

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ず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

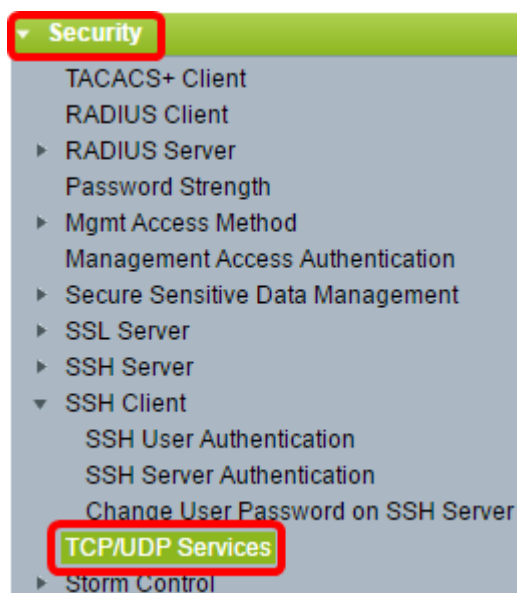
設定 SSH クライアント ユーザ認証設定

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

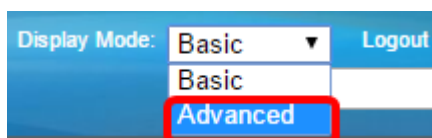
SSH ユーザ認証方法を選択するのにこのページを使用して下さい。パスワード方式が選択される場合デバイスのユーザ名 および パスワードを設定できます。また Ron Rivest を生成できますパブリックかプライベートキー方式が選択される場合アディ・シャミアおよびレオナルド・エーデルマン (RSA) または Digital Signature Algorithm (DSA) はキー入力します。

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ため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。

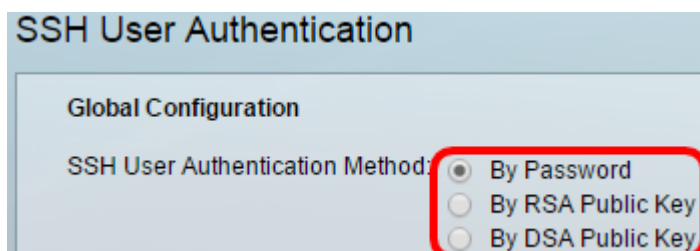
ステップ 1. Webベース ユーティリティへのログインは > SSH クライアント > SSH ユーザ認証 『Security』を選択し。



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。

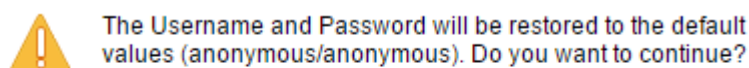
- 暗号化される—このオプションはパスワードの暗号化されたバージョンを入力することを可能にします。
- プレーンテキスト—このオプションは平文 パスワードを入力することを可能にします。

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。

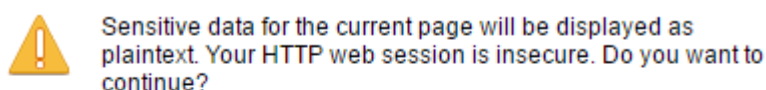
ステップ 5. 認証の設定を保存するために『Apply』 をクリックして下さい。

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。



Don't show me this again

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。

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	60:aa:27:3c:37:52:c2:a5:7c:d0:4a:a5:04:92:47:74
<input type="checkbox"/>	DSA	Auto Generated	1c:54:fe:25:98:fb:d2:1a:45:f5:47:cb:a8:00:be:eb

Generate Edit... Delete Details

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たりして続行するために『OK』をクリックします。



Generating a new key will overwrite the existing key. Do you want to continue?



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。

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	60:aa:27:3c:37:52:c2:a5:7c:d0:4a:a5:04:92:47:74
<input type="checkbox"/>	DSA	Auto Generated	1c:54:fe:25:98:fb:d2:1a:45:f5:47:cb:a8:00:be:eb

Generate Edit... Delete Details

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。

Key Type: 

Public Key: 

Comment:

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。

When a Key is entered, it should contain the "BEGIN" and "END" markers.

Key Type:

Public Key:

```
--- BEGIN SSH2 PUBLIC KEY ---  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAADAQABAAQDAQDAb0QFu6yktUlebpLhpETIs79pWy+k0F8g4x  
ovw+0T55Bq2pys5O7FwoxKTLIXFVW5CFdRw26QS2w0oLnH0TecsC13qzhFuOEVBPhKC  
akyEuy6x8fFsKwdLIld8iUVIbyXk4psIDQD2u0U7AHVRH4ITcXpinexS0MQ==  
--- END SSH2 PUBLIC KEY ---
```

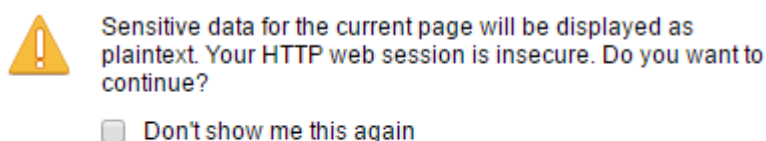
Private Key: Encrypted

Plaintext

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移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。

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	60:aa:27:3c:37:52:c2:a5:7c:d0:4a:a5:04:92:47:74
<input type="checkbox"/>	DSA	Auto Generated	1c:54:fe:25:98:fb:d2:1a:45:f5:47:cb:a8:00:be:eb

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。

 The selected user defined key will be deleted and replaced by an auto generated key. Do you want to continue?

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。

SSH User Key Details

SSH Server Key Type: RSA

Public Key: --- BEGIN SSH2 PUBLIC KEY ---
 Comment: RSA Public Key
 AAAAB3NzaC1yc2EAAAADAQABAAQgQDAb0QFu6yktUlebpLhpETIs79pV
 Rowv+0T55Bq2pys5O7FwoxKTLIXFWW5CFdRw26QS2w0oLnH0TecsCI3qzH
 7LYhakyEuy6x6fFsKwdLlId8iUVlbyXk4psIDQD2u0U7AHVRH4ITcXpinexS0M
 --- END SSH2 PUBLIC KEY ---

Private Key (Encrypted): --- BEGIN SSH2 ENCRYPTED PRIVATE KEY ---
 Comment: RSA Private Key
 UM5POag2XRmC4XxM1VhmxNkAdj+ml75ZsprMYh/PkuAVm40EHk41YQDg
 +zh87iJBUpwHPId1ivhgjBJuF9sFtKTIU3DKUg1IOrKcM90JapMOyDpD7M+4
 gBd08SbtMQWZdFy7hj6rSTCO0YPKpVhkylBwye44QdjCaCGojE/FIKuMHBz
 dkVPHkwi2ExfbENqD60yc7pFex+oaah/ugmYgjBmOnNbrViXCrHiUSAKUWz
 RUDaVM7V2u67+yw+yNJ+XvRYkhsQZRON8cOi4ilHV1MImJoRGrdiuR/CjE
 X3zOhmB8o6iyCa32MPlhy08yfPN4YgrHh0cpxeWcY1ZRIG0vZ4lxUJ423xYL
 rdclnoll4EWSk+sj1vzrGidXHCRzQkkMqLp+E5zl9npJc0t6+64tKqAD3CVaHk
 VwR5JXrle2vHdik2af2AO3JZsobtTO0dMSA5zPdN4CCERPLAEaACTCQOkE
 MqHATSyFcG+h0X2MitxV5XsWUaJe/dH/BNeljYrzKRF6y9V37PFBizSLAtE2
 62u0QPBRglLu6lL4j4jCtN54PauVkr48mw3JgsWszKXgHmSx/ok7Tu4gPcn
 UI37c0vNZwDadMZ/1ZKLEkBOJtJIJevDsWslvclKZAvoSmLu2B20hUM2uor1
 5GngylqcT5vYLMGpDL2k2PzUgFuLvbaOFzIri1c1czqjy+JCbP/cl7TAOeGA7
 LtCY8DrAo8y5O15CcgUIZJddWLRqunDGpygscAaor050vG3/5A1C8YRMh2F
 86OuHWS+0HHqnJnmgrOICj/O/DISeRnHkr8juT1sBuwpFDd+wT0L/KzRN1L
 4OwOYCjkdgm7GgOl2eOnY9YvyD/RyjcMm11JFA1RwPCSQWhyPrZgcCQS
 0FLgLKZNZ1XNjkdqDBmb6CfyvXeGP76EH+EQ==
 --- END SSH2 PRIVATE KEY ---

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。

cisco Language: E

Port Gigabit PoE Stackable Managed Switch

SSH User Authentication

Success. To permanently save the configuration, go to the [File Operations](#) page or c

Global Configuration

SSH User Authentication Method: By Password
 By RSA Public Key
 By DSA Public Key

Credentials

✱ Username: (0/70 characters used)

✱ Password: Encrypted
 Plaintext (Default Password)

SSH User Key Table

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input type="checkbox"/>	RSA	User Defined	60:aa:27:3c:37:52:c2:a5:7c:d0:4a:a5:04:92:47:74
<input type="checkbox"/>	DSA	Auto Generated	1c:54:fe:25:98:fb:d2:1a:45:f5:47:cb:a8:00:be:eb

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。