在Cisco ESA GUI上新增/匯入新的PKCS#12證書

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[問題](#)
[因應措施](#)

簡介

本檔案介紹如何在Cisco Email Security Appliance(ESA)GUI上新增/匯入公#12加密標準(PKCS)加密憑證。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco ESA
- AsyncOS 7.1及更高版本

問題

自AsyncOS 7.1.0及更高版本以來，可以在電子郵件裝置的GUI中管理/新增證書。但是，對於此新證書，它必須是PKCS#12格式，因此此要求會在收到證書頒發機構(CA)證書後新增一些額外步驟。

生成PKCS#12證書還需要私鑰證書。如果從Cisco ESA CLI命令**certconfig**運行證書簽名請求(CSR)，您將不會收到私鑰證書。當您使用在GUI選單(「郵件策略」>「簽名金鑰」)中建立的私鑰證書生成PKCS#12證書和CA證書時，該證書將無效。

因應措施

1. 如果您的工作站沒有安裝OpenSSL應用程式，請安裝。可以從此處下載Windows版本。確保在OpenSSL Win32之前安裝Visual C++ 2008 Redistributable。
2. 在此使用模板建立指令碼以生成CSR和私鑰。指令碼將如下所示：**openssl req -new -newkey rsa:2048 -nodes -out test_example.csr -keyout test_example.key -subj**

"/C=AU/ST=NSW/L=Sydney/O=Cisco Systems/OU=IronPort/CN=test.example.com"

3. 將指令碼複製並貼上到OpenSSL視窗中，然後按**Enter**鍵。

   C:\OpenSSL-Win32\bin>openssl req -new -newkey rsa:2048 -nodes -out test_example.csr -keyout test_example.key -subj "/C=AU/ST=NSW/L=Sydney/O=Cisco Systems/OU=IronPort/CN=test.example.com"

   輸出：

   ```
   test_example.csr and test_example.key in the C:\OpenSSL-Win32\bin or in the
   'bin' folder where OpenSSL is installed
   test_example.csr = Certificate Signing Request
   example.key = private key
   ```

4. 使用.CSR檔案請求CA證書。

5. 收到CA憑證後，將其另存為**cacert.pem**檔案。將私鑰檔案**test_example.key**重新命名為**test_example.pem**。現在，可以使用OpenSSL產生PKCS#12憑證。

   指令:

   openssl pkcs12 -export -out cacert.p12 -in cacert.pem -inkey test_example.pem

   如果使用的CA證書和私鑰正確，OpenSSL會提示您輸入**Export Password**，然後再次確認密碼。否則，它會通知您所使用的證書和金鑰不匹配，因此無法繼續該過程。

   輸入：

   ```
   cacert.pem = CA certificate
   test_example.pem = private key
   Export password: ironport
   ```

   輸出：

   ```
   cacert.p12 (the PKCS#12 certificate)
   ```

6. 轉到IronPort GUI選單，**Network > Certificate**。

選擇**Add Certificate**。
在**Add Certificate**選項中選擇**Import Certificate**。
選擇**Choose**並瀏覽到步驟5中生成的PKCS#12證書的位置。
輸入您在OpenSSL中產生PKCS#12憑證時使用的相同密碼(在本案例中密碼為**ironport**)。
選擇「**Next**」，下一個螢幕將顯示用於證書的屬性詳細資訊。
選擇**Submit**。
選擇**Commit changes**。

執行完這些步驟後，新憑證會新增到憑證清單中，並且可以指派給使用者使用。