

# 在交換機上配置安全外殼(SSH)使用者身份驗證設定

## 目標

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。身份驗證通過公共金鑰進行，使用者可以使用公共金鑰建立到特定網路的SSH連線。

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伺服器的其它裝置建立安全且加密的連線。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。

本文提供如何在受管交換機上配置客戶端使用者身份驗證的說明。

## 適用裝置

- Sx200系列
- Sx300系列
- Sx350系列
- SG350X系列
- Sx500系列
- Sx550X系列

## 軟體版本

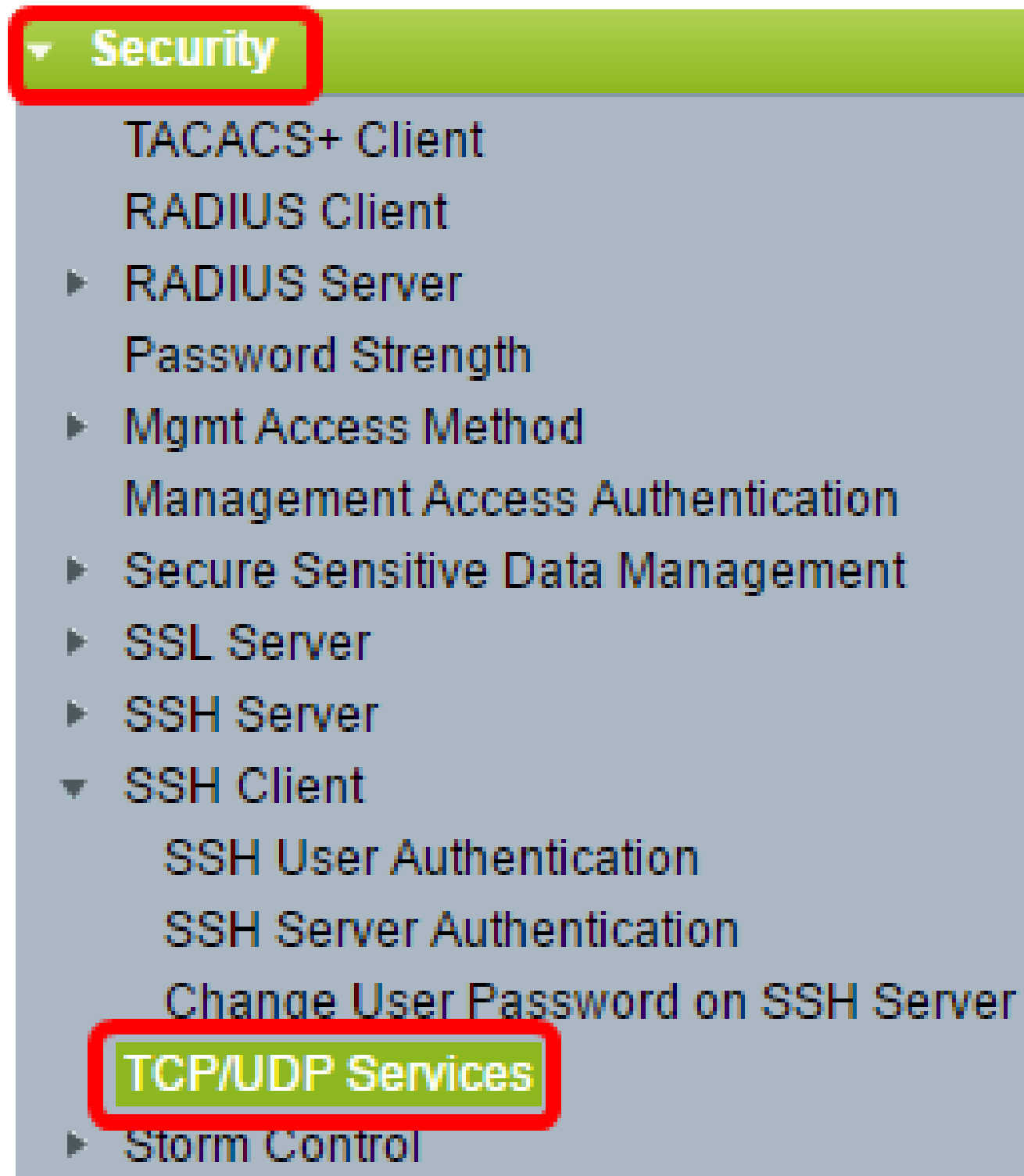
- 1.4.5.02 - Sx200系列、Sx300系列、Sx500系列
- 2.2.0.66 - Sx350系列、SG350X系列、Sx550X系列

## 配置SSH客戶端使用者身份驗證設定

## 啟用SSH服務

注意：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。

# TCP/UDP Services

HTTP Service:	<input checked="" type="checkbox"/>	Enable
HTTPS Service:	<input checked="" type="checkbox"/>	Enable
SNMP Service:	<input type="checkbox"/>	Enable
Telnet Service:	<input type="checkbox"/>	Enable
SSH Service:	<input checked="" type="checkbox"/>	Enable

**Apply** **Cancel**

步驟 3.按一下Apply以啟用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

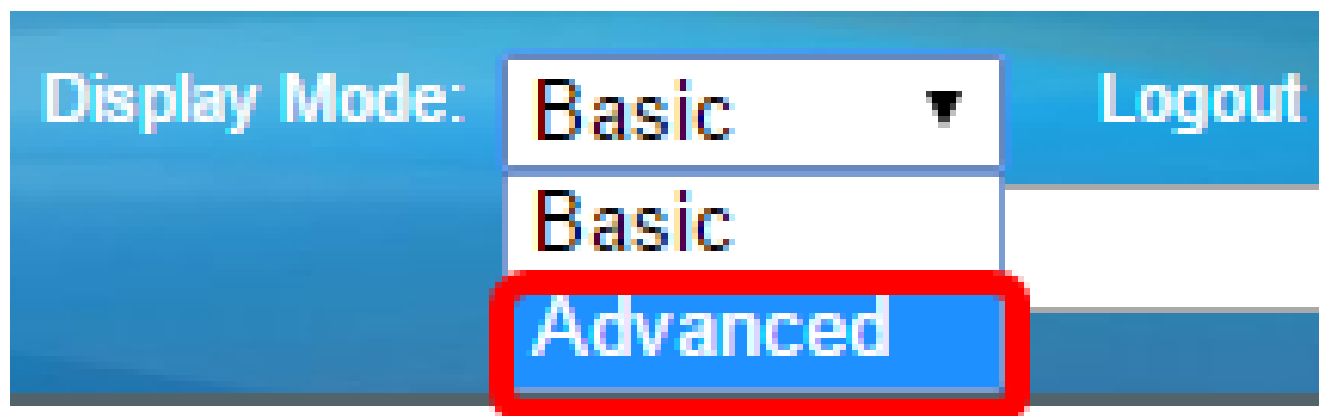
名稱和密碼。如果選擇了公鑰或私鑰方法，您還可以生成Ron Rivest、Adi Shamir和Leonard Adleman(RSA)或數位簽章演算法(DSA)金鑰。

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鍵，則重新生成這些鍵。

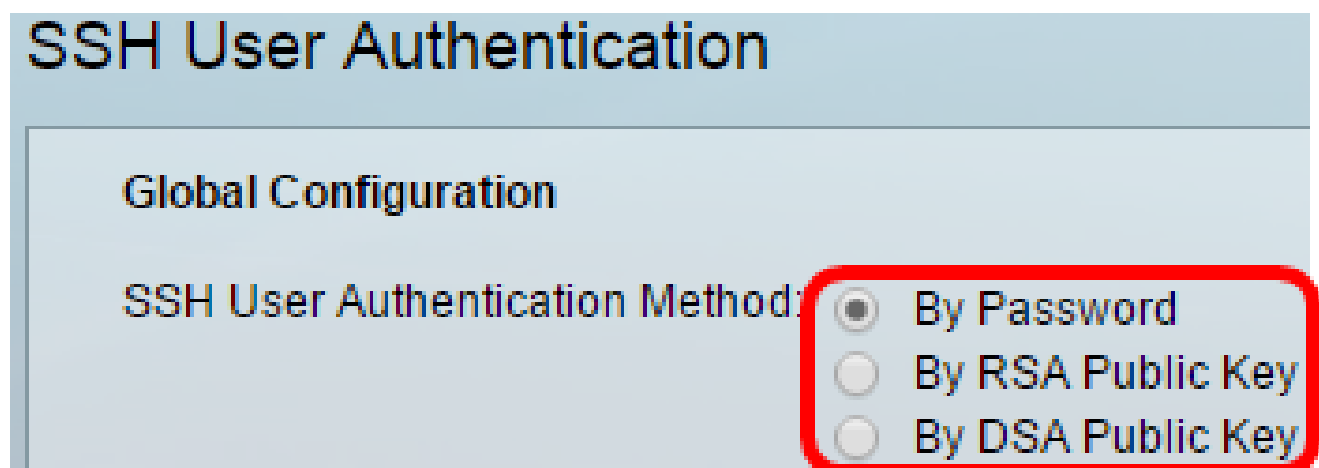
步驟 1. 登入到基於Web的實用程式，然後選擇Security > SSH Client > SSH User Authentication。



注意：如果您有Sx350、SG300X或Sx500X，請從Display Mode下拉選單中選擇Advanced，以切換到Advanced模式。



步驟 2.在Global Configuration下，按一下所需的SSH User Authentication Method。



注意：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：

- 按密碼 — 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。
- 通過DSA公鑰 — 此選項允許您使用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。

注意：在本示例中，選擇了「按密碼」。

步驟 3.在Credentials區域，在Username欄位中輸入使用者名稱。

Credentials

Username: ciscosbuser1 (0/70 characters used)

Password:  Encrypted AUy3Nne84DHjTuVuzd1A!  
 Plaintext (Default Password)

Apply Cancel Restore Default Credentials Display Sensitive Data as Plaintext

注意：在本示例中，使用了ciscosbuser1。

步驟4。（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。

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

選項包括：

- Encrypted — 此選項可讓您輸入密碼的加密版本。
- 明文 — 此選項可讓您輸入純文字檔案密碼。

注意：在本示例中，選擇純文字檔案並輸入純文字檔案密碼。

步驟 5.按一下「Apply」以儲存驗證設定。

步驟6。（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以繼續。

注意：使用者名稱和密碼將還原為預設值：anonymous/anonymous。



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

OK Cancel

步驟7. ( 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。



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



## 配置SSH使用者金鑰表

步驟 8.選中要管理的金鑰的覈取方塊。

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

注意：在本示例中，選擇了RSA。

步驟9. ( 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以繼續。



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



步驟10. ( 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	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

步驟11。(可選)從Key Type下拉選單中選擇金鑰型別。

Key Type:

Public Key:



注意：在本示例中，選擇了RSA。

步驟12。(可選)在Public Key欄位中輸入新的公鑰。



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  
AAAAB3NzaC1yc2EAAAADAQABAAQgQDAb0QFu6yktUlebpLhpETIs79pWy+k0F8g4x  
ovv+0T55Bq2pys5O7FwoxKTLIXFVW5CFdRw26QS2w0oLnH0TecsCI3qzhFuOEvBPhK  
skyEuy6x8fFsKwdLlId8iUVIbyXk4psIDQD2u0U7AHVRH4ITcXpinexS0MQ==  
--- END SSH2 PUBLIC KEY ---
```

Private Key:  Encrypted

Plaintext

步驟13。(可選)在Private Key (私鑰)欄位中輸入新的私鑰。

注意：您可以編輯私鑰，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14。(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。



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



步驟 15.按一下「Apply」以儲存變更，然後按一下「Close」。

步驟16。(可選) 按一下Delete以刪除檢查的金鑰。

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

步驟17。(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。



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



步驟18。(可選) 按一下Details檢視選中金鑰的詳細資訊。

## 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  
gBd08SbtMQWZdFy7hj6rSTCO0YPKpVhkylBwye44QdjCaCGojE/FIKuMHBz  
dkVPHkwi2ExfbENqD60yc7pFex+oaah/ugmYgjBmOnNbrViXCriHiUSAKUWz  
RUDaVM7V2u67+yw+/yNJ+XvRYkhsQZRON8cOi4ilHV1MImJoRGrdiuR/CjE  
X3zOhmB8o6iyCa32MPlhy08yfPN4YgrHh0cpxeWcY1ZRIG0vZ4lxUJ423xYL  
rdclnoll4EWSk+sj1vzrGidXHCRzQkkMqLp+E5zl9npJc0t6+64tKqAD3CVaHk  
VwR5JXrle2vHdik2af2AO3JZsobtTO0dMSA5zPdN4CCERPLAEaActCQOkE  
MqHATSyFcG+h0X2MitxV5XsWUaJe/dH/BNeljYrzKRF6y9V37PFBizSLAtE2  
62u0QPBRglLu6lL4j4jCtN54PauVkr48mw3JgsWszKXgHmSx/ok7Tu4gPcn  
UI37c0vNZwDadMZ/1ZKLEkBOJtJIJevDsWslvclKZAvoSmLu2B20hUM2uor1  
5GngylqcT5vYLMGpDL2k2PzUgFuLvbafzlr1c1czqy+jCbP/cl7TAOeGA7  
LtcY8DrAo8y5O15CcgUIZJddWLRqunDGpygscAaor050vG3/5A1C8YRMh2F  
86OuHWS+0HHqnJnmgrOICj/O/DiSeRnHkr8juT1sBuwpFDd+wT0L/KzRN1L  
4OwOYCjkdgm7GgOI2eOnY9YvyD/RyjCmM11JFA1RwPCSQWhyPrZgcCQS  
0FLgLKZNZ1XNjkdqDBmb6CfyvXeGP76EH+EQ==
```

---- END SSH2 PRIVATE KEY ----

Back


Display Sensitive Data as Plaintext

步驟19。(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。

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

現在，您應該在託管交換機上配置客戶端使用者身份驗證設定。

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。