

臺灣網路認證股份有限公司 TAIWAN-CA. Inc. 台北市 100 延平南路 85 號 10 樓 電話:02-2370-8886 傳真:02-2370-0728 www.twca.com.tw

機密等級:公開 版本:V5.0 文件編號:MNT-03-161 生效日期: 109年3月3日

# 目 錄

1.目的	1
2.範圍	2
3.参考資料	3
4.定義	4
5.作業程序	5
5.1 IIS 轉 TOMCAT 格式	5
5.2 TOMCAT 轉 IIS 格式	17
6.附件	

本資料為臺灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或 轉變成任何其他形式使用。 The information contained herein is the exclusive property of TWCA and shall not be distributed

## 1.目的

- 1.1. 介紹 SSL 憑證 IIS 及 Tomcat 格式互轉步驟及 SSL 伺服器數位憑證安 裝說明。
- 1.2. 符合本公司資訊安全政策之規範。

# 2.範圍

2.1. 本操作手册適用於 IIS 或 Tomcat 伺服器憑證格式互轉。

# 3.参考資料

魚。

本資料為臺灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉變成任何其他形式使用。 The information contained herein is the exclusive property of TWCA and shall not be distributed,

# 4.定義

無。

## 5.作業程序

- 5.1 IIS 轉 TOMCAT 格式
  - 5.1.1 新增憑證管理單元
  - 5.1.1.1 開啟 MMC 主控台

點選	開始	→點選	執行	→輸入	mmc	並按下	確定	0
----	----	-----	----	-----	-----	-----	----	---

	×
輸入程式、資料夾、文件或網際網路資源的名稱,Wind 會自動開啟。	OWS
mmc	•
必須有系統管理權限才能建立此工作。	
確定 取消 瀏覽(B)	
0	輸入程式、資料夾、文件或網際網路資源的名稱,Wind 會自動開啟。 ◎ 必須有系統管理權限才能建立此工作。 ■ 確定 取消 瀏覽(8)

🧱 主控台1 - [主控台根目錄]		
🚰 檔案 E 執行 (A) 檢視 (V) 我的最愛 (○) 視窗 (W) 說明 (H)		_8×
□□ 主控台根目録 名稱 □	動作	
這個檢視沒有項目可顯示。	主控台根目錄	*
	其他動作	•

5.1.1.2 新增/移除嵌入式管理單元

點選檔案→點選新增/移除嵌入式管理單元。



5.1.1.4 新增憑證管理單元(2)

選擇電腦帳戶→點選下一步。



5.1.1.5 新增憑證管理單元(3)

點選本機電腦(執行這個主控台的電腦)→點選完成。



5.1.1.6 新增憑證管理單元完成



#### 5.1.2 匯出憑證

5.1.2.1 點選展開主控台根目錄內的憑證(本機電腦)→個人→憑證,在 欲匯出的伺服器憑證上按右鍵所有工作→點選匯出。



5.1.2.2 啟動歡迎使用憑證匯出精靈→點選下一步。





## 5.1.2.4 點選個人資訊交換-PKCS#12(.PFX)→勾選如果可能的話,包含 憑證中所有的憑證→點選下一步。





匯入憑證時需使用)



# 5.1.2.6 點選瀏覽→指定一個匯出檔案存放的路徑與檔名(副檔名固定 為.PFX)→點選下一步。

÷	☞ 憑證匯出精靈	×
	要匯出的檔案 請指定您要匯出的檔案名稱	
	檔案名稱(E): C:\Users\Administrator\mypfxfile.pfx	)
	下-步(N) !	取消

	<b>今出准述际</b> 中转叠
	元成認識性自己相思
	您已經成功地完成憑證匯出精靈。
100 - Contraction - Contractio	您已指定下列新設定:
	檔案名稱 C:\Users\Administrator'   匯出金鑰 是   包含憑證路徑中的所有憑證 是   檔案格式 個人資訊交換 (*.pfx)
	<上一步(B) 完成 取消
3. 西田精靈 王	
出成功。	

5.1.3 使用 JAVA keytool 軟體將 PFX 檔轉換 JKS 金鑰資料庫檔

keytool -importkeystore -srckeystore mypfxfile.pfx -

srcstoretype pkcs12 -destkeystore clientcert.jks -

deststoretype JKS

mypfxfile.pfx:由 IIS 匯出之金鑰憑證交換檔絕對路徑

clientcert.jks:將 mypfxfile.pfx 轉換成 JKS 金鑰資料庫輸出之檔案路徑與名稱



#### 設定 mykeystore.jks 密碼(建議跟第七頁匯出 pfx 所設的密碼一致)



#### 再次輸入 mykeystore.jks 密碼(建議跟第七頁匯出 pfx 所設的密碼一致)

**國命令提示字元 - keytool -importkeystore -srckeystore D:\mypfxfile.pfx -srcstoretype pkcs12 -destkey... \_□>**× C:\Users\tas191>keytool -importkeystore -srckeystore D:\mypfxfile.pfx -srcstoret▲ ype pkcs12 -destkeystore C:\mykeystore.jks -deststoretype JKS 請輸入目的地金鑰儲存庫密碼: 重新輸入新密碼:

#### 輸入 mykeystore.pfx 密碼(第七頁匯出 pfx 所設的密碼)

**○ 命令提示字元 - keytool -importkeystore -srckeystore D:\mypfxfile.pfx -srcstoretype pkcs12 -destkey... \_□ ×** C:\Users\tas191>keytool -importkeystore -srckeystore D:\mypfxfile.pfx -srcstoret▲ ype pkcs12 -destkeystore C:\mykeystore.jks -deststoretype JKS 請輸入目的地金鑰儲存庫密碼: 重新輸入新密碼: 請輸入來源金鑰儲存庫密碼: \_輸入 mykeystore.pfx 密

#### 匯出成功



本資料為臺灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉變成任何其他形式使用。 The information contained herein is the exclusive property of TWCA and shall not be distributed,

5.1.4 匯入憑證鏈

5.1.4.1 將憑證鏈檔(根憑證 root.cer、中繼憑證 uca.cer)存放至%JDK%\bin

目錄下(實際目錄可自行決定)。

5.1.4.2 請將憑證由上至下(根憑證 root.cer、中繼憑證 uca.cer)一一匯入金鑰

儲存庫。

5.1.4.2.1 匯入根憑證 root.cer

keytool -import -trustcacerts -alias root -file root.cer -keystore C:\mykeystore.jks

C:\Program Files\Java\jdk1.8.0\_191\bin>keytool -import -trustcacerts -alias root -file root.cer -keystore C:\mykeystore.jks

指令參數說明如下(指令反白部份請依實際配置決定)

參數	說 明
-import	匯入憑證必要指令
-	建立為信任的憑證鏈
trustcacerts	
-alias	設定根憑證別名,請自行決定即可
-file	要匯入的根憑證路徑及名稱,請依實際位置指定
-keystore	keystore 檔案所在路徑及名稱,請依實際位置指定

#### 輸入金鑰儲存庫密碼: 重新輸入新密碼・

此時會要求輸入金鑰儲存庫密碼,請直接輸入金鑰儲存庫密碼並確認

# 信任這個憑證? [否]:

如出現上面訊息,請輸入 y 再按 Enter 即可,

## 憑證已新增至金鑰儲存庫中

出現「憑證已新增至金鑰儲存庫中」即匯入完成。

#### 5.1.4.2.2 匯入中繼憑證 uca.cer

keytool -import -trustcacerts -alias uca -file uca.cer -keystore C:\mykeystore.jks

本資料為臺灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉變 成任何其他形式使用。

#### C:\Program Files\Java\jdk1.8.0\_191\bin>keytool -import -trustcacerts -alias uca file uca.cer -keystore C:\mykeystore.jks

指令參數說明如下(指令反白部份請依實際配置決定)

參數	說 明
-import	匯入憑證必要指令
-	建立為信任的憑證鏈
trustcacerts	
-alias	設定中繼憑證別名,請自行決定即可
-file	要匯入的中繼憑證路徑及名稱,請依實際位置指定
-keystore	keystore 檔案所在路徑及名稱,請依實際位置指定

### 輸入金鑰儲存庫密碼:

此時會要求輸入金鑰儲存庫密碼,請直接輸入金鑰儲存庫密碼,

### 憑證已新增至金鑰儲存庫中

出現「憑證已新增至金鑰儲存庫中」即匯入完成。

5.1.5 使用 keytool 檢視 JKS 金鑰資料庫檔案內容

keytool -v -list -keystore mykeystore.jks mykeystore.jks:將 mypfxfile.pfx 轉換成 JKS 金鑰資料庫輸出之檔案路徑與名稱



#### 輸入 mykeystore.jks 檔密碼

📾 命令提示字元 - keytool -v -list -keystore D:\clientcert.jks	_ 🗆 🗙
<b>C:\Users\tas191&gt;keytool -v -list -keystore</b> C:\mykeystore.jks 輸入金鑰儲存庫密碼:	

即可檢視 mykeystore.jks 檔內容,金鑰儲存庫項目必須大於1為正常

本資料為臺灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉變 成任何其他形式使用。

_	C:\Program Files\Java\jdk1.8.0_191>keytool -list -keystore C:\mykeystore.jks 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
金鑰別名	root, 2018/11/27, trustedCertEntry, 憑證指紋 (SHA1): CF:9E:87:6D:D3:EB:FC:42:26:97:A3:B5:A3:7A:A0:76:A9:06:23:48 uca, 2018/11/27, trustedCertEntry, 憑證指紋 (SHA1): FD:54:E4:64:3B:49:70:5A:2A:AA:E5:06:53:C4:F5:6C:2D:F8:08:3D keyname, 2018/11/27, PrivateKeyEntry, 憑證指紋 (SHA1): 99:AC:40:24:F6:D9:4C:0B:00:43:AB:39:3D:92:EA:5A:6E:D3:9E:4F

5.1.6 調整設定

5.1.6.1 接著請依您的伺服器版本進行 SSL 及憑證的設定。

本資料為臺灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉變成任何其他形式使用。 The information contained herein is the exclusive property of TWCA and shall not be distributed,

5.2 TOMCAT 轉 IIS 格式

5.2.1 利用 keytool 將 JKS 轉換成 PFX,指令如下:(來源、目的金鑰儲存庫 的密碼都用同一組)

keytool -importkeystore -srckeystore {JKS 檔案路徑} -destkeystore {PFX 檔案路徑}

-srcalias {JKS 金鑰別名} -srcstoretype jks -deststoretype pkcs12

C:\Users\tas191>keytool -importkeystore -srckeystore D:\test.jks -destkeystore D :\mytest.pfx -srcalias keyname -srcstoretype jks -deststoretype pkcs12 請輸入目的地金鑰儲存庫密碼: 重新輸入新密碼: 請輸入來源金鑰儲存庫密碼:

5.2.2 參考 IIS 操作手冊,從匯入憑證鏈(根憑證、中繼憑證、伺服器憑證)章 節繼續完成所有憑證安裝步驟,其中伺服器憑證就是剛剛匯出的 mytest.pfx。

本資料為臺灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉變成任何其他形式使用。 The information contained herein is the exclusive property of TWCA and shall not be distributed,

# 6.附件

魚。

本資料為臺灣網路認證股份有限公司專有之財產,非經書面許可,不准透露或使用本資料,亦不准複印,複製或轉變成任何其他形式使用。 The information contained herein is the exclusive property of TWCA and shall not be distributed,