

匯智資訊股份有限公司

SSL 數位憑證

Tomcat 5.x / 6.x / 7.x 憑證安裝說明

【版權及商標聲明】

本文件由 Cloudmax 匯智製作，並保留所有權利。

文件提供之安裝步驟僅供參考，詳細狀況依伺服器版本或所在網路環境、架構而有些微差別，請依實際狀況或系統提供商資訊為準，若於安裝上有任何問題可與我們聯繫，將有專員引導您排除障礙。

本文件所引用之各商標及商品名稱分屬其合法註冊公司所有，絕無侵權之意，特此聲明。

【有限擔保責任聲明】

Cloudmax 匯智盡力製作本說明文件其正確性，但不擔保本文件無任何瑕疵，亦不為使用本說明文件而引起之衍生利益損失或意外損毀之損失擔保責任。若對本文件有任何疑問與建議，可利用下方資訊與我們聯繫：

電話：+886-2-2718-7200

傳真：+886-2-2718-1922

信箱：service@cloudmax.com.tw

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

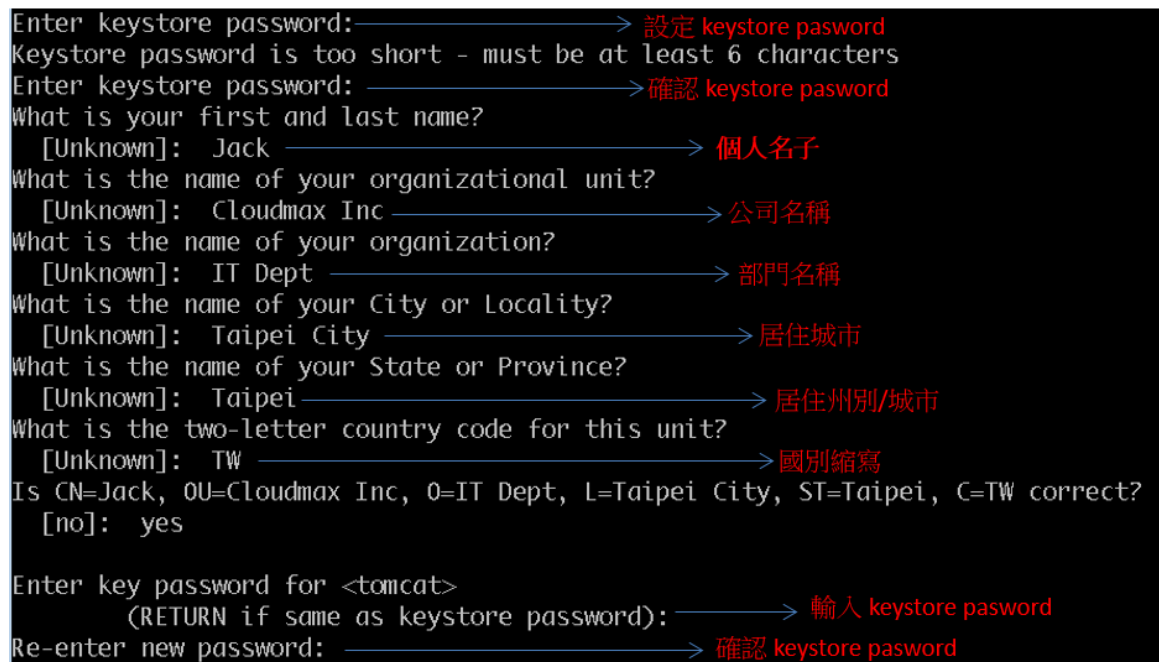
[Windows]

```
%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 pasword  
Keystore password is too short - must be at least 6 characters  
Enter keystore password: _____> 確認 keystore pasword  
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 pasword  
Re-enter new password: _____> 確認 keystore pasword
```

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> -out 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>
```