

スイッチでのセキュアシェル(SSH)ユーザ認証設定の設定

目的

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)を介してサードパーティ製プログラムでスイッチを設定できます。

CLIモードでSSHを使用すると、より高度な設定を安全な接続で実行できます。SSH接続は、ネットワーク管理者が物理的にネットワークサイトにいない場合に、リモートでネットワークのトラブルシューティングを行う際に役立ちます。スイッチを使用すると、管理者はSSHを介してネットワークに接続するユーザを認証および管理できます。認証は、ユーザが特定のネットワークへのSSH接続を確立するために使用できる公開キーを介して行われます。

SSHクライアント機能は、SSHプロトコル上で実行されるアプリケーションで、デバイスの認証と暗号化を提供します。これにより、デバイスはSSHサーバを実行する別のデバイスに対して安全で暗号化された接続を確立できます。認証と暗号化を使用すると、SSHクライアントは安全でないTelnet接続を介した安全な通信を可能にします。

この記事では、管理対象スイッチでクライアントユーザ認証を設定する方法について説明します。

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クライアントユーザ認証設定の設定

SSHサービスの有効化

注：工場出荷時のデフォルト設定でアウトオブボックスデバイス（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

▼ Security

- TACACS+ Client
- RADIUS Client
- ▶ RADIUS Server
- Password Strength
- ▶ Mgmt Access Method
- Management Access Authentication
- ▶ Secure Sensitive Data Management
- ▶ SSL Server
- ▶ SSH Server
- ▼ SSH Client
 - SSH User Authentication
 - SSH Server Authentication
 - Change User Password on SSH Server
- ▶ Storm Control

TCP/UDP Services

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。

TCP/UDP Services

HTTP Service: Enable

HTTPS Service: Enable

SNMP Service: Enable

Telnet Service: Enable

SSH Service: Enable

Apply

Cancel

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ユーザ認証設定の設定

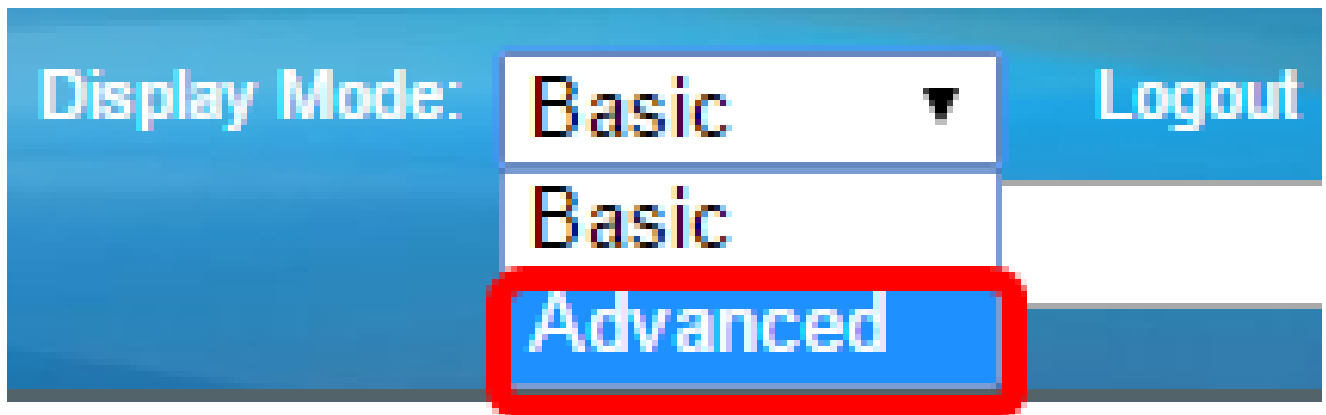
このページを使用して、SSHユーザ認証方法を選択します。パスワード方式が選択されている場合は、デバイスにユーザ名とパスワードを設定できます。公開キー方式または秘密キー方式を選択した場合は、Ron Rivest、Adi Shamir and Leonard Adleman(RSA)キーまたはデジタル署名アルゴリズム(DSA)キーを生成することもできます。

RSAおよびDSAのデフォルトキーペアは、デバイスの起動時に生成されます。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の暗号化に使用されます。RSAキーはデフォルトで使用されます。ユーザがこれらのキーの一方または両方を削除すると、キーは再生成されます。

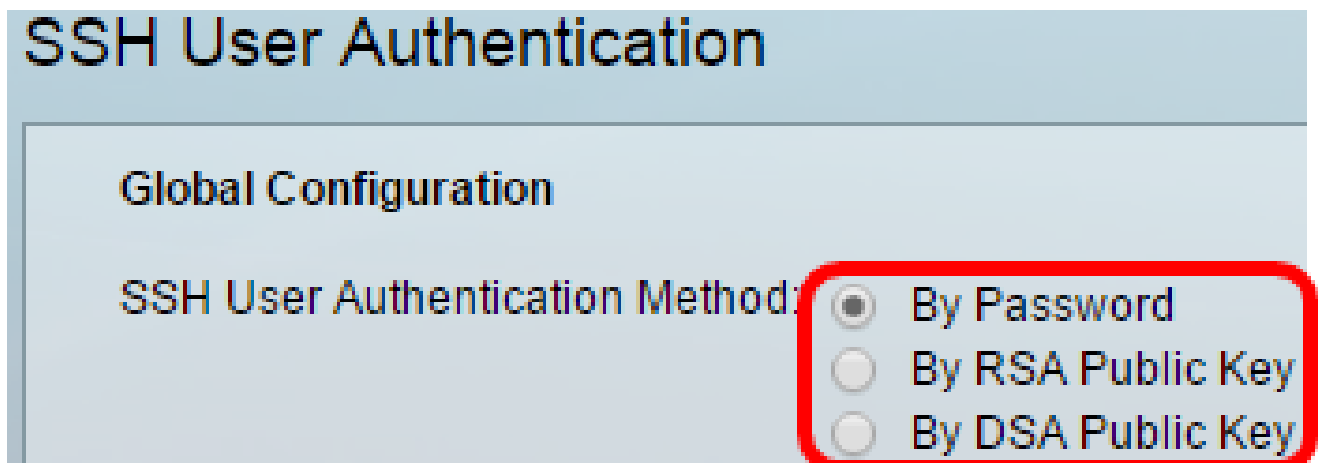
ステップ 1 : Webベースのユーティリティにログインし、Security > SSH Client > SSH User Authenticationの順に選択します。



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 : Global Configurationで、目的のSSH User Authentication Methodをクリックします。



注 : デバイス (SSHクライアント) がSSHサーバへのSSHセッションを確立しようとする
と、SSHサーバはクライアント認証に次のいずれかの方法を使用します。

- By Password : このオプションでは、ユーザ認証用のパスワードを設定できます。これはデフォルト設定で、デフォルトのパスワードはanonymousです。このオプションを選択する場合は、ユーザ名とパスワードのクレデンシャルがSSHサーバで確立されていることを確認します。
- By RSA Public Key : このオプションを使用すると、ユーザ認証にRSA公開キーを使用できます。RSAキーは、大きな整数の因数分解に基づく暗号化キーです。このキーは、SSHユーザ認証に使用される最も一般的なタイプのキーです。
- By DSA Public Key : このオプションを使用すると、ユーザ認証にDSA公開キーを使用できます。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に時間がかかるため、SSHユーザ認証では一般的に使用されません。

注 : この例では、By Passwordが選択されています。

ステップ 3 : Credentials領域で、Usernameフィールドにユーザ名を入力します。

Credentials

☛ Username: ciscosbuser1 (0/70 characters used)

☛ Password: Encrypted AUy3Nne84DHjTuVuzd1A!
 Plaintext (Default Password)

Apply Cancel Restore Default Credentials Display Sensitive Data as Plaintext

注：この例では、ciscosbuser1が使用されています。

ステップ4: (オプション) ステップ2で「パスワード使用」を選択した場合は、方式をクリックし、EncryptedフィールドまたはPlaintextフィールドにパスワードを入力します。

☛ Password: Encrypted AUy3Nne84DHjTuVuzd1A!
 Plaintext Ci\$C0SBSwi+ch

次のオプションがあります。

- Encrypted : このオプションでは、パスワードの暗号化バージョンを入力できます。
- 「プレーンテキスト」 - このオプションでは、プレーンテキストのパスワードを入力できません。

注：この例では、プレーンテキストが選択され、プレーンテキストのパスワードが入力されます。

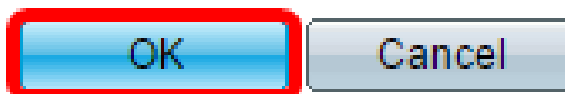
ステップ 5 : Applyをクリックして、認証設定を保存します。

ステップ6: (オプション) Restore Default Credentialsをクリックしてデフォルトのユーザ名とパスワードを復元し、OKをクリックして続行します。

注：ユーザ名とパスワードはデフォルト値のanonymous/anonymousに戻ります。



The Username and Password will be restored to the default values (anonymous/anonymous). Do you want to continue?



ステップ7: (オプション) Display Sensitive Data as Plaintextをクリックして、ページの機密データをプレーンテキスト形式で表示し、OKをクリックして続行します。



Sensitive data for the current page will be displayed as plaintext. Your HTTP web session is insecure. Do you want to continue?

Don't show me this again



SSHユーザキーテーブルの設定

ステップ8: 管理するキーのチェックボックスをオンにします。

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

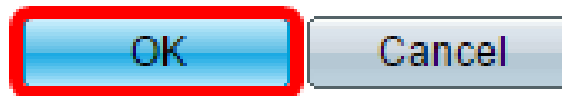
Generate Edit... Delete Details

注: この例では、RSAが選択されています。

ステップ9: (オプション) Generateをクリックして、新しいキーを生成します。新しいキーはチェックされたキーを上書きし、OKをクリックして続行します。



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



ステップ10: (オプション) Editをクリックして、現在のキーを編集します。

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) Key Typeドロップダウンリストからキータイプを選択します。

Key Type:

⚙️ Public Key:



注：この例では、RSAが選択されています。

ステップ12: (オプション) Public Keyフィールドに新しい公開キーを入力します。

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  
AAAAB3NzaC1yc2EAAAADAQABAAQDAAb0QFu6yktUlebpLhpETIs79pWy+k0F8g4x  
ovv+0T55Bq2pys5O7FwoxKTLIXFVW5CFdRw26QS2w0oLnH0TecsCI3qzhFuOEvBPhK  
skyEuy6x8fFsKwdLIId8iUVIbyXk4psIDQD2u0U7AHVRH4ITcXpinexS0MQ==  
--- END SSH2 PUBLIC KEY ---
```

Private Key: Encrypted

Plaintext

ステップ13: (オプション) Private Keyフィールドに新しい秘密キーを入力します。

注：秘密キーを編集して[暗号化]をクリックすると、現在の秘密キーが暗号化されたテキストとして表示されます。[プレーンテキスト]をクリックすると、現在の秘密キーがプレーンテキストで表示されます。

ステップ14: (オプション) Display Sensitive Data as Plaintextをクリックして、ページの暗号化されたデータをプレーンテキスト形式で表示し、OKをクリックして続行します。



Sensitive data for the current page will be displayed as plaintext. Your HTTP web session is insecure. Do you want to continue?

Don't show me this again

ステップ 15 : Applyをクリックして変更を保存し、Closeをクリックします。

ステップ16: (オプション) Deleteをクリックして、チェックしたキーを削除します。

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17: (オプション) 次を示す確認メッセージが表示されたら、OKをクリックしてキーを削除します。



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) Detailsをクリックして、チェックしたキーの詳細を表示します。

SSH User Key Details

SSH Server Key Type: RSA

Public Key:

---- BEGIN SSH2 PUBLIC KEY ----

Comment: RSA Public Key

```
AAAAB3NzaC1yc2EAAAADAQABAAQgQDAB0QFu6yktUlebplhpETIs79pV  
Rovv+0T55Bq2pys5O7FwoxKTLIXFW5CFdRw26QS2w0oLnH0TecsCI3qzF  
7LYhakyEuy6x6fFsKwdLlId8iUVlbyXk4psIDQD2u0U7AHVRH4ITcXpinexS0M  
---- END SSH2 PUBLIC KEY ----
```

Private Key (Encrypted):

---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----

Comment: RSA Private Key

```
UM5POag2XRmC4XxM1VhmxNkAdj+ml75ZsprMYh/PkuAVm40EHk41YQDg  
+zh87iJBUpwHPId1ivhgjBJuF9sFtKTIU3DKUg1lOrKcM90JapMOyDpD7M+4  
gBd08SbtMQWZdFy7hj6rSTCO0YPKpVhkyIBwye44QdjCaCGojE/FIKuMHBz  
dkVPHkwi2ExfbENqD60yc7pFex+oaah/ugmYgjBmOnNbrViXCrHiUSAKUWz  
RUDaVM7V2u67+yw+/yNJ+XvRYkhsQZRON8cOi4iIHV1MImJoRgrdiuR/CjE  
X3zOhmB8o6iyCa32MPlhy08yfPN4YgrHh0cpxeWcY1ZRIG0vZ4lxUJ423xYL  
rdclnoll4EWSk+sj1vzrGidXHCRzQkkMqLp+E5zl9npJc0t6+64tKqAD3CVaHk  
VwR5JXrle2vHdik2af2AO3JZsobtTO0dMSA5zPdN4CCERPLAEaActCQOkE  
MqHATSyFcG+h0X2MitxV5XsWUaJe/dH/BNeljYrzKRF6y9V37PFBizSLAtE2  
62u0QPBRglLu6IL4j4jCtN54PauVkr48mw3JgsWszKXgHmSx/ok7Tu4gPcn  
UI37c0vNZwDadMZ/1ZKLEkBOJtJIJevDsWslvclKZAvoSmLu2B20hUM2uor1  
5GngylqcT5vYLMGpDL2k2PzUgFuLvbafzLri1c1czqy+jCbP/cl7TAOeGA7  
LtCY8DrAo8y5O15CcgUIZJddWLRqunDGpygscAaor050vG3/5A1C8YRMh2F  
86OuHWS+0HHqnJnmgrOICj/O/DiSeRnHkr8juT1sBuwpFDd+wT0L/KzRN1L  
4OwOYCjkdgm7GgOI2eOnY9YvyD/RyjCmM11JFA1RwPCSQWhyPrZgcCQS  
0FLgLKZNZ1XNjkdqDBmb6CfyvXeGP76EH+EQ==  
---- END SSH2 PRIVATE KEY ----
```

Back


Display Sensitive Data as Plaintext

ステップ19: (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。

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

これで、管理対象スイッチでクライアントユーザの認証設定が完了しました。

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。