配置安全Web裝置GUI證書

目錄

簡介

本檔案說明為安全網路裝置(SWA)管理Web介面設定憑證的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- SWA管理。

思科建議您：

- 已安裝物理或虛擬SWA。
- 對SWA圖形使用者介面(GUI)的管理訪問。
- 對SWA命令列介面(CLI)的管理訪問。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

Web使用者介面憑證

首先，我們需要選擇要在SWA管理Web使用者介面(Web UI)中使用的證書型別。

預設情況下，SWA使用「思科裝置演示證書：」

- CN =思科裝置演示證書
- O =思科系統公司
- L =聖荷西
- S =加利福尼亞
- C =美國

您可以在SWA中建立自簽名證書，也可以導入由內部證書頒發機構(CA)伺服器生成的您自己的證書。

生成證書簽名請求(CSR)時，SWA不支援包括主題備用名稱(SAN)。此外，SWA自簽名證書也不支援SAN屬性。要使用具有SAN屬性的證書，您必須自己建立並簽署證書，確保證書中包含必要的SAN詳細資訊。生成此證書後，您可以將其上傳到SWA以供使用。此方法允許您指定多個主機名、IP地址或其他識別符號，為您的網路環境提供更大的靈活性和安全性。

注意：證書必須包含私鑰，並且私鑰必須是PKCS#12格式。

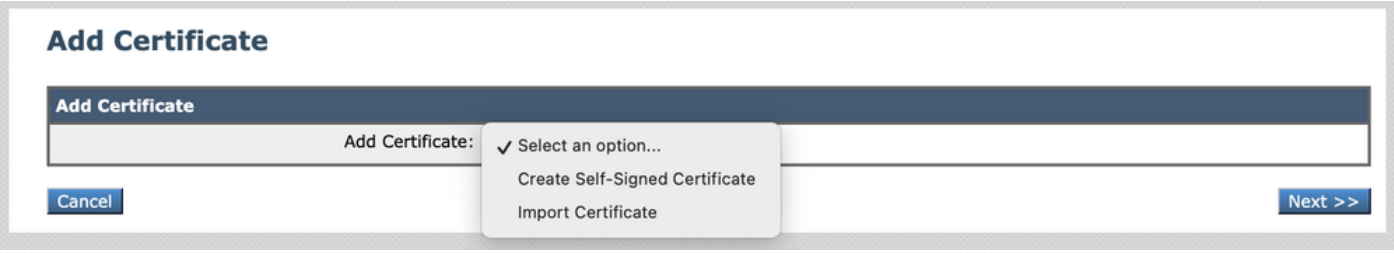
修改Web介面憑證的步驟

步驟 1.登入到GUI，然後從頂部選單中選擇Network。

步驟 2. 選擇Certificate Management。

步驟 3.從裝置證書中選擇增加證書。

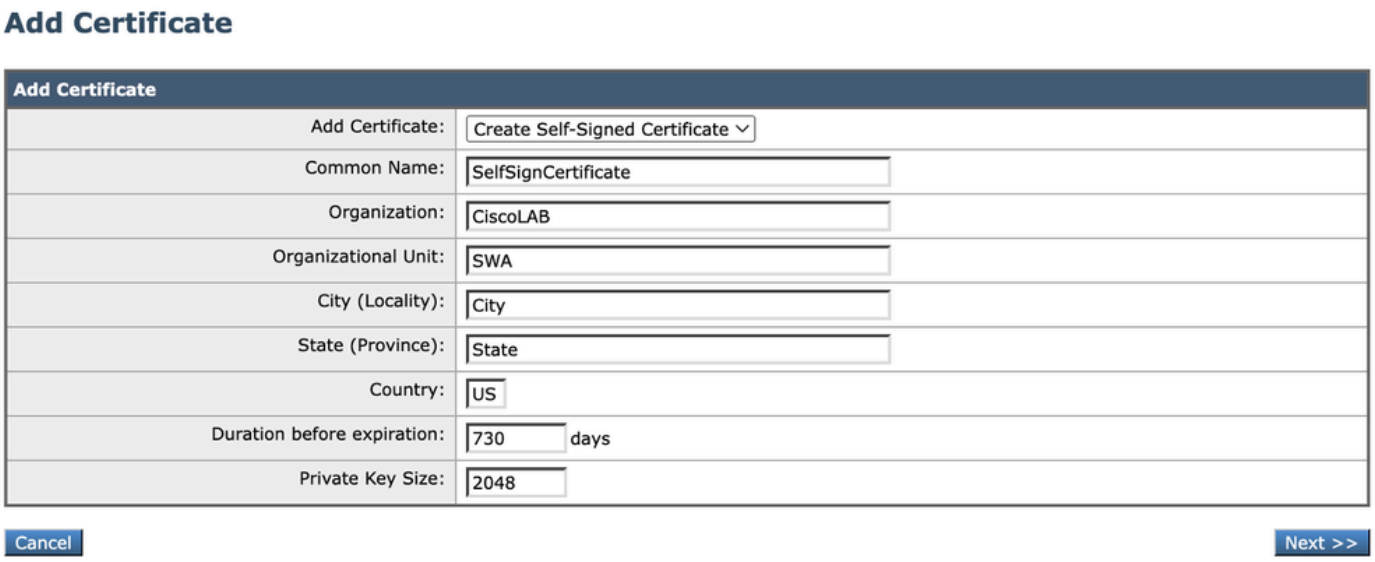
步驟 4. 選擇證書型別(自簽名證書或導入證書)。



影像-選擇憑證型別

步驟 5. 如果選擇Self-Signed Certificate，請執行以下步驟。否則，請跳到步驟6。

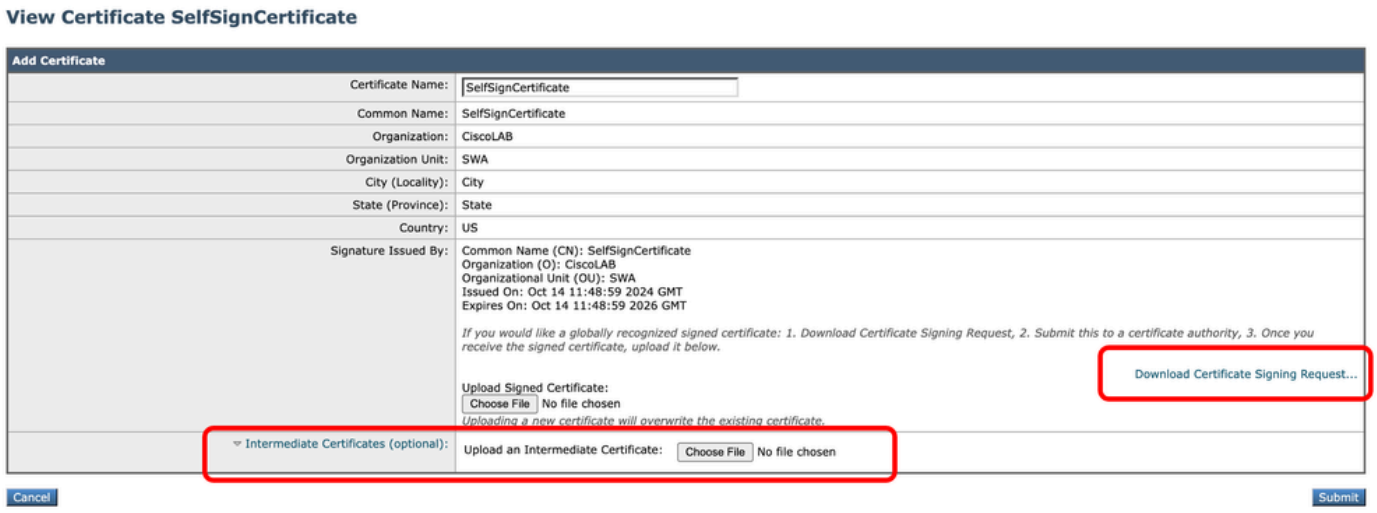
第5.1步：填寫欄位。



影象-自簽名證書詳細資訊

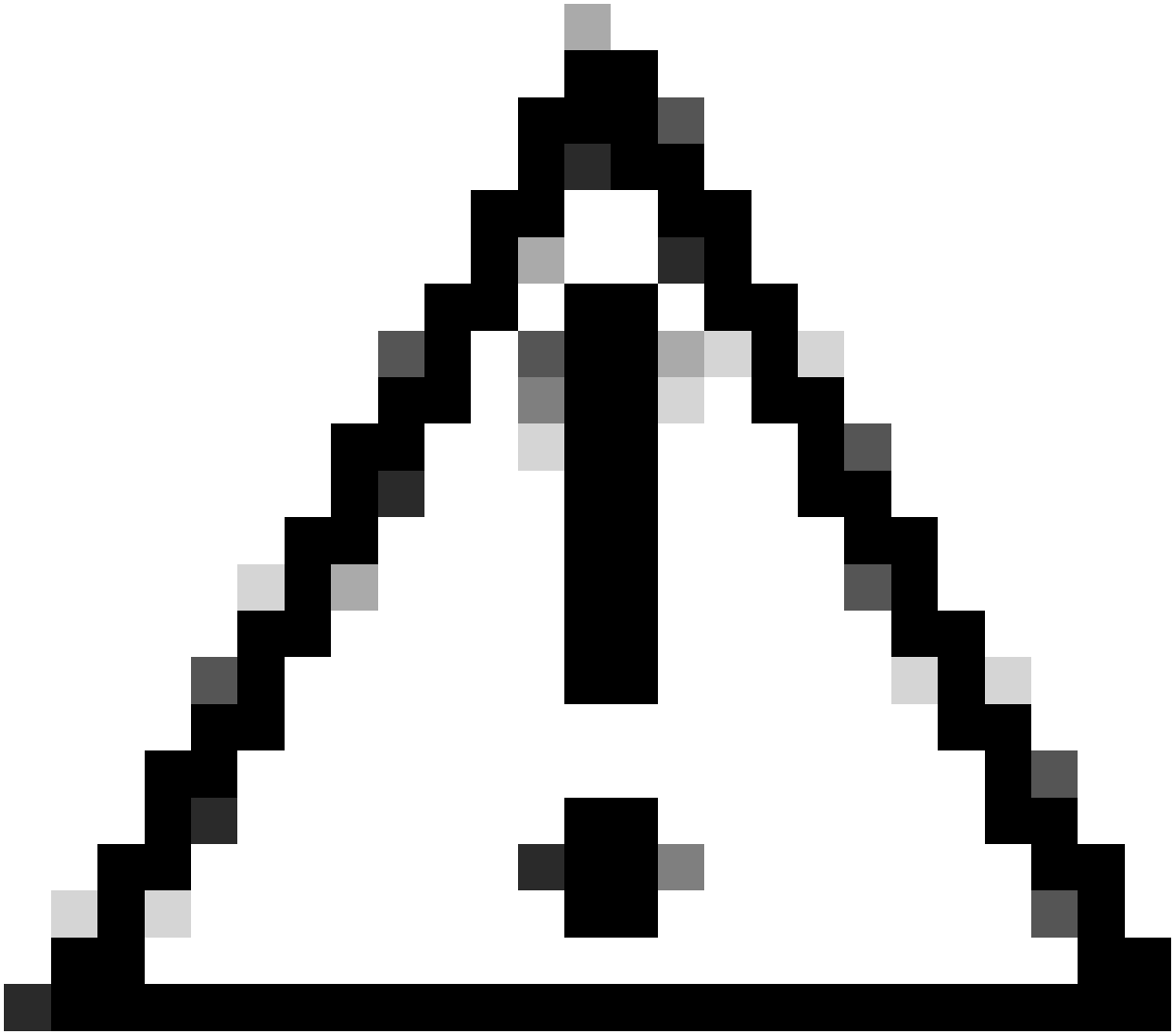
注意：私鑰大小必須在2048到8192範圍內。

步驟 5.2.按「Next」（下一步）。



影像-下載CSR

步驟 5.3.（可選）您可以下載CSR並用您的組織CA伺服器對其進行簽名，然後上傳簽名證書並提交。



注意：如果您希望使用CA伺服器簽署CSR，請確保在簽署或上傳簽名證書之前提交和提交頁面。 在CSR生成過程中建立的配置檔案包含您的私鑰。

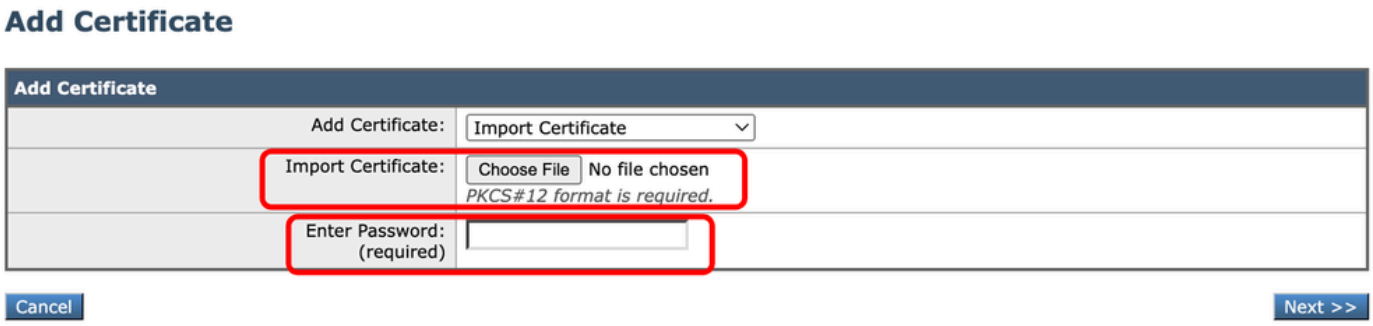
第5.4步：提交（如果當前自簽名證書合適）。

步驟 5.5. 請跳到步驟7。

步驟 6. 如果您選擇Import Certificate。

步驟 6.1.匯入憑證檔案（需要PKCS#12格式）。

步驟 6.2.輸入憑證檔案的密碼。



影像-匯入憑證

步驟 6.3.按「Next」（下一步）。

步驟 6.4. 提交變更。

步驟 7.提交更改。

步驟 8.登入到CLI。

步驟 9. 鍵入certconfig，然後按Enter。

步驟 10. 鍵入SETUP。

步驟 11.鍵入Y，然後按Enter。

注意：證書更改後，當前登入Web使用者介面的管理使用者可能會遇到連線錯誤，並且可能會丟失未提交的更改。只有當瀏覽器未將憑證標示為受信任時，才會發生這種情況。

步驟 12. 選擇2 從可用的證書清單中選擇。

步驟 13. 選擇要用於GUI的所需證書數量。

步驟 14. 如果您有中間證書，並且想要增加它們，則鍵入Y，否則鍵入N。

注意：如果需要增加中間證書，您必須將中間證書貼上為PEM格式並以「.」結尾(僅點)。

```
SWA_CLI> certconfig

Choose the operation you want to perform:
- SETUP - Configure security certificate and key.
- OCSPVALIDATION - Enable OCSP validation of certificates during upload
- RESTRICTCERTSIGNATURE - Enable restricted signature validation of certificates during upload
- OCSPVALIDATION_FOR_SERVER_CERT - Enable OCSP validation for server certificates
- FQDNVALIDATION - FQDN validation for certificate
[]> SETUP

Currently using the demo certificate/key for HTTPS management access.

When the certificate is changed, administrative users who are currently logged in to the web user inter
occurs only if the certificate is not already marked as trusted by the browser.
```

```
Do you want to continue? [Y]> Y

Management (HTTPS):
Choose the operation you want to perform:
1. PASTE - Copy paste cert and key manually
2. SELECT - select from available list of certificates
[1]> 2

Select the certificate you want to upload
1. SelfSignCertificate
2. SWA_GUI.cisco.com
[1]> 1

Do you want add an intermediate certificate? [N]> N

Successfully updated the certificate/key for HTTPS management access.
```

步驟 15. 鍵入commit以儲存更改。

從命令列測試證書

您可以使用openssl指令檢查憑證：

```
openssl s_client -connect
```

```
:
```

在本示例中，主機名是SWA.cisco.com，管理介面設定為預設（TCP埠8443）。

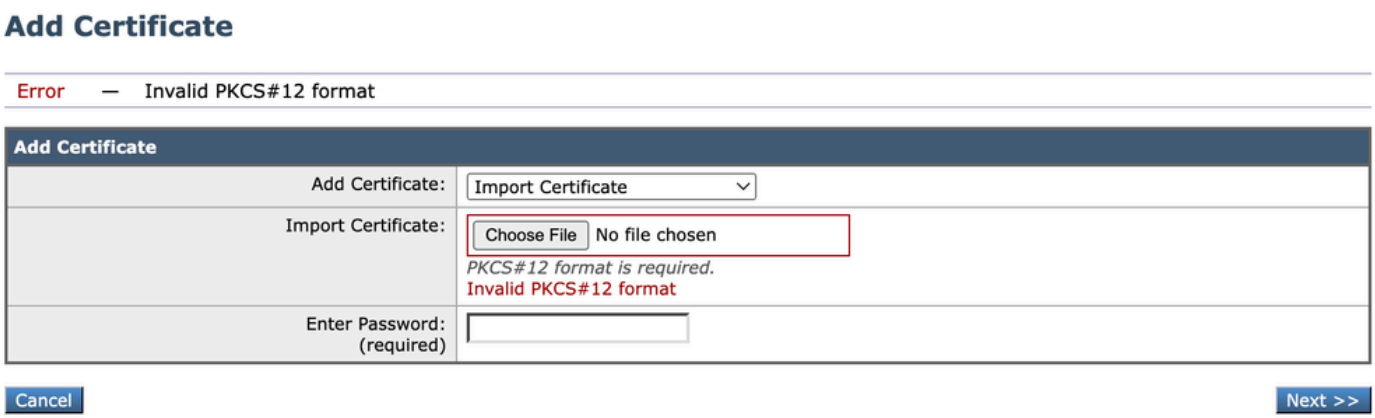
在輸出的第二行中，您可以看到憑證詳細資訊：

```
openssl s_client -connect SWA.cisco.com:8443
CONNECTED(00000003)
depth=0 C = US, CN = SelfSignCertificate, L = City, O = CiscoLAB, ST = State, OU = SWA
```

常見錯誤

以下是嘗試建立或修改GUI憑證時可能會遇到的一些常見錯誤。

錯誤：無效的PKCS#12格式



映像-無效的PKCS#12格式

此錯誤可能有兩個原因：

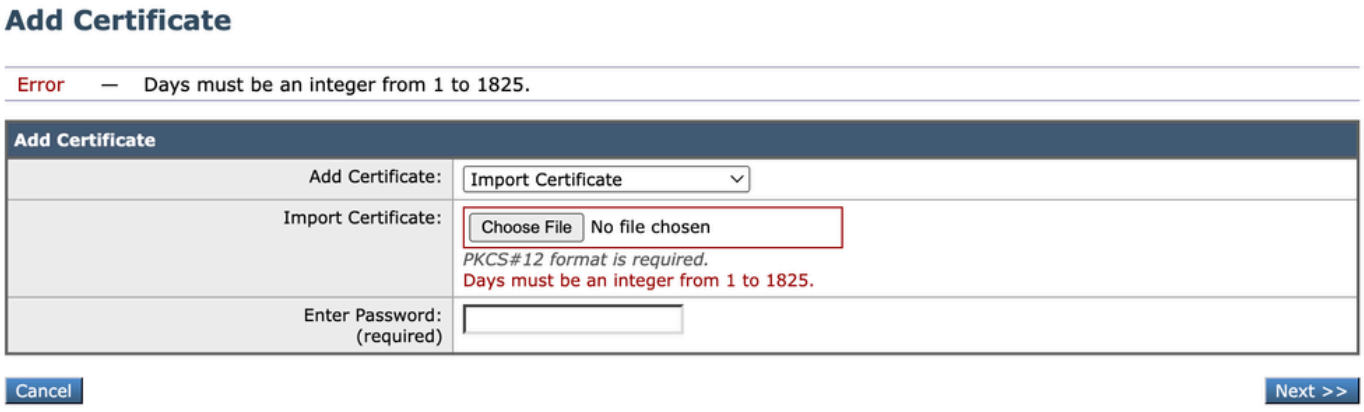
1. 憑證檔案已損毀且無效。

   嘗試開啟憑證。如果開啟時發生錯誤，您可以重新產生或再次下載憑證。

2. 先前產生的CSR不再有效。

   生成CSR時，您必須確保選中Submit和Commit選項。原因是註銷或更改頁面時未儲存CSR。您在產生CSR時建立的設定檔包含成功上傳憑證所需的私密金鑰。 一旦此設定檔消失，私密金鑰就會消失。因此，必須產生另一個CSR，然後再次將另一個CSR交給您的CA。

天數必須是整數



影像-天數必須是整數錯誤

此錯誤是由於上載的證書已過期或具有0天的有效性所致。

要解決此問題，請檢查證書到期日期，並確保您的SWA日期和時間正確。

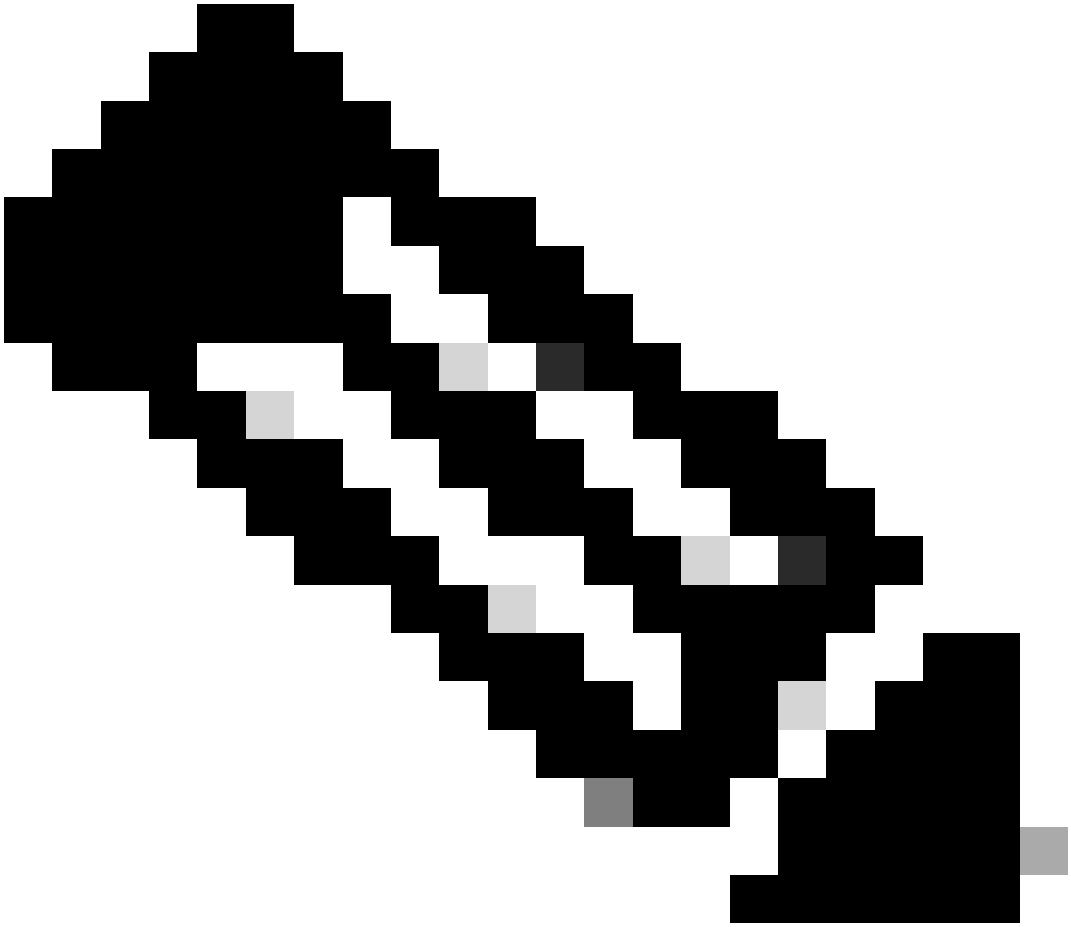
憑證驗證錯誤

此錯誤表示根CA或中間CA未增加到SWA中的受信任的根證書清單中。若要解決此問題，如果您同時使用根CA和中間CA：

1. 將根CA上傳到SWA，然後提交。

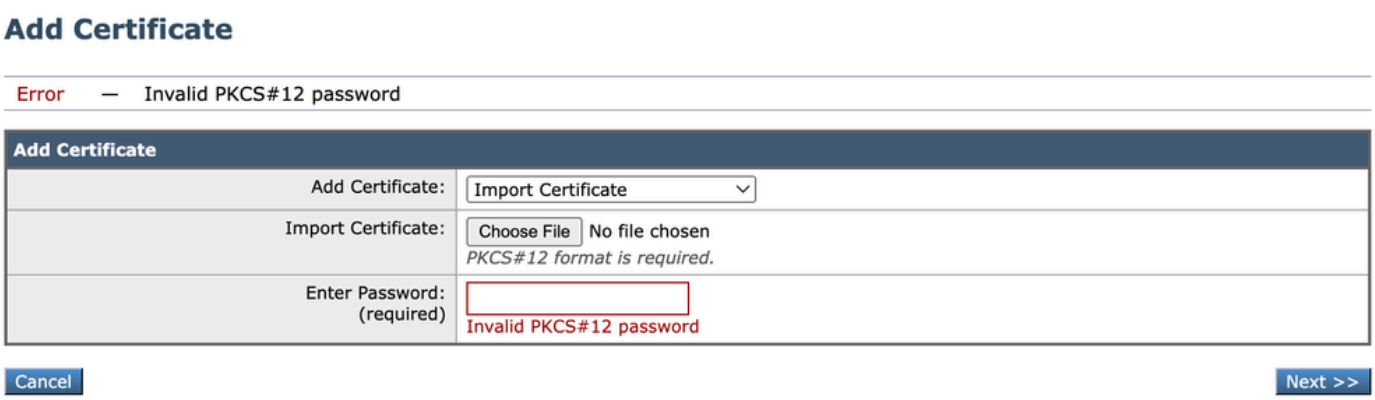
2. 上傳中繼CA，然後再次提交更改。

3. 上傳GUI憑證。



注意：要上傳根或中間CA，請從GUI：網路。在Certificate Management部分中，選擇Manage Trusted Root Certificates。在自定義受信任的根證書中，按一下導入以上傳CA證書。

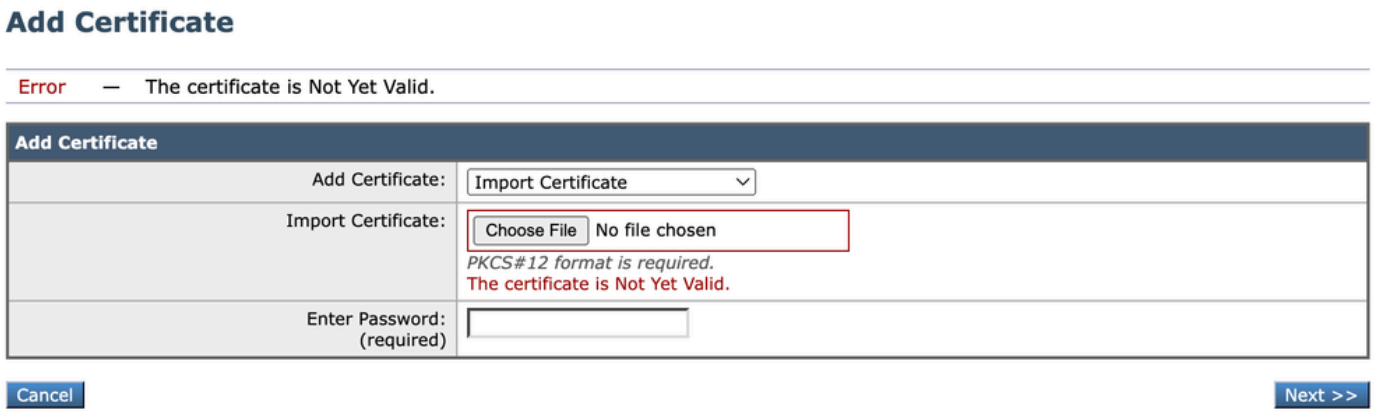
密碼無效



影象-密碼無效

此錯誤表示PKCS#12憑證密碼不正確。若要解決此問題，請鍵入正確的密碼，或重新生成證書。

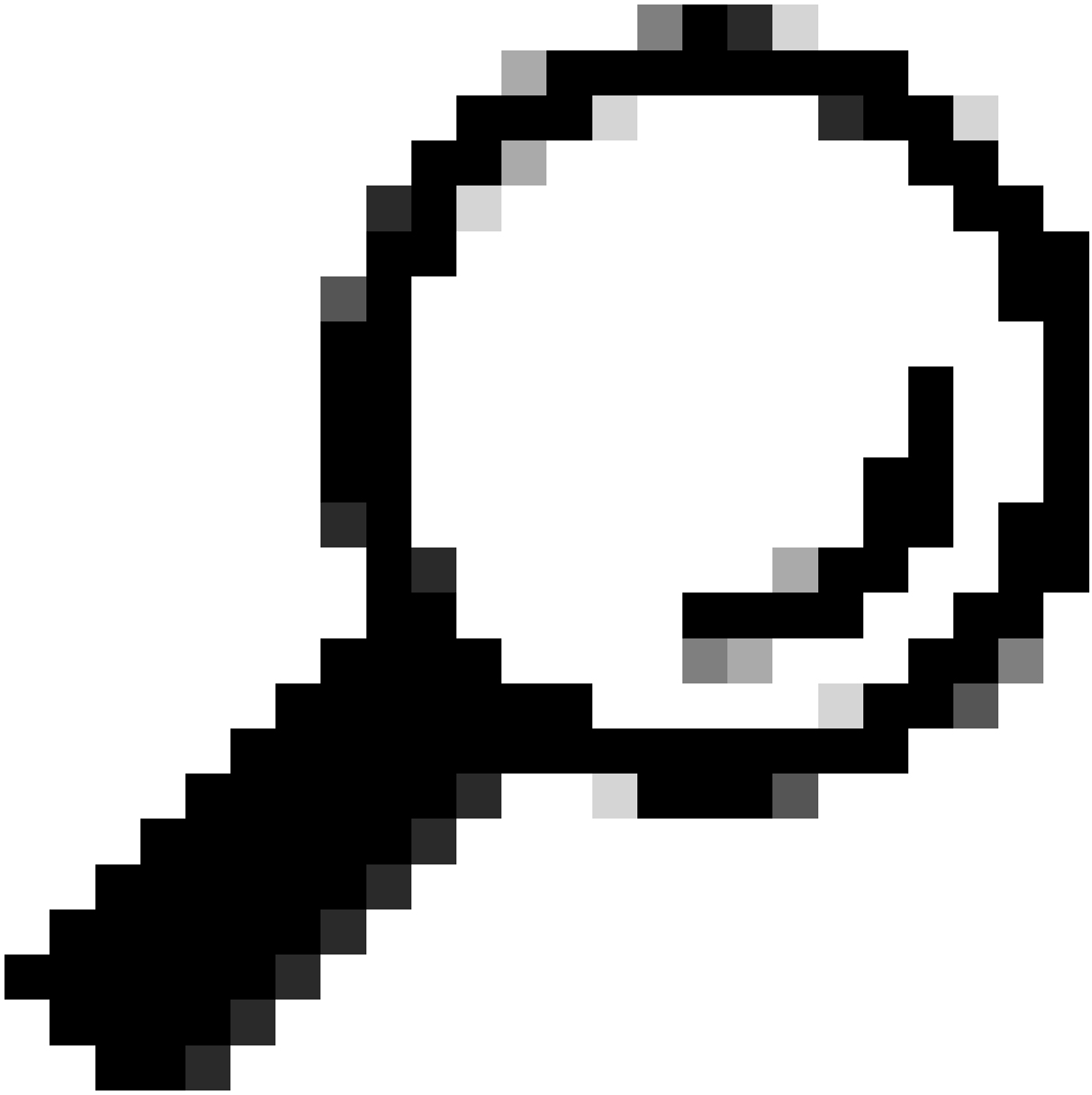
憑證尚未生效



影像-憑證尚未生效

1. 確保SWA日期和時間正確。

2. 檢查證書日期並確保「不早於」日期和時間正確。



提示：如果您剛生成證書，請等待一分鐘，然後上傳證書。

從CLI重新啟動GUI服務

若要重新啟動WebUI服務，您可以從CLI執行下列步驟：

步驟 1.登入到CLI。

步驟 2.鍵入diagnostic(這是一個隱藏命令，不會使用TAB自動鍵入)。

步驟 3.選擇服務。

步驟 4. 選擇WEBUI。

步驟 5. 選擇重新啟動。

相關資訊

- AsyncOS 15.0 for Cisco Secure Web Appliance使用手冊- GD（常規部署）-對終端使用者進行策略應用分類[Cisco Secure Web Appliance] -思科

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）。