SG350XG和SG550XG上的韌體升級/備份和映像交換

目標

本文檔的目的是解釋如何升級、備份或交換SG350XG和SG550XG交換機上的韌體。

使用最新韌體是提高安全性和效能的最佳實踐。可將多個韌體版本儲存到交換機上，並在需要時進行交換。也可以備份韌體版本。這在發生裝置故障時儲存韌體的備份副本很有用。

適用裝置

- SG350XG
- SG550XG

軟體版本

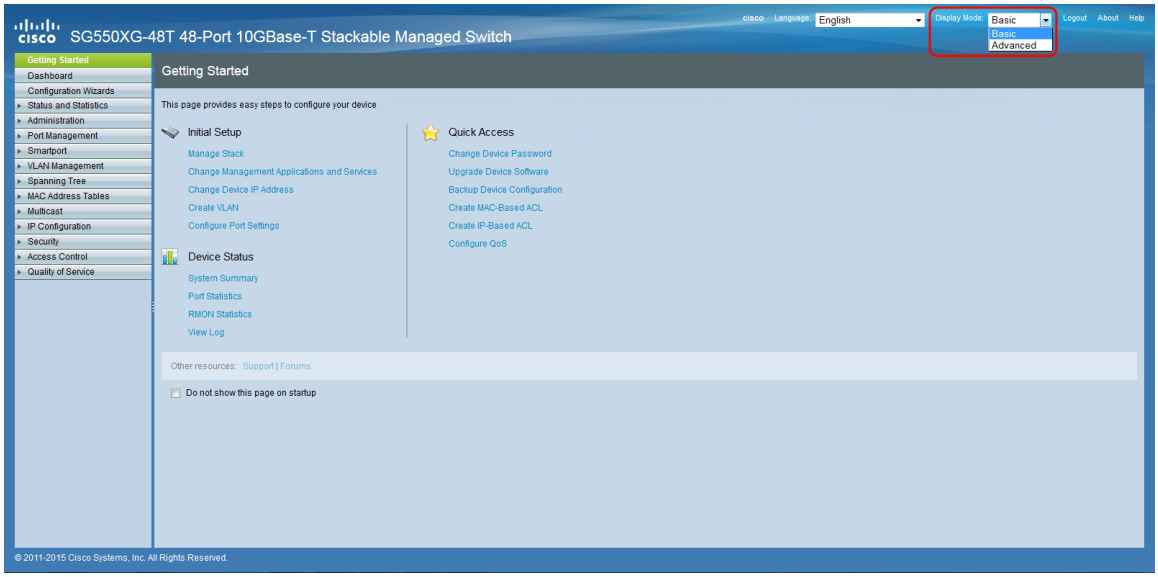
- v2.0.0.73

步驟表

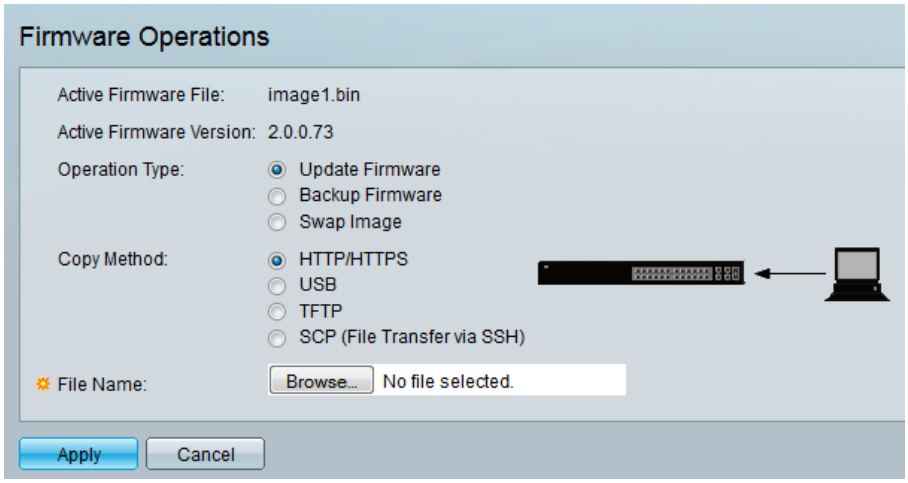
1. 登入
2. 更新/備份韌體
   - 方法：HTTP/HTTPS
   - 方法：USB
   - 方法：TFTP
   - 方法：SCP
3. 交換影象

登入

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

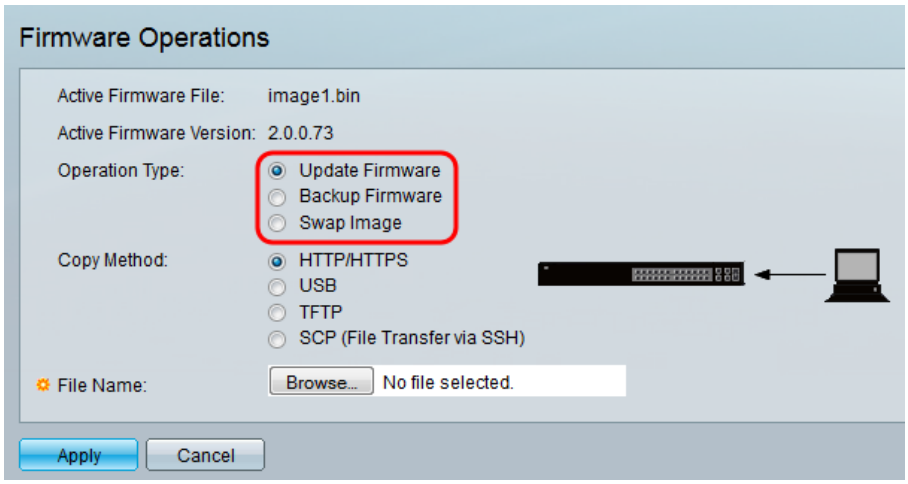


步驟1.登入到Web配置實用程式，然後選擇**Administration > File Management > Firmware Operations**。*Firmware Operations* 頁面隨即開啟。



注意：您可以在「活動韌體檔案」(*Active Firmware File*)欄位和「活動韌體版本」(*Active Firmware* Version)欄位中檢視*當前韌體檔案和*版本。

步驟2.在*Operation Type*區域中按一下所需*的單選*按鈕。



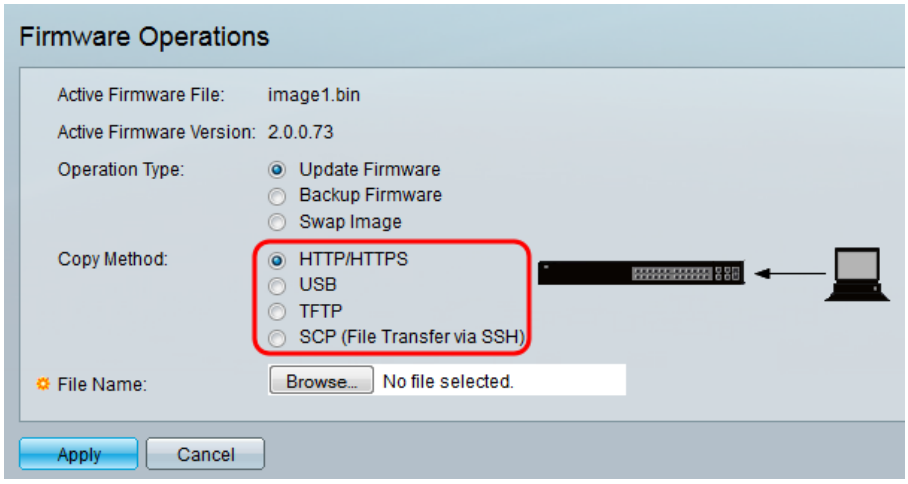
這些選項說明如下：

- Update Firmware — 更新裝置的韌體。

- Backup Firmware — 建立裝置韌體的備份。
- 交換映像 — 使用儲存在裝置快閃記憶體中的韌體更改裝置的韌體。

更新/備份韌體

步驟1。按一下*Copy Method*一節中單選按鈕以顯示所需的檔案傳輸方法。

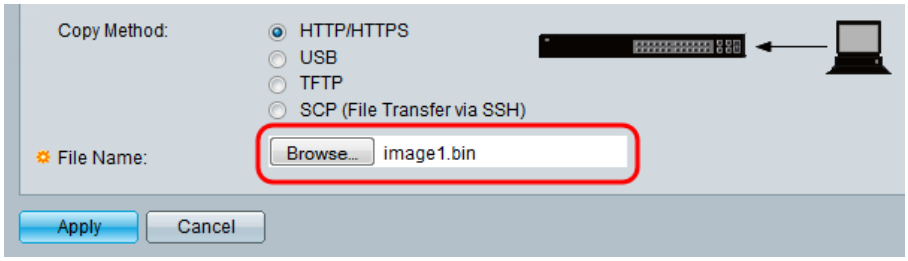


這些選項說明如下：

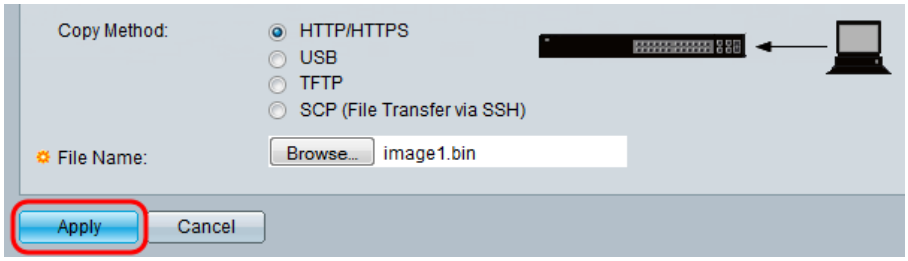
- HTTP/HTTPS -使用瀏覽器提供的工具。
- USB — 使用交換機的USB埠。
- TFTP — 簡單式檔案傳輸通訊協定(TFTP)是一種簡單檔案傳輸通訊協定，允許使用者端從遠端主機取得檔案或將檔案上傳到遠端主機。
- SCP (File Transfer via SSH) — 安全複製協定(SCP)支援網路上主機之間的檔案傳輸，它使用安全外殼(SSH)進行資料傳輸，並使用相同的身份驗證機制，從而確保傳輸中資料的真實性和機密性。

HTTP/HTTPS

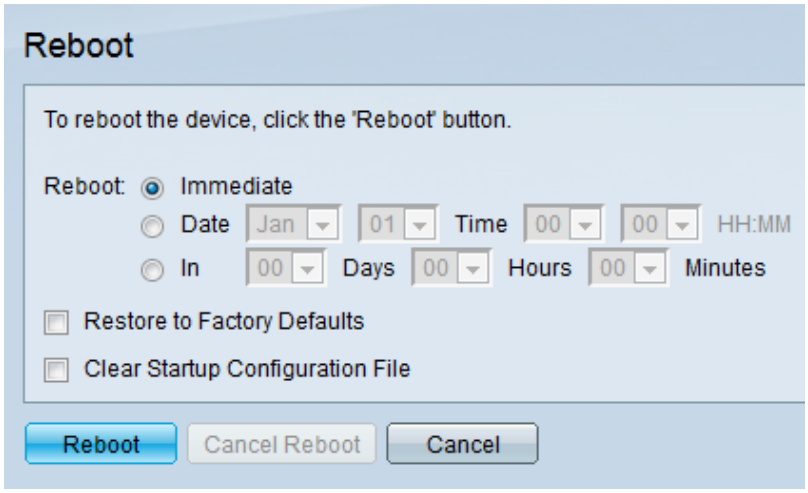
步驟1.在*File Name*欄位中按一下**Browse**按鈕，以選擇要更新的映像檔。此步驟與HTTP/HTTPS備份無關。



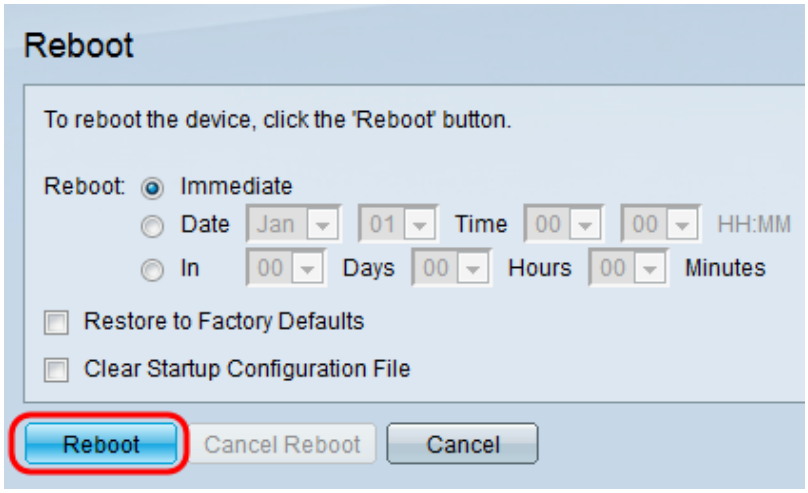
步驟2.按一下**Apply**。



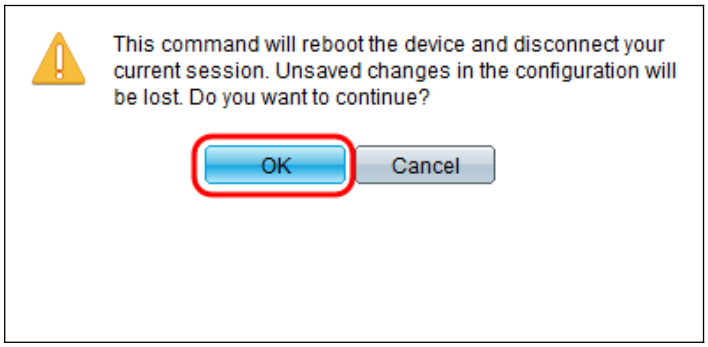
步驟3.導覽至**Administration > Reboot**。*Reboot*頁面開啟。



步驟4.按一下**Reboot**。將顯示確認視窗。



步驟5.按一下**「Ok」**。

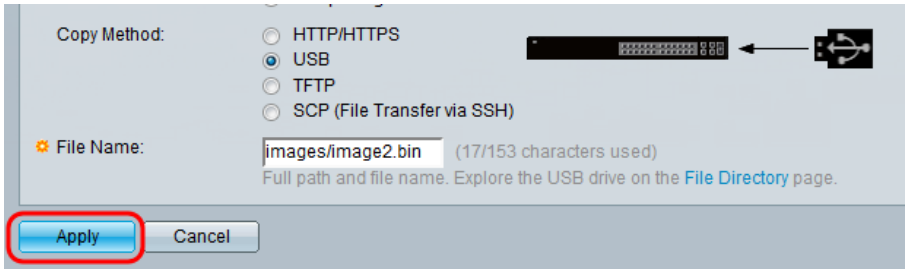


附註：裝置現在將重新啟動，這將斷開當前會話。重新引導完成後，將連線一個新會話。

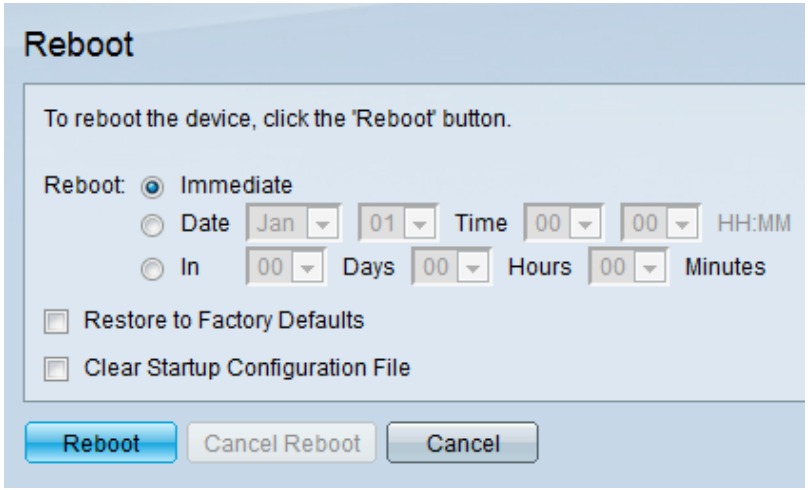
USB

步驟1。在*File Name* 欄位中輸入位於USB上的映像檔案的路徑。

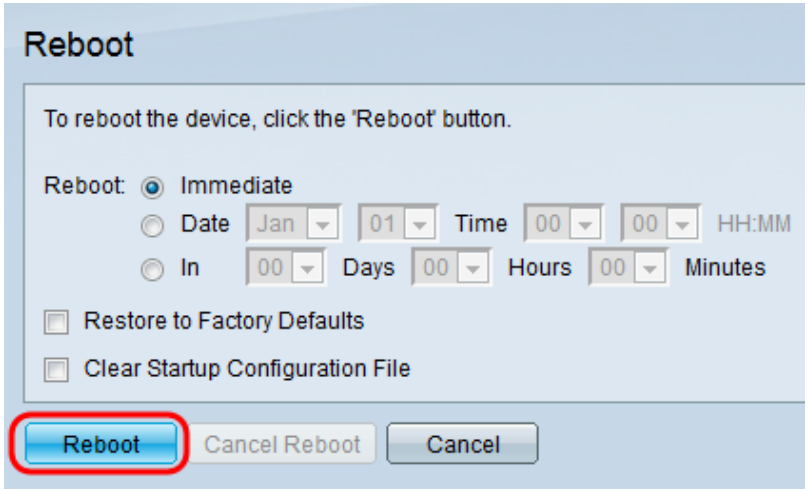
步驟2.按一下**Apply**。



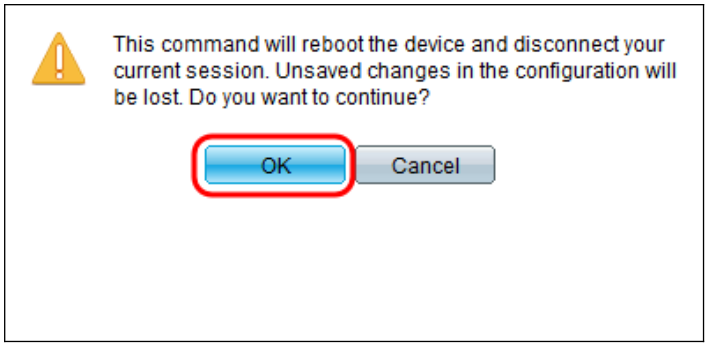
步驟3.在Web配置實用程式上，**選擇Administration > Reboot**。*Reboot*頁面開啟。



步驟4.按一下**Reboot**。



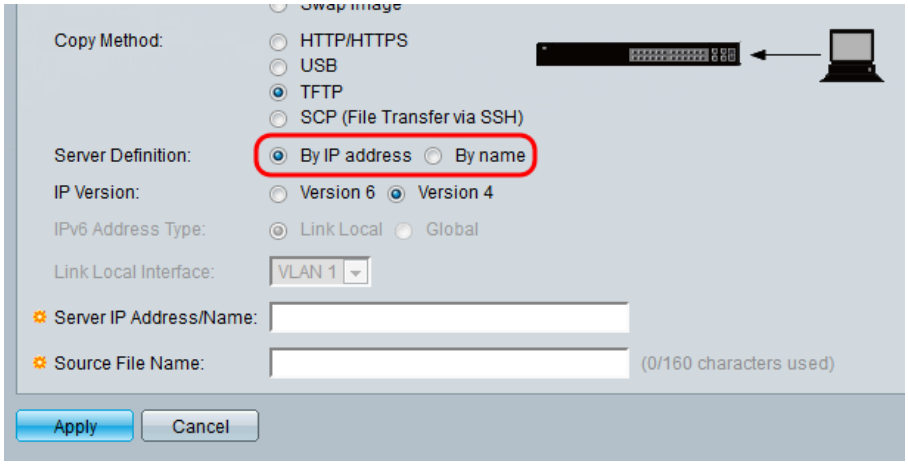
步驟5.出現確認視窗。按一下「**OK**」（**確定**）。



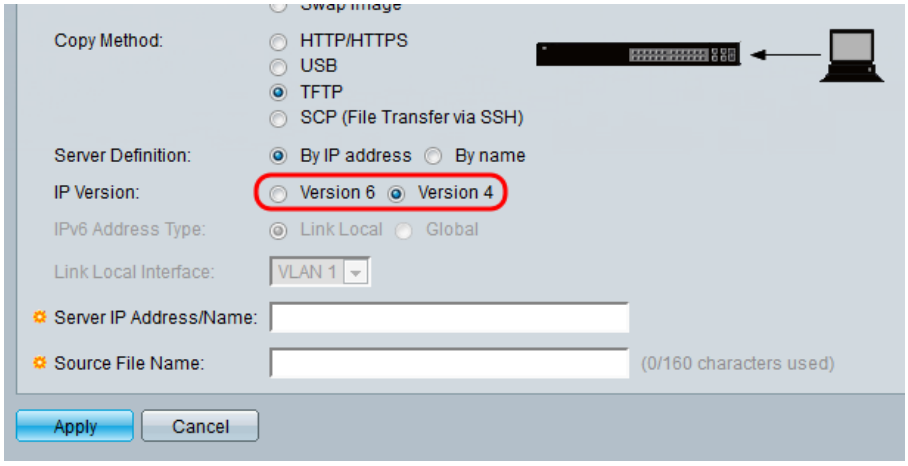
附註：裝置現在將重新啟動，這將斷開當前會話。重新引導完成後，將連線一個新會話。

TFTP

步驟1.選擇相應的單選按鈕，確定您要如何定義TFTP伺服器。伺服器可以按**IP地址**或**按名稱**定義。如果選擇**By name**，請跳至步驟5。



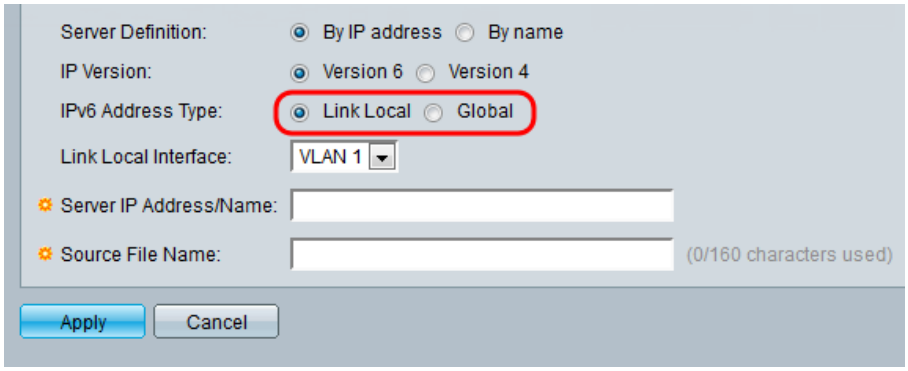
步驟2.（可選）選擇伺服器IP地址的版本。如果選擇**版本4**，請跳至步驟5。



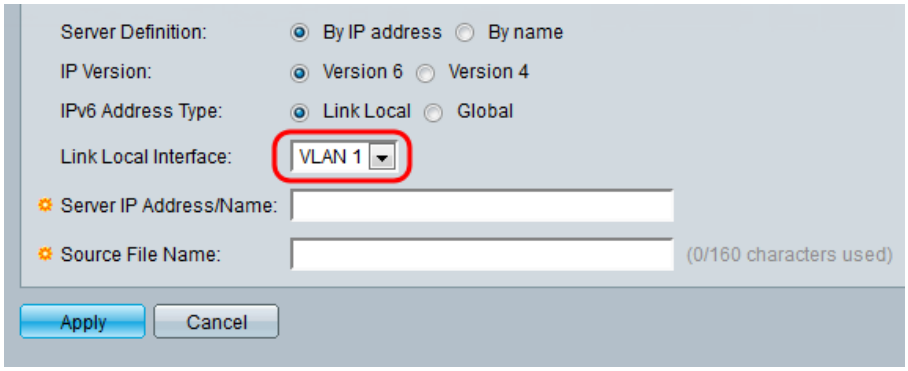
這些選項說明如下：

- IPv4 - 32位（4位元組）地址。
- IPv6 - IPv4的後繼路由器，由128位（8位元組）地址組成。

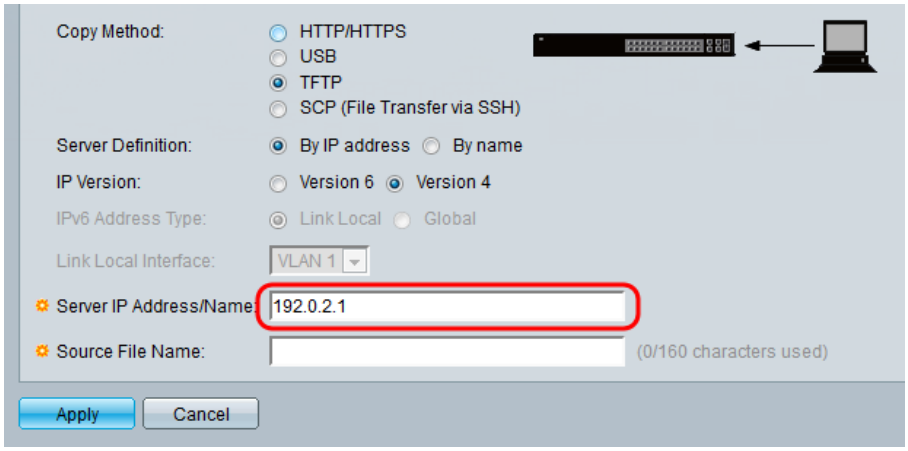
步驟3.（可選）選擇IPv6地址型別。您可以為地址型別選擇**Link Local**或**Global**。如果選擇**Global**，請跳至步驟5。



步驟4.（可選）從*Link Local Interface*下拉選單中選擇所需的VLAN。

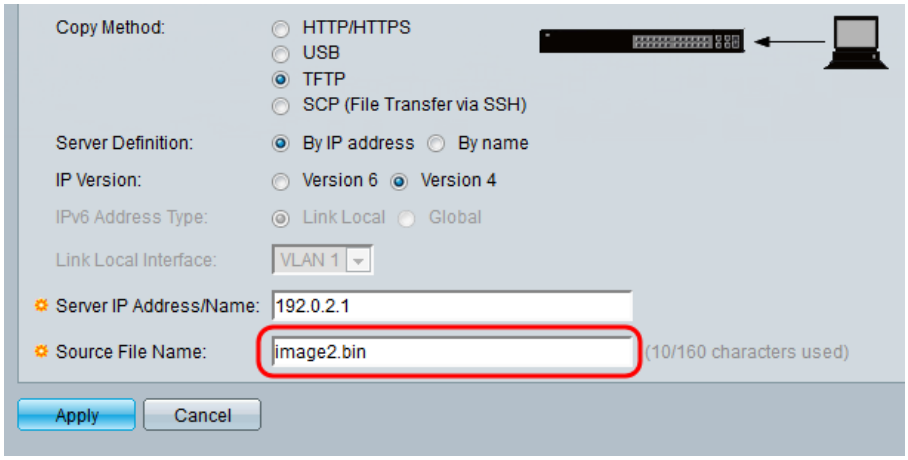


步驟5.在*Server IP Address/Name*欄位中輸入伺服器的名稱或IP地址。



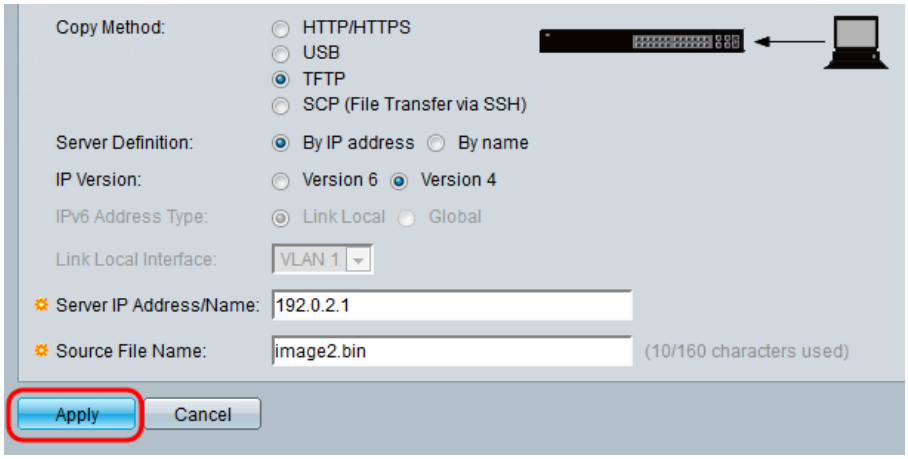
附註：以下欄位取決於步驟1中所選的選項。

步驟6.在「*Source/Destination File* Name」*字段中輸入檔案*名。



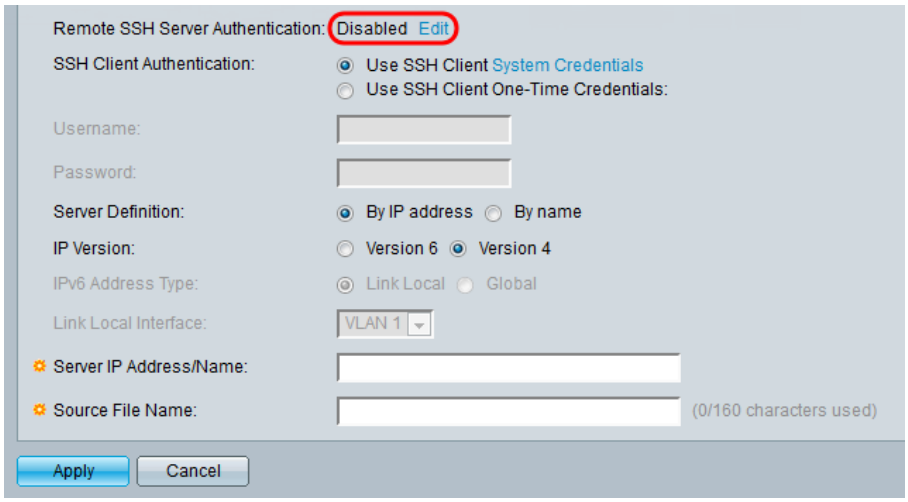
附註：以下欄位的標題為「*Destination File Name* for Backup by TFTP」。

步驟7.按一下**Apply**。



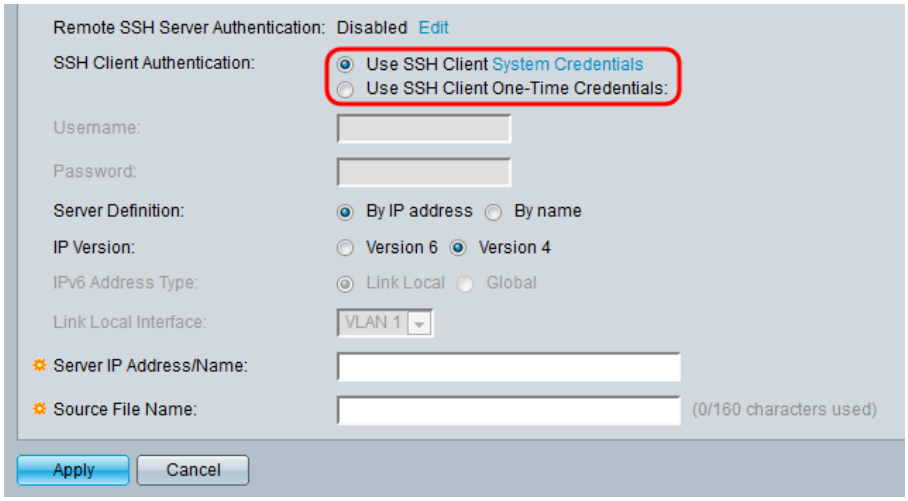
SCP（通過SSH傳輸檔案）

步驟1。要啟用SSH伺服器身份驗證（預設情況下禁用），請按一下**Edit** by *Remote SSH Server Authentication*。這會將您帶到*Client SSH* UserAuthentication頁面以配置SSH使用者。



附註：有關SSH客戶端系統憑據的詳細資訊，請參閱SSH使用者身份驗證文章。

步驟2.在*SSH Client Authentication*欄位中選擇所需的SSH身份驗證。

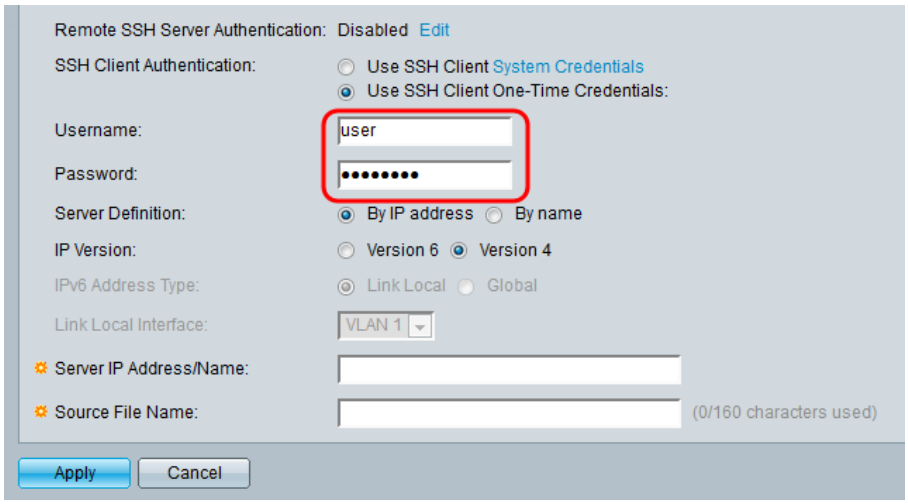


可用選項定義如下：

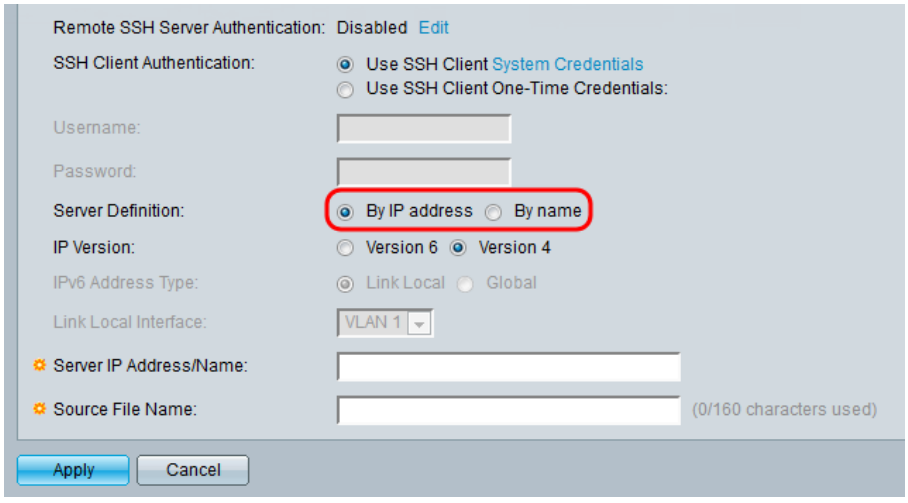
- 使用SSH客戶端系統憑證 — 設定永久SSH使用者憑證。按一下
- **系統憑**據：轉至「*SSH使用者身份驗*證」頁，在該頁可一次性設定使用者/密碼以供將來使用
- 使用SSH客戶端一次性憑證 — 設定一次性SSH使用者憑證。

附註：有關SSH客戶端系統憑據的詳細資訊，請參閱SSH使用者身份驗證文章。

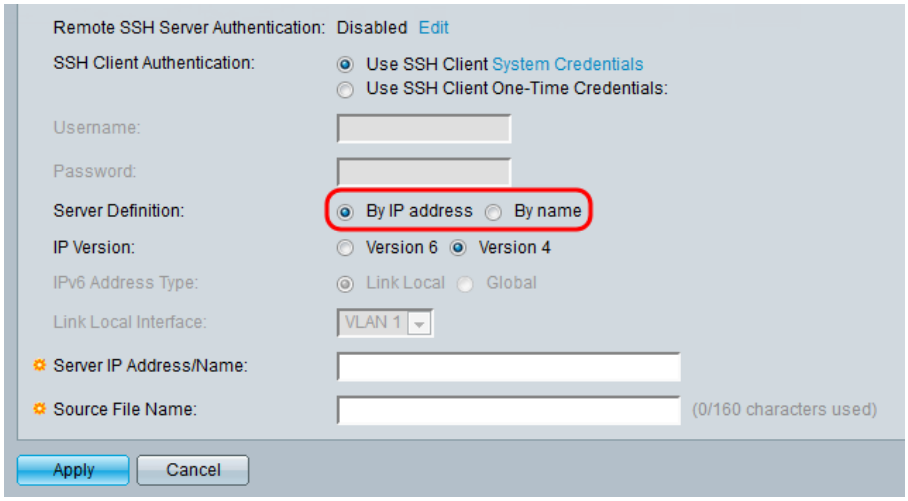
步驟3.（可選）在各自的欄位中輸入所需的*Username*和*Password*。



步驟4.選擇相應的單選按鈕，以便確定您要如何定義SCP伺服器。伺服器可以按**IP地址**或**按名稱**。如果選擇**By name**，請跳至步驟8。



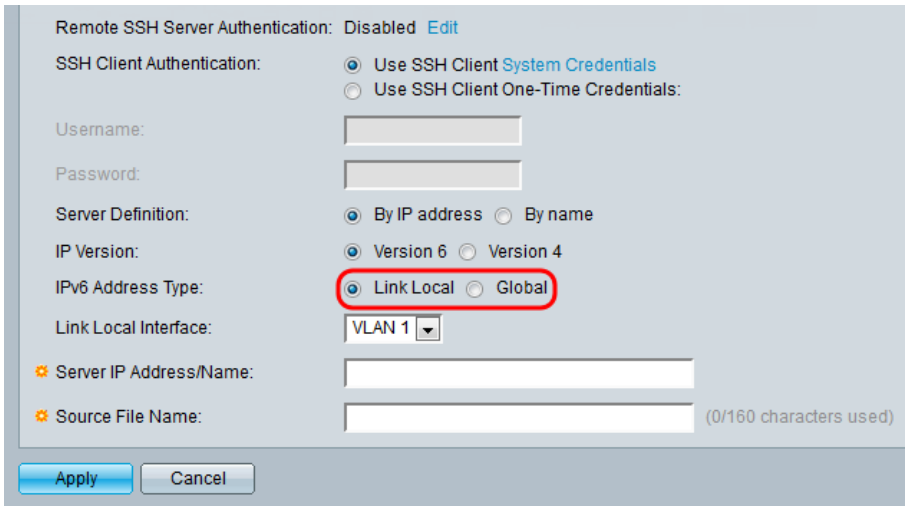
步驟5.（可選）選擇伺服器IP地址的版本。如果選擇**版本4**，請跳至步驟8。



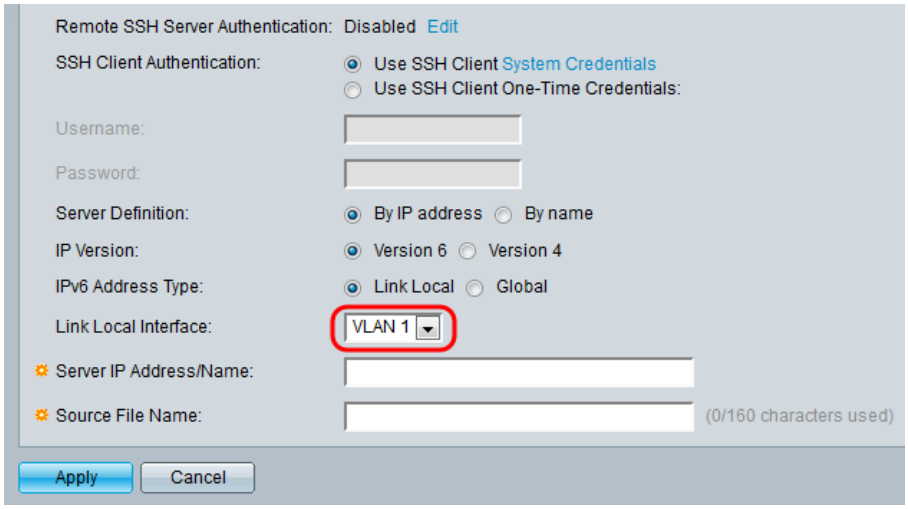
這些選項說明如下：

- IPv4 - 32位（4位元組）地址。
- IPv6 - IPv4的後繼路由器，由128位（8位元組）地址組成。

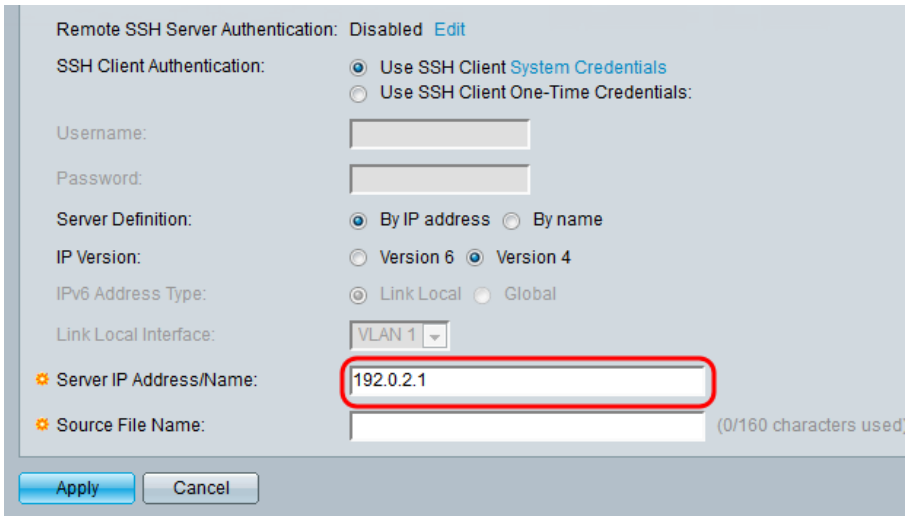
步驟6.（可選）選擇IPv6地址型別。您可以為地址型別選擇**Link Local**或**Global**。如果選擇**Global**，請跳至步驟8。



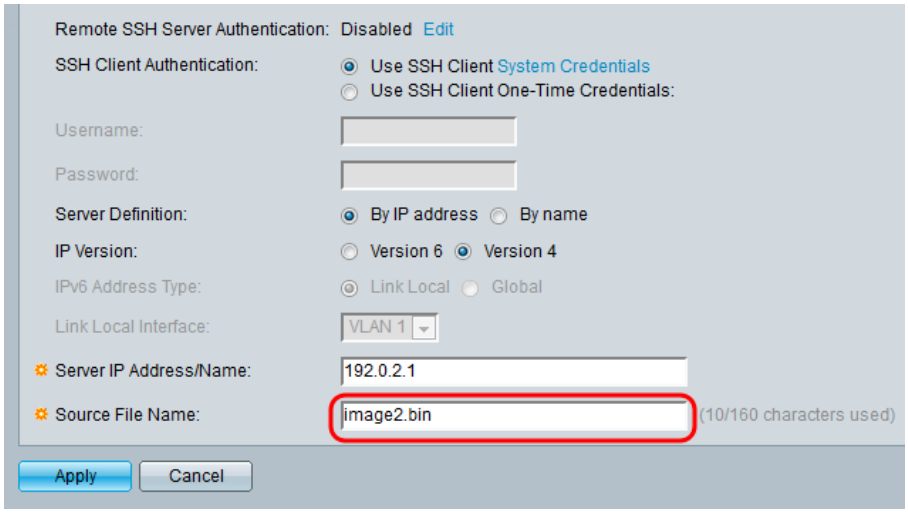
步驟7。（可選）從*Link Local Interface*下拉選單中選擇所需的VLAN。



步驟8.在*Server IP Address/Name*欄位中輸入伺服器的名稱或IP地址。

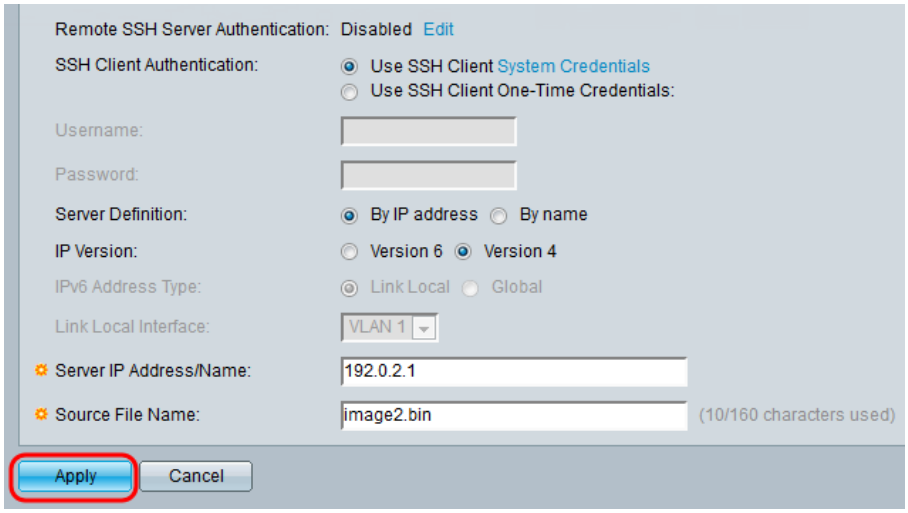


步驟9.在 *來源/Destination 檔案名稱* 欄位.



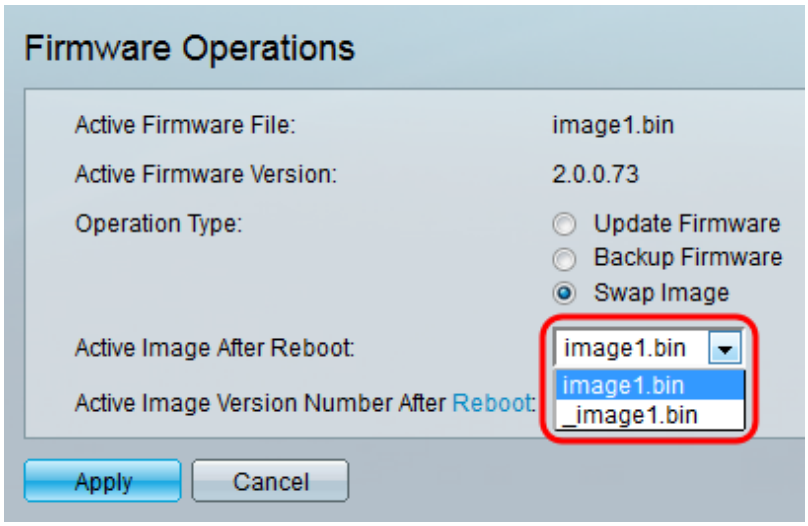
附註：該欄位標題為*Destination File Name for Backup by SCP*。

步驟10.按一下**Apply**。

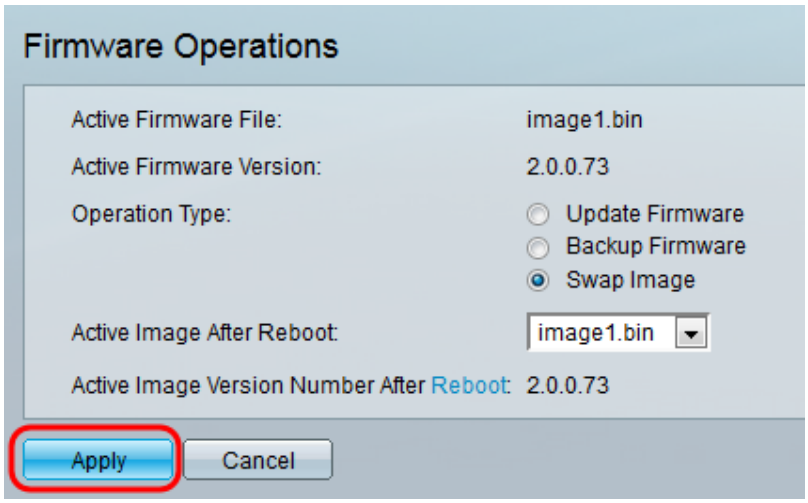


交換影象

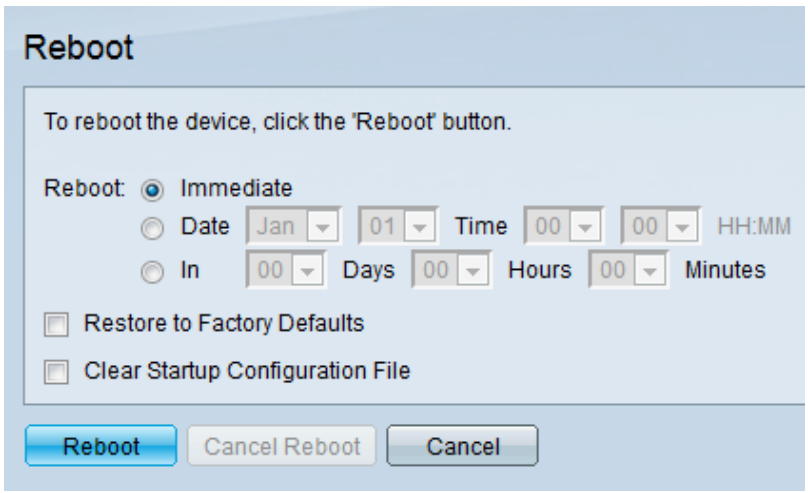
步驟1.從*Active Image After*重新開機後下拉式清單中選擇您想要在重新開機後處於使用中的韌體檔案。



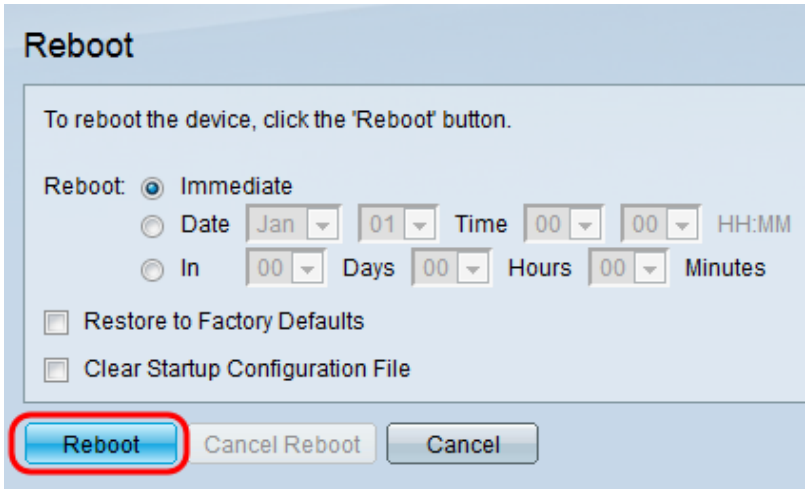
步驟2.按一下**Apply**。



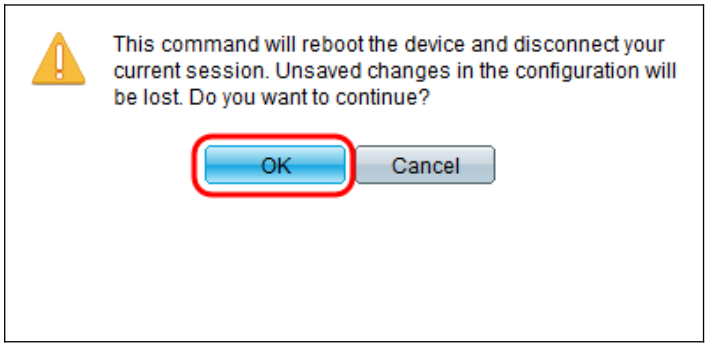
步驟3.在Web配置實用程式上選擇**Administration > Reboot**。*Reboot*頁面開啟。



步驟4.按一下**Reboot**。將顯示確認視窗。



步驟5.按一下「Ok」。



附註：裝置現在將重新啟動，這將斷開當前會話。重新引導完成後，將連線一個新會話。

檢視與本文相關的影片……

[按一下此處檢視思科的其他技術對話]