



# SSL 數位憑證

Tomcat 5.x / 6.x / 7.x 安裝說明

## 目錄

一、 產生憑證請求檔.....	1
二、 憑證安裝.....	2
1. 安裝憑證 - 由 CSR 申請的憑證.....	2
2. 安裝憑證 - 由線上申請的憑證.....	3
3. 設定 server.xml 設定檔.....	3
4. 重啟 tomcat service.....	3
三、 憑證匯出 ( 伺服器憑證匯出 ).....	4
1. Windows.....	4
2. UNIX.....	4

## 一、產生憑證請求檔

### 1. 執行下列命令產生 Keystore file

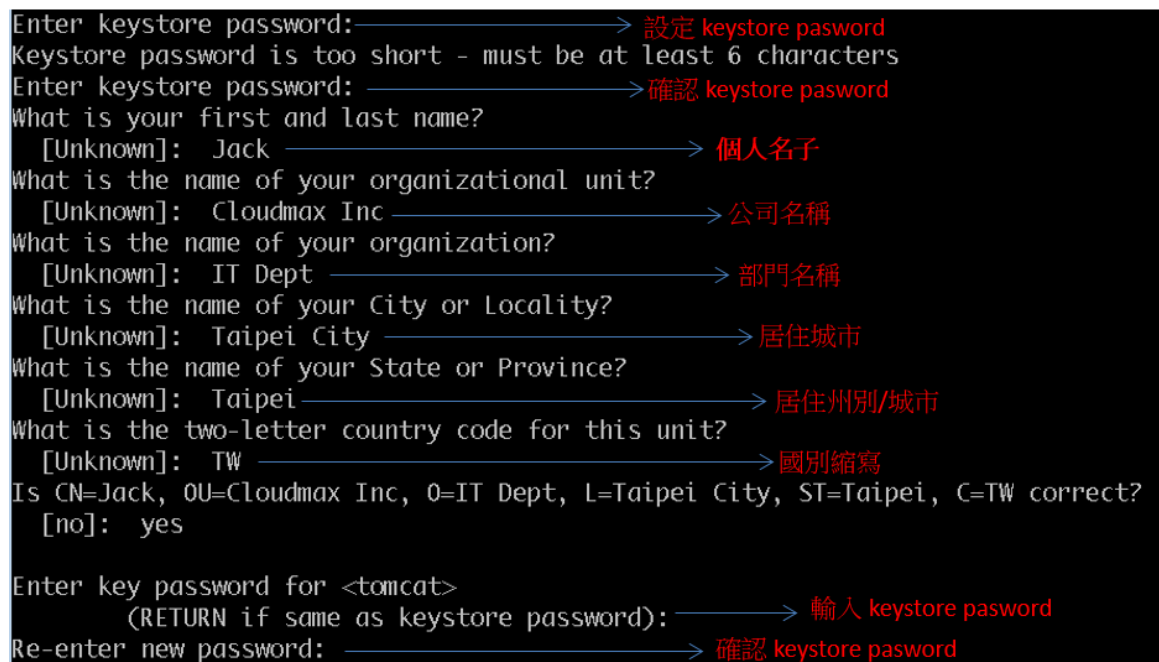
[ Windows ]

```
%JAVA_HOME%\bin\keytool -genkey -alias <your_keystore_filename> -keyalg RSA -  
keysize 2048 -keystore <your_keystore_filename>
```

[ CentOS or RedHat ]

```
$JAVA_HOME/bin/keytool -genkey -alias <your_keystore_filename> -keyalg RSA -  
keysize 2048 -keystore <your_keystore_filename>
```

### 2. 輸入憑證資訊



```
Enter keystore password: _____ → 設定 keystore password  
Keystore password is too short - must be at least 6 characters  
Enter keystore password: _____ → 確認 keystore password  
What is your first and last name?  
[Unknown]: Jack _____ → 個人名子  
What is the name of your organizational unit?  
[Unknown]: Cloudmax Inc _____ → 公司名稱  
What is the name of your organization?  
[Unknown]: IT Dept _____ → 部門名稱  
What is the name of your City or Locality?  
[Unknown]: Taipei City _____ → 居住城市  
What is the name of your State or Province?  
[Unknown]: Taipei _____ → 居住州別/城市  
What is the two-letter country code for this unit?  
[Unknown]: TW _____ → 國別縮寫  
Is CN=Jack, OU=Cloudmax Inc, O=IT Dept, L=Taipei City, ST=Taipei, C=TW correct?  
[no]: yes  
  
Enter key password for <tomcat>  
(RETURN if same as keystore password): _____ → 輸入 keystore password  
Re-enter new password: _____ → 確認 keystore password
```

### 3. 產生憑證請求檔(CSR)

[ Windows ]

```
%JAVA_HOME%\bin\keytool -certreq -keyalg RSA -alias <your_domain_name> -file  
<your_csr_name> -keystore <your_keystore_filename>
```

[ CentOS or RedHat ]

```
$JAVA_HOME/bin/keytool -certreq -keyalg RSA -alias <your_domain_name> -file  
<your_csr_name> -keystore <your_keystore_filename>
```

## 二、憑證安裝

### 1. 安裝憑證 – 由 CSR 申請的憑證

#### 1.1 安裝根憑證

[ Windows ]

```
%JAVA_HOME%\bin\keytool-import -alias <your_root_ca_name>-keystore  
<your_keystore_filename>-trustcacerts-file <your_root_filename>
```

[ CentOS or RedHat ]

```
$JAVA_HOME/bin/keytool -import -alias <your_root_ca_name>-keystore  
<your_root_ca_name>-trustcacerts-file <your_root_filename>
```

#### 1.2 安裝中繼憑證

[ Windows ]

```
%JAVA_HOME%\bin\keytool -import-alias "intermed"-keystore  
<your_keystore_filename>-trustcacerts-file  
<your_intermediate_certificate_filename>
```

[ CentOS or RedHat ]

```
$JAVA_HOME/bin/keytool-import-alias " intermed "-keystore  
<your_keystore_filename>-trustcacerts-file  
<your_intermediate_certificate_filename>
```

#### 1.3 安裝伺服器憑證

[ Windows ]

```
%JAVA_HOME%\bin\keytool-import-keystore <your_keystore_filename>-  
trustcacerts-file <your_name_of_the_certificate_filename>
```

[ CentOS or RedHat ]

```
$JAVA_HOME/bin/keytool-import-keystore <your_keystore_filename>-  
trustcacerts-file <your_name_of_the_certificate_filename>
```

## 2. 安裝憑證 - 由線上申請的憑證

### 2.1 將憑證資料轉換成 PKCS12 格式

```
openssl pkcs12 -export -in <your_server_cert>-inkey <your_server_key> -certfile  
<your_root_ca_cert> poc.cludmax.com.tw.p12
```

### 2.2 將 PKCS12 轉成 JKS 檔案格式

```
keytool -importkeystore -srckeystore <your_cert_p12_filepath> -destkeystore  
<your_keystore_filepath> -srcstoretype pkcs12
```

## 3. 設定 server.xml 設定檔

```
<  
Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"  
maxThreads="150" scheme="https" secure="true"  
clientAuth="false" sslProtocol="TLS"  
keystoreFile="<your_keystore_filepath>" keystorePass=" your_keystore_password"  
>
```

## 4. 重啟 tomcat service

### 三、憑證匯出 ( 伺服器憑證匯出 )

#### 1. Windows

```
%JAVA_HOME%/bin/keytool-export-keystore <your_keystore_filename>-alias  
<your_name_of_the_certificate>-file <your_certificate_filename>
```

#### 2. UNIX

```
$JAVA_HOME/bin/keytool-export-keystore <your_keystore_filename>-alias  
<your_name_of_the_certificate>-file <your_certificate_filename>
```