

# 在思科商務350系列交換器上設定安全殼層 (SSH)使用者驗證設定

## 目標

本文提供有關如何在思科商務350系列交換器上設定使用者端使用者驗證的說明。

## 簡介

安全殼層(SSH)是一種通訊協定，可為特定網路裝置提供安全的遠端連線。此連線提供的功能與Telnet連線類似，只是經過加密。SSH允許管理員通過命令列介面(CLI)使用第三方程式配置交換機。

在通過SSH的CLI模式下，管理員可以在安全連線中執行更高級的配置。在網路管理員實際不在網路站點的情況下，SSH連線對於遠端排除網路故障非常有用。交換機讓管理員驗證和管理使用者通過SSH連線到網路。身份驗證通過使用者可用於建立到特定網路的SSH連線的公鑰進行。

SSH客戶端功能是通過SSH協定運行的應用程式，用於提供裝置身份驗證和加密。它使裝置能夠與運行SSH伺服器的另一裝置建立安全加密連線。通過身份驗證和加密，SSH客戶端允許通過不安全的Telnet連線進行安全通訊。

## 適用裝置 | 軟體版本

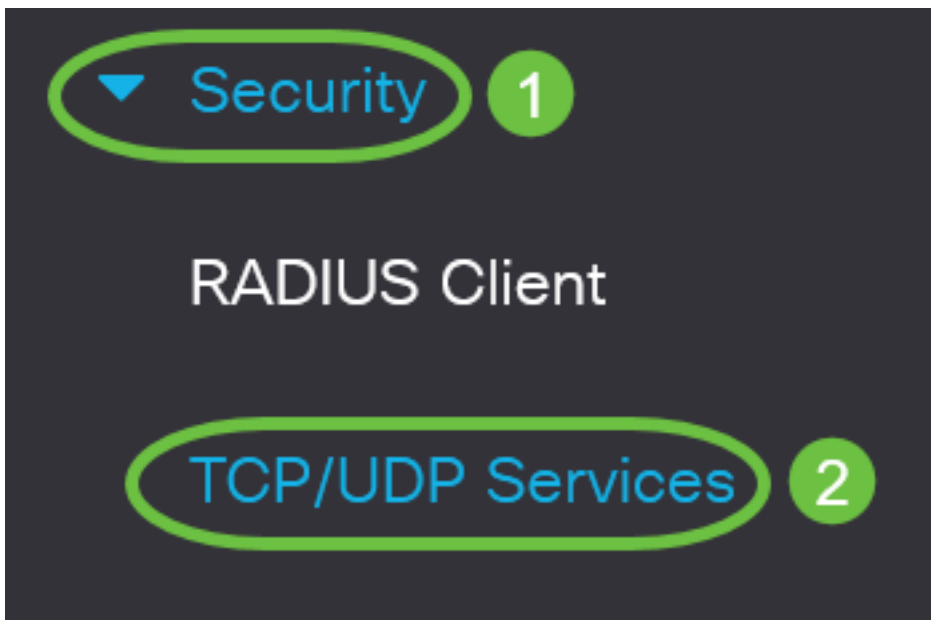
- CBS350([產品手冊](#)) | 3.0.0.69(下載[最新版本](#))
- CBS350-2X([產品手冊](#)) | 3.0.0.69(下載[最新版本](#))
- CBS350-4X([產品手冊](#)) | 3.0.0.69(下載[最新版本](#))

## 配置SSH客戶端使用者身份驗證設定

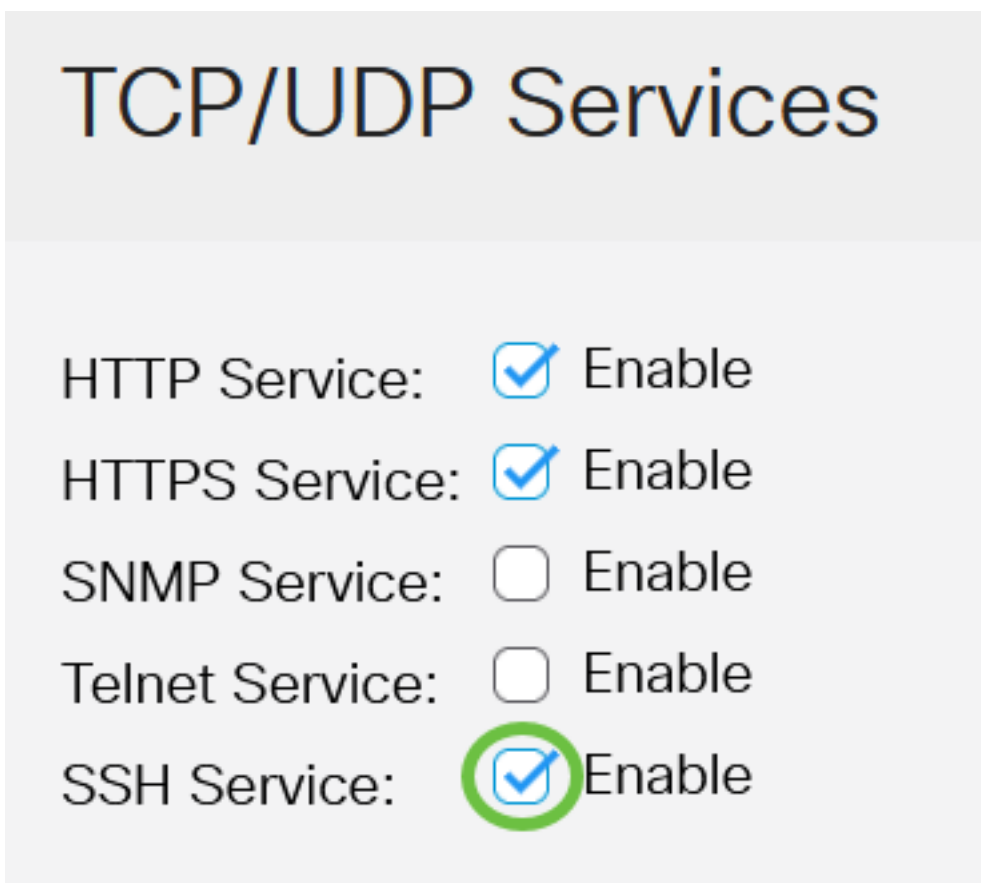
### 啟用SSH服務

為了支援開箱即用裝置（出廠預設配置的裝置）的自動配置，預設情況下禁用SSH伺服器身份驗證。

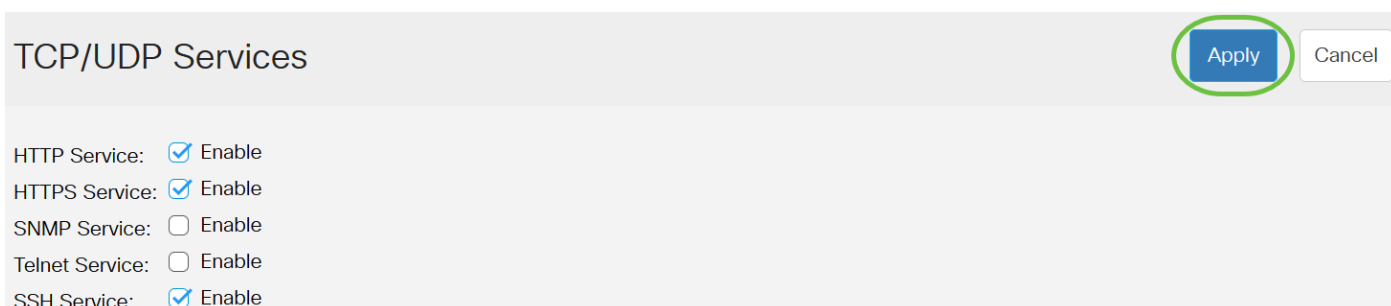
步驟1. 登入到基於Web的實用程式，然後選擇Security > TCP/UDP Services



步驟2.選中SSH Service 覆取方塊以啟用通過SSH訪問交換機命令提示符。



步驟3.按一下Apply 啟用SSH服務。

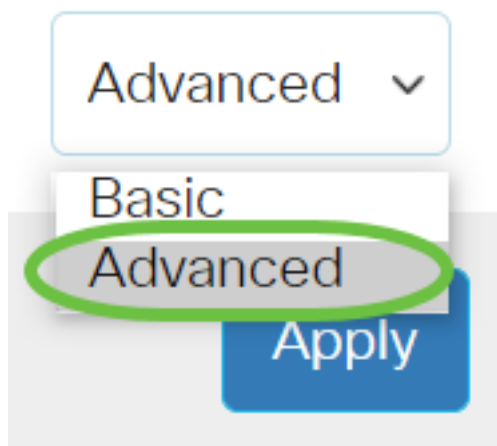


配置SSH使用者身份驗證設定

使用此頁可以選擇SSH使用者身份驗證方法。如果選擇密碼方法，則可以在裝置上設定使用者名稱和密碼。如果選擇了公鑰或私鑰方法，您還可以生成Ron Rivest、Adi Shamir和Leonard Adleman(RSA)或數位簽章演算法(DSA)金鑰。

引導裝置時，會為該裝置生成RSA和DSA預設金鑰對。其中一個金鑰用於加密從SSH伺服器下載的資料。預設情況下使用RSA金鑰。如果使用者刪除其中一個或兩個金鑰，則重新生成它們。

步驟1.登入到交換機的基於Web的實用程式，然後在「顯示模式」下拉選單中選擇「高級」。



步驟2.從選單中選擇Security > SSH Client > SSH User Authentication。

▼ Security

1

TACACS+ Client

RADIUS Client

▶ RADIUS Server

Password Strength

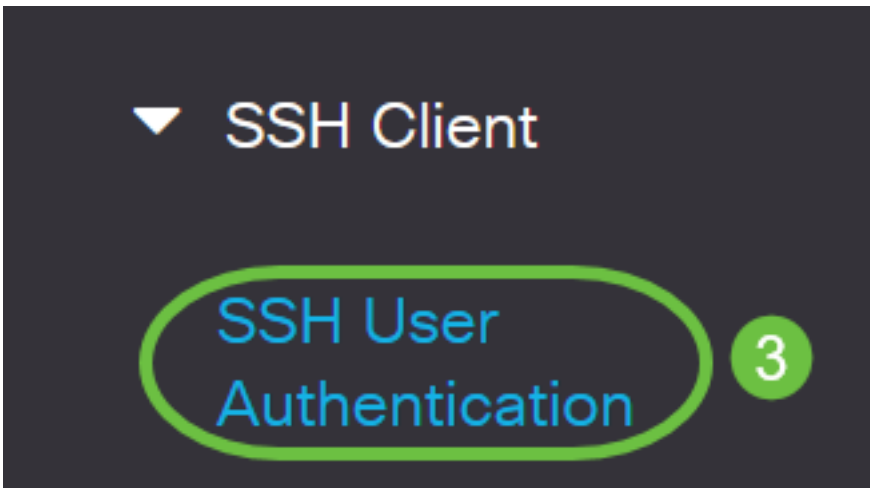
▶ Mgmt Access Method

Management Access  
Authentication

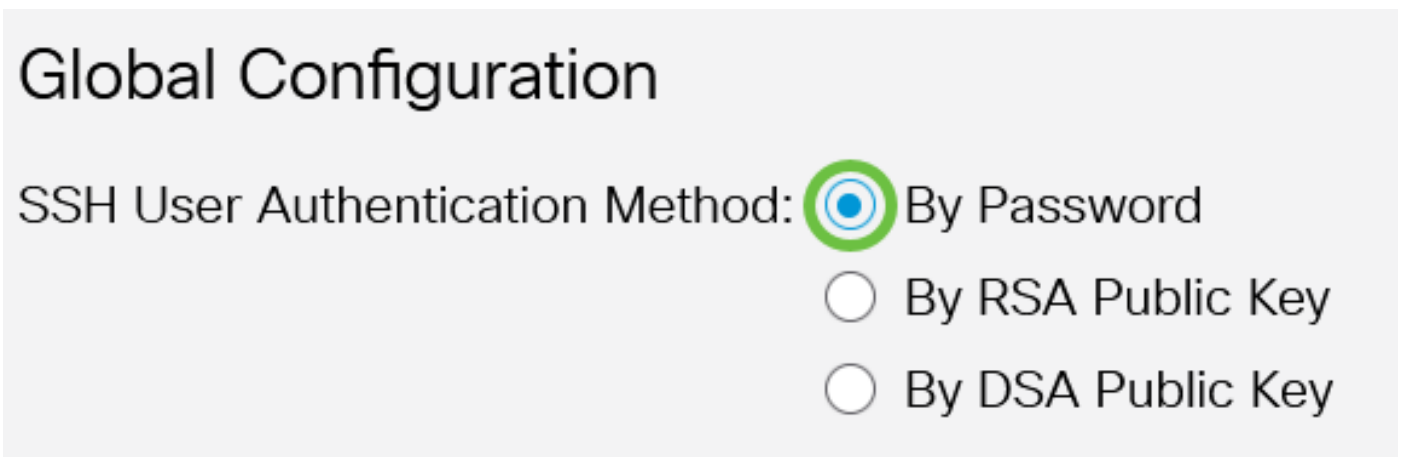
▶ Secure Sensitive Data  
Management

▶ SSL Server

▶ SSH Server



步驟3.在Global Configuration下，按一下所需的SSH使用者身份驗證方法。



當裝置 (SSH客戶端) 嘗試建立到SSH伺服器的SSH會話時，SSH伺服器使用以下方法之一進行客戶端身份驗證：

- By Password — 此選項可讓您配置用於使用者身份驗證的密碼。這是預設設定，預設密碼為匿名。如果選擇此選項，請確保已在SSH伺服器上建立使用者名稱和密碼憑據。
- By RSA Public Key — 此選項可讓您使用RSA公鑰進行使用者身份驗證。RSA金鑰是基於大整數分解的加密金鑰。此金鑰是用於SSH使用者身份驗證的最常見金鑰型別。
- By DSA Public Key — 此選項可讓您使用DSA公鑰進行使用者身份驗證。DSA金鑰是基於ElGamal離散演算法的加密金鑰。此金鑰不常用於SSH使用者身份驗證，因為身份驗證過程需要較長時間。

在本示例中，選擇了By Password。

步驟4.在Credentials區域中，在Username欄位中輸入使用者名稱。



在本例中，使用了ciscosuser1。

步驟5. (可選) 如果您在步驟2中選擇了按密碼，請按一下該方法，然後在 *Encrypted* 或 *Plaintext* 欄位中輸入密碼。

Credentials

Username:  (12/70 characters used)

Password:  Encrypted   Plaintext  (Default Password: anonymous)

選項包括：

- Encrypted — 此選項可讓您輸入密碼的加密版本。
- 明文 — 此選項可讓您輸入明文密碼。

在此示例中，選擇純文字檔案並輸入純文字檔案密碼。

步驟6. 按一下 **Apply** 以儲存驗證組態。

SSH User Authentication

By RSA Public Key  
 By DSA Public Key

Credentials

Username:  (12/70 ch)

Password:  Encrypted   Plaintext

**Apply** Cancel

步驟7. (可選) 按一下 **Restore Default Credentials** 以恢復預設的使用者名稱和密碼，然後按一下 **OK** 繼續。

SSH User Authentication

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

使用者名稱和密碼將恢復為預設值：匿名/匿名。

步驟8. (可選) 按一下**將敏感資料顯示為純文字檔案**以純文字檔案格式顯示頁面的敏感資料，然後按一下**OK**繼續。

SSH User Authentication

Apply

Cancel

Restore Default Credentials

Display Sensitive Data as Plaintext

Global Configuration

# Confirm Display Method Change

X



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

OK

Cancel

## 配置SSH使用者金鑰表

步驟9. 選中您要管理的金鑰的覈取方塊。

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

在本示例中，選擇了RSA。

步驟10. (可選) 按一下**Generate**以生成新金鑰。新金鑰將覆蓋選中的金鑰，然後按一下**OK**繼續。

## SSH User Key Table

<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

## Confirm Key Generation

X







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

步驟11. ( 可選 ) 按一下 **Edit** 以編輯當前鍵。

## SSH User Key Table

<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

步驟12. ( 可選 ) 從 Key Type 下拉選單中選擇金鑰型別。



# Edit SSH Client Authentication Settings

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

Key Type:

Public Key:



在本示例中，選擇了RSA。

步驟13。（可選）在*Public Key*欄位中輸入新的公鑰。

## 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  
AAAAB3NzaC1yc2EAAAADAQABAAQCy9BJ+eTyaNva9u8G8VZgLqYuM8NHNoVh9WtPdKmBp004VvhTXfPqGCzg4/llFlpm  
hf4lmgpX+XB7aLCI3Ch0vsuLJEahjrCS5iRCvEPrh9oUoec/GBCFhe7zXYHprXkoGBC4I0SXbVS5xKpxuSwLIDsxgY10  
/9lpXWKK8uN2r7P2PVJI1APr2RnjUe1LVZTfrpMSqZ6UB+QtNtvaed46vTOwjgCb4+y+zFYpQjlvZCAuMoaWkljQFslXMBOLL  
/D/cydxLa887DJQaMjPnu4G0PuQALWtT88h5hsHpZEhmcptoC00B+AuBy0mXG6leE5bKFDpb2UFLJzHodD0fC9b  
----- END SSH2 PUBLIC KEY -----
```

Private Key:  Encrypted

Plaintext

Apply

Close

Display Sensitive Data as Plaintext

步驟14。（可選）在*Private Key*（私鑰）欄位中輸入新的私鑰。

您可以編輯私鑰，並且可以按一下「已加密」將當前私鑰顯示為加密文本，或者按一下「純文字檔案」將當前私鑰顯示為純文字檔案。

步驟15。（可選）按一下**Display Sensitive Data as Plaintext**以純文字檔案格式顯示頁面的加密資料，然後按一下**OK**繼續。

## 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  
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

步驟16. 按一下**Apply**以儲存變更，然後按一下**Close**。

## 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  
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

步驟17。（可選）按一下**Delete**以刪除檢查的金鑰。

### 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

步驟18。（可選）出現如下所示的確認消息提示後，按一下**OK**刪除該金鑰。

## Delete User Generated Key

X



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

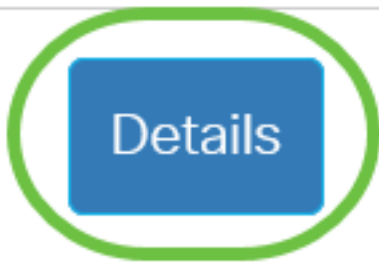
OK

Cancel

步驟19。（可選）按一下**Details**檢視選中金鑰的詳細資訊。

# SSH User Key Table

Generate



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=CxBoUggllUWLBwkarVUG9jbM4OQUdSPdr  
VmHGNkIRJVg3nxO2wmw10xcYy7YZLPaoriNd/obTuGZ4jOqhSgfQckqhibcSNdlaUrw  
w1v4QBwH8UbGNw1yV/SaECMuFre/VzYdRP  
/RvGDNCNOphqMMJyCQ3D+WG2136I+li+U3Kn9BObOsSn+gz7c1OvNoXQ9t+NvtJDF  
3MfMhmVwx0XIEKgMZgV+ennjipMPja0FP8HGblh  
/hOPdhUIPmaRheE3hsDS1S9TJXLu7RnG0TrknL+QUFqZeRT3jSablwZsaGyE8oklpP5E  
K9qsLJZlqeMm2gWjziB  
----- END SSH2 PUBLIC KEY -----  
Private Key (Encrypted): ----- BEGIN SSH2 ENCRYPTED PRIVATE KEY -----  
Comment: RSA Private Key  
AkNK2himPem2VeoSwyp0U+1FXk81mva9RGX2rBMhCDIj/79rYDLBnYKdSHk3A7Hqg0  
aDjeLKVROxyRccQ0UivFp70SYz6mmjfrvwAXgCnZonkhv8WO+Ktz0tLliHAj2gWaXerYB  
D5suizX+RQnlR0A0z1I05G663mEMVcOT

步驟20。(可選)按一下頁面頂部的**Save**按鈕，將更改儲存到啟動配置檔案中。



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



## SSH User Authentication

Apply

Cancel

Res

現在，您已在思科商務350系列交換器上設定使用者端使用者驗證設定。