

適用於SG350XG和SG550XG交換器的使用者端安全殼層(SSH)使用者驗證

目標

安全殼層(SSH)是一種提供到特定裝置的安全遠端連線的協定。350XG和550XG系列託管交換機可讓您通過身份驗證和管理使用者通過SSH連線到裝置。身份驗證通過公鑰進行，因此使用者可使用此金鑰建立到特定裝置的SSH連線。如果網路管理員不在網路站點，SSH連線對於遠端排除網路故障非常有用。

本文說明了如何在SG350XG和SG550XG系列託管交換機上配置客戶端使用者身份驗證。

適用裝置

- SG350XG
- SG550XG

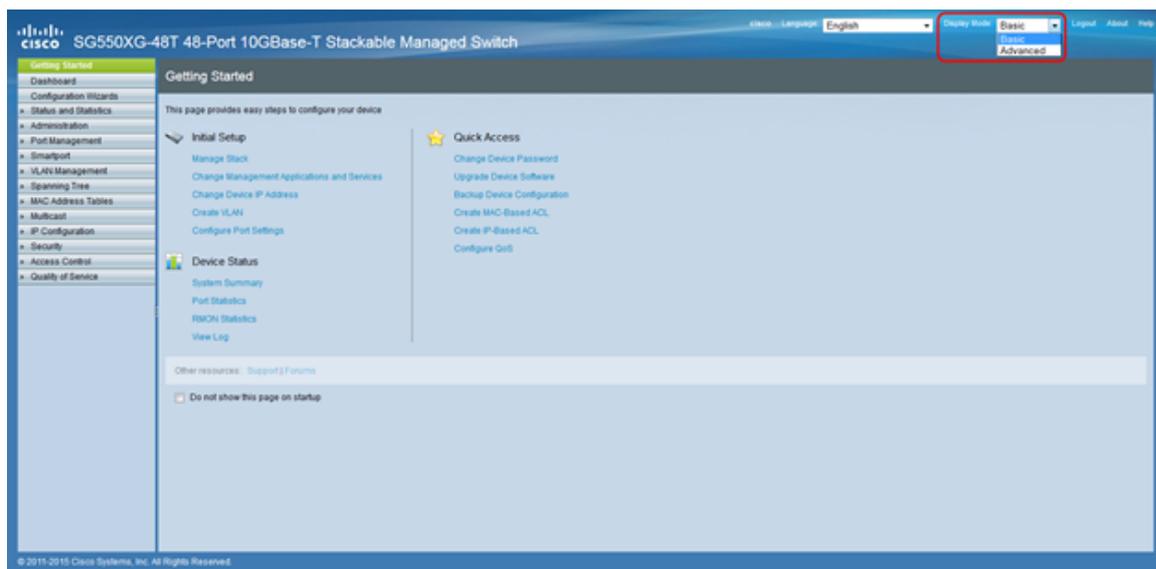
軟體版本

- v2.0.0.73

配置SSH 使用者端 驗證

全域組態

附註：以下螢幕截圖來自高級顯示。點選螢幕右上角的 *Display Mode* 下拉選單即可切換此模式



步驟1. 登入到Web配置實用程式並選擇 **Security > SSH Client > SSH User Authentication**。將開啟 *SSH User Authentication* 頁面：

SSH User Authentication

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: anonymous)

SSH User Key Table

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input type="checkbox"/>	RSA	Auto Generated	6f:bf:d8:12:60:74:ea:4c:68:a1:76:91:e5:8f:a4:d1
<input type="checkbox"/>	DSA	Auto Generated	24:31:b0:3c:5c:94:74:35:ba:d1:ce:c6:f7:16:84:48

步驟2. 在 *SSH User Authentication Method* 欄位中，按一下所需全域性身份驗證方法的單選按鈕。

SSH User Authentication

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: anonymous)

可用的選項如下：

- By Password — 此選項可讓您配置用於使用者身份驗證的密碼。輸入密碼或保留預設值「anonymous」。
- By RSA Public Key — 此選項允許您使用RSA公鑰進行使用者身份驗證。RSA用於加密和簽名。如果選擇此選項，請在SSH使用者金鑰表塊中建立RSA公鑰和私鑰。
- 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僅用於簽名。如果選擇此選項，請在SSH使用者金鑰表塊中建立DSA公鑰/私鑰。

步驟3. 找到 *Credentials* 區域。在「Username」欄位中，輸入使用者名稱。

SSH User Authentication

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: anonymous)

Apply Cancel Restore Default Credentials Display Sensitive Data as Plaintext

步驟4.如果在步驟2中選擇了By Password，請在Password欄位中按一下所需密碼方法的單選按鈕。預設密碼為「anonymous」。

SSH User Authentication

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: anonymous)

Apply Cancel Restore Default Credentials Display Sensitive Data as Plaintext

可用選項說明如下：

- 已加密 — 輸入加密的密碼。
- 明文 — 輸入口令作為純文字檔案。

步驟5.按一下Apply 以儲存驗證組態。

SSH User Authentication

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: anonymous)

Apply Cancel Restore Default Credentials Display Sensitive Data as Plaintext

步驟6。(可選)若要還原預設使用者名稱和密碼，請按一下Restore Default Credentials。預設密碼為「anonymous」。

SSH User Authentication

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: anonymous)

步驟7. (可選) 若要以純文字檔案或加密文本形式檢視敏感資料，請按一下 **Display Sensitive Data as Plaintext/Encrypted**。

SSH User Authentication

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: anonymous)

附註：該按鈕的名稱將根據當前設定而改變。該按鈕將始終切換資料的顯示。

SSH使用者金鑰表

本節介紹如何管理SSH使用者表。

步驟1. 導航到 **SSH使用者金鑰表**。在顯示的清單中，選中要管理的金鑰所左側的覈取方塊。

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a
<input type="checkbox"/>	DSA	User Defined	6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c

步驟2. (可選) 按一下 **Generate** 以生成新金鑰。新鍵會覆蓋選定的鍵。系統將顯示確認視窗。按一下「OK」以繼續。

<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a
<input type="checkbox"/>	DSA	User Defined	6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c

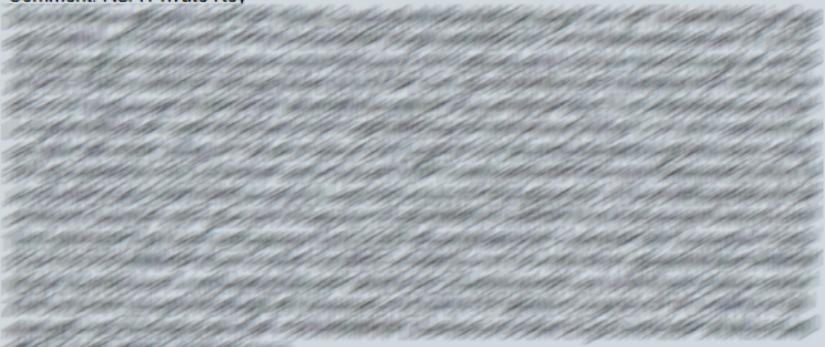
步驟3. (可選) 按一下 **Delete** 以刪除選定的項。系統將顯示確認視窗。按一下 **OK** 繼續。

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a
<input type="checkbox"/>	DSA	User Defined	6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c

步驟4. (可選) 按一下**Details**檢視選定金鑰的詳細資訊。

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a
<input type="checkbox"/>	DSA	User Defined	6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c

系統將顯示SSH User Key Details頁面。按一下**Back**返回SSH使用者金鑰表。

SSH User Key Details	
SSH Server Key Type:	RSA
Public Key:	<pre> ---- BEGIN SSH2 PUBLIC KEY ---- Comment: RSA Public Key AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxb XRqFXeMQ2LNyUTCK8hcu0zVSipsQ8AFRZmpnaVkEgSunFK5YYJ2AckP9NyMlikhWfRWm UXT6SBOK/BJk7GPXhcs0JE6II3uPCyiC50vzGRBGhWSH/oGBxMqkavDGpcToaDyKQ== ---- END SSH2 PUBLIC KEY ---- </pre>
Private Key (Encrypted):	<pre> ---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ---- Comment: RSA Private Key </pre>  <pre> ---- END SSH2 PRIVATE KEY ---- </pre>

步驟5. 按一下**Edit**以編輯選取的金鑰。

SSH User Key Table			
<input type="checkbox"/>	Key Type	Key Source	Fingerprint
<input checked="" type="checkbox"/>	RSA	User Defined	8e:06:e1:fe:ab:4d:1f:cf:14:5c:e3:11:cd:8f:1e:8a
<input type="checkbox"/>	DSA	User Defined	6a:b3:3e:9e:83:c3:3b:da:57:f7:29:89:15:a7:dc:0c

*Edit SSH Client Authentication Settings*視窗開啟：

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  
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF;  
-----END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted

Plaintext

步驟6.從Key Type下拉選單中選擇所需的金鑰型別。

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  
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF;  
-----END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted

Plaintext

可用的選項如下：

- RSA - RSA用於加密和簽名。
- DSA - DSA僅用於簽名。

步驟7.在公鑰欄位中，您可以編輯目前的公鑰。

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  
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF;  
-----END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted

Plaintext

步驟8.在 *Private Key* 欄位中，您可以編輯目前的私鑰。按一下

Encrypted 單選按鈕檢視當前私鑰是否加密。否則，按一下 **Plaintext** 單選按鈕可將當前私鑰視為純文字檔案。

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  
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF;  
-----END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted

Plaintext

步驟9.按一下 **Apply** 以儲存變更。

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  
AAAAB3NzaC1yc2EAAAADAQABAAQCAeTjr4/8xsROwDkFBY7efsV5v59RNAwzJdZsxbXRqF;  
-----END SSH2 PUBLIC KEY -----
```

Private Key: Encrypted

Plaintext