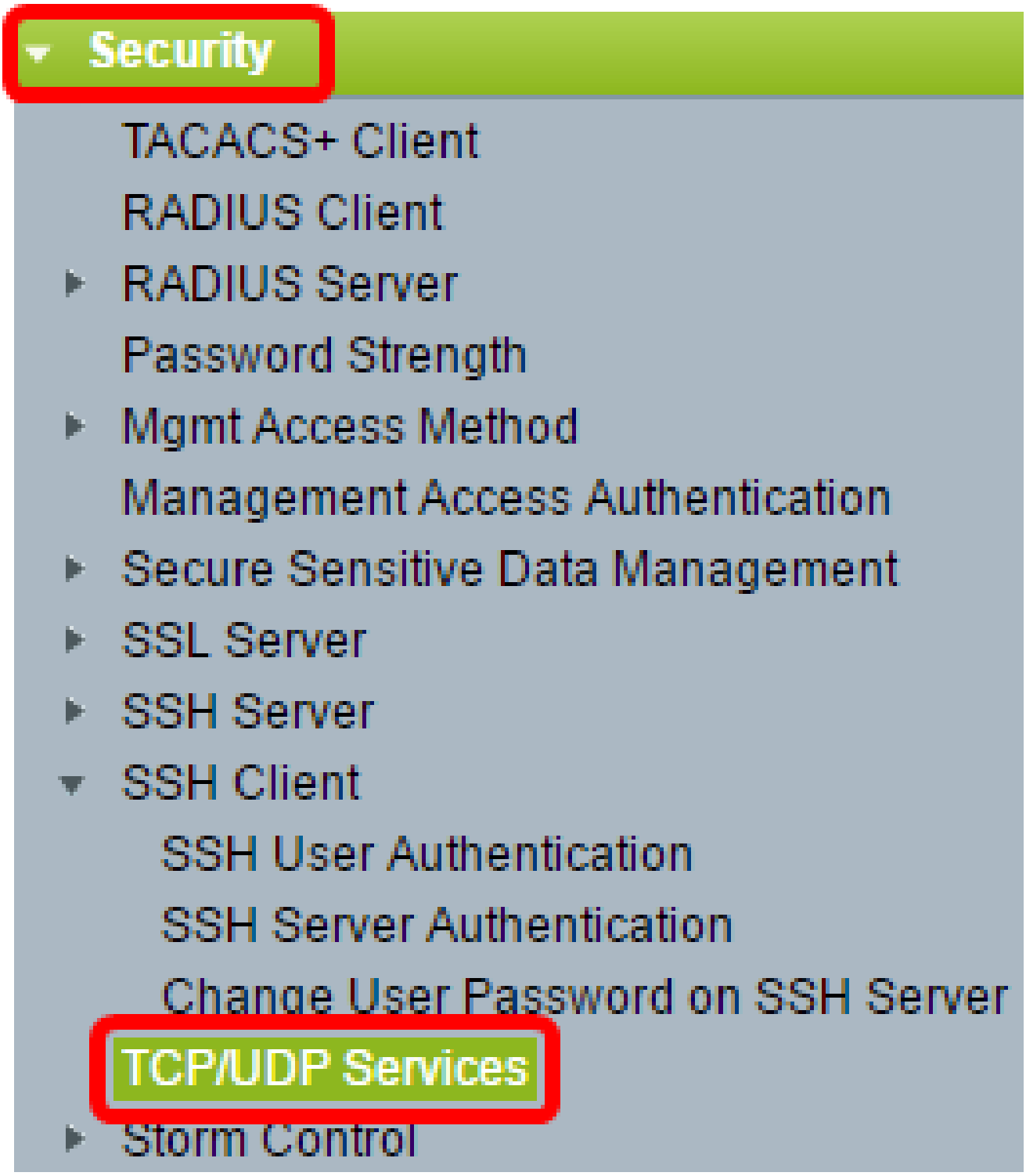
SSHサーバ認証を有効にすると、デバイスで実行されているSSHクライアントは、次の認証プロセスを使用してSSHサーバを認証します。

- デバイスは、受信したSSHサーバの公開キーのフィンガープリントを計算します。
- デバイスは、SSH Trusted Serversテーブルで、SSHサーバのIPアドレスとホスト名を検索します。次の3つの結果のいずれかが発生する可能性があります。

1. サーバのアドレスとホスト名、およびフィンガープリントの両方に一致するものが見つかると、サーバが認証されます。
2. 一致するIPアドレスとホスト名が見つかっても、一致するフィンガープリントがない場合は、検索が続行されます。一致するフィンガープリントが見つからない場合、検索は完了し、認証は失敗します。
3. 一致するIPアドレスとホスト名が見つからない場合、検索は完了し、認証は失敗します。
    - 信頼できるサーバのリストにSSHサーバのエントリが見つからない場合、プロセスは失敗します。

注：工場出荷時のデフォルト設定でアウトオブボックススイッチの自動設定をサポートするために、SSHサーバ認証はデフォルトで無効になっています。

ステップ 1：Webベースのユーティリティにログインし、Security > TCP/UDP Servicesの順に選択します。

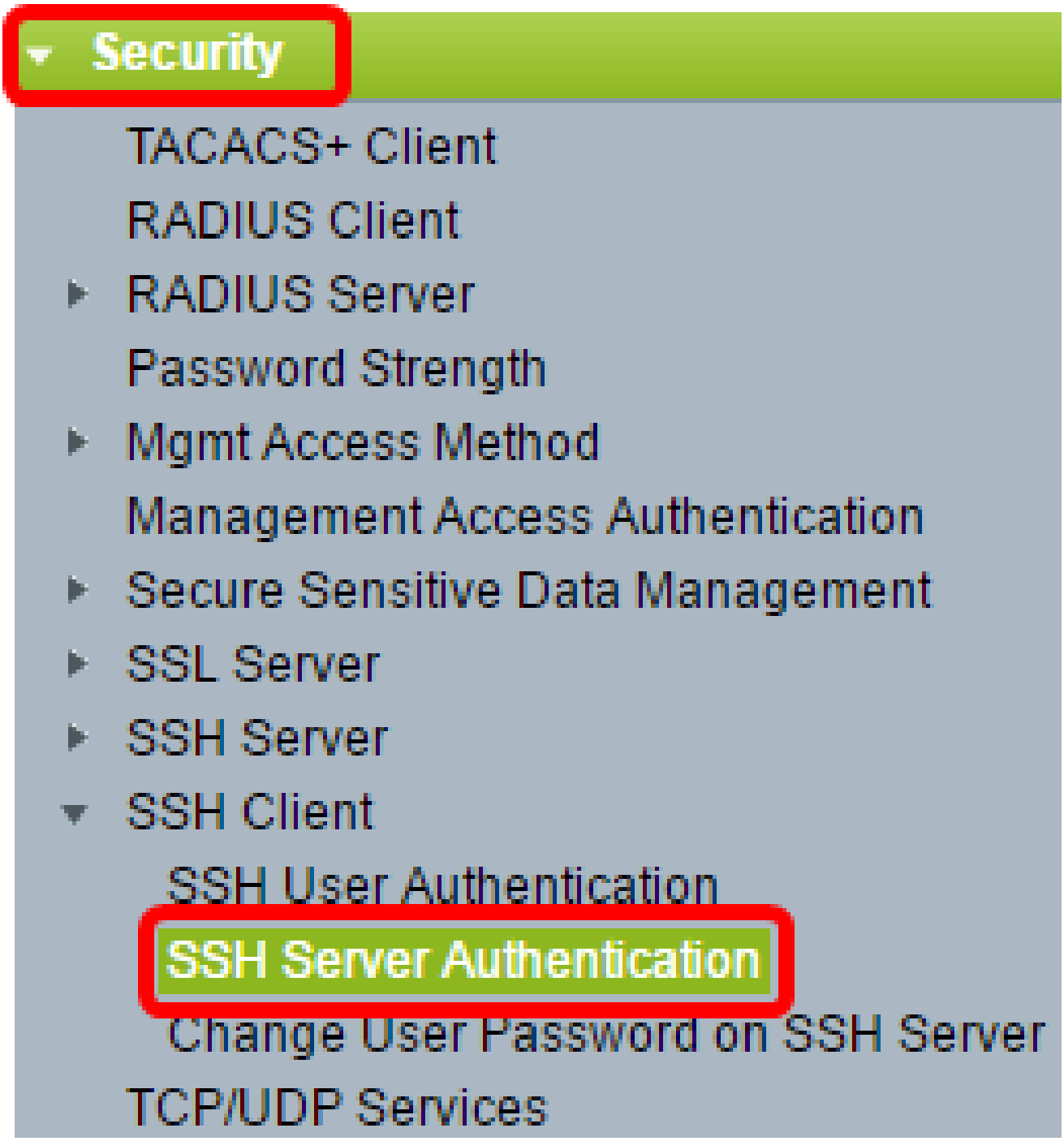


ステップ 2：SSH Serviceチェックボックスをオンにして、SSHを介したスイッチコマンドプロンプトのアクセスを有効にします。

ステップ 3：Applyをクリックして、SSHサービスを有効にします。

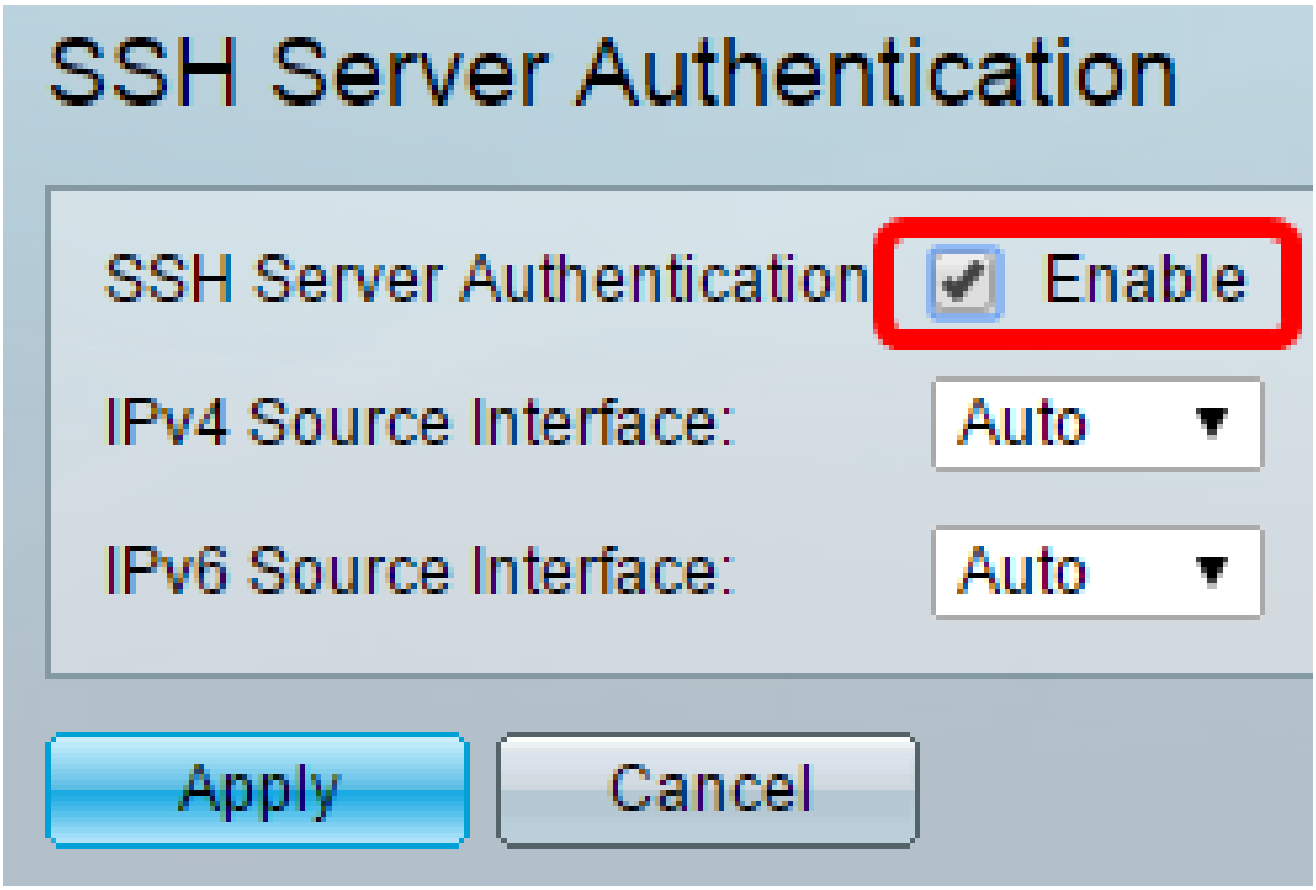
SSHサーバ認証の設定

ステップ 1：Webベースのユーティリティにログインし、Security > SSH Client > SSH Server Authenticationの順に選択します。

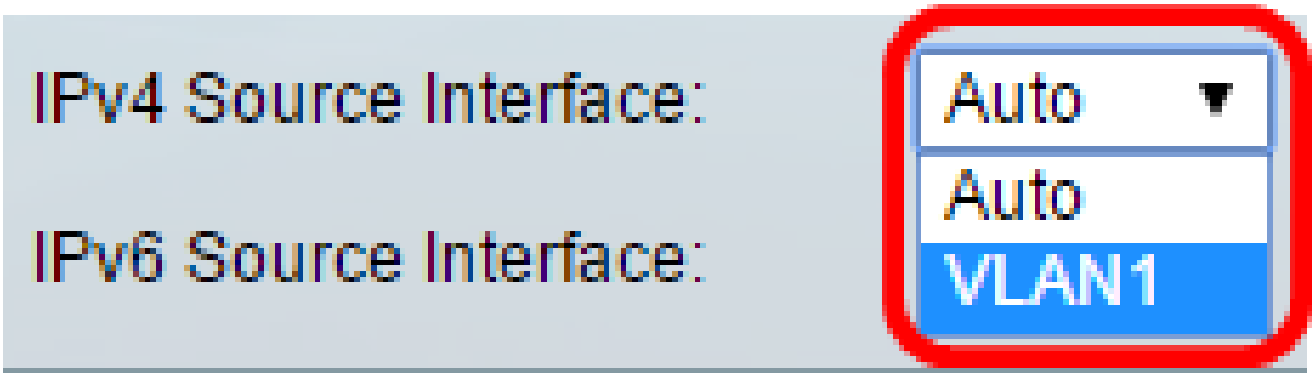


注：Sx350、SG300X、またはSx500Xをお持ちの場合は、[表示モード]ドロップダウンリストから[詳細]を選択して[詳細]モードに切り替えてください。

ステップ 2：Enable SSH Server Authenticationチェックボックスにチェックマークを入れて、SSHサーバ認証をイネーブルにします。

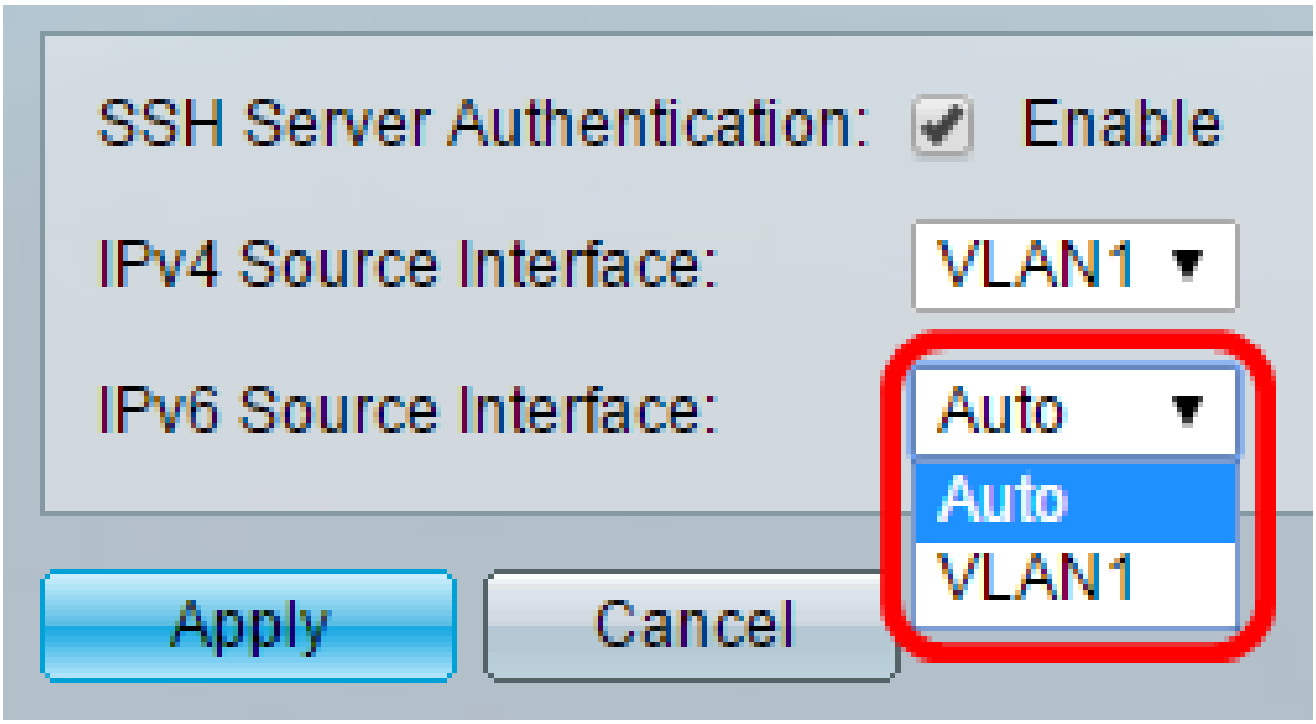


ステップ3: (オプション) IPv4 Source Interfaceドロップダウンリストで、IPv4 SSHサーバとの通信に使用するメッセージの送信元IPv4アドレスとしてIPv4アドレスが使用される送信元インターフェイスを選択します。



注：Autoオプションが選択されている場合、システムは発信インターフェイスで定義されたIPアドレスから送信元IPアドレスを取得します。この例では、VLAN1が選択されています。

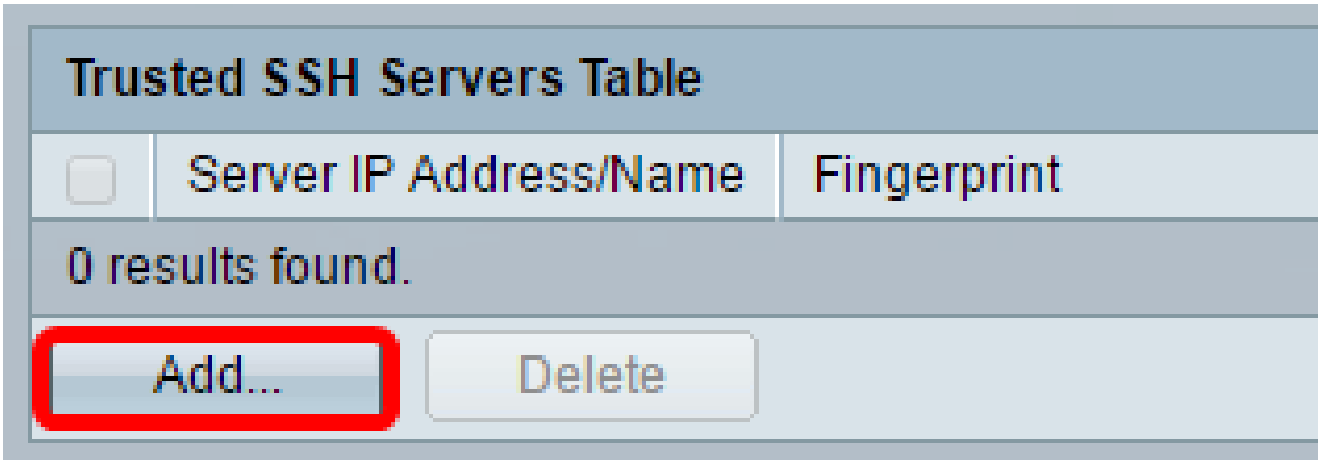
ステップ4: (オプション) IPv6 Source Interfaceドロップダウンリストで、IPv6 SSHサーバとの通信に使用するメッセージの送信元IPv6アドレスとしてIPv6アドレスが使用される送信元インターフェイスを選択します。



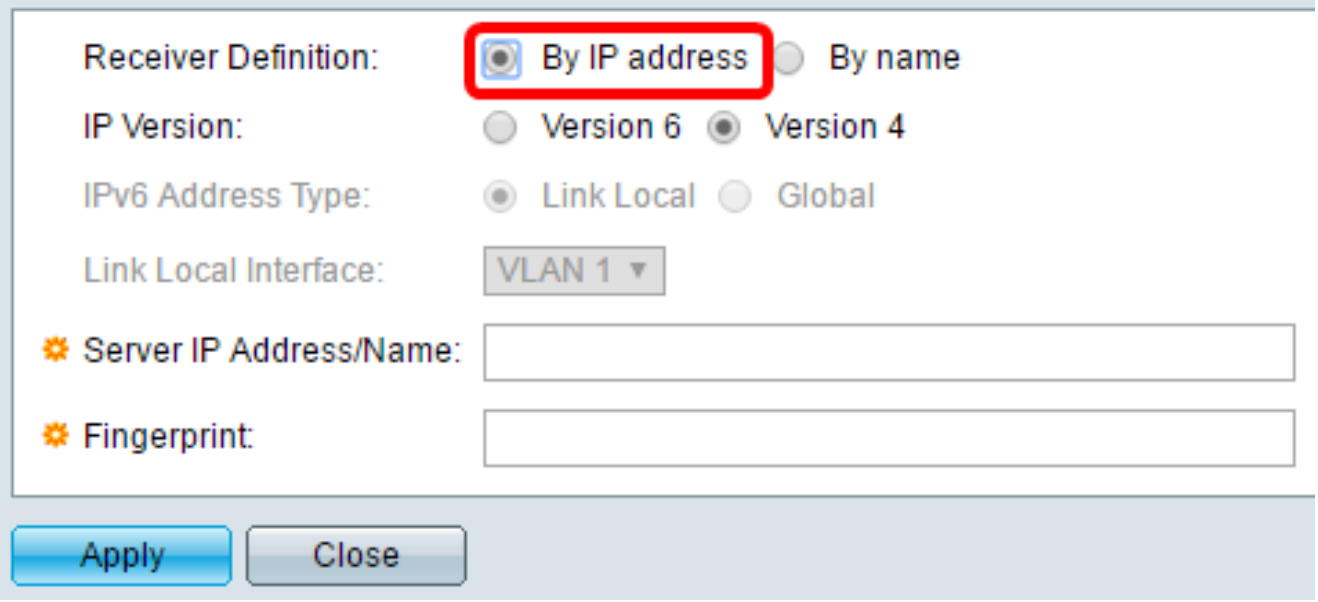
注：この例では、Autoオプションが選択されています。システムは、発信インターフェイスで定義されたIPアドレスから送信元IPアドレスを取得します。

ステップ 5：[APPLY] をクリックします。

手順 6：信頼できるサーバを追加するには、Trusted SSH Serversテーブルの下にあるAddをクリックします。



手順 7：Receiver Definition領域で、SSHサーバを定義するために使用可能な方法のいずれかをクリックします。

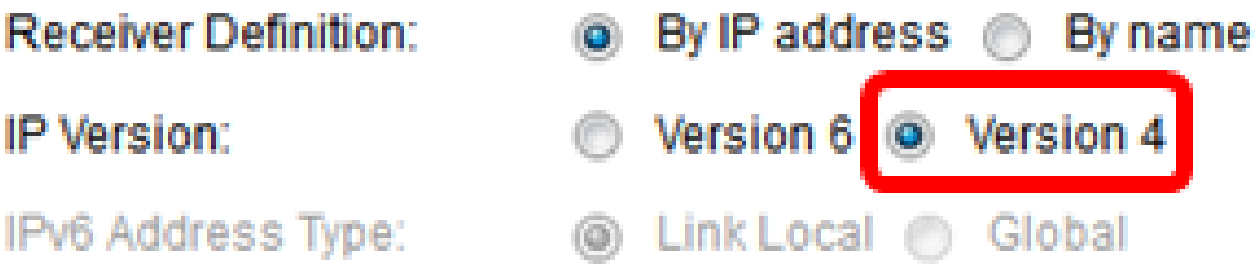


次のオプションがあります。

- By IP Address：このオプションでは、SSHサーバにIPアドレスを定義できます。
- By Name：このオプションでは、完全修飾ドメイン名を使用してSSHサーバを定義できます。

注：この例では、By IP addressが選択されています。名前を指定する場合は、ステップ11に進みます。

ステップ8: (オプション) ステップ6で「IPアドレスによる」を選択した場合は、「IPバージョン」フィールドでSSHサーバのIPバージョンをクリックします。

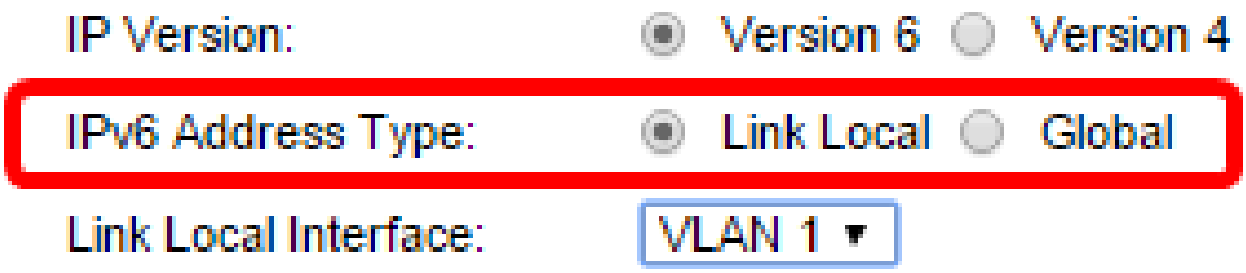


使用可能なオプションは次のとおりです。

- バージョン6：このオプションでは、IPv6アドレスを入力できます。
- バージョン4：このオプションでは、IPv4アドレスを入力できます。

注：この例では、バージョン4が選択されています。IPv6オプションボタンは、スイッチにIPv6アドレスが設定されている場合にのみ使用できます。

ステップ9: (オプション) ステップ7でIPアドレスのバージョンとしてバージョン6を選択した場合は、[IPv6アドレスタイプ]でIPv6アドレスのタイプをクリックします。

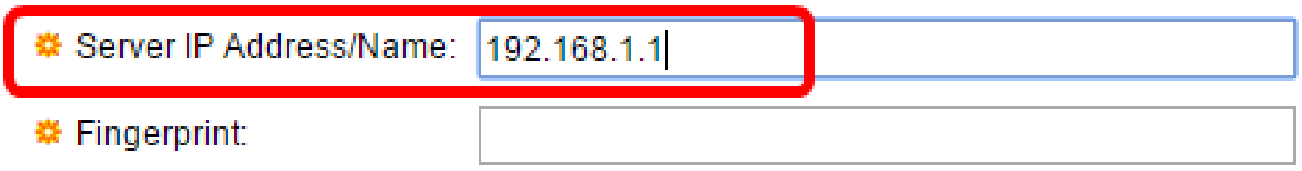


使用可能なオプションは次のとおりです。

- リンクローカル：IPv6アドレスは、単一のネットワークリンク上のホストを一意に識別します。リンクローカルアドレスはFE80のプレフィックスを持ち、ルーティング可能ではなく、ローカルネットワーク上の通信にのみ使用できます。1つのリンクローカルアドレスだけがサポートされます。リンクローカルアドレスがインターフェイスに存在する場合、この エントリによって設定内のアドレスが置き換えられます。このオプションはデフォルトで選択されています。
- グローバル：IPv6アドレスは、他のネットワークから可視で到達可能なグローバルユニキャストです。

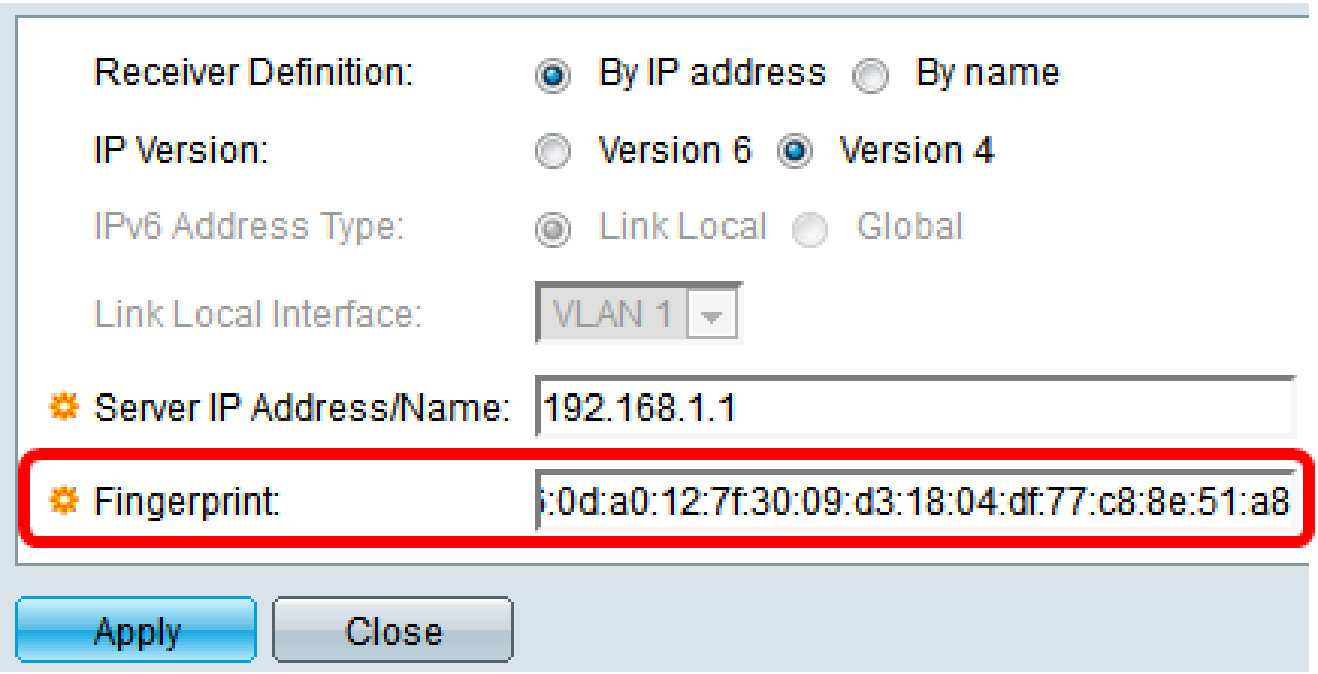
ステップ10: (オプション) ステップ9でIPv6アドレスタイプとして「リンクローカル」を選択した場合は、「リンクローカルインターフェイス」ドロップダウンリストから適切なインターフェイスを選択します。

ステップ 11Server IP Address/Nameフィールドに、SSHサーバのIPアドレスまたはドメイン名を入力します。



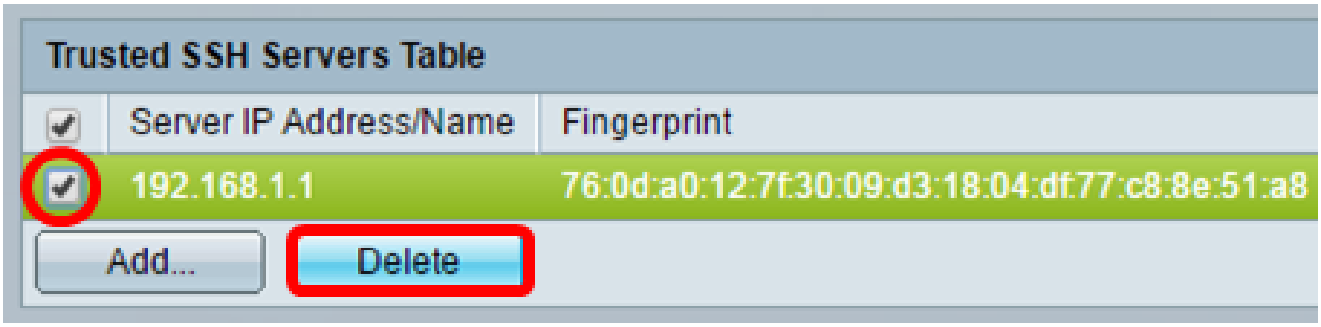
注：この例では、IPアドレスが入力されています。

ステップ 12Fingerprintフィールドに、SSHサーバのフィンガープリントを入力します。フィンガープリントは、認証に使用される暗号化キーです。この場合、フィンガープリントはSSHサーバの有効性を認証するために使用されます。サーバのIPアドレス/名前とフィンガープリントが一致すると、SSHサーバが認証されます。

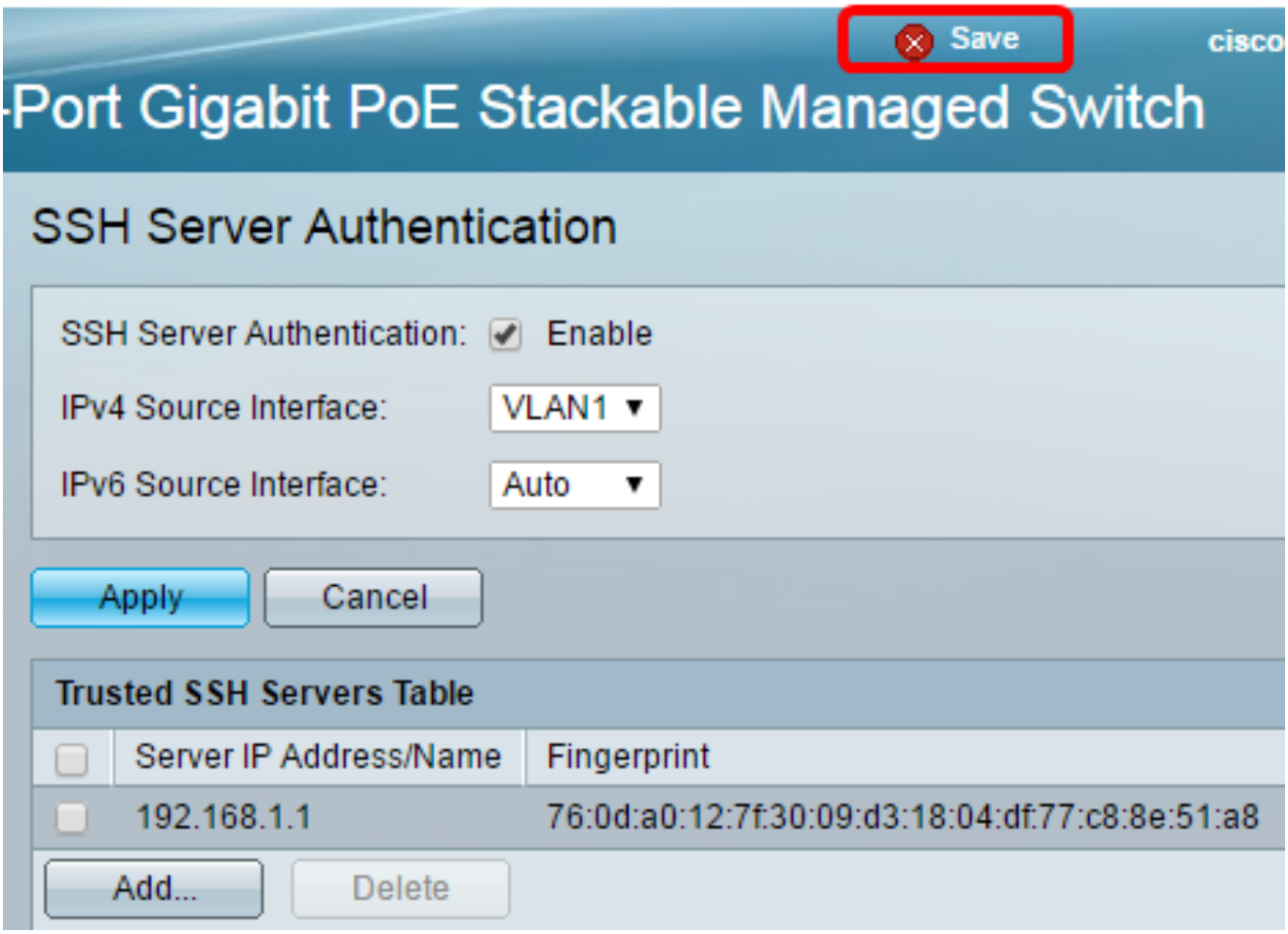


ステップ 13Applyをクリックして、設定を保存します。

ステップ14: (オプション) SSHサーバを削除するには、削除するサーバのチェックボックスをオンにして、Deleteをクリックします。



ステップ15: (オプション) ページ上部のSaveボタンをクリックして、スタートアップコンフィギュレーションファイルへの変更を保存します。



これで、管理対象スイッチでSSHサーバの認証設定を行ったはずです。

この記事の関連ビデオを見る...

シスコの他のテクニカルトークを表示するには、こちらをクリックしてください

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。