中華電信通用憑證管理中心（PublicCA）

Imperva SecureSphere 憑證請求檔製作與憑證安裝手冊

Imperva SecureSphere為資料庫安全稽核硬體，以下步驟若與您持有版本有差異，請參考原廠手冊或請原廠技術支援，適度調整相關安裝步驟。

1.於 Windows PC 上使用 Java JDK 1.7 使用 keytool 產製金鑰對，

執行 keytool -genkeypair -alias vecert -keyalg RSA -keysize 2048 -validity 3650 -keystore vecert.jks -storepass 密碼 -keypass 密碼 -dname "CN=sso-ve-mbms.cht.com.tw,O=Chunghwa Telecom Co.\, Ltd.,C=TW" -ext san=dns:sso-ve-mbms.cht.com.tw,dns:nonsso-ve-mbms.cht.com.tw

以上 CN 與 O 所輸入為範例，請以貴公司組織名稱與通用名稱填寫。憑證簽發時註記之唯一識別名稱與網站名稱仍以您於 PublicCA 網站所填寫資料並經憑證註冊審驗人員審驗的為準。

2.請參考以下指令產生憑證請求檔 csr：

keytool -keystore vecert.jks -storepass 密碼 -keypass 密碼 -certreq -alias vecert -file vecert.csr -ext san=dns:sso-ve-mbms.cht.com.tw,dns:nonsso-ve-mbms.cht.com.tw

3. 此時憑證請求檔(certreq.txt)製作完成，請持憑證請求檔至中華電信通用憑證管理中心網站（http://publicca.hinet.net/）依照網頁說明申請 SSL 憑證。

4. 若屬於中華電信公司各單位申請 SSL 憑證者，請從企業入口網站選擇電子表單之資訊表單「IS14-伺服器應用軟體憑證申請/異動單」提出申請。

5. 下載憑證串鏈，包含三張憑證，分別是(1)eCA 根憑證(ePKI Root CA 憑證，也就是中華電信憑證總管理中心自簽憑證)、(2)PublicCA 中繼憑證(中華電信通用憑證管理中心自身憑證)與(3)PublicCA 簽發給用戶的 SSL 伺服器憑證，可採以下兩種方式之一取得：

A. 您若是本公司之客戶，技術聯絡人的電子郵件信箱會收到憑證串鏈壓縮檔，解壓縮後包括三個檔案，分別是eCA根憑證(檔名為ROOTeCA_64.crt)、PublicCA中繼憑證檔名為PublicCA_64.crt與xxHD73xxxxxx.crt是簽發給用戶的SSL伺服器軟體憑證，其中xxHD73xxxxxx是SSL憑證申請書的申請單號。
若是中華電信之所屬單位，於經審驗核准申請之電子表單的資訊表單「IS 14-伺服器應用軟體憑證申請/異動單」頁面下方，可以下載憑證串鏈壓縮檔，解壓

縮後可以取得憑證串鏈三個檔案。

B. 從網站查詢與下載：

eCA憑證：http://epki.com.tw/download/ROOTeCA_64.crt

PublicCA憑證：http://publicca.hinet.net/CHTM/download/PublicCA_64.crt

SSL憑證下載：您若是本公司之客戶，請至PublicCA網站點選「SSL憑證服務」再點選「SSL憑證查詢及下載」，進行SSL憑證下載。

若您是中華電信之員工，負責管理單位之伺服器，請至http://chtra.cht.com.tw/ 點選「憑證與卡片作業」，再點選「憑證查詢」，下載SSL憑證。

6.請參考以下 keytool 用法，將 SSL 憑證與私密金鑰轉換為 PKCS #12 檔案格式

-importkeystore [-v]
[-srckeystore <來源金鑰儲存庫>] [-destkeystore <目標金鑰儲存庫>]
[-srcstoretype <來源儲存庫類型>] [-deststoretype <目標儲存庫類型>]
[-srcstorepass <來源儲存庫密碼>] [-deststorepass <目標儲存庫密碼>]
[-srcprotected] [-destprotected]
[-srcprovidername <來源提供者名稱>]
[-destprovidername <目標提供者名稱>]
[-srcalias <來源別名> [-destalias <目標別名>]
[-srckeypass <來源主密碼>] [-destkeypass <目標主密碼>]]
[-noprompt]
[-providerclass <提供者類別名稱> [-providerarg <引數>]] ...
[-providerpath <路徑清單>]

.

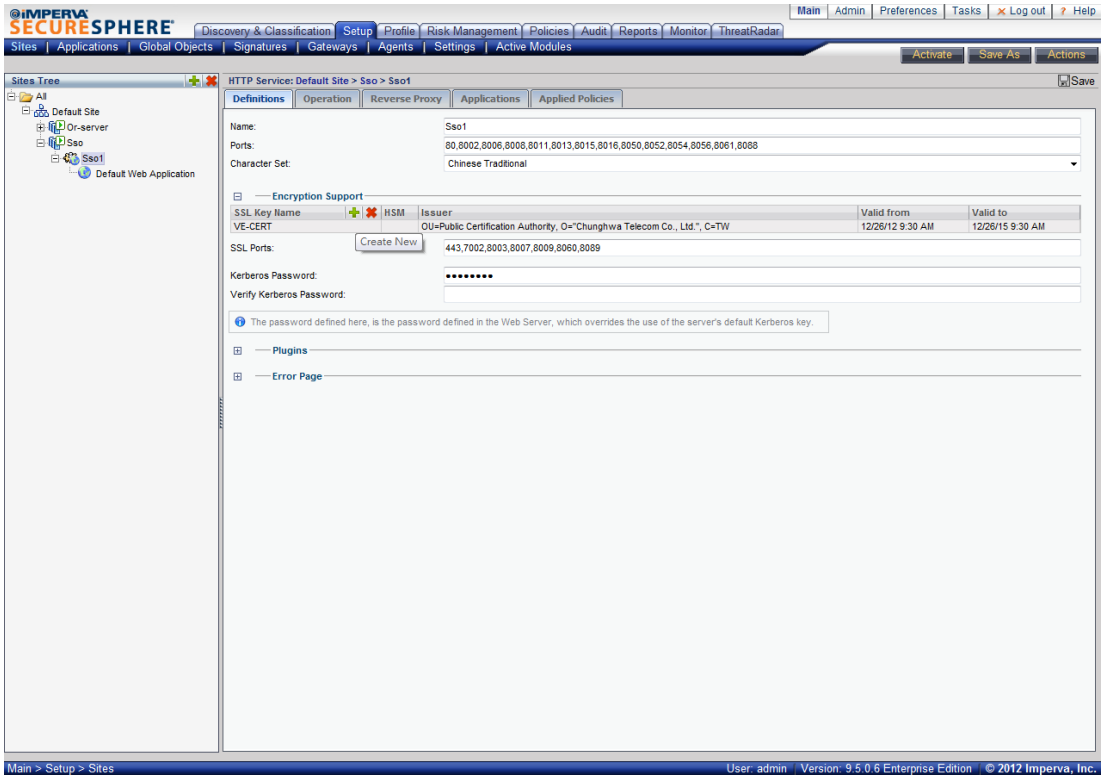
C:\OpenSSL-Win32\bin>keytool -importkeystore -srckeystore .keystore -destkeystore tomcat.pfx -srcstoretype jks -deststoretype pkcs12 -srcalias tomcat -destalias tomcat

請輸入目標金鑰儲存庫密碼：

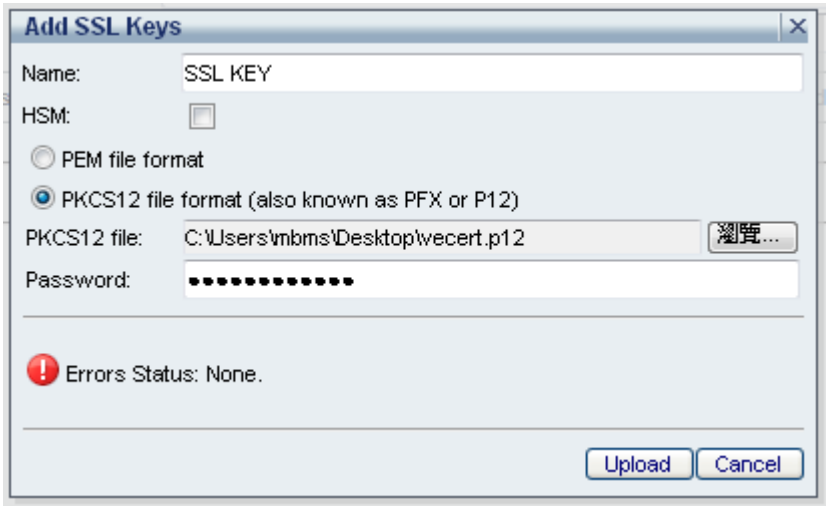
請輸入來源金鑰儲存庫密碼：

7. 請登入 iMPERVA 設備

8. 請點選 Setup，在左邊樹狀結構中選擇監聽 HTTPS 封包的 Service
9. 在 Encryption Support 區點選綠色的+號



10. 如下圖選擇 PKCS12 file format，瀏覽並選擇檔案路徑及輸入密碼，再點選 Upload 即可。



11. 如果正確完成，在 Encryption Support 就會顯示正確的簽章資訊