

Cisco Business 350シリーズ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

この記事では、Cisco Business 350シリーズ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。

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。

SSHを介したCLIモードでは、管理者はセキュアな接続でより高度な設定を実行できます。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存在しない場合に、ネットワークをリモートでトラブルシューティングする際に役立ちます。スイッチを使用すると、管理者はユーザを認証および管理して、SSH経由でネットワークに接続できます。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、デバイスの認証と暗号化を提供するためにSSHプロトコル上で実行されるアプリケーションです。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セキュア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クライアントは非セキュアTelnet接続を介したセキュアな通信を可能にします。

該当するデバイス | ソフトウェアバージョン

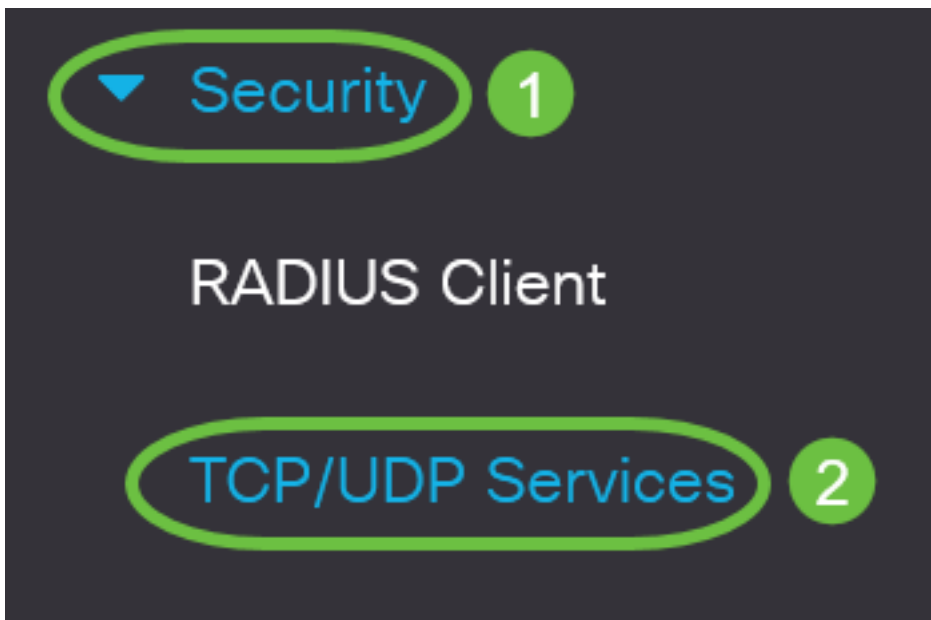
- CBS350 ([データシート](#)) | 3.0.0.69 ([最新版をダウンロード](#))
- CBS350-2X([データシート](#)) | 3.0.0.69 ([最新版をダウンロード](#))
- CBS350-4X([データシート](#)) | 3.0.0.69 ([最新版をダウンロード](#))

SSHクライアントユーザ認証設定の設定

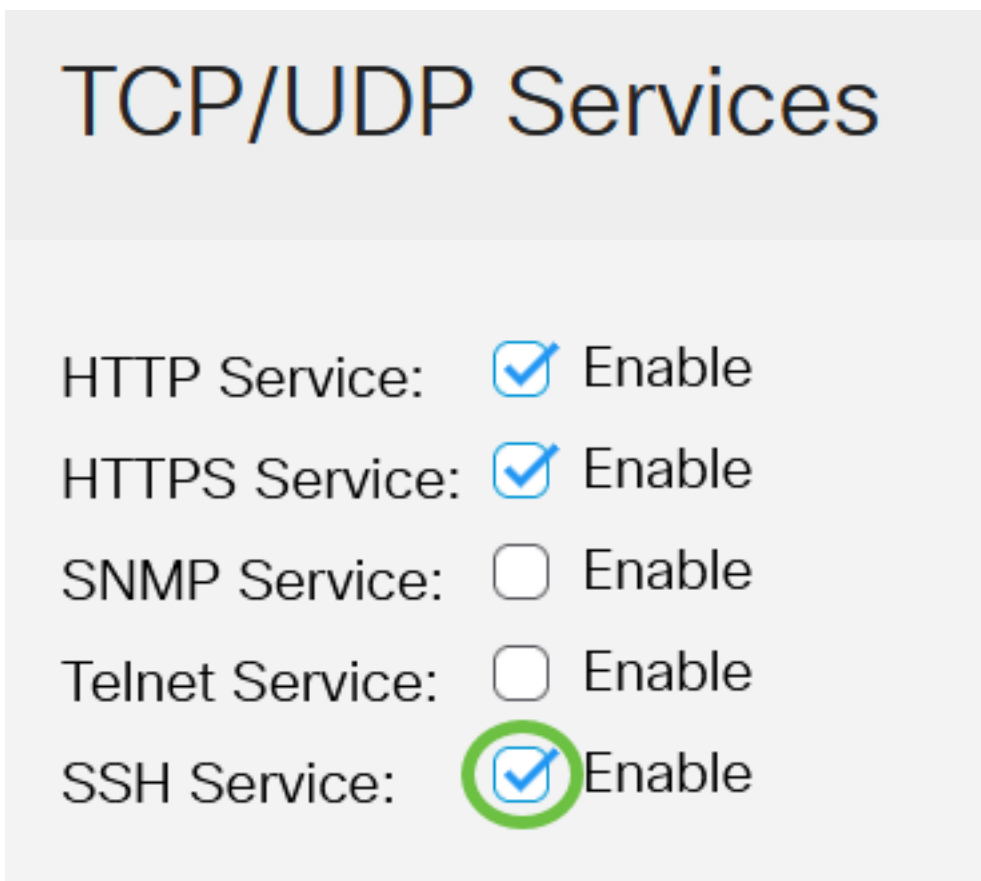
SSHサービスの有効化

アウトオブボックスデバイス (工場出荷時のデフォルト設定のデバイス) 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。

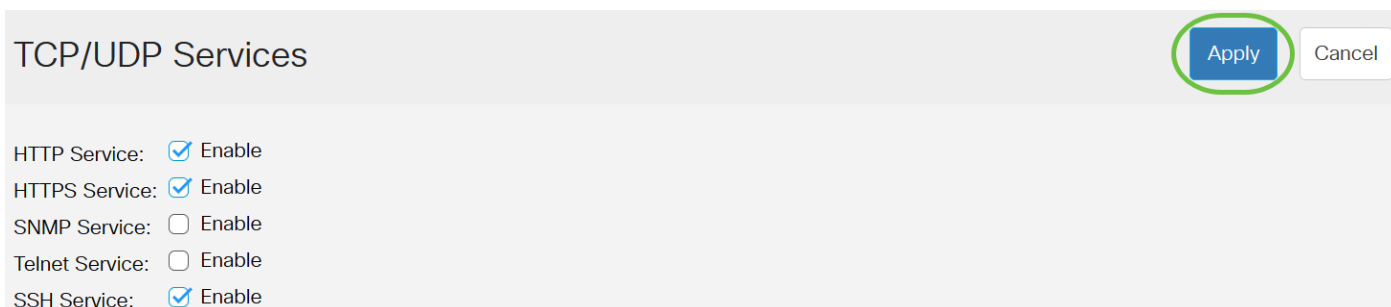
ステップ1: Webベースのユーティリティにログインし、[Security] > [TCP/UDP Services]を選択します



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。

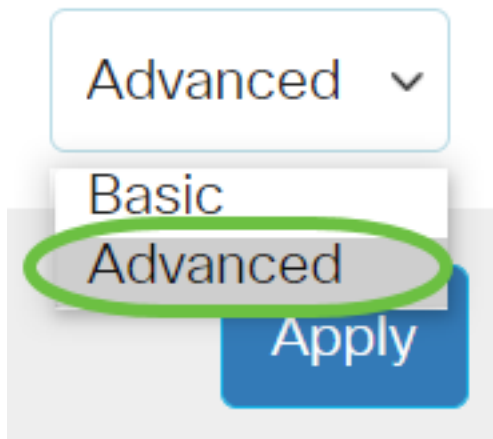


SSHユーザ認証設定の設定

このページを使用して、SSHユーザ認証方式を選択します。パスワード方式を選択すると、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、Leonard Adleman(RSA)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と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1つまたは両方を削除すると、再生成されます。

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：メニューから[Security] > [SSH Client] > [SSH User 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

▼ SSH Client

SSH User
Authentication

3

ステップ3:[Global Configuration]で、目的の[SSH User Authentication Method]をクリックします。

Global Configuration

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

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時、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。

- [パスワード別(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、デフォルトパスワードはanonymousです。このオプションを選択した場合は、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。
- [RSA公開キー別(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キーのタイプです。
- DSA公開キー : このオプションでは、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ユーザ認証には一般的に使用されません。

この例では、[By Password]が選択されています。

ステップ4:[Credentials]領域で、[Username]フィールドにユーザ名を入力します。

Credentials

✳ Username: (12/70 characters used)

✳ Password: Encrypted

Plaintext (Default Password: anonymous)

この例では、ciscobuser1が使用されています。

ステップ5: (オプション) ステップ2で「パスワード別」を選択した場合は、メソッドをクリックし、「暗号化」または「プレーンテキスト」フィールドにパスワードを入力してください。

Credentials

✳ Username: (12/70 characters used)

✳ Password: Encrypted

Plaintext (Default Password: anonymous)

次のオプションがあります。

- [暗号化(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す。

この例では、プレーンテキストを選択し、プレーンテキストのパスワードを入力します。

ステップ6:[Apply]をクリックして認証設定を保存します。

SSH User Authentication

Apply

Cancel

By RSA Public Key

By DSA Public Key

Credentials

Username:

ciscosbuser1

(12/70 ch

Password:

Encrypted

AUy3Nne84DHjTuVuzd1Ays

Plaintext

C1\$C0SBSwi+ch

ステップ7: (オプション) デフォルトのユーザー名とパスワードを復元するには、「デフォルトのクレデンシャルを復元する」をクリックし、「OK」をクリックして続行します。

SSH User Authentication

Apply

Cancel

Restore Default Credentials

Global Configuration

Confirm Restore Default Credentials

X



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

OK

Cancel

ユーザ名とパスワードがデフォルト値に戻ります。匿名/匿名

ステップ8: (オプション) ページの機密データをプレーンテキスト形式で表示するには、「機密データをプレーンテキストとして表示」をクリックし、「OK」をクリックして続行します。

Confirm Display Method Change



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

OK

Cancel

SSHユーザキーテーブルの設定

ステップ9：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

Generate



Details



Key Type

Key Source

Fingerprint



RSA

Auto Generated

MD5:c0:b4:8a:25:26:52:56:8f:4e:f5:a4:fa:a7:cc:0a:b2



DSA

Auto Generated

MD5:03:c8:0b:9b:a2:88:86:f8:49:0d:d2:51:81:f3:cd:c6

この例では、RSAが選択されています。

ステップ10: (オプション) 新しいキーを生成するには、[生成]をクリックします。新しいキーが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。

SSH User Key Table

Generate



Details



Key Type

Key Source

Fingerprint



RSA

Auto Generated

MD5:c0:b4:8a:25:26:52:56:8f:4e:f5:a4:fa:a7:cc:0a:b2



DSA

Auto Generated

MD5:03:c8:0b:9b:a2:88:86:f8:49:0d:d2:51:81:f3:cd:c6

Confirm Key Generation

X



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

OK

Cancel

ステップ11: (オプション) 現在のキーを編集するには、[編集]をクリックします。

SSH User Key Table

Generate



Details

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	Auto Generated	MD5:c0:b4:8a:25:26:52:56:8f:4e:f5:a4:fa:a7:cc:0a:b2
<input type="checkbox"/>	DSA	Auto Generated	MD5:03:c8:0b:9b:a2:88:86:f8:49:0d:d2:51:81:f3:cd:c6

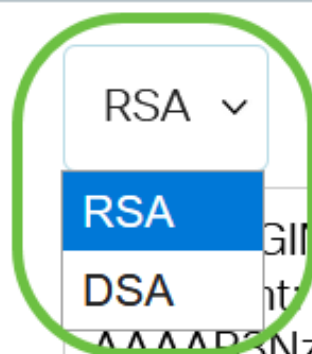
ステップ12: (オプション) [Key Type]ドロップダウンリストからキータイプを選択します。

Edit SSH Client Authentication Settings

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

Key Type:

Public Key:



この例では、RSAが選択されています。

ステップ13: (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。

Edit SSH Client Authentication Settings

X

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  
AAAAB3NzaC1yc2EAAAADAQABAAQCy9BJ+eTyaNva9u8G8VZgLqYuM8NHNoVh9WtPdKmBp004VvhTXfPqGCzg4/IIflpm  
hf4lmgpX+XB7aLCi3Ch0vsuLJEahjrCS5iRCvEPrh9oUoec/GBCFhe7zXYHPrXkoGBC4I0SXBVS5xKpxuSwLIDsxgY10  
/9lpXWKK8uN2r7P2PVJI1APr2RnjlUe1LVZTfrpMSqZ6UB+QtNtvaed46vTowjgCb4+y+zFYpQjlvZCAuMoaWkljQFslXMBOLL  
/D/cydxLa887DJQaMjPnu4G0PuQALWtT88h5hsHpZEhmcptoC00B+Auby0mXG6leE5bKFDpb2UFLJzHodD0fC9b  
----- END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted

Plaintext

Apply

Close

Display Sensitive Data as Plaintext

ステップ14: (オプション) [秘密キー]フィールドに新しい秘密キーを入力します。

秘密キーを編集したり、[暗号化]をクリックして現在の秘密キーを暗号化テキストとして表示したり、[プレーンテキスト]をクリックして現在の秘密キーをプレーンテキストで表示したりできます。

。

ステップ15: (オプション) ページの暗号化データをプレーンテキスト形式で表示するには、[機密データをプレーンテキストとして表示する]をクリックし、[OK]をクリックして続行します。

Edit SSH Client Authentication Settings

X

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  
AAAAB3NzaC1yc2EAAAADAQABAAQCy9BJ+eTyaNva9u8G8VZgLqYuM8NHNoVh9WtPdKmBp004VvhTXfPqGCzg4/IIflpm  
hf4lmgpX+XB7aLCi3Ch0vsuLJEahjrCS5iRCvEPrh9oUoec/GBCFhe7zXYHPrXkoGBC4I0SXBVS5xKpxuSwLIDsxgY10  
/9lpXWKK8uN2r7P2PVJI1APr2RnjlUe1LVZTfrpMSqZ6UB+QtNtvaed46vTowjgCb4+y+zFYpQjlvZCAuMoaWkljQFslXMBOLL  
/D/cydxLa887DJQaMjPnu4G0PuQALWtT88h5hsHpZEhmcptoC00B+Auby0mXG6leE5bKFDpb2UFLJzHodD0fC9b  
----- END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted

Plaintext

Apply

Close

Display Sensitive Data as Plaintext

Confirm Display Method Change

X



Sensitive data for the current page will be displayed as plaintext. Do you want to continue?

Don't show me this again

OK

Cancel

ステップ16:[Apply]をクリックして変更を保存し、[Close]をクリックします。

Edit SSH Client Authentication Settings

X

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

Key Type:

RSA

Public Key:

```
----- BEGIN SSH2 PUBLIC KEY -----  
Comment: RSA Public Key  
AAAAB3NzaC1yc2EAAAADAQABAAQBAQC9BJ+eTyaNva9u8G8VZgLqYuM8NHNoVh9WtPdKmbP004VvhTXfPqGCzg4/IIFlpm  
hf4ImgpX+XB7aLCI3Ch0vsuLJEahjrCS5iRCvEPrh9oUoec/GBCFhe7zXYHpRXkoGBC4I0SXBVS5xKpxuSwLIDsxgY10  
/9lpXWKK8uN2r7P2PVJI1APr2RnjUe1LVZTfrpMSqZ6UB+QtNtvaed46vTOWjgCb4+y+zFYpQjlvZCAuMoaWkljQFsiXMBOLL  
/D/cydxLa887DJQaMjPnu4G0PuQALWtT88h5hsHpZEhmcptoC00B+Auby0mXG6leE5bKFDpb2UFLJzHodD0fC9b  
----- END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted

Plaintext

Apply

Close

Display Sensitive Data as Plaintext

ステップ17: (オプション) チェックしたキーを削除するには、[削除]をクリックします。

SSH User Key Table

Generate



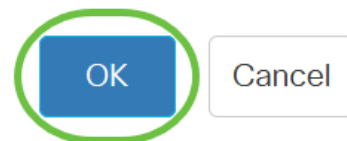
Details

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	MD5:02:26:b2:5c:56:51:b6:cf:db:fa:f7:b5:1a:26:7e:33
<input type="checkbox"/>	DSA	Auto Generated	MD5:03:c8:0b:9b:a2:88:86:f8:49:0d:d2:51:81:f3:cd:c6

ステップ18: (オプション) 次に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。

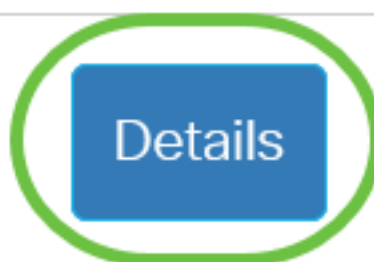


The selected user defined key will be deleted and replaced by an auto generated key. Do you want to continue?



ステップ19: (オプション) [Details]をクリックし、チェックしたキーの詳細を確認します。

SSH User Key Table



Key Type

Key Source

Fingerprint

SSH User Key Details

Back

SSH Server Key Type: RSA
Public Key: ----- BEGIN SSH2 PUBLIC KEY -----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAADAQABAAQ=CxBoUggILUWLBwkarVUG9jbM4OQUDsPdr
VmHGNkIRJVg3nxO2wmw10xckYy7YZLPaoriNd/obTuGZ4jOqhSgfQckqhibcSNdlaUrw:
w1v4QBwH8UbGNw1yV/SaECMuFre/VzYdRP
/RvGDNCNOphqMMJyCQ3D+WG2136l+li+U3Kn9BOBoOsSn+gz7c1OvNoXQ9t+NvtJDF
3MfMhmvwx0XIEKgMZgV+ennjipMPja0FP8HGblh
/hOPdhUIPmaRheE3hsDS1S9TJXLu7RnG0TrknL+QUFqZeRT3jSablwZsaGyE8oklpP5E
K9qsLJZlqeMm2gWjziB
----- END SSH2 PUBLIC KEY -----
Private Key (Encrypted): ----- BEGIN SSH2 ENCRYPTED PRIVATE KEY -----
Comment: RSA Private Key
AkNK2himPem2VeoSwyp0U+1FXk81mva9RGX2rBMhCDlj/79rYDLBnYKdSHk3A7Hqg0
aDjeLKVROxyRccQ0UivFp70SYz6mmjfrvwAXgCnZoNkhv8WO+Ktz0tLliHAj2gWaXerYB
D5suzX+RQnlR0Δ0z1I05G663mEMVcOT

ステップ20: (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。



CBS350-8P-E-2G - swi...



SSH User Authentication

Apply

Cancel

Res

これで、Cisco Business 350シリーズスイッチのクライアントユーザ認証設定が完了しました。