中華電信 HiPKI 憑證管理中心（OVTLSCA）

WebLogic 伺服器 SSL 憑證請求檔製作與憑證安裝手冊

本手冊的操作程序，係執行於 Windows 環境平台上，與您所使用的版本或環境可能有差異，請您參考您的 WebLogic Server 使用手冊或請 WebLogic Server 廠商提供技術協助，適度調整申請步驟。

目錄

WebLogic SSL 憑證請求檔製作手冊

一、製作憑證請求檔

1. 開始前，請先確認您 Java 的版本

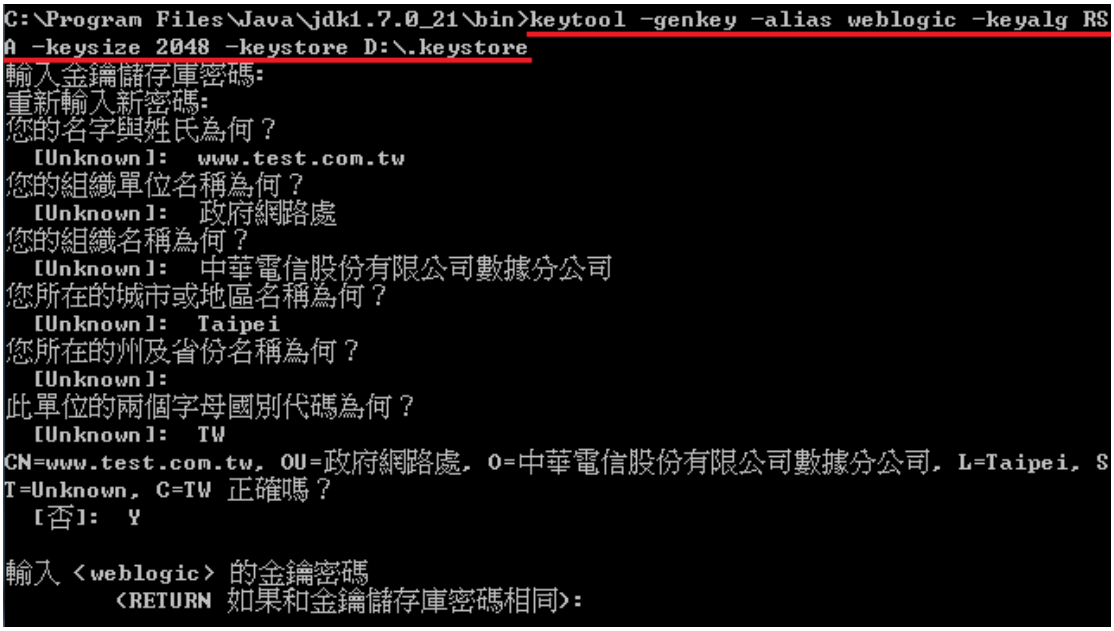
   由於 WebLogic 的底層是 Java，如果其所使用的 Java(JDK)版本是 1.5 版以前的版本，將無法安裝 RSA 4096 位元金鑰長度的憑證，因為舊版的 Java 最多只支援 RSA 2048 bits 的金鑰長度，這將造成 Java Keystore 不會將根憑證、中繼憑證及 SSL 憑證視為 1 個憑證串鏈，結果在 SSL Handshake 中，中繼憑證就不會被送到 Client 端，建議請使用最新版本的 Java(JDK)版本。

2. 開啟命令提示字元。

3. 在 %JAVA_HOME%\bin 目錄下，請執行

   keytool -genkey -alias <金鑰的 alias name> -keyalg RSA -keysize 2048 -keystore <keystore 儲存路徑>(請自行輸入需要的路徑與檔名)。

   - **若您非第 1 次申請憑證，請確認您所指定的路徑與檔名不會覆蓋線上正在使用的憑證。**
   - **此指令會在指定目錄下產生".keystore"檔(內含私密金鑰)，請勿於提出憑證申請後重複執行此指令，否則舊的".keystore"檔將會被覆蓋。**
   - 依照國際密碼學之規範，2014 年起不要再使用 RSA 1024 位元之憑證，請產製 RSA 2048 位元(含)以上金鑰長度的金鑰對。
   - 請妥善保管此".keystore"檔。



4. 出現「輸入 keystore(金鑰儲存庫)密碼」: 請輸入一個密碼，用以保護此儲存庫(**請妥善保存此組密碼**)。
5. 接著依照畫面填入所需資料：

您的名字與姓氏為何?	網站名稱(ex: www.test.com.tw)
您的組織單位名稱為何？	單位名稱(ex: IT)
您的組織名稱為何？	組織名稱(ex: CHT)
您所在的城市或地區名稱為何？	城市(ex: Taipei)
您所在的州及省份名稱為何？	可不填，按 Enter 跳過
此單位的兩個字母國別代碼為何？	填入 TW

6. 檢查所輸入的資料是否正確, 若正確, 請輸入 Y。
7. 出現「輸入 <weblogic> 的金鑰密碼」: 您可以按 Enter 讓金鑰密碼與金鑰儲存庫相同，或是獨立設定金鑰密碼，稍後再設定 WebLgoic 時，會需要輸入金鑰儲存庫密碼與金鑰密碼。
8. 在 %JAVA_HOME%\bin 下，執行
   keytool -certreq -alias <上一步驟所用的 alias name> -file <憑證請求檔儲存路徑> -keystore <keystore 檔案所在路徑>

二、此時憑證請求檔(certreq.txt)製作完成，使用憑證請求檔至中華電信公開金鑰基礎建設服務網站（https://chtca.hinet.net/）依照網頁說明申請 SSL 憑證。

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。

補充說明 1: 中華電信公開金鑰基礎建設服務之程式會擷取憑證請求檔中的公開金鑰，但不會使用憑證請求檔中於上圖所輸入之資訊，而是以於申請網頁上所填入的組織資訊與完全吻合網域名稱(Fully Qualified Domain Name, FQDN)為準，並記載於所簽發的 SSL 憑證裡面的欄位[如憑證主體名稱(Subject Name)之一般名稱(Common Name)或憑證主體別名(Subject Alternative Name)等欄位]。

補充說明 2:若您是申請多網域 SSL 憑證或萬用網域 SSL 憑證,僅需要產生 1 個憑證請求檔(產生憑證請求檔之過程就是幫您的伺服器產製 1 對金鑰對，私密金鑰與密碼由伺服器管理者保管，公開金鑰會包含在憑證請求檔內，憑證管理中心審驗您的身分與網域名稱擁有權或控制權後,所簽發的憑證會記載申請者的組織資訊、完全吻合網域名稱與公開金鑰在 SSL 憑證內。後續先安裝 SSL 憑證串鏈於產生憑證請求檔之站台，再將私密金鑰與憑證備份後匯入其他站台，不同廠牌伺服器之匯出與匯入可參考手冊或寫電子郵件給本管

理中心技術客服信箱 caservice@cht.com.tw 詢問，不需要每個網站站台都分別產生憑證請求檔。

WebLogic SSL 憑證安裝操作手冊

一、下載憑證串鏈，包含 4 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)eCA to HRCA 交互憑證(eCA 簽發給 HRCA 之交互憑證)、(3)HiPKI OV TLS CA 中繼憑證(中華電信 HiPKI OV TLS 憑證管理中心自身憑證)與(4)OV TLS CA 簽發給用戶的 SSL 伺服器憑證，可採以下兩種方式之一取得：

1. 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 4 個檔案，分別是 eCA 根憑證(檔名為 ROOTeCA_64.crt)、eCA to HRCA 交互憑證(檔名為 eCA1-to-HRCA1.crt)、OV TL SCA 中繼憑證(檔名為 OVTLSCA1_b64.crt)與用戶端 SSL 伺服器軟體憑證(檔名為 32 個英數字所組成，此為憑證序號)。
   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 4 個檔案。
2. 從網站查詢與下載：
   eCA 憑證：
   https://eca.hinet.net/download/ROOTeCA_64.crt
   eCA to HRCA 憑證：
   https://eca.hinet.net/download/eCA1-to-HRCA1.crt
   HiPKI OV TLS CA 憑證：
   https://eca.hinet.net/repository-h/download/OVTLSCA1_b64.crt
   SSL 憑證下載：您若是本公司之客戶，請至 CHTCA 網站點選「TLS 憑證效期查詢及下載」，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 https://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。

二、SSL 憑證安裝，請使用您之前產生憑證請求檔的 Keystore 來執行匯入動作（依信任關係，由最上層憑證，依序往下安裝）

1. 安裝根憑證。
   在 %JAVA_HOME%\bin 目錄下執行
   keytool -import -alias eCA -file D:\ROOTeCA_64.crt -keystore D:\.keystore
   - 請依實際您存放檔案的位置調整指令。
   - 待出現 Enter keystore password：請輸入密碼。
   - 待出現 Trust this certificate：請輸 yes。
2. 安裝交互憑證。

在 %JAVA_HOME%\bin 目錄下執行

keytool -import -alias eCAtoHRCA -file D:\eCA1-to-HRCA1.crt -keystore D:\.keystore

- 請依實際您存放檔案的位置調整指令。
- 待出現 Enter keystore password：請輸入密碼。

3. 安裝中繼憑證。

在 %JAVA_HOME%\bin 目錄下執行

keytool -import -alias OVTLSCA1 -file D:\OVTLSCA1_b64.crt -keystore D:\.keystore

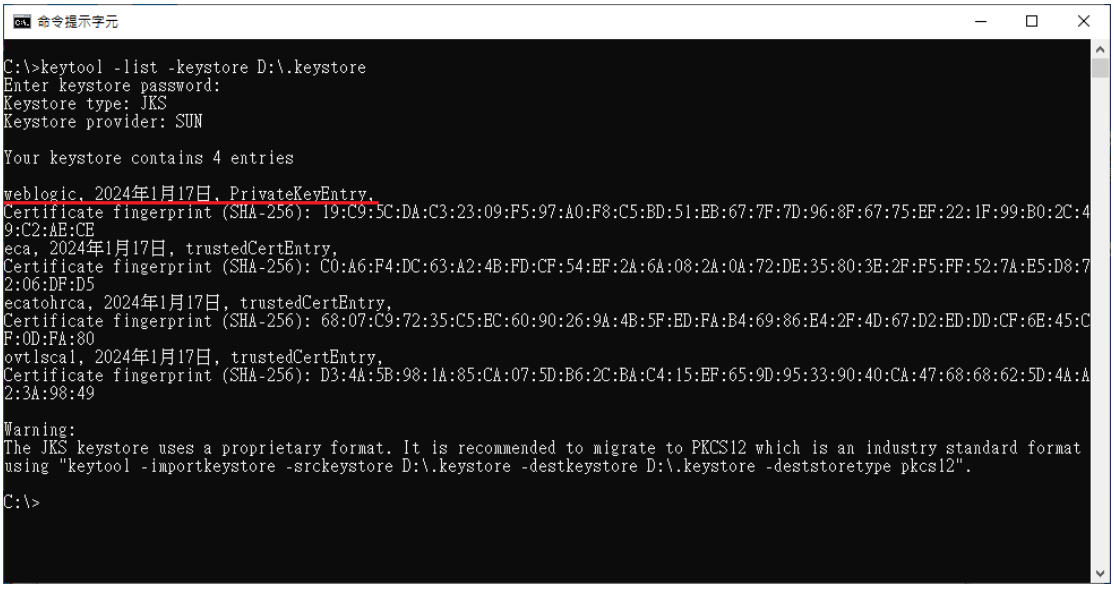
- 請依實際您存放檔案的位置調整指令。
- 待出現 Enter keystore password：請輸入密碼。

4. 確認 PrivateKeyEntry 的 alias name

在%JAVA_HOME%\bin 目錄下執行

keytool -list -keystore D:\.keystore

- 請依實際您存放檔案的位置調整指令。
- 待出現 Enter keystore password：請輸入密碼。
- 找到 PrivateKeyEntry 對應的 alias name，**範例為 weblogic**
- 若您的 keystore 沒有 PrivateKeyEntry，放入 server 後，SSL 也無法成功連線。請找出原 keystore 檔案，或是重新申請。



5. 匯入 SSL 伺服器應用軟體憑證。

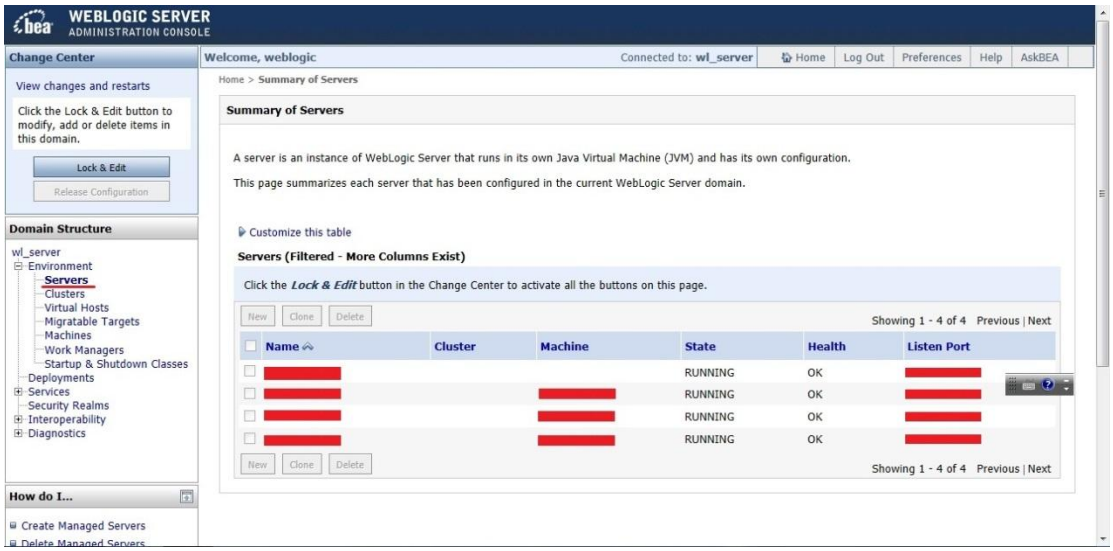
在%JAVA_HOME%\bin 目錄下執行

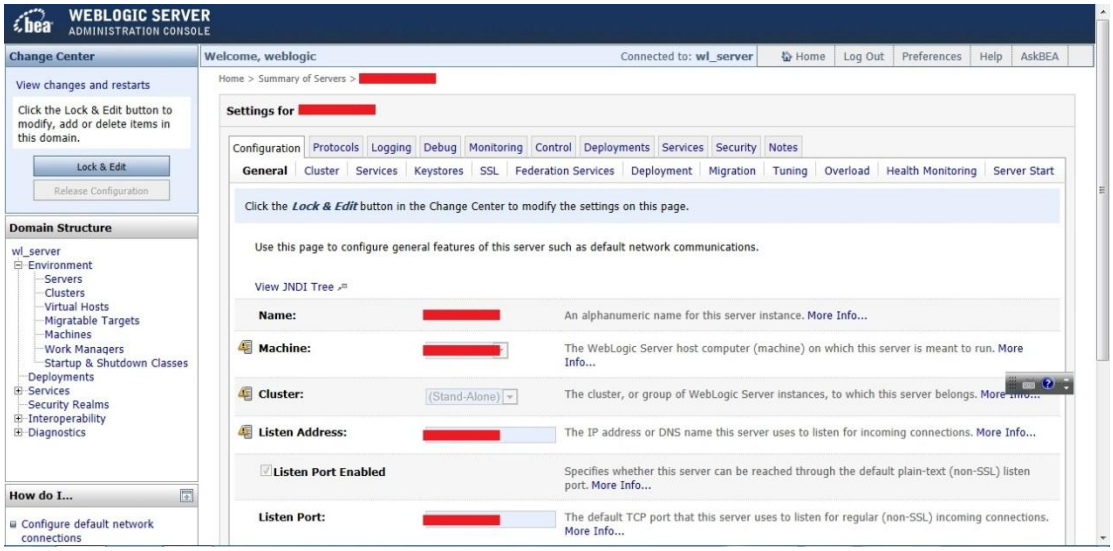
keytool -import -alias weblogic -file D:\5A4A7FB6FE24F6FFAC50A623568C6E9F.cer -keystore D:\.keystore

- 請依實際您存放檔案的位置調整指令。
- 待出現 Enter keystore password：請輸入密碼。

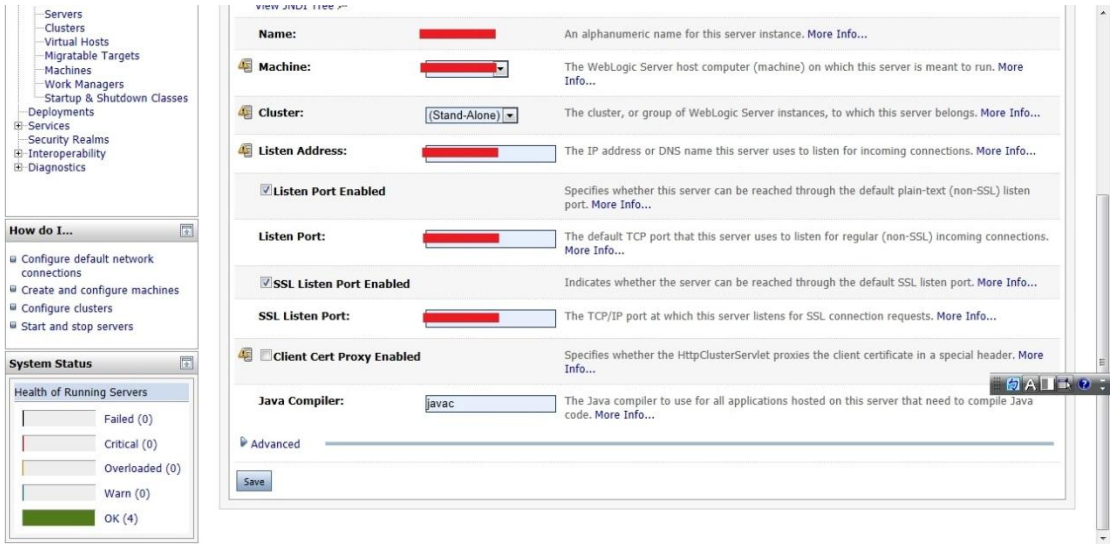
6. 修改 WebLogic https 參數設定

- 進入 WebLogic Console: 點選「Server」→選擇要安裝 SSL 憑證的 Server→點選「General」

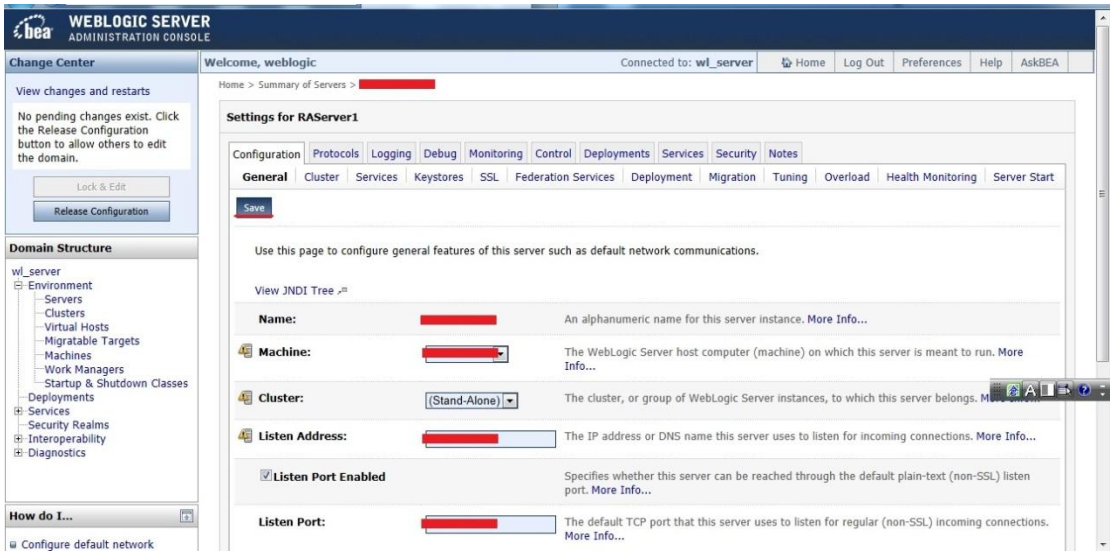




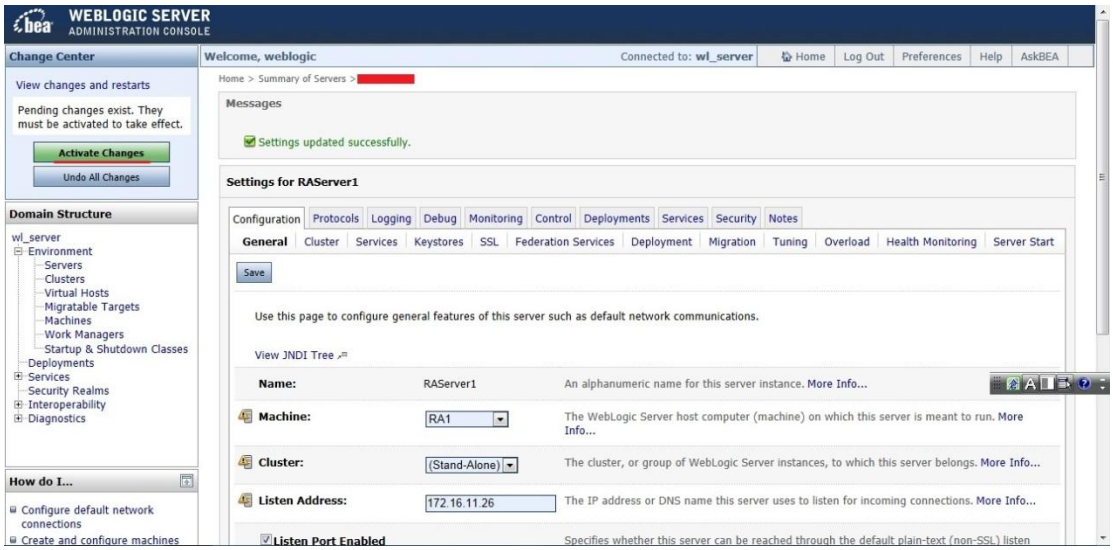
- 檢查 WebLogic 伺服器 SSL 連線的連接埠已經啟動：勾選「SSL Listen Port Enabled」

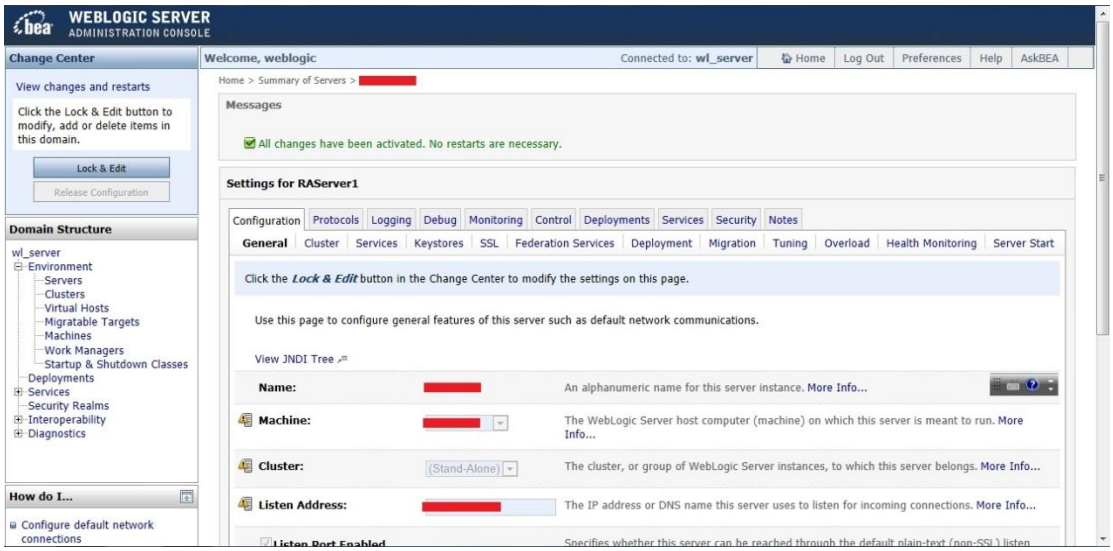


- 在頁面最上方或最下方點選「Save」

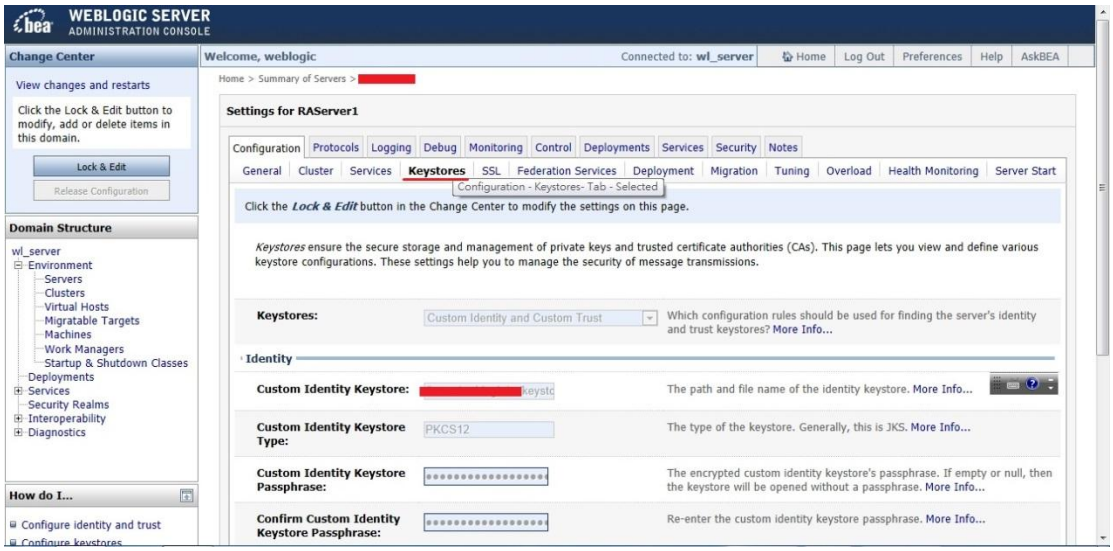


並在左上方選項點選「Activate Changes」

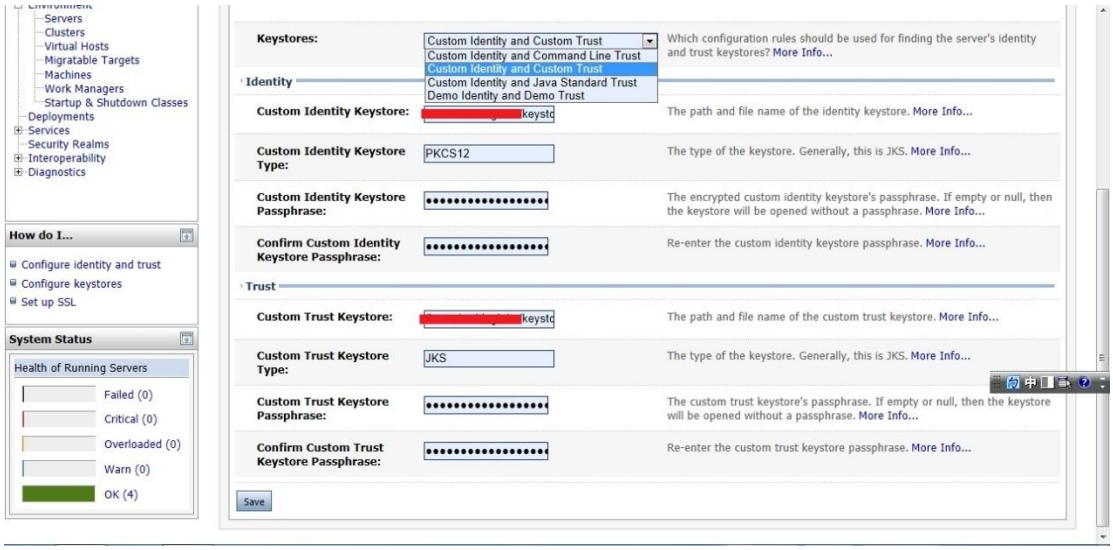




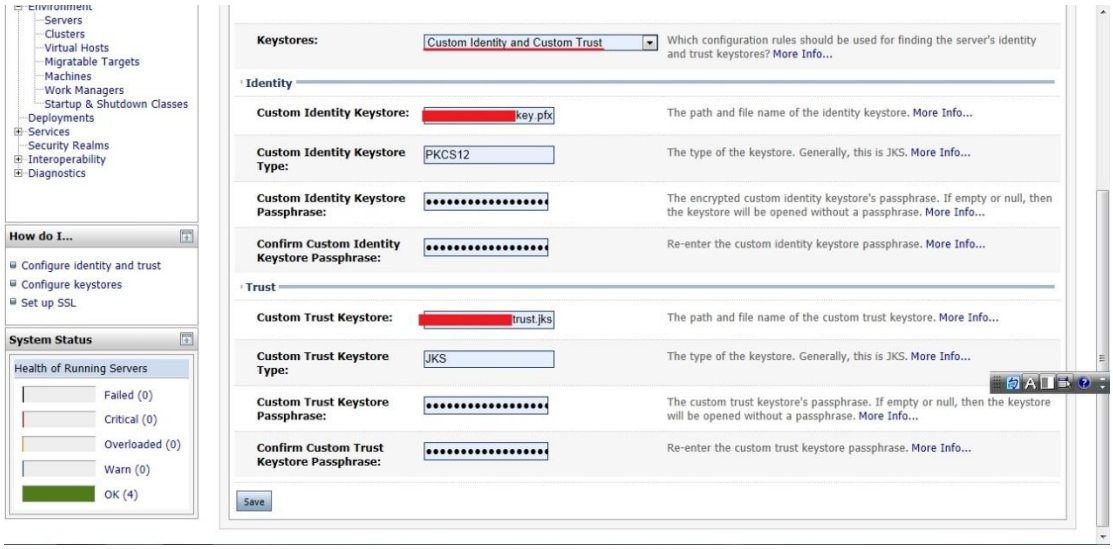
- 點選「Keystores」→點選左上方「Lock & Edit」



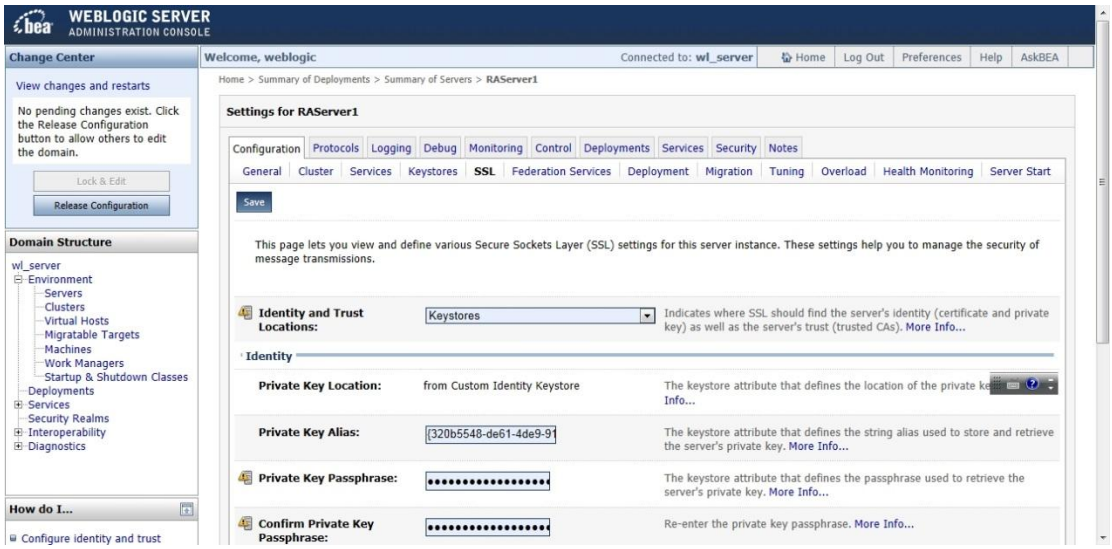
- 選擇「Custom Identity And Custom Trust」

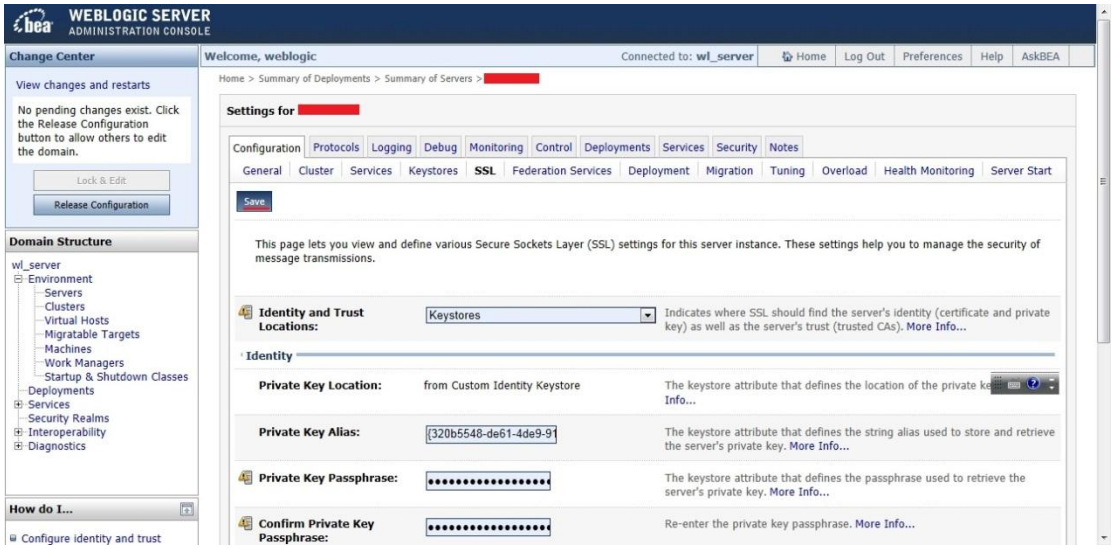


在頁面最上方或最下方點選「Save」

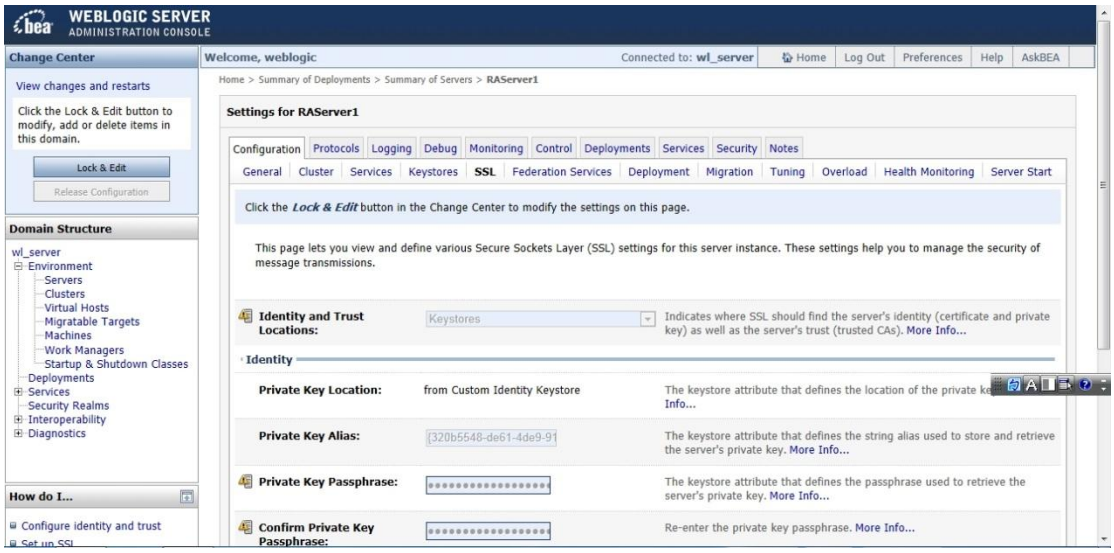


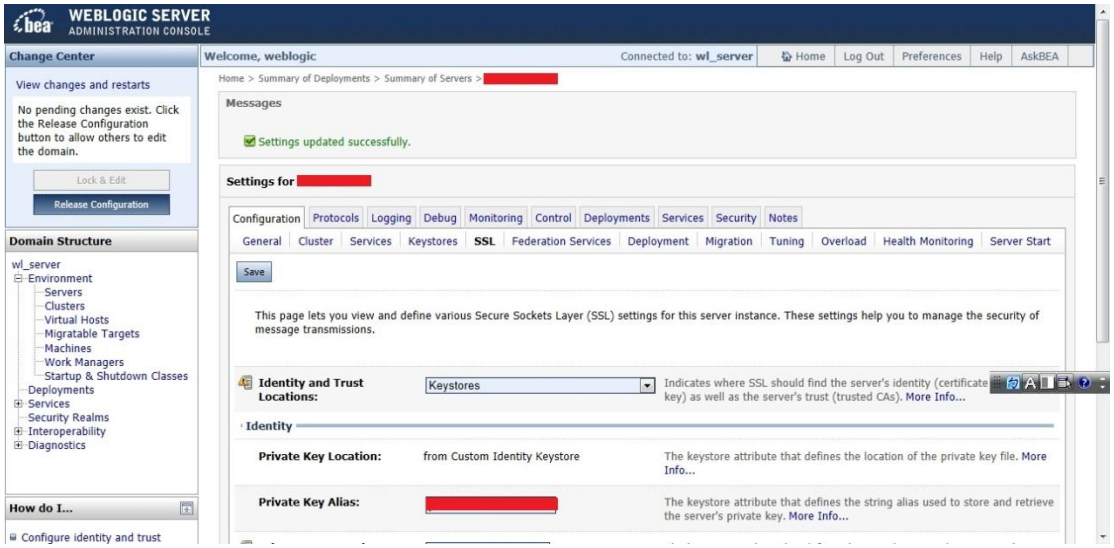
- 點選「SSL」→於「Private Key Alias」輸入私密金鑰的 alias 名稱，並點選「Save」





- 點選左上方選項「Activate Changes」





7. 重新啟動 WebLogic
8. 成功後，請以 https 連線試試加密通道。
9. **依照您的網路架構，您可能需要於防火牆開啟對應 https 的 port。**

三、安裝 SSL 安全認證標章：

請用戶參考技術聯絡人的電子郵件信箱所收到 SSL 憑證串鏈電子郵件內文的 SSL 安全認證標章安裝說明，將網站 SSL 安全認證標章安裝成功，網友可瀏覽您所維護網站所安裝 SSL 憑證的狀態與資訊。

請中華電信公司負責維護網站的同仁，參考從企業入口網站的電子表單之資訊表單「IS14-伺服器應用軟體憑證申請/異動單」所下載 SSL 憑證串鏈檔案中的 SSLSealispec.txt，將網站 SSL 安全認證標章安裝成功。