スイッチの設定 セキュア シェル（SSH）ユーザ認証設定

目標

セキュア シェル（SSH）はプロトコルです特定のネットワークデバイスにセキュア リモート 接続を提供する。 この接続は Telnet接続に類似したである、但し例外としては暗号化されます機能性を提供します。 SSH は管理者がサード パーティ プログラムで Command Line Interface （CLI）によってスイッチを設定することを可能にします。

SSH による CLI モードでは、管理者は信頼できる接続のより多くの拡張設定を実行できます。 SSH 接続はネットワークをリモートで解決することで役立ちます、ネットワーク管理者がネットワーク サイトで物理的にいなければ。 スイッチは管理者がユーザを認証し、SSH によってネットワークに接続するために管理することを可能にします。 認証は公開キーによってユーザが特定のネットワークへの SSH 接続を確立するのに使用できること行われます。

デバイス 認証および暗号化を提供するために SSH プロトコルを作動させる SSH クライアント 機能はアプリケーションです。 それは SSH サーバを実行する別のデバイスにセキュアおよび暗号化された接続を作ることをデバイスが可能にします。 認証および暗号化を使って、安全でない Telnet接続上のセキュアコミュニケーションを SSH クライアント可能に。

この技術情報は方法で手順を管理されたスイッチのクライアントのユーザ 認証を設定する提供します。

適当なデバイス

- 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

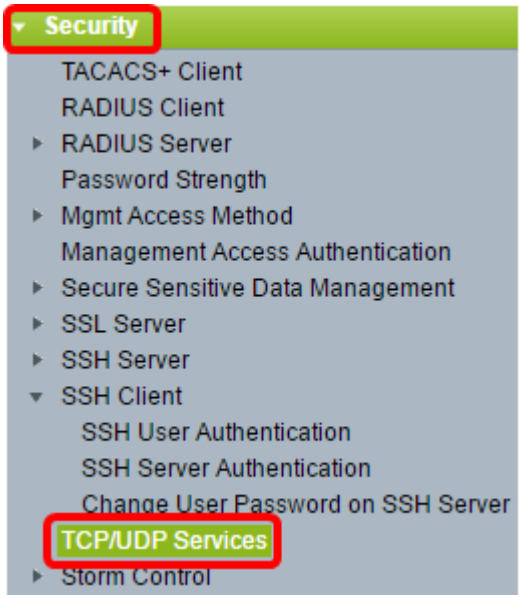
設定 SSH クライアント ユーザ認証設定

イネーブル SSH サービス

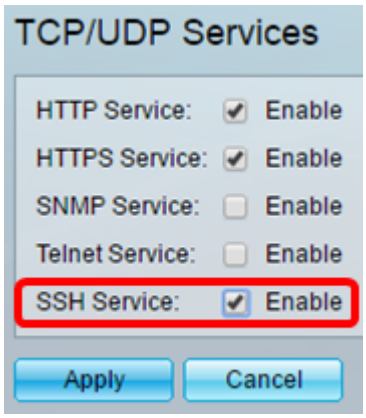
注: のボックス デバイス（工場出荷時のデフォルト設定を用いるデバイス）の自動設定をサポートするために、SSH サーバ認証はデフォルトで無効に なります。

ステップ 1. Webベース ユーティリティへのログインは **> TCP/UDP サービス** 『Security』

を選択 し、



呼び出します。 SSH によってスイッチ コマンド プロンプトのアクセスをイネーブルにするために **SSH サービス** チェックボックスをチェックして下さい。



ステップ 3. SSH サービスを有効に するために『Apply』 をクリック して下さい。

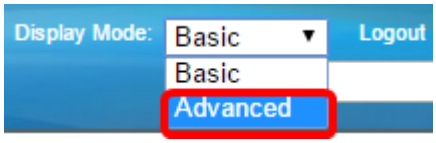
SSH ユーザ認証設定を設定して下さい

SSH ユーザ認証認証方法を選択するのにこのページを使用して下さい。 パスワード 方式が選択される場合デバイスのユーザ名 および パスワードを設定できます。 また Ron Rivest を生成できますパブリックかプライベートキー 方式が選択される場合アディ・ シャミアおよびレオナルド・ エーデルマン（ RSA ）または Digital Signature Algorithm （ DSA ）はキー入力します。

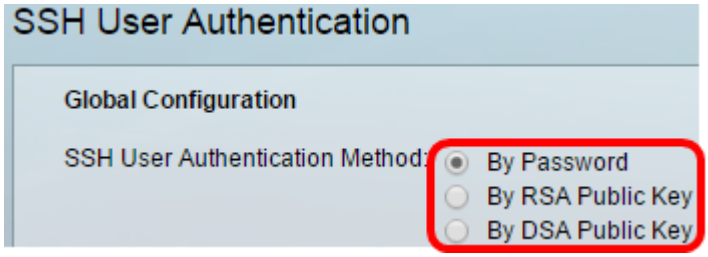
RSA および DSA DEFAULT 鍵ペアはデバイスのためにそれが起動したあるとき作成されます。 これらのキーの 1 つは SSH サーバからダウンロードされるデータを暗号化するのに使用されています。 RSA キーはデフォルトで使用されます。 ユーザが 1 つのまたは両方のキーを削除する場合、彼らは再生します。

ステップ 1. Webベース ユーティリティへのログインは **> SSH クライアント > SSH ユーザ認証** 『Security』 を選択 し。

注: Sx350、SG300X、または Sx500X があれば、表示 モード ドロップダウン リストから『Advanced』 を選択 することによる拡張モードへのスイッチ。



呼び出します。 グローバルコンフィギュレーションの下で、望ましい SSH ユーザ認証認証方法をクリックして下さい。

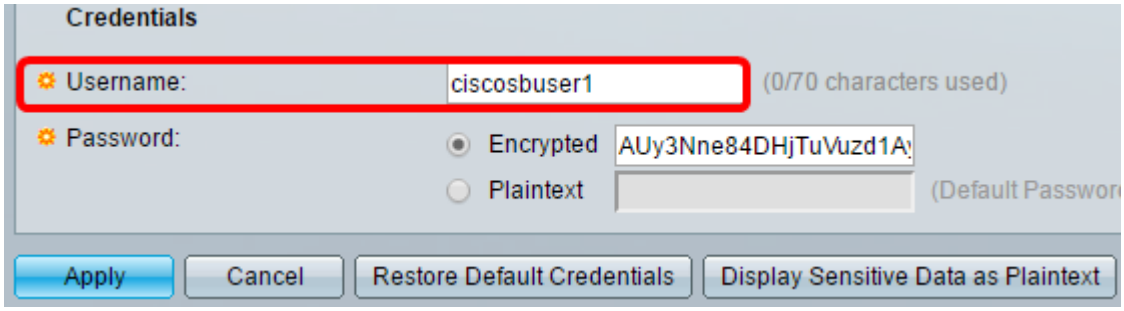


注: デバイス (SSH クライアント) が SSH サーバに SSH セッションを設定するように試みるとき SSH サーバはクライアント認証のために次のいずれかのメソッドを使用します:

- password —このオプションによってユーザ認証のためのパスワードを設定することを許可します。 これはデフォルト設定であり、デフォルトパスワードは匿名です。 このオプションが選択される場合、ユーザ名 および パスワード 資格情報が SSH サーバで確立されたことを確かめて下さい。
- RSA 公開キーによって—このオプションはユーザ認証のために RSA 公開キーを使用することを可能にします。 RSA キーは大きい整数の因数分解に基づく暗号化キーです。 このキーは SSH ユーザ認証に使用するキーのもっとも一般的な型です。
- DSA 公開キーによって—このオプションはユーザ認証のために DSA 公開キーを使用することを可能にします。 DSA キーは ElGamal 離散アルゴリズムに基づく暗号化キーです。 このキーは認証プロセスのより多くの時間かかるので SSH ユーザ認証のために広く使われていません。

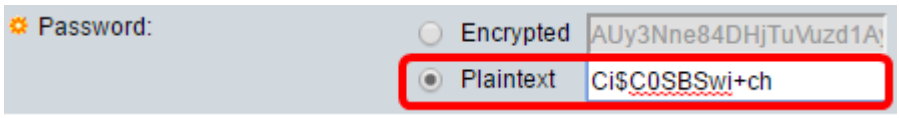
注: パスワードによるこの例では、選択されます。

ステップ 3 資格情報 エリアでは、*Username フィールド*でユーザネームを入力して下さい。



注: この例では、ciscosbuser1 は使用されます。

ステップ 2 のパスワードによって選択した場合ステップ 4.（オプションの）は、方式をクリックしましたりそして*暗号化*されたまたは*プレーンテキスト* フィールドでパスワードを入力します。



次のオプションがあります。

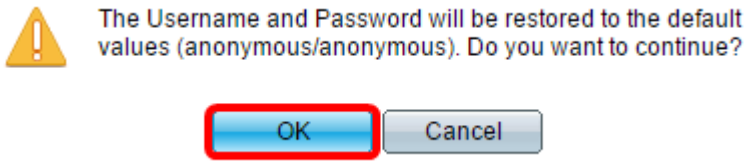
- 暗号化される—このオプションはパスワードの暗号化されたバージョンを入力することを可能にします。
- プレーンテキスト—このオプションは平文 パスワードを入力することを可能にします。

注: この例では、プレーンテキストは選択され、平文 パスワードは入力されます。

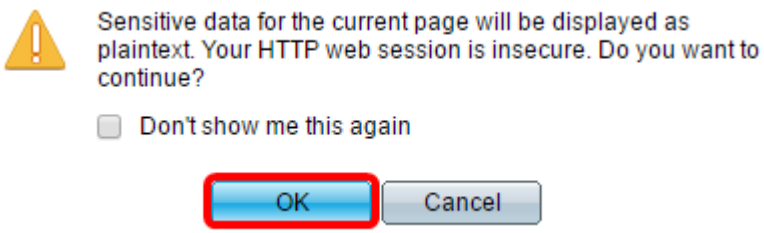
ステップ 5.認証の設定を保存するために『Apply』 をクリック して下さい。

ステップ 6.（オプションの）はデフォルトユーザ名およびパスワードを回復するために**既定の資格情報を**『Restore』 をクリック しましたりそして続行するために『OK』 をクリック します。

注: ユーザ名 および パスワードはデフォルト値に復元する: 匿名/匿名。

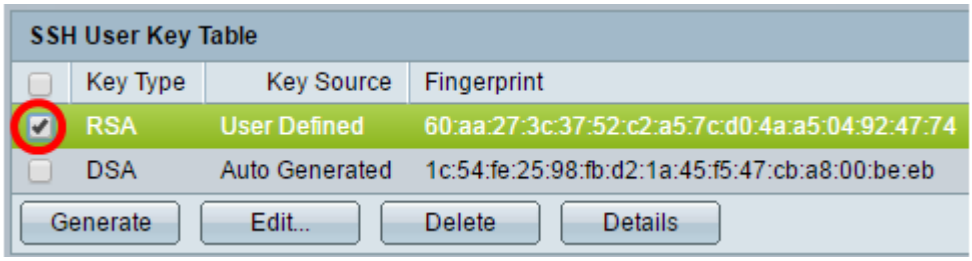


ステップ 7.（オプションの）は**プレーンテキストとして**プレーンテキストフォーマットでページの機密データを示すために**機密データを**『Display』 をクリック しましたりそして続行するために『OK』 をクリック します。



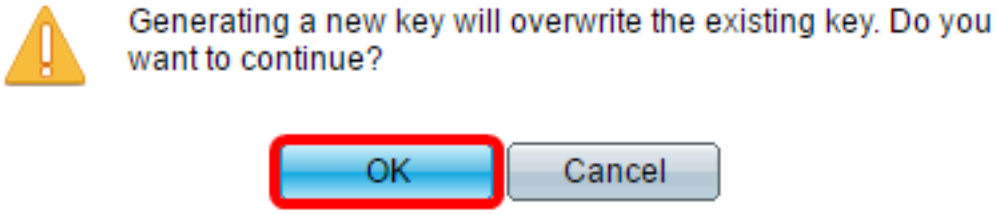
設定 SSH User 鍵 表

ステップ 8 管理したいキーのチェックボックスをチェックして下さい。

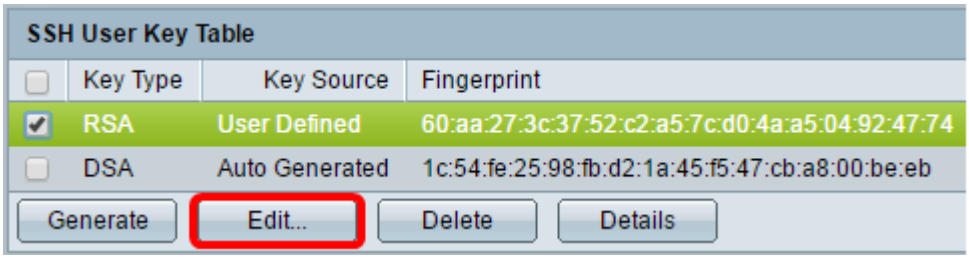


注: この例では、RSA は選択されます。

ステップ 9.（オプションの）は New 鍵を生成するために『Generate』 をクリック します。 New 鍵はチェックされたキーを無効にしましたりそして続行するために『OK』 をクリック します。



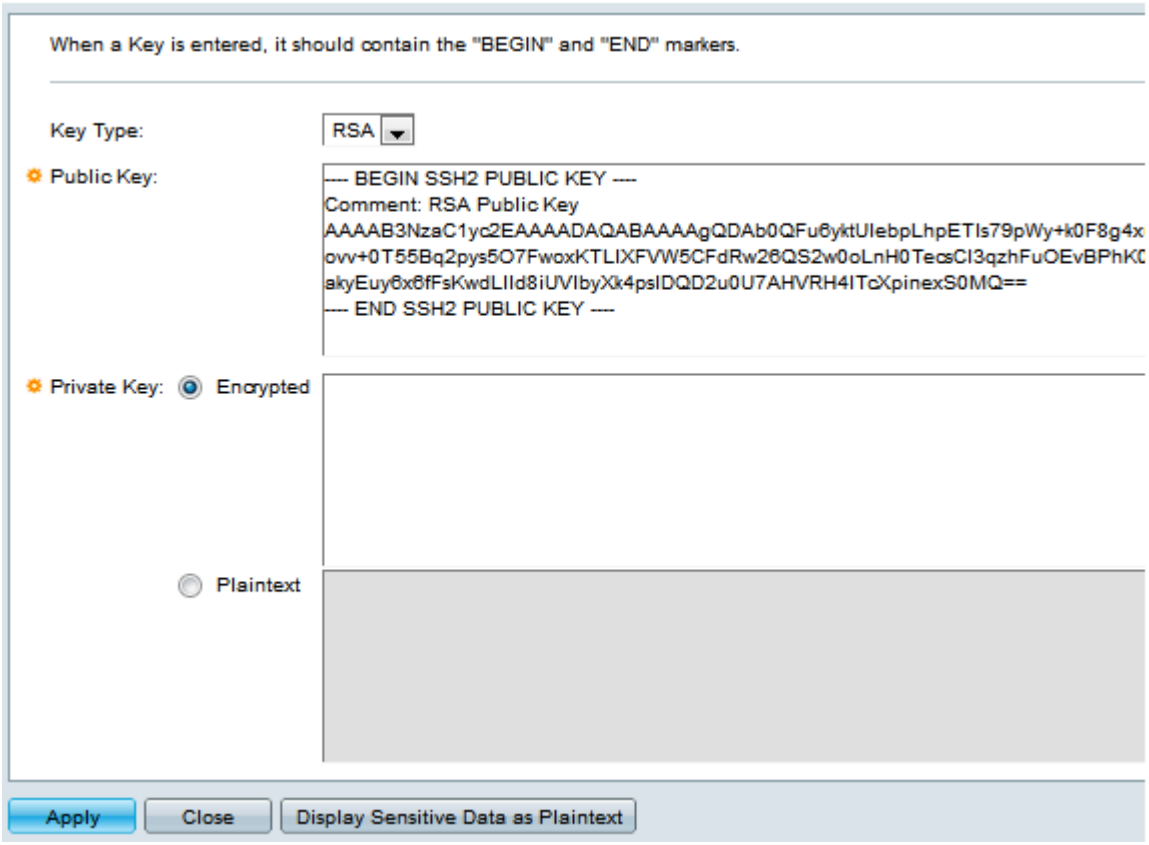
ステップ 10.（オプションの）は現在のキーを編集するために『Edit』 をクリック します。



ステップ 11.（オプションの）はキーの種類ドロップダウン リストからキーの種類を選択します。

注: この例では、RSA は選択されます。

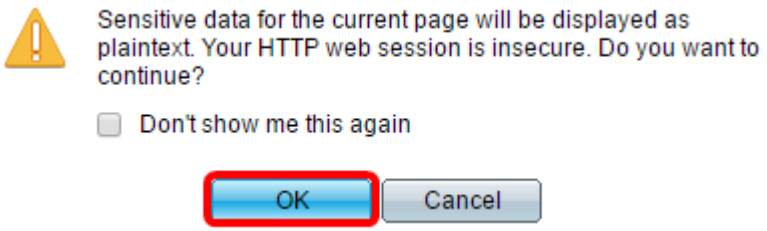
ステップ 12 : （オプションの）*公開キー* フィールドで新しい公開キーを入力して下さい。



ステップ 13： （オプションの）プライベートキー フィールドで新しいプライベートキーを入力して下さい。

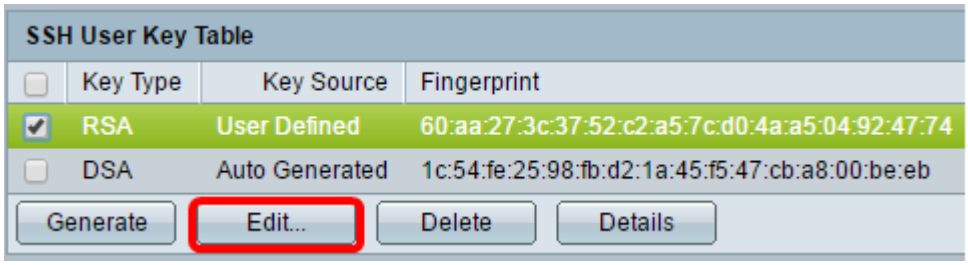
注: プライベートキーを編集、平文の現在のプライベートキーを参照するために現在のプライベートキーと同時に暗号化されたテキスト、かプレーンテキストを見るために暗号化されてクリックできます。

ステップ 14： （オプションの）プレーンテキストフォーマットのページの暗号化されたデータが続行するためにそして『OK』 をクリック することを示すために**プレーンテキストとして機密データを**『Display』 をクリック して下さい。

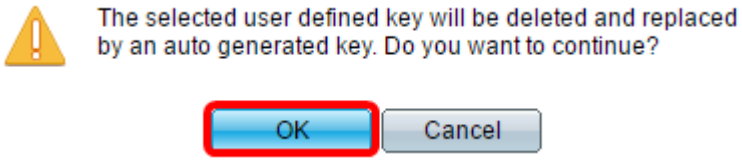


ステップ 15： 変更を保存するために『Apply』 をクリック しそして『Close』 をクリック して下さい。

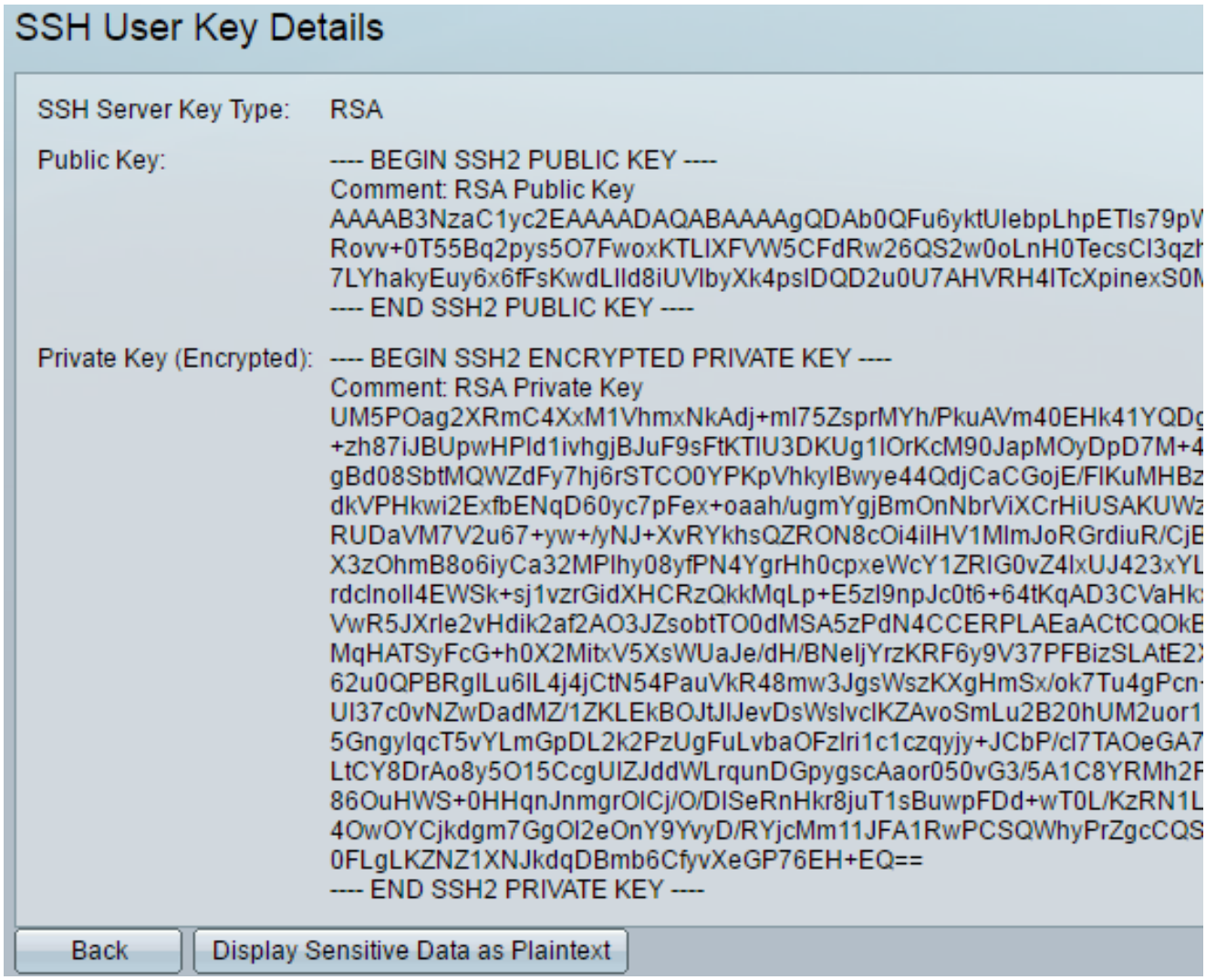
ステップ 16： （オプションの）チェックされたキーを削除するために『Delete』 をクリック して下さい。



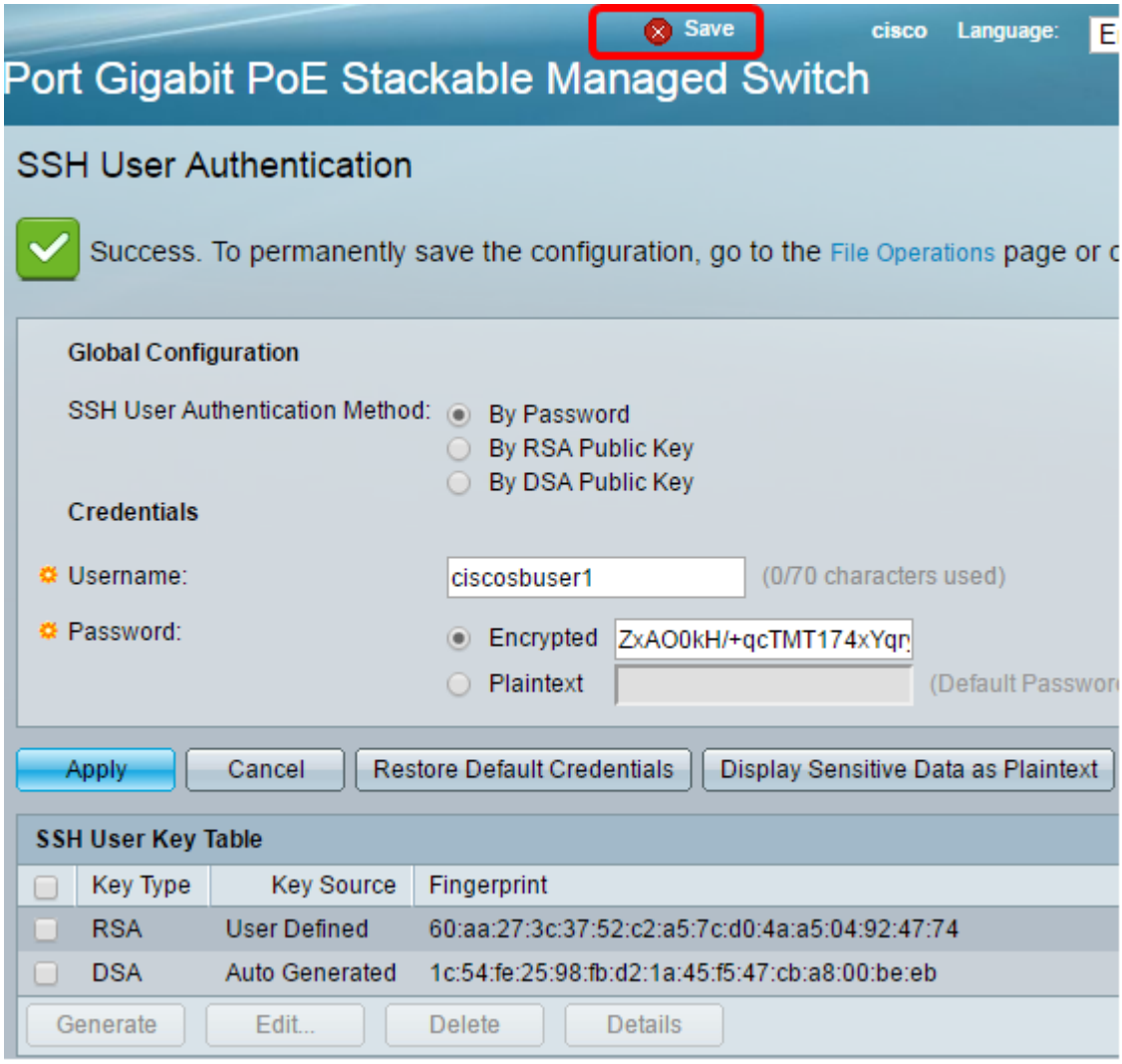
ステップ 17： （オプションの）、キーを削除するために『OK』 をクリック しなさい下記に示されているように一度確認のメッセージによってプロンプト表示しました。



ステップ 18： （オプションの）チェックされたキーの詳細を参照するために『Details』 をクリック して下さい。



ステップ 19： （オプションの）スタートアップ コンフィギュレーション コンフィギュレーション・ ファイルへの変更を保存するためにページの上部分で **SAVE ボタンを**クリック して下さい。



今管理されたスイッチのクライアントのユーザ認証設定を行う必要があります。