Cisco Business 350スイッチでのSSH認証

目的

この記事では、Cisco Business 350シリーズ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。

概要

セキュアシェル(SSH)は、特定のネットワークデバイスに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)を使用して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サーバとして使用するため、ネットワーク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場合、セキュリティが強化されます。

該当するデバイス |ソフトウェアバージョン

- CBS350（データシート） | 3.0.0.69（最新版をダウンロード）
- CBS350-2X(データシート) | 3.0.0.69（最新版をダウンロード）
- CBS350-4X(データシート) | 3.0.0.69（最新版をダウンロード）

SSHサーバ認証設定の設定

SSHサービスの有効化

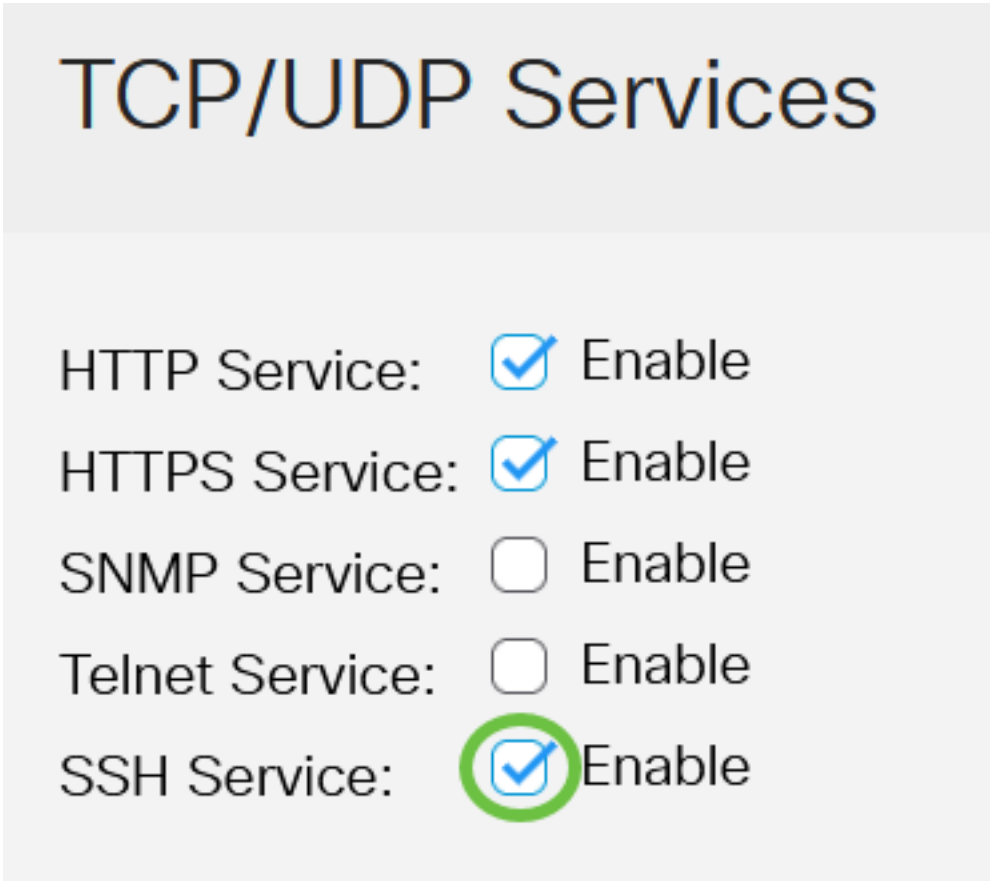
SSHサーバ認証が有効になっている場合、デバイスで実行されているSSHクライアントは、次の認証プロセスを使用してSSHサーバを認証します。

- デバイスは、SSHサーバの受信した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信頼サーバのテーブルで、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になります。
  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エントリが見つかった場合、サーバは認証されます。
  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、検索が完了し、認証が失敗します。
  3. 一致するIPアドレスとホスト名が見つからない場合、検索が完了し、認証が失敗します。
  4. 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。

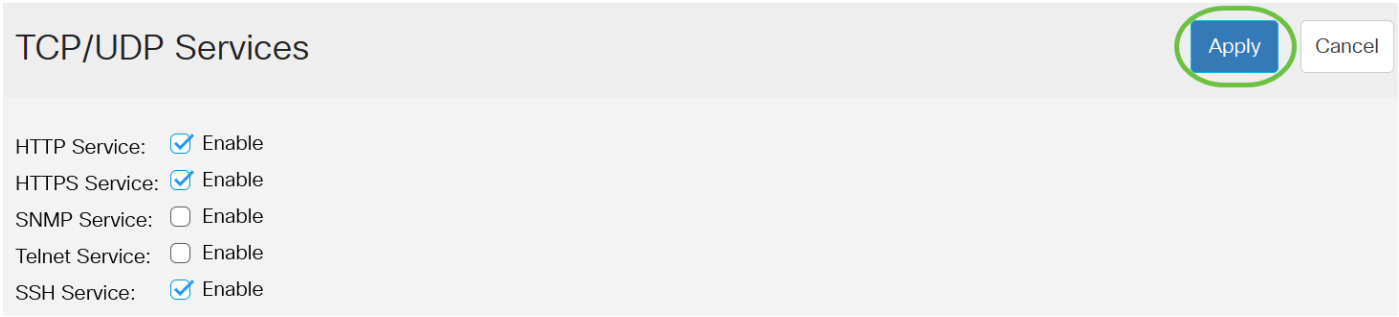
工場出荷時のデフォルト設定でアウトオブボックススイッチの自動設定をサポートするために、SSHサーバ認証はデフォルトで無効になっています。

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]を選択します。**

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へのアクセスを有効にします。

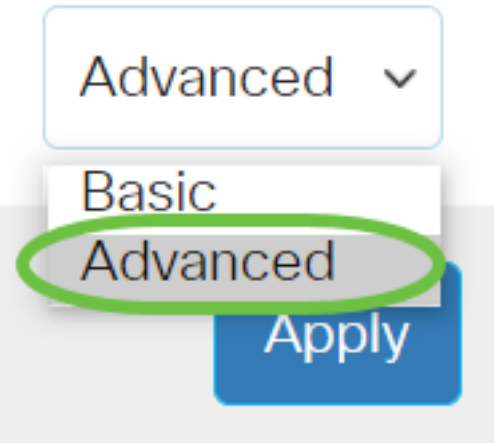


ステップ3:[Apply]をクリックしてSSHサービスを有効にします。

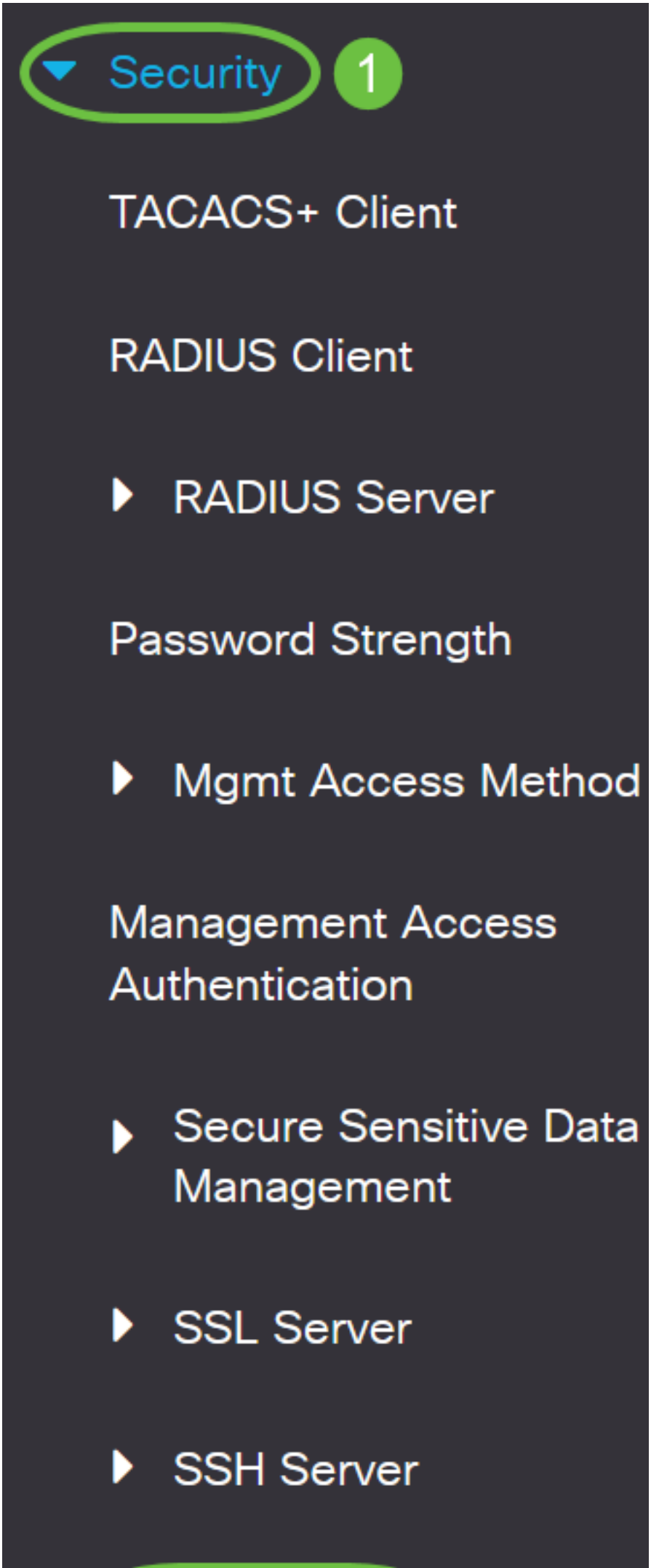


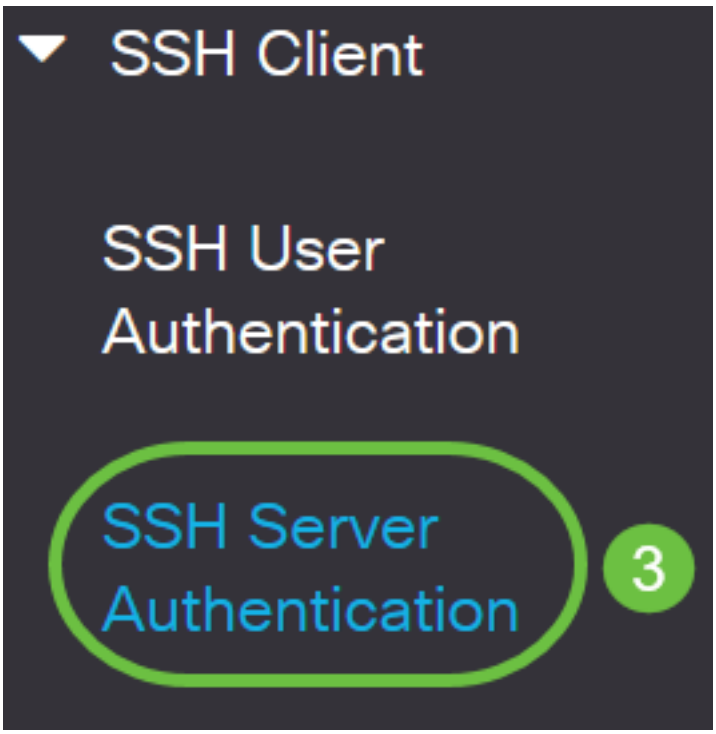
SSHサーバ認証設定の設定

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から[Advanced]を選択します。

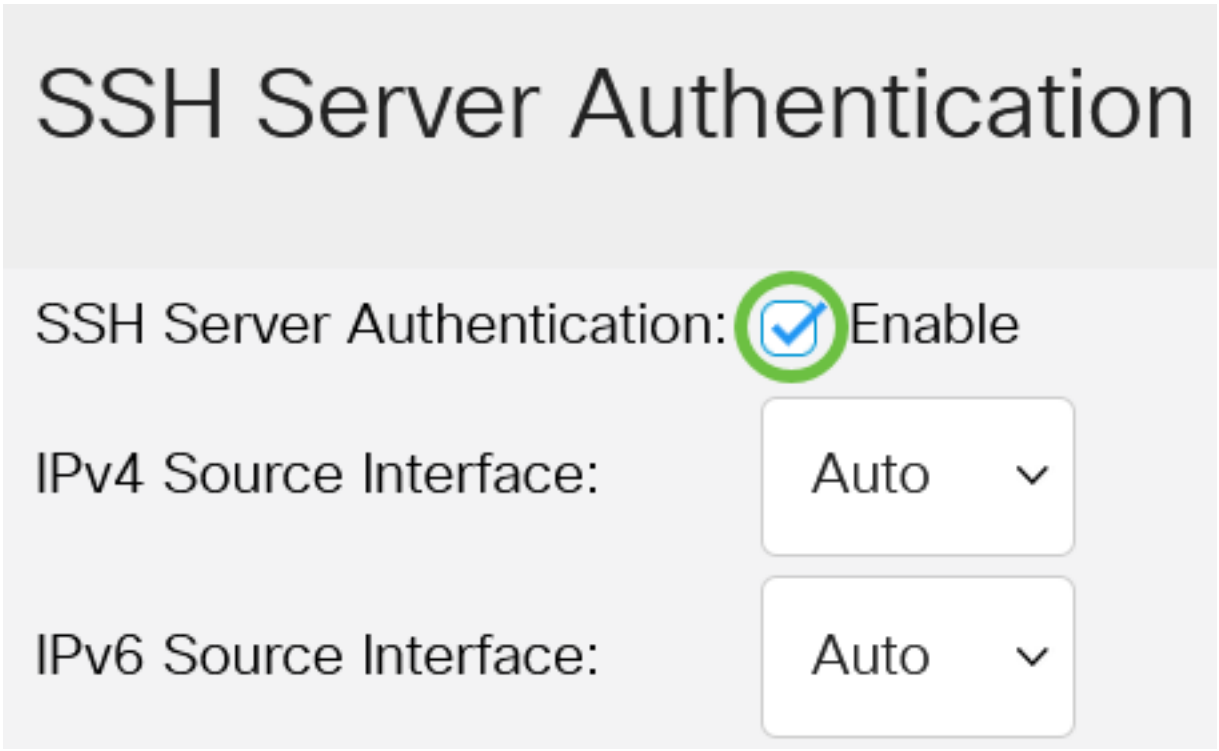


ステップ2:**[Security] > [SSH Client] > [SSH Server Authentication]を選択します。**

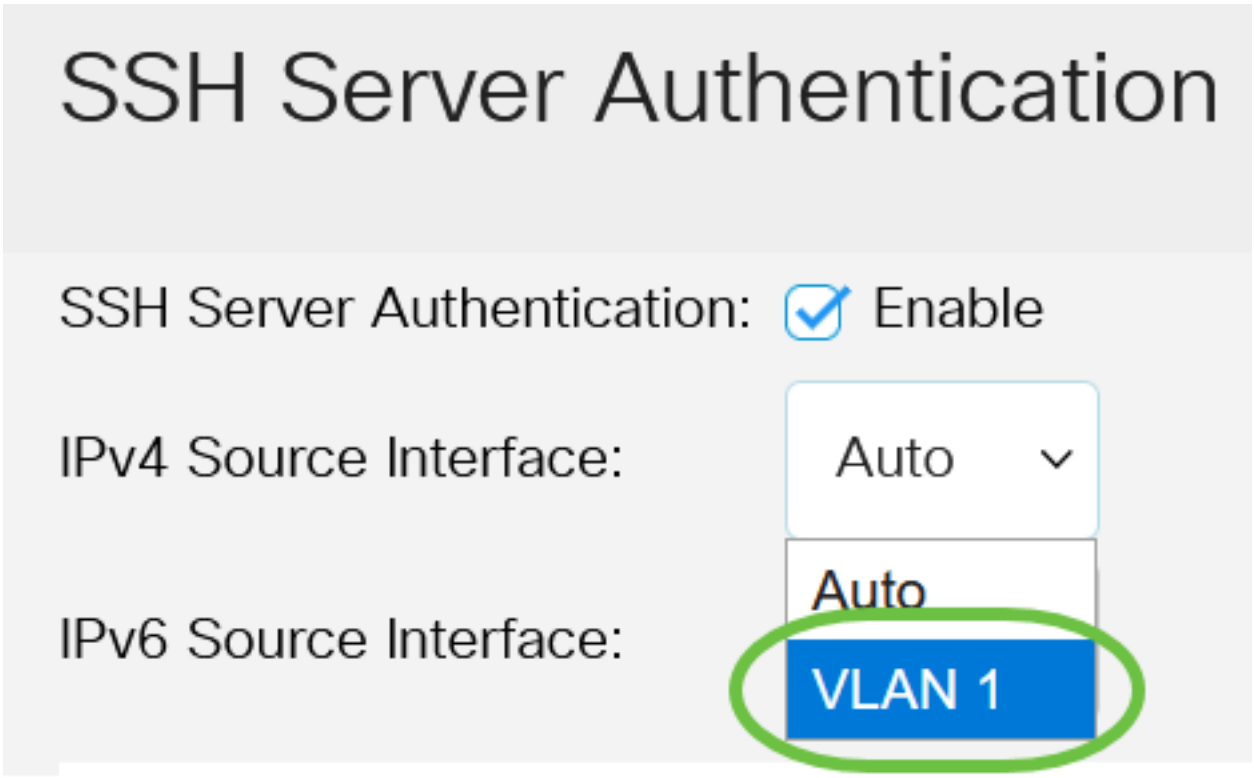

Security
1
TACACS+ Client
RADIUS Client
RADIUS Server
Password Strength
Mgmt Access Method
Management Access Authentication
Secure Sensitive Data Management
SSL Server
SSH Server



ステップ2:[Enable SSH Server Authentication]チェックボックスをオンにして、SSHサーバ認証を有効にします。

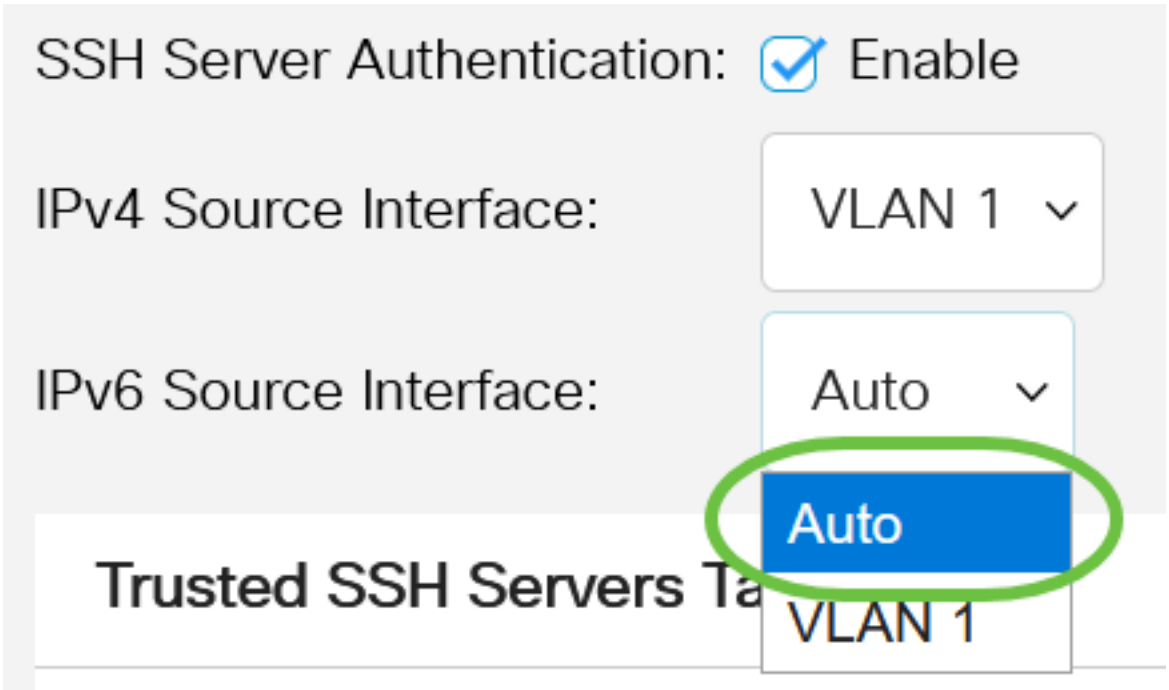


ステップ3:（オプション）[IPv4 Source Interface]ドロップダウンリストで、IPv4アドレスがIPv4 SSHサーバとの通信で使用されるメッセージの送信元IPv4アドレスとして使用される送信元インターフェイスを選択します。



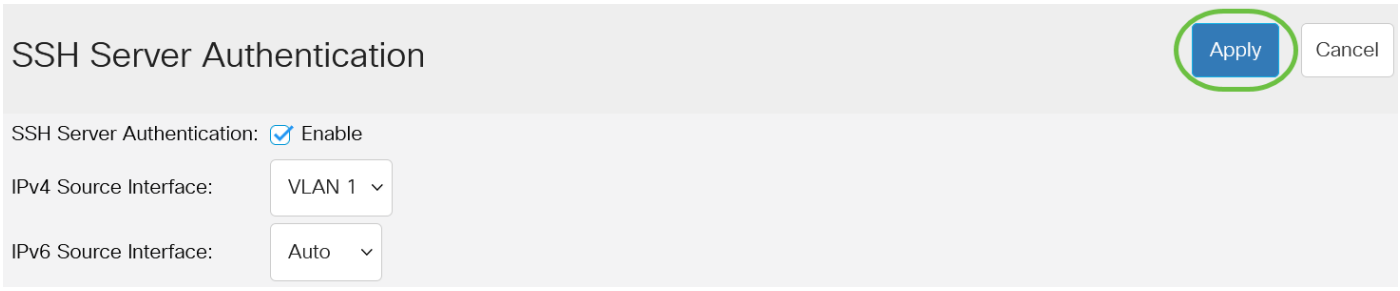
[Auto]オプションを選択すると、システムは発信インターフェイスで定義されたIPアドレスから送信元IPアドレスを取得します。この例では、VLAN1が選択されています。

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アドレスがIPv6 SSHサーバとの通信で使用されるメッセージの送信元IPv6アドレスとして使用される送信元インターフェイスを選択します。

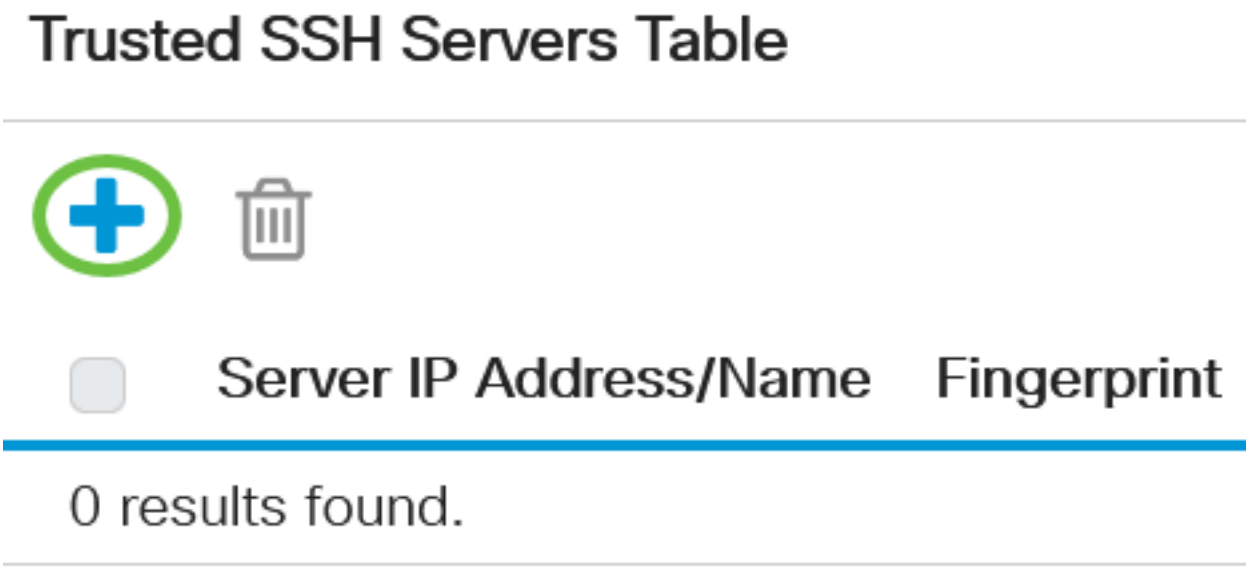


この例では、[Auto]オプションが選択されています。システムは、発信インターフェイスで定義されたIPアドレスから送信元IPアドレスを取得します。

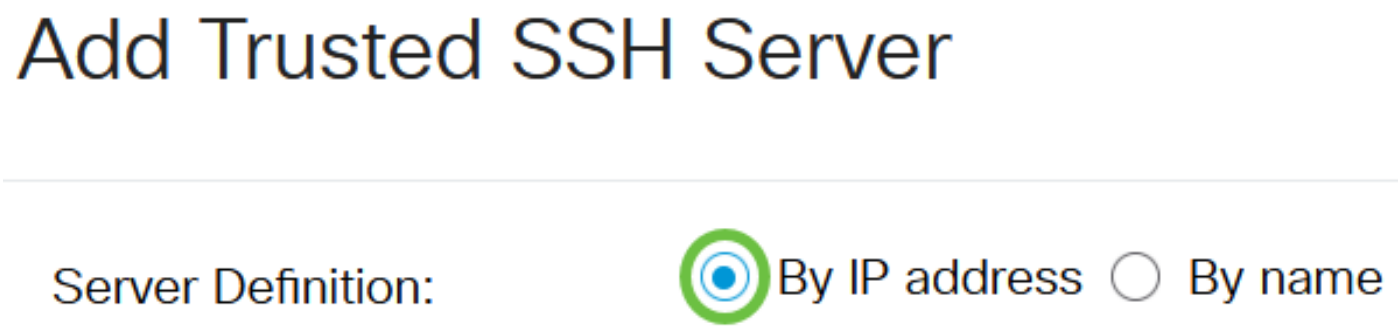
ステップ5:[Apply]をクリックします。



ステップ6：信頼できるサーバを追加するには、[Trusted SSH Servers Table]の**[Add]**をクリックします。



ステップ7:[Server Definition（サーバの定義）]領域で、使用可能な方法のいずれかをクリックしてSSHサーバを定義します。

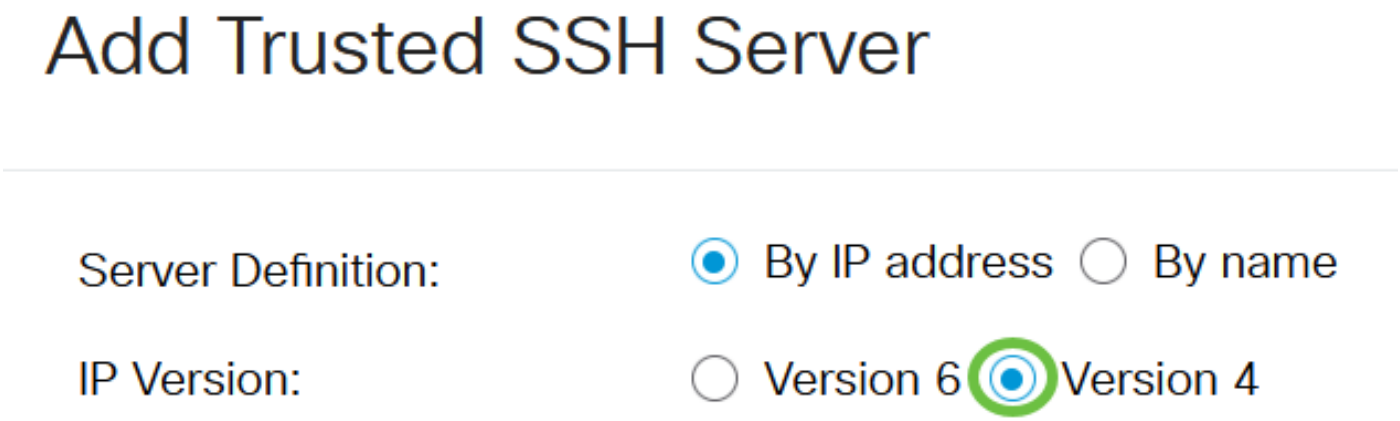


次のオプションがあります。

- [IPアドレス別(IP Address 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でSSHサーバを定義できます。

この例では、[By IP address]が選択されています。[名前]を選択した場合は、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[By IP address]を選択した場合は、[IP Version]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。

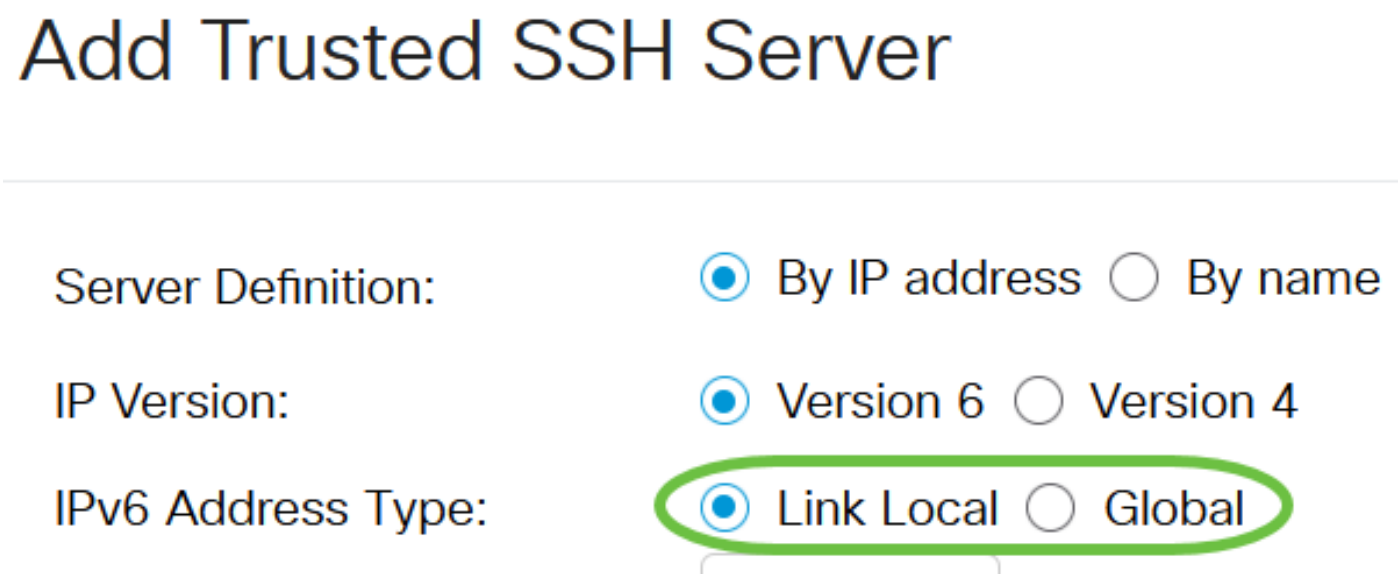


使用可能なオプションは次のとおりです。

- 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。

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 Address Type]でIPv6アドレスのタイプをクリックします。

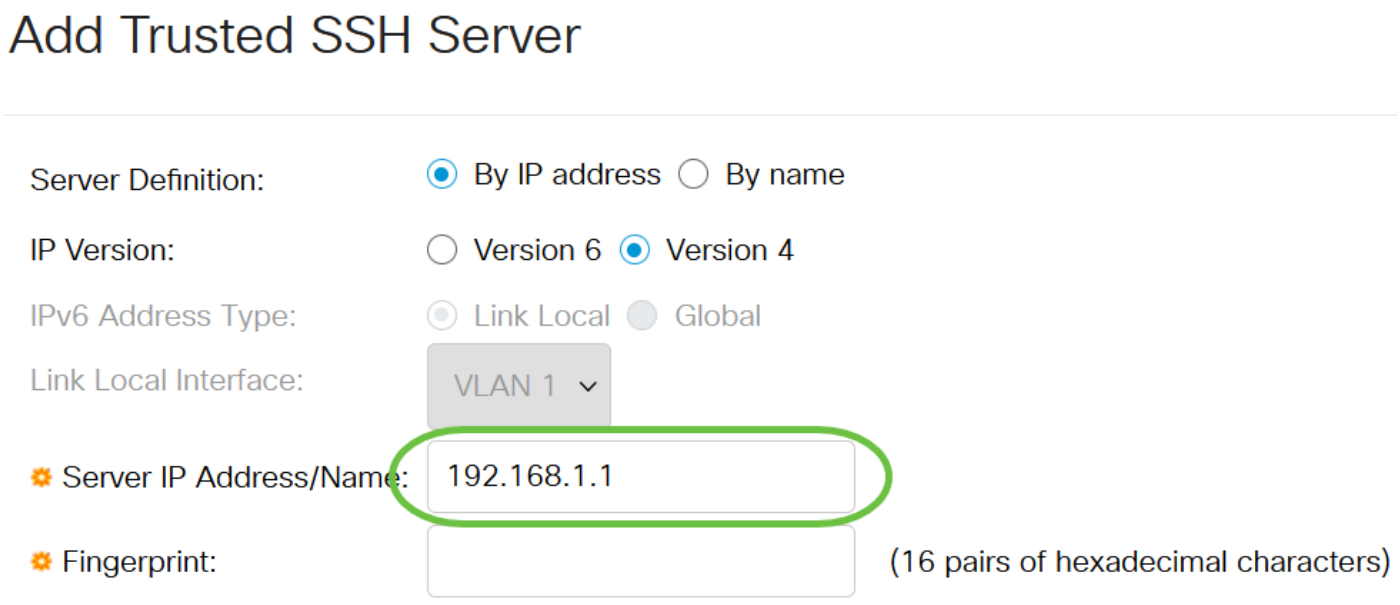


使用可能なオプションは次のとおりです。

- 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のプレフィクスはFE80で、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。インターフェイスにリンクローカルアドレスが存在する場合は、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。

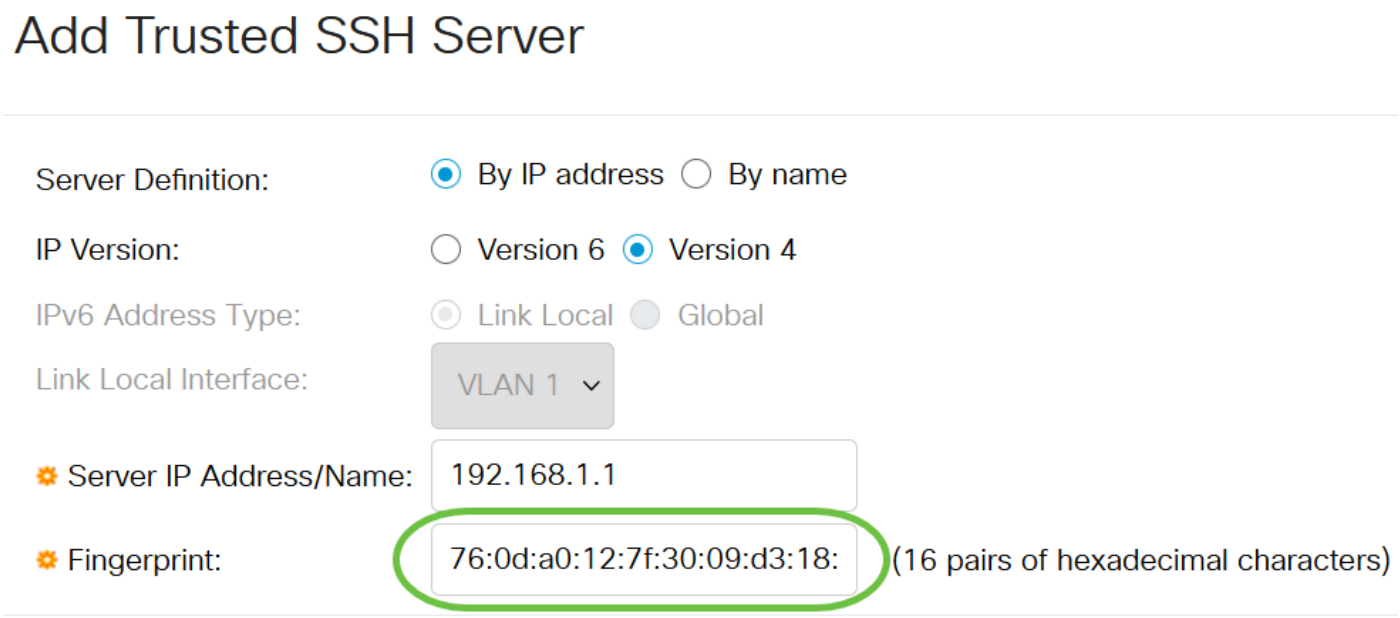
ステップ10:（オプション）ステップ9でIPv6アドレスタイプとして[Link Local]を選択した場合は、[Link Local Interface]ドロップダウンリストで適切なインターフェイスを選択します。

ステップ11:[*Server 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。

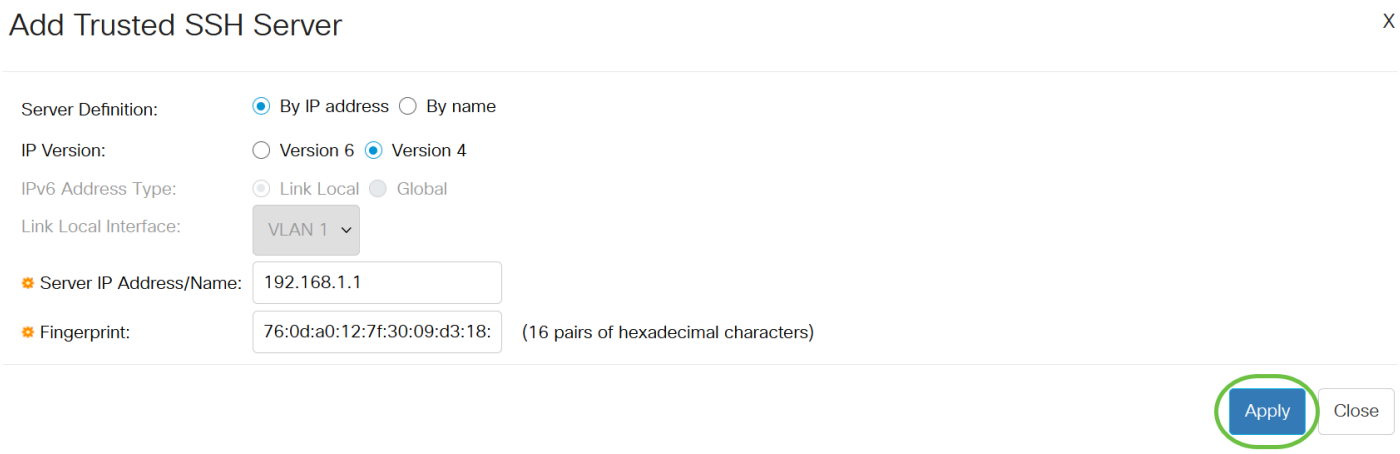


この例では、IPアドレスを入力します。

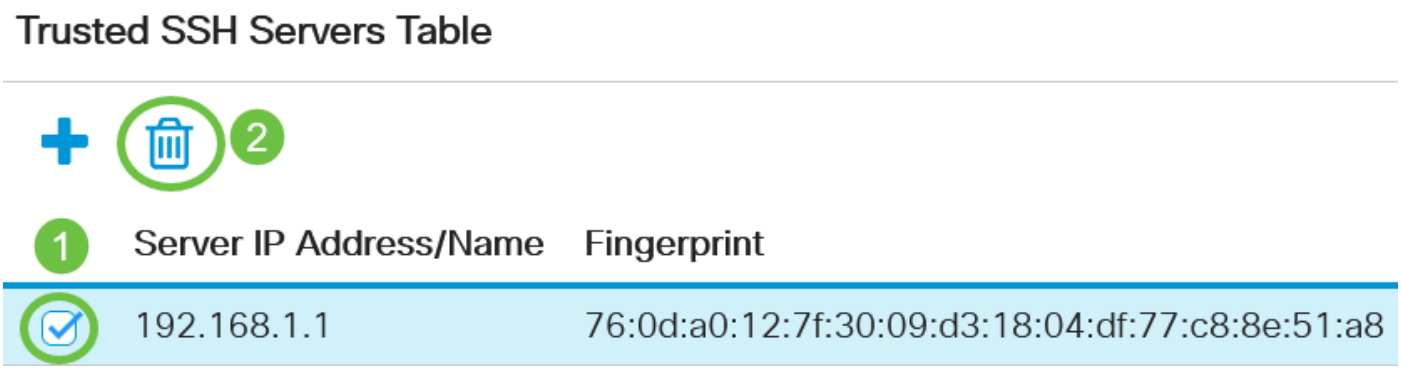
ステップ12:[フィンガープリント(*Fingerprint)]*フィールドに、SSHサーバのフィンガープリントを入力します。フィンガープリントは、認証に使用される暗号化キーです。この場合、フィンガープリントはSSHサーバの有効性を認証するために使用されます。サーバのIPアドレス/名前とフィンガープリントが一致する場合、SSHサーバが認証されます。



ステップ13:[Apply]をクリックし、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、[Delete]をクリックします。



ステップ15:（オプション）ページの上部にある[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。

SSH Server Authentication

これで、Cisco Business 350シリーズスイッチのSSHサーバ認証設定が完了しました。

CBS350スイッチに関する詳細な記事をお探しですか？詳細については、次のリンクを参照してください。

IPアドレスの設定 スタック設定 スタックモードセレクタ スタッキングのガイドライン SSHサーバ認証 パスワードの回復 PuTTYによるCLIへのアクセス VLAN の作成 スイッチのリセット