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

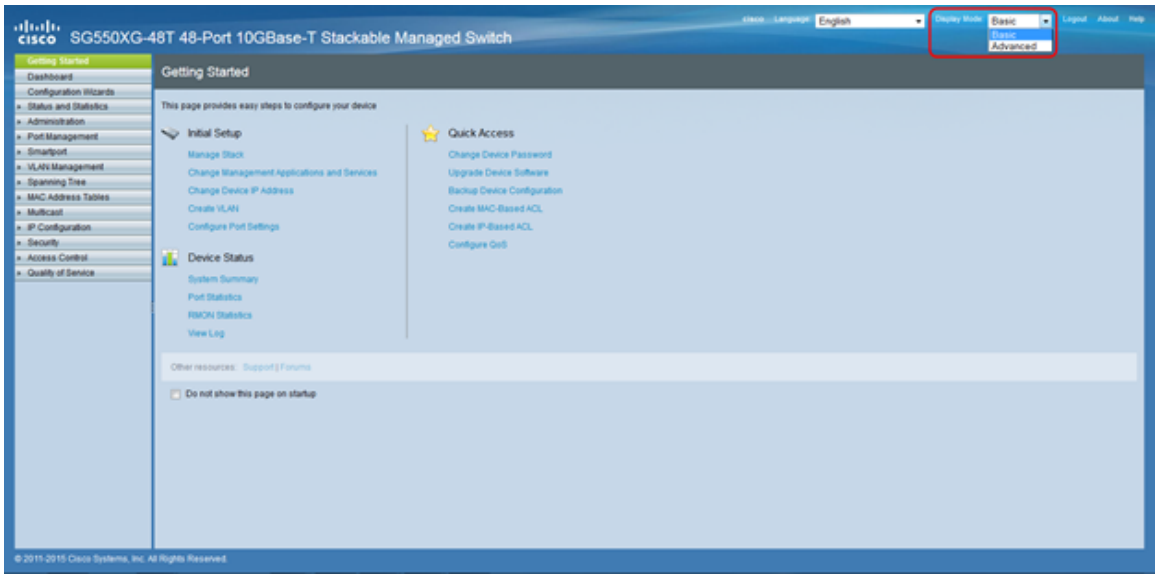
軟體版本

- v2.0.0.73

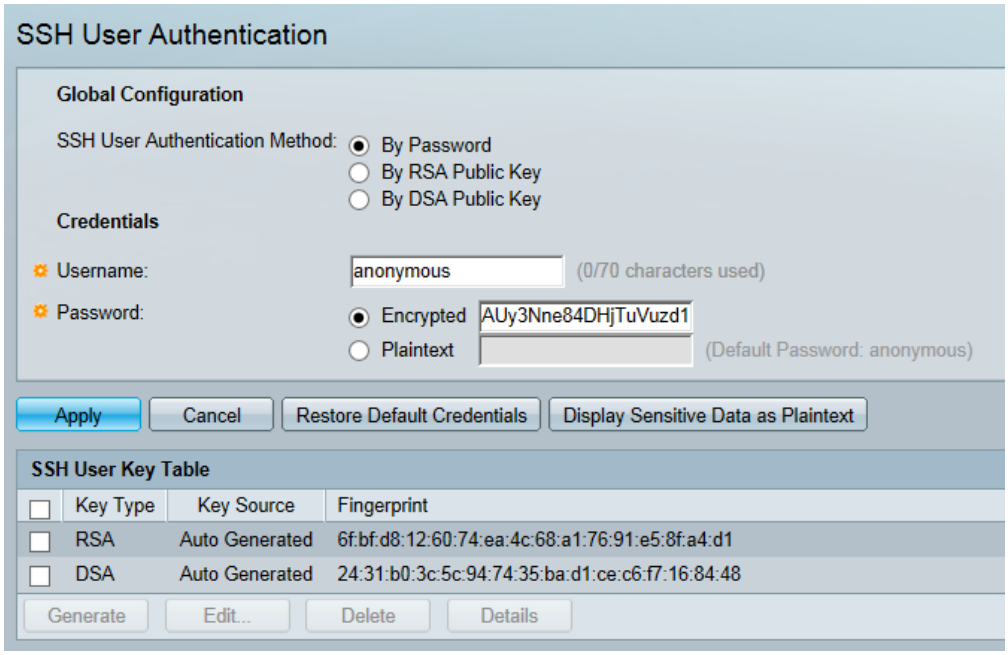
配置SSH 使用者端 驗證

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：



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。

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。

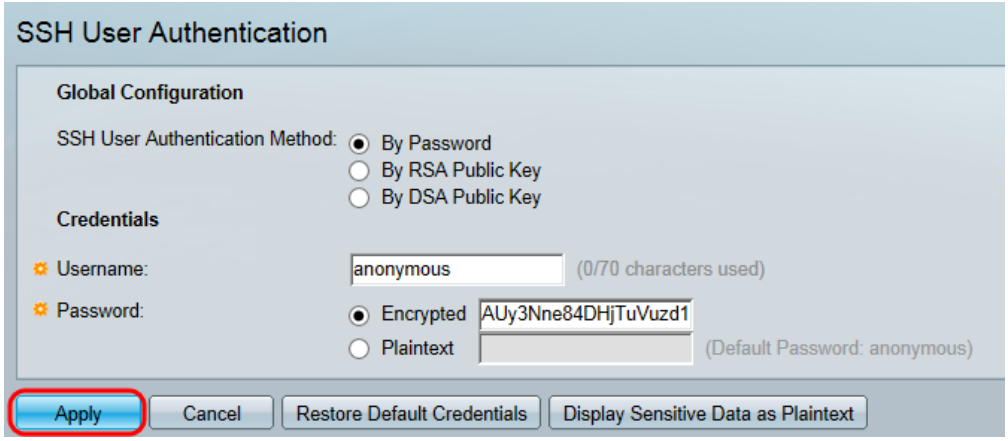
步驟3.找到*Credentials*區域。在「*Username*」欄位中，輸入使用者名稱。

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」。

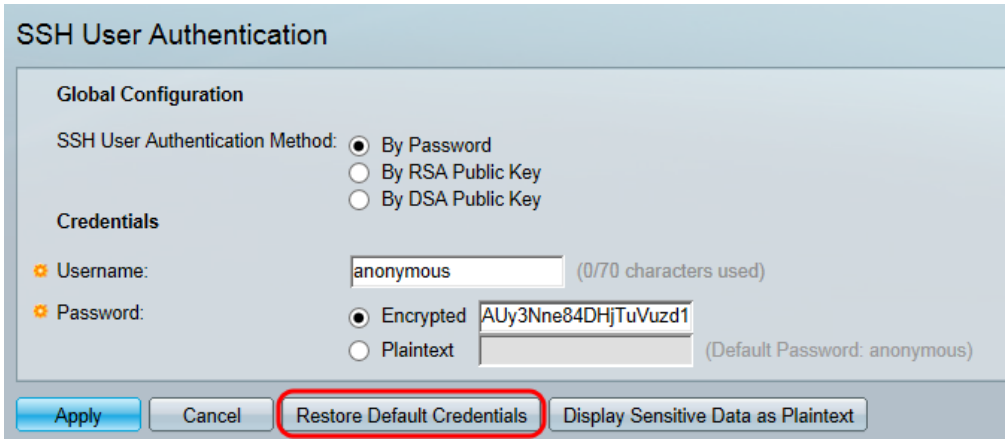
可用選項說明如下：

- 已加密 — 輸入加密的密碼。
- 明文 — 輸入口令作為純文字檔案。

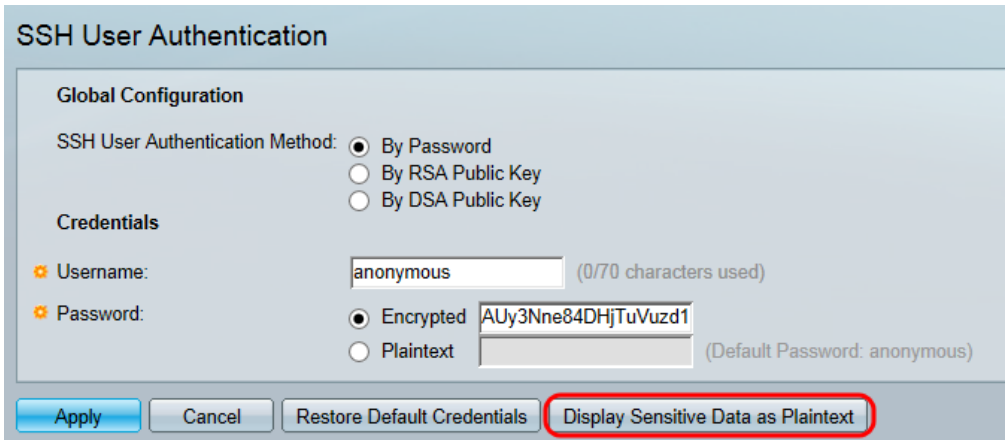
步驟5.按一下**Apply** 以儲存驗證組態。



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」。



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**。

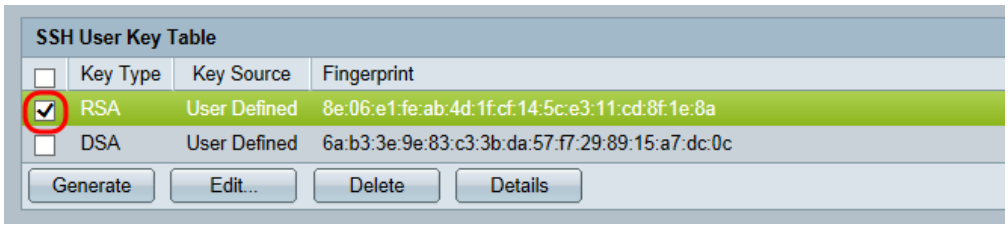


附註：該按鈕的名稱將根據當前設定而改變。該按鈕將始終切換資料的顯示。

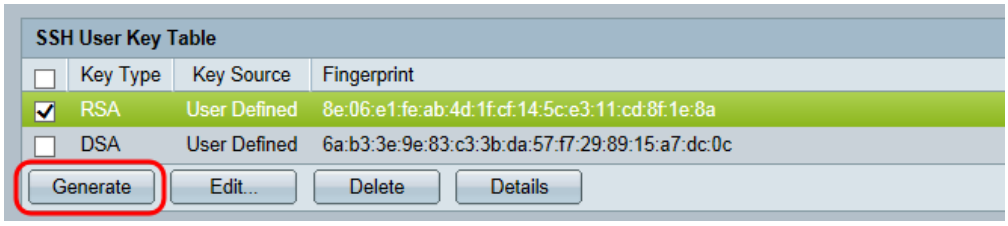
SSH使用者金鑰表

本節介紹如何管理SSH使用者表。

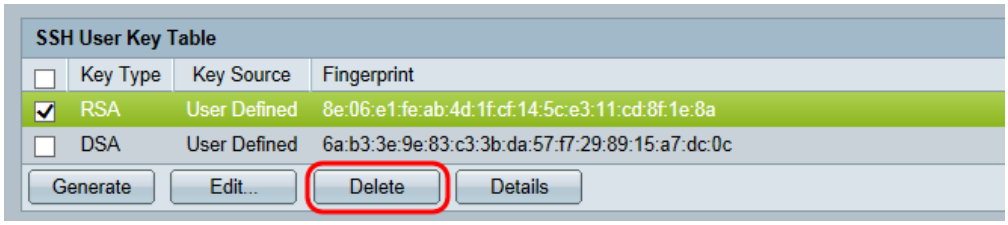
步驟1.導航到*SSH使用者金鑰表*。在顯示的清單中，選中要管理的金鑰所左側的覈取方塊。



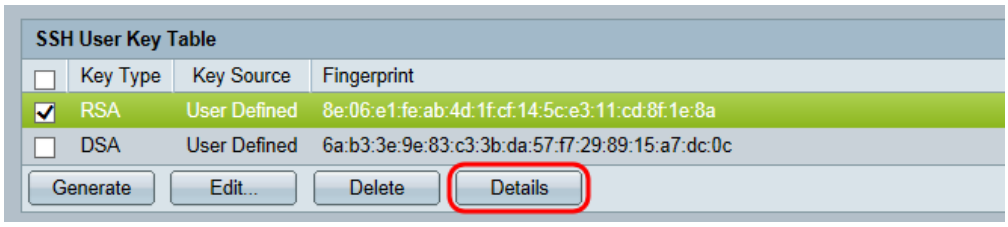
步驟2。（可選）按一下**Generate**以生成新金鑰。新鍵會覆蓋選定的鍵。系統將顯示確認視窗。按一下「**OK**」以繼續。



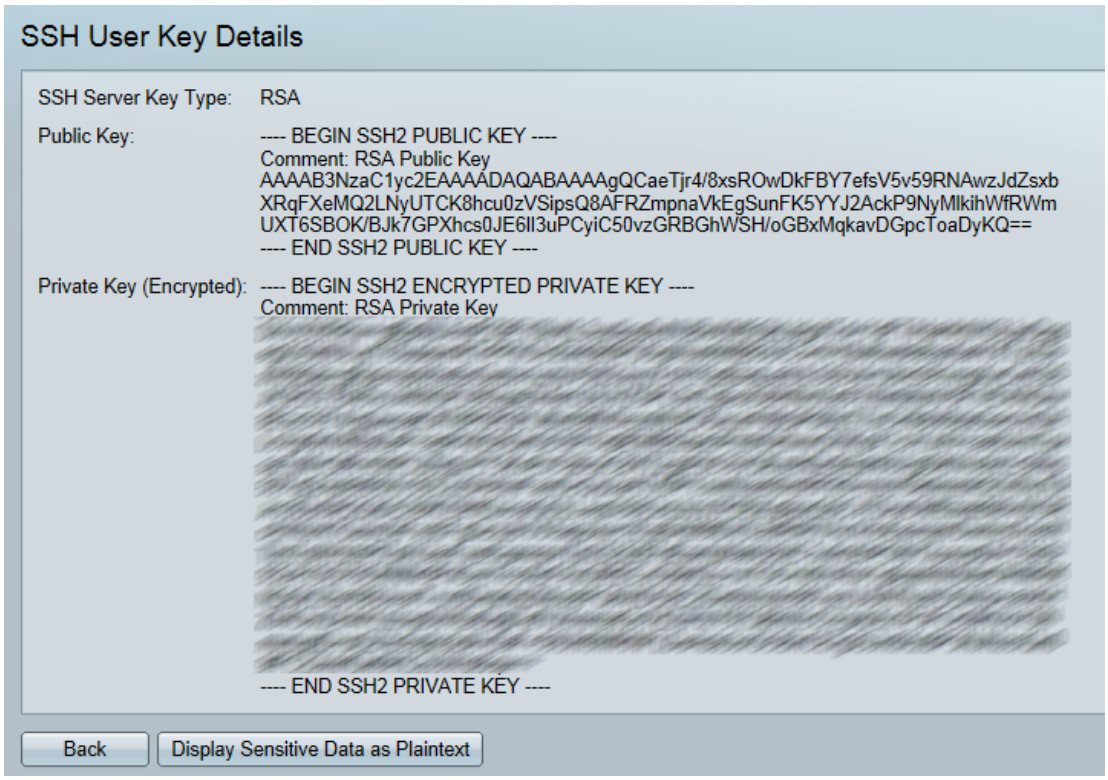
步驟3。（可選）按一下**Delete**以刪除選定的項。系統將顯示確認視窗。按一下**OK**繼續。



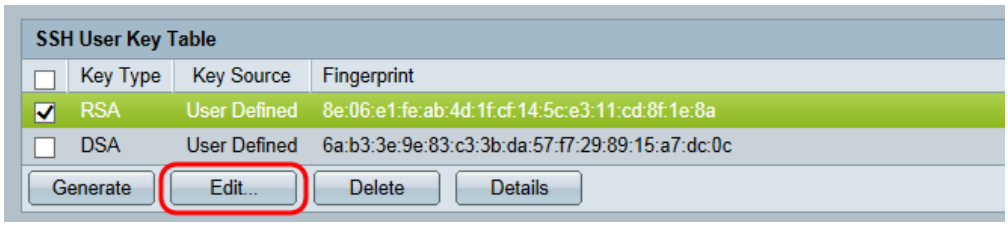
步驟4.（可選）按一下**Details**檢視選定金鑰的詳細資訊。



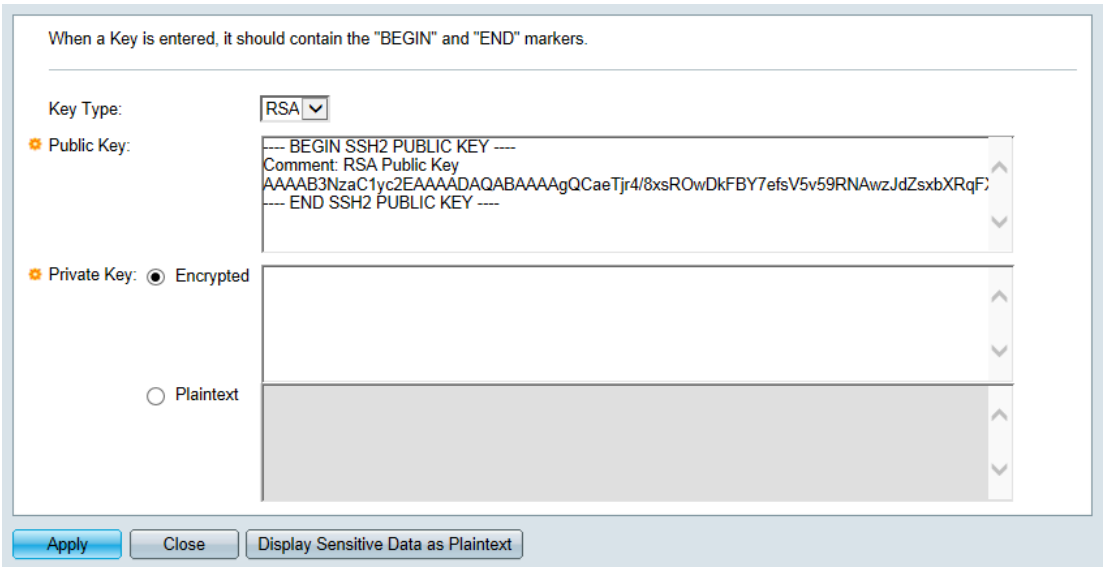
系統將顯示SSH User Key Details頁面。按一下**Back**返回SSH使用者金鑰表。



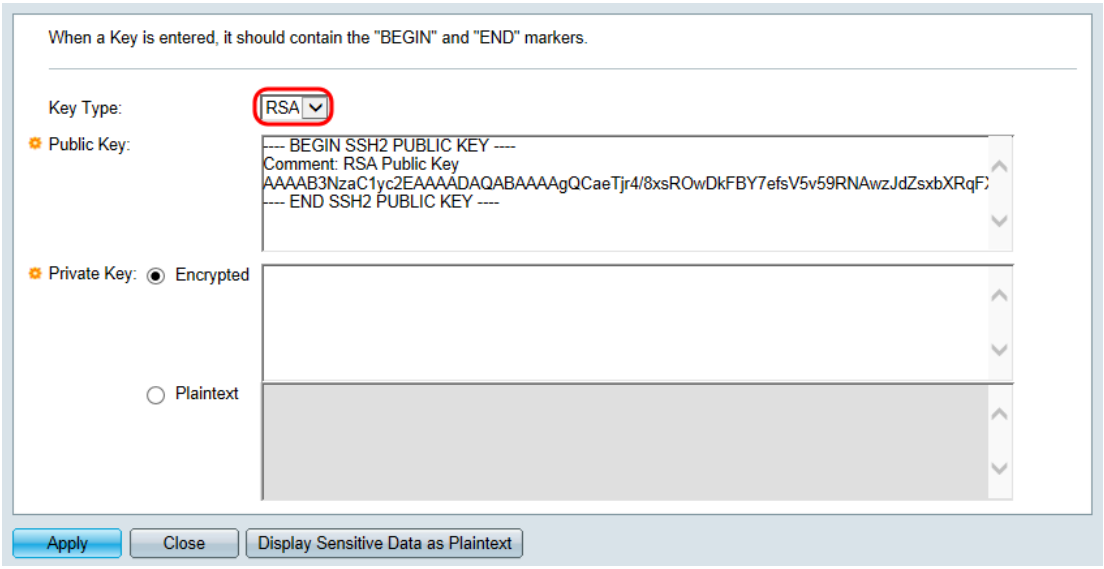
步驟5.按一下**Edit**以編輯選取的金鑰。



*Edit SSH Client Authentication Settings*視窗開啟：



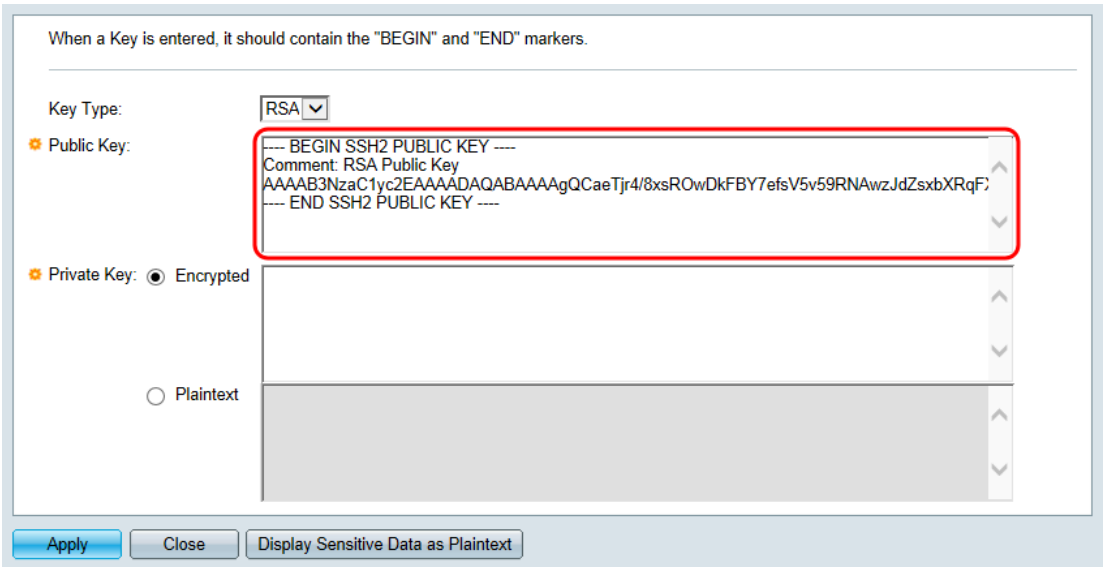
步驟6.從*Key Type*下拉選單中選擇所需的金鑰型別。



可用的選項如下：

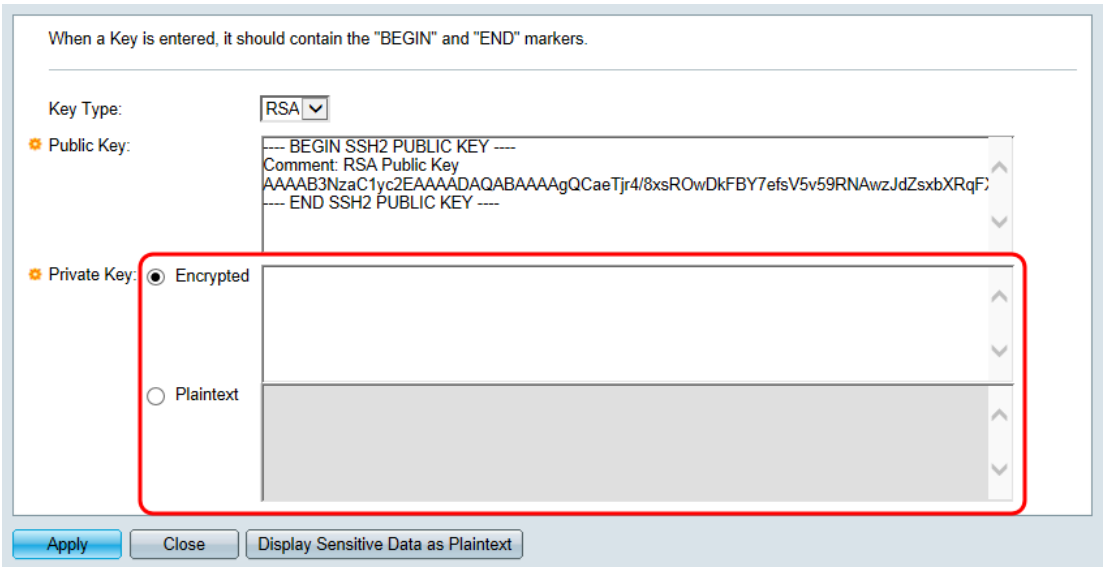
- RSA - RSA用於加密和簽名。
- DSA - DSA僅用於簽名。

步驟7.在公鑰欄位中，您可以編輯目前的公鑰。



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。



步驟9.按一下**Apply** 以儲存變更。