

中華電信通用憑證管理中心(PublicCA)

Weblogic 伺服器 SSL 憑證請求檔製作與憑證安裝手冊

聲明：本手冊之智慧財產權為中華電信股份有限公司（以下簡稱本公司）所有，本公司保留所有權利。本手冊所敘述的程序係將本公司安裝相關軟體的經驗分享供申請 SSL 伺服器軟體憑證用戶參考，若因參考本手冊所敘述的程序而引起的任何損害，本公司不負任何損害賠償責任。

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	2
Weblogic SSL 憑證安裝手冊	5
附件一：更換 SHA256 憑證.....	12

Weblogic SSL 憑證請求檔製作手冊

一、確認 Java 版本

- 1.1 由於 jBoss 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 eCA 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 eCA 憑證、PublicCA 憑證及 SSL 憑證視為 1 個憑證串鏈，結果在 SSL Handshake 中，PublicCA 憑證就不會被送到 Client 端，建議請使用最新版本的 Java(JDK)版本。

二、如何產生「金鑰對」

- 2.1 開啟命令提示字元。

- 2.2 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)。

- 若您非第一次申請憑證，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。

```
C:\Program Files\Java\jdk1.7.0_21\bin>keytool -genkey -alias weblogic -keyalg RSA -keysize 2048 -keystore D:\.keystore
輸入金鑰儲存庫密碼:
重新輸入新密碼:
您的名字與姓氏為何?
  [Unknown]: www.test.com.tw
您的組織單位名稱為何?
  [Unknown]: 政府網路處
您的組織名稱為何?
  [Unknown]: 中華電信股份有限公司數據分公司
您所在的城市或地區名稱為何?
  [Unknown]: Taipei
您所在的州及省份名稱為何?
  [Unknown]:
此單位的兩個字母國別代碼為何?
  [Unknown]: TW
CN=www.test.com.tw, OU=政府網路處, O=中華電信股份有限公司數據分公司, L=Taipei, S
T=Unknown, C=TW 正確嗎?
  [否]: Y
輸入 <weblogic> 的金鑰密碼
      <RETURN 如果和金鑰儲存庫密碼相同):
```

- 2.3 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)。

- 2.4 出現「您的名字與姓氏為何?」:請填入欲申請的網站名稱
ex: www.test.com.tw。
- 2.5 出現「您的組織單位名稱為何?」:請填入公司單位名稱。
- 2.6 出現「您的組織名稱為何?」:請填入公司名稱。
- 2.7 出現「您所在的城市或地區名稱為何?」:請填入公司所在地。
- 2.8 出現「您所在的州及省份名稱為何?」:可以不用輸入,按 Enter 跳過。
- 2.9 出現「此單位的兩個字母國別代碼為何?」:請填入 TW。
- 2.10 檢查所輸入的資料是否正確,若正確,請輸入 Y。
- 2.11 出現「輸入 <weblogic> 的金鑰密碼」:您可以按 Enter 讓金鑰儲存庫與金鑰密碼相同,或是獨立設定金鑰密碼,稍後再設定 weblogic 時,會需要輸入金鑰儲存庫密碼與金鑰密碼。

三、如何產製憑證請求檔

- 3.1 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>**

```
C:\Program Files\Java\jdk1.7.0_21\bin>keytool -certreq -alias weblogic -file D:\certreq.txt -keystore D:\.keystore  
輸入金鑰儲存庫密碼:
```

- 3.2 出現「輸入 keystore(金鑰儲存庫)密碼」:請輸入上一個步驟所設定的密碼。
- 3.3 請複製憑證請求檔(certreq.txt)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(以文字編輯器如記事本開啟憑證請求檔,全選及複製檔案內容,將憑證請求檔貼上 SSL 憑證申請網頁之表單。)。若屬於中華電信公司各單位申請 SSL 憑證者,請持憑證請求檔至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。
- 3.4 補充說明 1: 中華電信通用憑證管理中心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步驟 2.4-2.9 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)為準而記載於所簽發的 SSL 憑證裡面的欄位[如憑證主體名稱(Subject Name)或憑證主體別名(Subject Alternative Name)等欄位]。
- 3.5 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,所簽發的憑證會包含客戶之組織身分、完全吻合網域名稱與公開金鑰在憑證內。後續先安裝 SSL 憑證串鍊在產生憑證請求檔之站台,再將私密

金鑰與憑證備份匯入其他站台，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 憑證安裝手冊

一、下載憑證串鏈，包含 3 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：

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 3 個檔案，分別是 eCA 根憑證(檔名為 ROOTeCA_64.crt)、PublicCA 中繼憑證(檔名為 PublicCA2_64.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 3 個檔案。

2. 從網站查詢與下載：

eCA 憑證：

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

PublicCA G2 憑證：

http://epki.com.tw/download/PublicCA2_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。

二、安裝 SSL 憑證，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)

2.1 安裝 eCA Root 憑證。

在 %JAVA_HOME%\bin 目錄下執行

```
keytool -import -alias eCA -file D:\ROOTeCA_64.crt -keystore <keystore  
檔案所在路徑>
```

- 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。

2.2 安裝 PublicCA G2 憑證。

在 %JAVA_HOME%\bin 目錄下執行

```
keytool -import -alias PublicCA2 -file D:\PublicCA2_64.crt -keystore  
<keystore 檔案所在路徑>
```

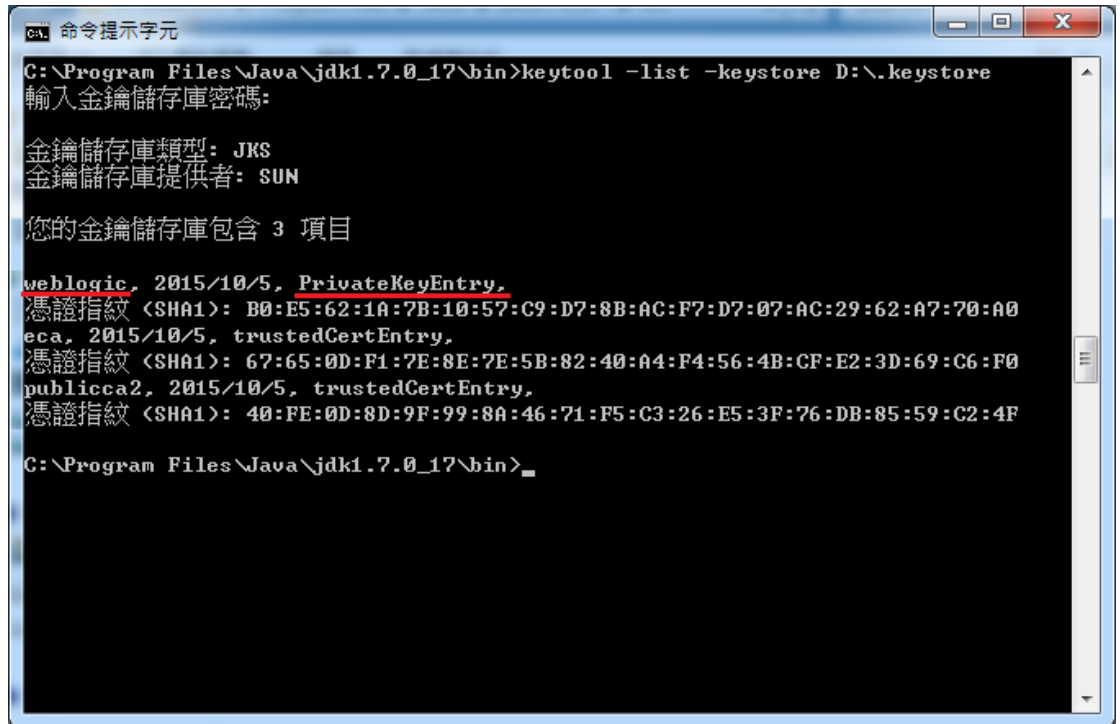
- 待出現 Enter keystore password：請輸入密碼。

2.3 確認 PrivateKeyEntry 的 alias name

在 %JAVA_HOME%\bin 目錄下執行

keytool -list -keystore <keystore 檔案所在路徑>

- 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。



```
ca. 命令提示字元
C:\Program Files\Java\jdk1.7.0_17\bin>keytool -list -keystore D:\.keystore
輸入金鑰儲存庫密碼:

金鑰儲存庫類型: JKS
金鑰儲存庫提供者: SUN

您的金鑰儲存庫包含 3 項目

weblogic, 2015/10/5, PrivateKeyEntry,
憑證指紋 (SHA1): B0:E5:62:1A:7B:10:57:C9:D7:8B:AC:F7:D7:07:AC:29:62:A7:70:A0
eca, 2015/10/5, trustedCertEntry,
憑證指紋 (SHA1): 67:65:0D:F1:7E:8E:7E:5B:82:40:A4:F4:56:4B:CF:E2:3D:69:C6:F0
publicca2, 2015/10/5, trustedCertEntry,
憑證指紋 (SHA1): 40:FE:0D:8D:9F:99:8A:46:71:F5:C3:26:E5:3F:76:DB:85:59:C2:4F

C:\Program Files\Java\jdk1.7.0_17\bin>
```

2.4 匯入 SSL 伺服器應用軟體憑證。

在 %JAVA_HOME%\bin 目錄下執行

keytool -import -alias <PrivateKeyEntry 的 alias name> -file D:\(憑證名稱.crt 或憑證名稱.cer) -keystore <keystore 檔案所在路徑>

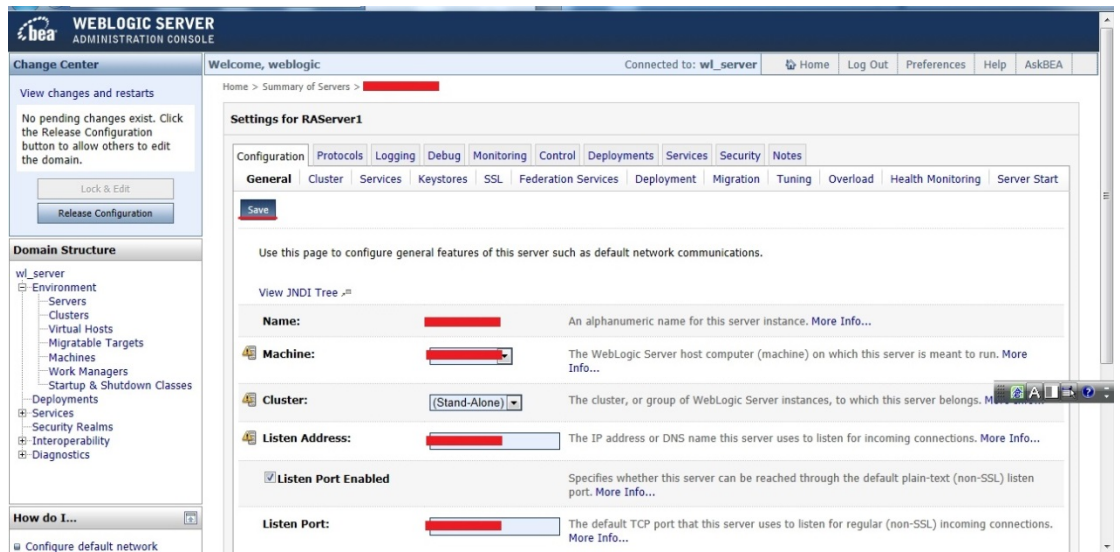
- 待出現 Enter keystore password：請輸入密碼。

2.5 修改 Weblogic https 參數設定

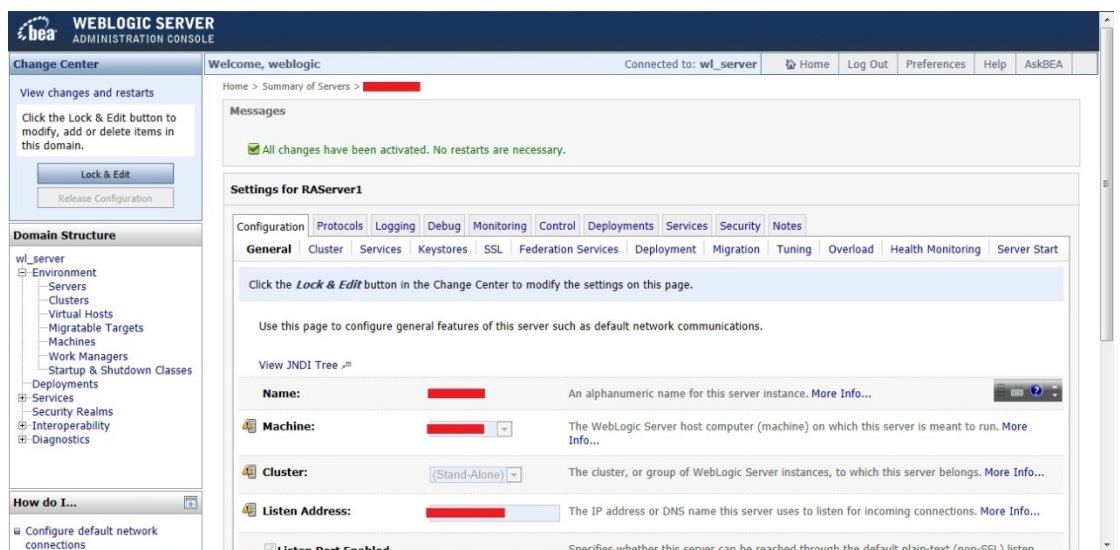
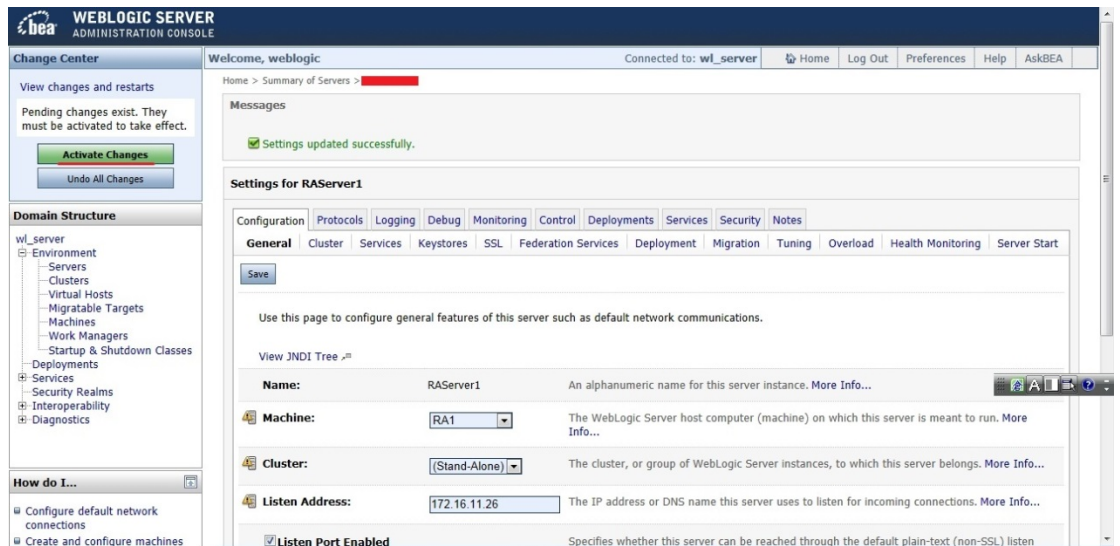
- 進入 Weblogic Console: 點選「Server」→選擇要安裝 SSL 憑證的 Server→點選「General」

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

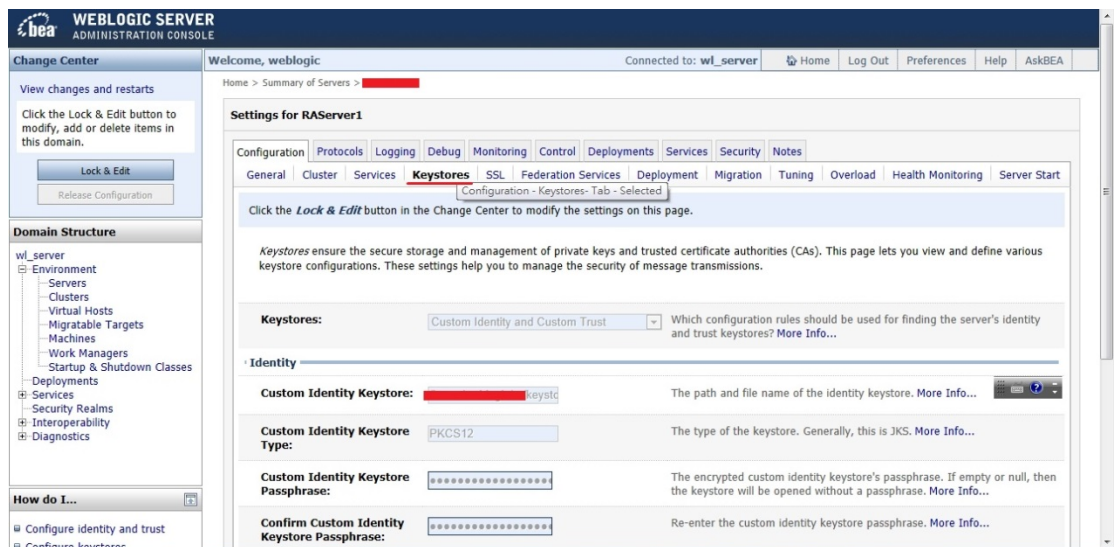
- 在頁面最上方或最下方點選「Save」



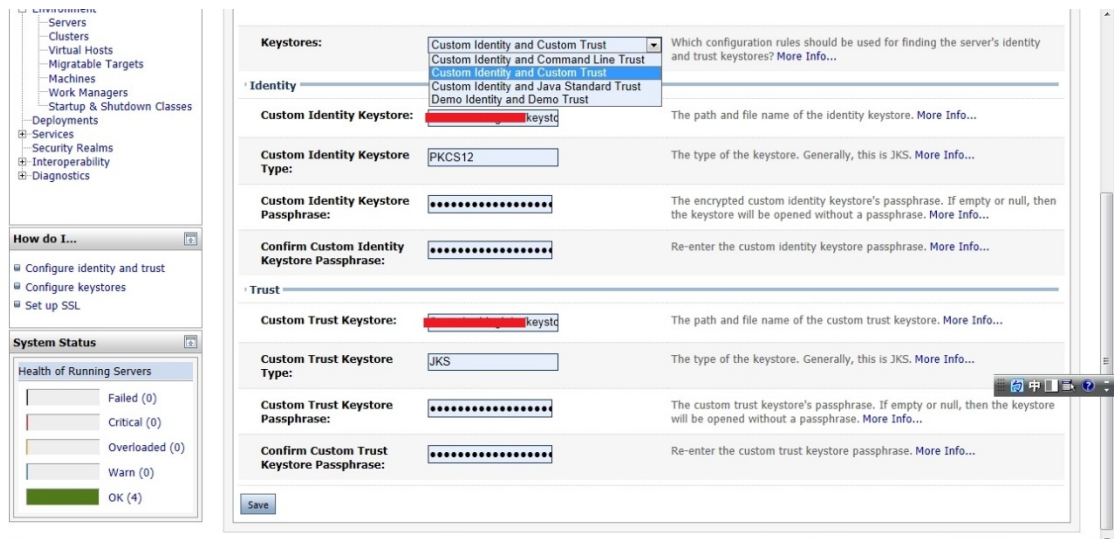
並在左上方選項點選「Activate Changes」



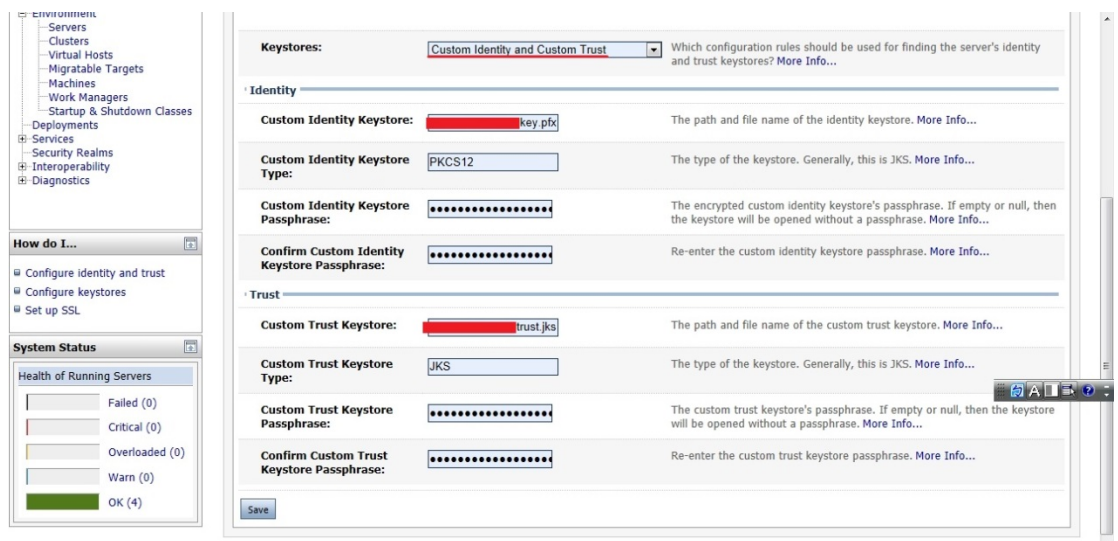
- 點選「Keystores」→點選左上方「Lock & Edit」



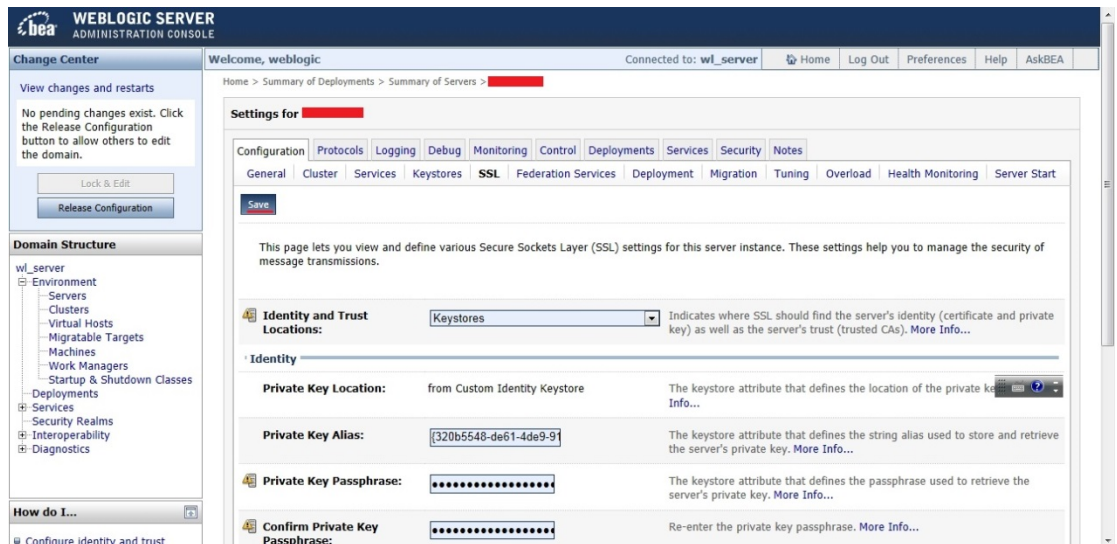
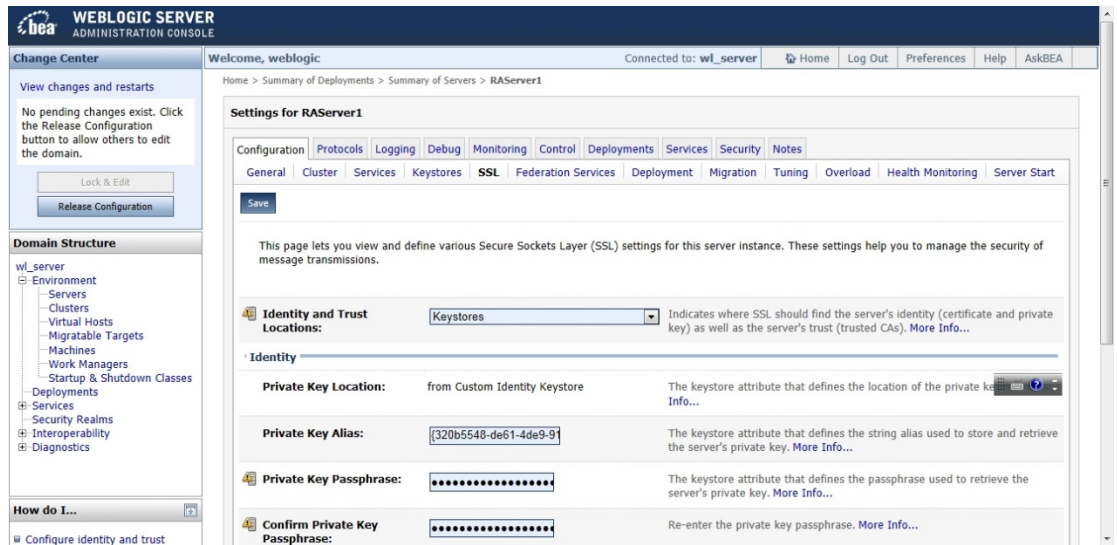
- 選擇「Custom Identity And Custom Trust」



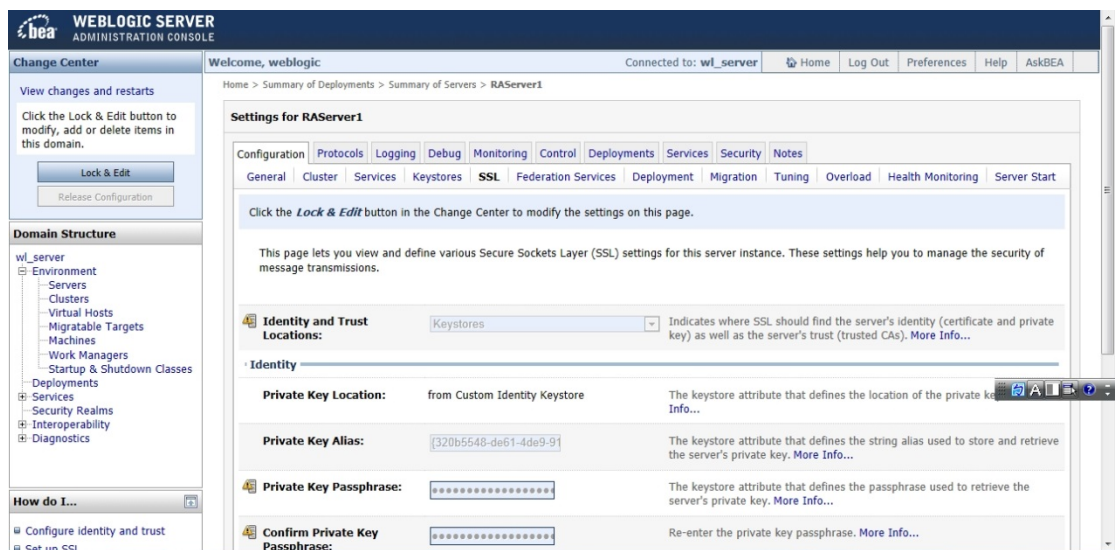
在頁面最上方或最下方點選「Save」

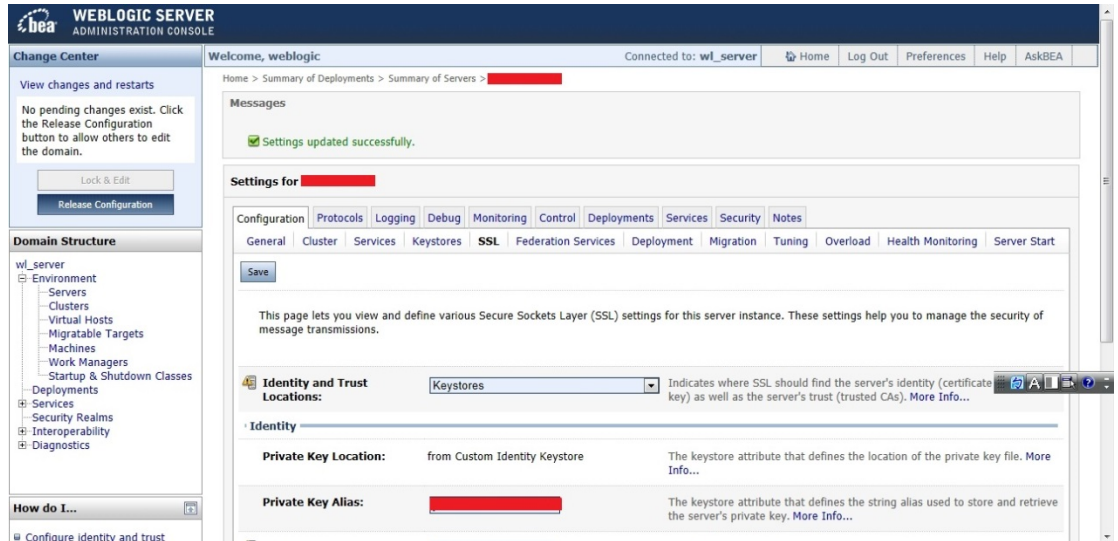


- 點選「SSL」→於「Private Key Alias」輸入私密金鑰的 alias 名稱，並點選「Save」



- 點選左上方選項「Activate Changes」





- 最後請將 Weblogic 重新啟動，並以 https 連線測試 SSL 加密通道。
- 依照您的網路架構，您可能需要於防火牆開啟對應 https 的 port。

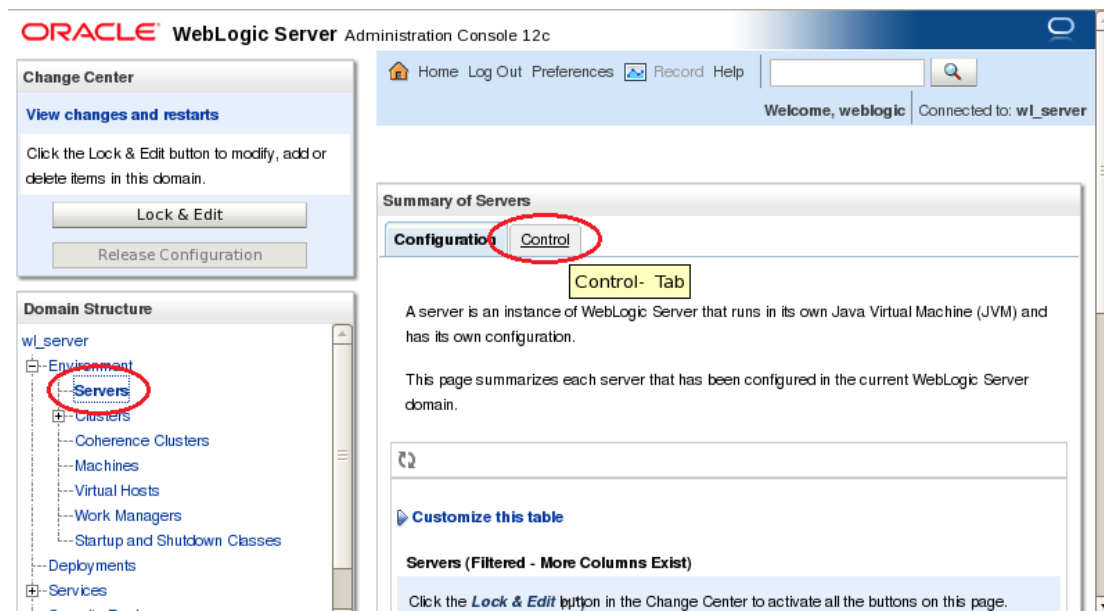
三、安裝 SSL 安全認證標章：

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。您也可參考 <http://publicca.hinet.net/SSL-01.htm> 下方有 SSL 安全認證標章之安裝說明。

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。

附件一：更換 SHA 256 憑證

- 適用於申請時，有同時取得 SHA-1、SHA 256 憑證。或是憑證在效期內，經由審驗人員再次核發 SHA 256 憑證者。
- 需要檔案：
 - 線上在使用的 .keystore 檔
 - PublicCA G2 中繼憑證：可於 zip 檔中取得
 - SHA256 用戶端憑證
- 安裝步驟：
 - **安裝 eCA Root 憑證。**（之前已安裝過，此步驟可忽略）
在 %JAVA_HOME%\bin 目錄下執行
keytool -import -alias eCA -file D:\ROOTeCA_64.crt -keystore D:\.keystore
 - **安裝 PublicCA G2 憑證。**
在 %JAVA_HOME%\bin 目錄下執行
keytool -import -alias PublicCAG2 -file D:\PublicCA2_64.crt -keystore D:\.keystore
 - **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:\(憑證名稱.crt 或憑證名稱.cer) -keystore D:\.keystore
- 最後請重新啟動 server 的 SSL，並以 https 連線測試 SSL 加密通道。



Domain Structure

- wl_server
 - Environment
 - Servers
 - Clusters
 - Coherence Clusters
 - Machines
 - Virtual Hosts
 - Work Managers
 - Startup and Shutdown Classes
 - Deployments
 - Services
 - Security Realms

How do I...

- Start and stop servers
- Start Managed Servers from the Administration Console
- Start Managed Servers in Admin mode
- Start Managed Servers in a cluster
- Configure the domain-wide administration port

Use this page to change the state of the servers in this WebLogic Server domain. Control operations on Managed Servers require starting the Node Manager. Starting Managed Servers in Standby mode requires the domain-wide administration port.

Customize this table

Servers (Filtered - More Columns Exist)

Start Resume Suspend v

Showing 1 to 4 of 4 Previous | Next

Shutdown v Restart SSL

	Server	Machine	State	Status of Last Action
<input type="checkbox"/>	Server1	Server1	RUNNING	None
<input checked="" type="checkbox"/>	Server2	Server2	RUNNING	None

Start Resume Suspend v

Showing 1 to 4 of 4 Previous | Next

Shutdown v Restart SSL

ORACLE WebLogic Server Administration Console 12c

Home Log Out Preferences Record Help

Welcome, weblogic Connected to: wl_server

Home > Summary of Servers

Server Life Cycle Assistant

Restart SSL Channels

You have selected the following servers to restart SSL and channels. Press 'Yes' to continue or 'No' to cancel.

- Server2

ORACLE WebLogic Server Administration Console 12c

Home Log Out Preferences Record Help

Welcome, weblogic Connected to: wl_server

Home > Summary of Servers

Messages

✔ SSL channels have been successfully restarted.

Summary of Servers

Configuration **Control**

Use this page to change the state of the servers in this WebLogic Server domain. Control operations on Managed Servers require starting the Node Manager. Starting Managed Servers in Standby mode requires the domain-wide administration port.

Customize this table

Servers (Filtered - More Columns Exist)

Start Resume Suspend v