

# 重新生成CUCM IM/P服務自簽名證書

## 目錄

---

### [簡介](#)

### [必要條件](#)

#### [需求](#)

#### [採用元件](#)

### [背景資訊](#)

#### [證書儲存利用率](#)

##### [Cisco Unified Presence \(CUP\)證書](#)

##### [Cisco Unified Presence -可擴展消息傳送和線上狀態協定\(CUP-XMPP\)證書](#)

##### [Cisco Unified Presence -可擴展消息傳送和線上狀態協定-伺服器到伺服器\(CUP-XMPP-S2S\)證書](#)

##### [IP安全\(IPSec\)憑證](#)

##### [Tomcat憑證](#)

### [憑證重新產生程式](#)

#### [CUP證書](#)

#### [CUP-XMPP證書](#)

#### [CUP-XMPP-S2S證書](#)

#### [IPSec憑證](#)

#### [Tomcat憑證](#)

### [刪除過期的信任憑證](#)

### [驗證](#)

### [疑難排解](#)

---

## 簡介

本文檔介紹在CUCM IM/P 8.x及更高版本中如何重新生成證書的建議分步過程。

## 必要條件

### 需求

思科建議您瞭解IM & Presence (IM/P)服務憑證。

### 採用元件

本文檔中的資訊基於IM/P版本8.x及更高版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 ( 預設 ) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

## 證書儲存利用率

### Cisco Unified Presence (CUP)證書

用於SIP聯合的安全SIP連線、用於Lync/OCS/LCS的Microsoft遠端呼叫控制、Cisco Unified Certificate Manager (CUCM)與IM/P之間的安全連線等。

### Cisco Unified Presence - 可擴展消息傳送和線上狀態協定(CUP-XMPP)證書

用於在XMPP會話建立時驗證XMPP客戶端的安全連線。

### Cisco Unified Presence - 可擴展消息傳送和線上狀態協定-伺服器到伺服器(CUP-XMPP-S2S)證書

用於驗證與外部聯合XMPP系統的XMPP域間聯合的安全連線。

### IP安全(IPSec)憑證

用於：

- 驗證災難恢復系統(DRS)/災難恢復架構(DRF)的安全連線
- 驗證IPSec隧道到集群中思科統一通訊管理器(CUCM)和IM/P節點的安全連線

### Tomcat憑證

用於：

- 驗證各種Web訪問，例如從群集中的其他節點訪問服務頁面和Jabber訪問。
- 驗證SAML單點登入(SSO)的安全連線。
- 驗證群集間對等體的安全連線。



**注意：**如果在統一通訊伺服器上使用SSO功能，並且重新生成Cisco Tomcat證書，則必須使用新證書重新配置SSO。在CUCM和ADFS 2.0上配置SSO的連結是：<https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/211302-Configure-Single-Sign-On-using-CUCM-and.html>。



**註：**CUCM證書再生/續訂流程的連結為：<https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/200199-CUCM-Certificate-Regeneration-Renewal-Pr.html>。

## 憑證重新產生程式

### CUP證書

步驟 1. 為叢集中的每個伺服器開啟圖形化使用者介面(GUI)。從IM/P發佈伺服器開始，然後依次打開每個IM/P使用者伺服器的GUI，並導航至 Cisco Unified OS Administration > Security > Certificate Management。

步驟 2. 從發佈伺服器GUI開始，選擇Find顯示所有證書。選擇cup.pem證書。打開後，選擇Regenerate，然後等到看到成功再關閉彈出

窗口。

步驟 3.請繼續後續的訂閱者，參閱步驟2中的相同程式。並完成叢集中的所有訂閱者。

步驟4.在所有節點上重新生成CUP證書後，必須重新啟動服務。



**注意：**如果線上狀態冗餘組配置選中了「啟用高可用性」，則Uncheck在重新啟動服務之前。可以訪問線上狀態冗餘組配置，其網址為CUCM Pub Administration > System > Presence Redundancy Group。重新啟動服務會導致IM/P暫時中斷，必須在生產時間以外完成。

按以下順序重新啟動服務：

· 登入發佈伺服器的Cisco Unified Serviceability：

a. Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. Restart Cisco SIP代理服務。

c.服務重新啟動完成後，繼續使用者和RestartCisco SIP代理服務。

d.從發佈者開始，然後繼續訂閱者。 Restart Cisco SIP代理服務(也可從Cisco Unified Serviceability > Tools > Control Center - Feature Services獲取)。

· 登入發佈伺服器的Cisco Unified Serviceability：

a. Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. Restart Cisco Presence Engine服務。

c.服務重新啟動完成後，繼續在使用者Restart 上使用思科線上狀態引擎服務。



**注意：**如果為SIP聯合配置，RestartCisco XCP SIP聯合連線管理器服務(位於Cisco Unified Serviceability > Tools > Control Center - Feature Services)。從發行者開始，然後繼續訂閱者。

## CUP-XMPP證書



**注意：**由於Jabber使用CUCM和IM/P Tomcat以及CUP-XMPP伺服器證書來驗證Tomcat和CUP-XMPP服務的連線，因此，這些CUCM和IM/P證書在大多數情況下都是CA簽署的。假設Jabber裝置沒有根證書和中間證書 ( CUP-XMPP證書的一部分) 安裝在其證書信任庫中，在這種情況下，Jabber客戶端會顯示不受信任證書的安全警告彈出窗口。如果尚未安裝在Jabber裝置信任儲存的證書中，則必須透過組策略、MDM、電子郵件等將根證書和任何中間證書推送到Jabber裝置，這取決於Jabber客戶端。



**注意：**如果CUP-XMPP證書是自簽名證書，且未在Jabber裝置證書的信任儲存中安裝CUP-XMPP證書，則Jabber客戶端會顯示不受信任證書的安全警告彈出窗口。如果尚未安裝，則必須透過組策略、MDM、電子郵件等將自簽名CUP-XMPP證書推送到Jabber裝置，具體取決於Jabber客戶端。

步驟 1.為群集中的每個伺服器打開GUI。從IM/P發佈伺服器開始，然後依次打開每個IM/P使用者伺服器的GUI並導航到Cisco Unified

## OS Administration > Security > Certificate Management。

步驟 2. 從發佈伺服器GUI開始，選擇Find顯示所有證書。從證 cup-xmpp.pem 書的type列中，確定證書是自簽名還是CA簽名。如果證 cup-xmpp.pem 書是第三方簽署的（型別CA簽署）分散式多SAN，請在生成多SAN CUP-XMPP CSR並提交給CA以獲取CA簽署的CUP-XMPP證書時檢視此連結；[使用CA簽署的多伺服器主題備用名稱配置統一通訊集群設定示例](#)。


如果證 cup-xmpp.pem 書是第三方簽署的（型別CA簽署）分發單節點（分發名稱等於證書的公用名稱），請在生成單節點CUP-XMPP CSR並提交給CA以獲取CA簽署的CUP-XMPP證書時檢視此連結；[Jabber完成證書驗證操作指南](#)。如果cup-xmpp.pem 證書是自簽名的，請繼續執行步驟3。

步驟 3. 選擇Find以顯示所有證書，然後選擇cup-xmpp.pem證書。打開後，選擇Regenerate，然後等到看到成功再關閉彈出窗口。

步驟 4. 請繼續後續的訂閱者；請參考步驟2中的相同程式，並完成叢集中所有訂閱者的程式。

步驟 5. 在所有節點上重新生成CUP-XMPP證書後，必須在IM/P節點上重新啟動Cisco XCP路由器服務。

---

 **注意：**如果線上狀態冗餘組配置選中了「啟用高可用性」，Uncheck將在服務重新啟動之前執行此操作。可以透過CUCM Pub Administration > System > Presence Redundancy Group訪問線上狀態冗餘組配置。重新啟動服務會導致IM/P暫時中斷，必須在生產時間以外完成。

---

· 登入發佈伺服器的Cisco Unified Serviceability：

a. Cisco Unified Serviceability > Tools > Control Center - Network Services.

b. Restart Cisco XCP路由器服務。

c. 服務重新啟動完成後，繼續在使用者端使用RestartCisco XCP路由器服務。

## CUP-XMPP-S2S證書


步驟 1. 為群集中的每個伺服器打開GUI。從IM/P發佈伺服器開始，然後依次打開每個IM/P使用者伺服器的GUI並導航到Cisco Unified OS Administration > Security > Certificate Management。

步驟 2. 從發佈伺服器GUI開始，選擇 Find顯示所有證書，然後選擇cup-xmpp-s2s.pem證書。打開後，選擇Regenerate，然後等到看到成功再關閉彈出窗口。

步驟 3. 繼續後續訂閱者並參考步驟2中的相同程式，然後完成叢集中所有訂閱者的程式。

步驟 4. 在所有節點上重新生成CUP-XMPP-S2S證書後，必須按照所述的順序重新啟動服務。

---

 **注意：**如果「在場冗餘組配置」選中了「啟用高可用性」，Uncheck則在重新啟動這些服務之前，會先選中此項。可以在CUCM Pub Administration > System > Presence Redundancy Group上訪問線上狀態冗餘組配置。重新啟動服務會導致IM/P暫時中斷，必須在生產時間以外完成。

---

· 登入發佈伺服器的Cisco Unified Serviceability：

a. Cisco Unified Serviceability > Tools > Control Center - Network Services.


- b. Restart Cisco XCP路由器服務。
- c. 服務重新啟動完成後，繼續在使用者Restart 上使用Cisco XCP路由器服務。

· 登入發佈伺服器的Cisco Unified Serviceability：


- a. Cisco Unified Serviceability > Tools > Control Center - Feature Services.
- b. Restart 「Cisco XCP XMPP Federation Connection Manager」服務。
- c. 服務重新啟動完成後，繼續Restart 在訂閱伺服器上使用Cisco XCP XMPP Federation Connection Manager服務。

## IPSec憑證

---

 **注意：** CUCM發佈伺服器中的證 ipsec.pem 書必須有效且存在於IPSec信任庫中的所有使用者（CUCM和IM/P節點）中。在標準部署中，訂閱者的 ipsec.pem 憑證不存在於發行者中，因為IPSec信任存放區。要驗證有效性，請將CUCM-PUB的 ipsec.pem 證書中的序列號與使用者中的IPSec-trust進行比較。它們必須匹配。

---

 **註：** DRS在源代理和本地代理之間使用基於安全套接字層(SSL)的通訊，對CUCM集群節點（CUCM和IM/P節點）之間的資料進行身份驗證和加密。DRS將IPSec證書用於其公鑰/私鑰加密。請注意，如果您從「證書管理」(Certificate Management)頁面刪除IPSEC信任儲存(hostname.pem)檔案，則DRS不會按預期工作。如果手動刪除IPSEC信任檔案，則必須確保將IPSEC證書上傳到IPSEC信任儲存。有關詳細資訊，請參閱《CUCM安全指南》中的證書管理幫助頁面。

---

步驟 1. 為群集中的每個伺服器打開GUI。從IM/P發佈伺服器開始，然後依次打開每個IM/P使用者伺服器的GUI並導航到Cisco Unified OS Administration > Security > Certificate Management。

步驟 2. 從發佈者GUI開始，選擇Find顯示所有證書。Choose ipsec.pem證書。打開後，選擇Regenerate，然後等到看到成功再關閉彈出窗口。


步驟 3. 繼續後續訂閱者並參考步驟2中的相同程式，然後完成叢集中所有訂閱者的程式。

步驟 4. 在所有節點重新生成IPSEC證書之後，再生Restart這些服務。導航到發佈伺服器的Cisco Unified Serviceability；Cisco Unified Serviceability > Tools > Control Center - Network Services。


- a. 選擇Cisco DRF主要服務Restart。
- b. 服務重新啟動完成後，在發佈伺服器上選擇Restart Cisco DRF Local service，然後繼續使用每個使用者的Restart Cisco DRF Local service。

## Tomcat憑證

---

 **注意：** 由於Jabber使用CUCM Tomcat和IM/P Tomcat和CUP-XMPP伺服器證書來驗證Tomcat和CUP-XMPP服務的連線，因此，這些CUCM和IM/P證書在大多數情況下都是CA簽署的。假設Jabber裝置沒有根證書和任何中間證書（屬於Tomcat證書的一部分）安裝在其證書信任庫中。在這種情況下，Jabber客戶端會顯示不受信任證書的安全警告彈出窗口。如果尚未安裝在Jabber裝置的證書信任儲存中，則必須透過組策略、MDM、電子郵件等將根證書和任何中間證書推送到Jabber裝置，這取決於Jabber客戶端。

---

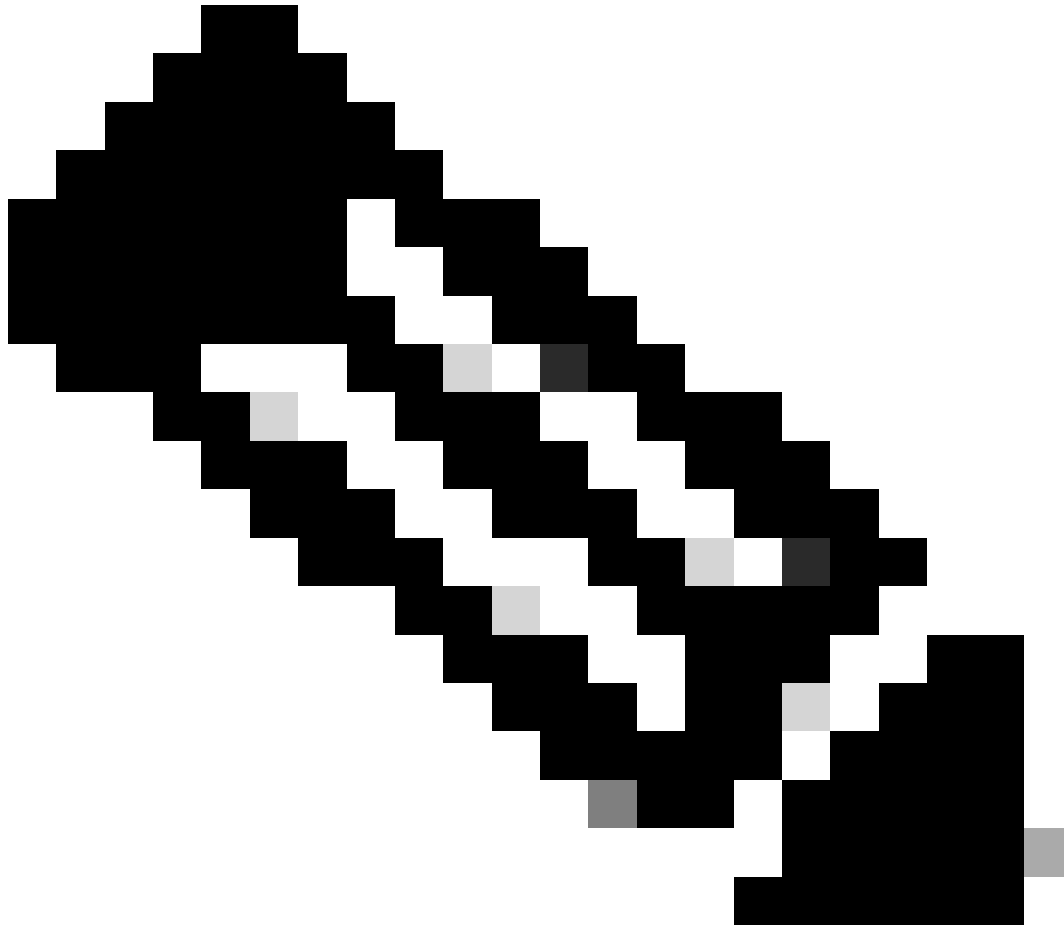
 **注意：**如果Tomcat證書是自簽名證書，且未在Jabber裝置的證書信任儲存中安裝Tomcat證書，則Jabber客戶端會顯示不受信任證書的安全警告彈出窗口。如果尚未安裝在Jabber裝置的證書信任儲存中，則必須透過組策略、MDM、電子郵件等將自簽名CUP-XMPP證書推送到Jabber裝置，這取決於Jabber客戶端。

步驟 1. 為群集中的每個伺服器打開GUI。從IM/P發佈伺服器開始，然後依次打開每個IM/P使用者伺服器的GUI並導航到Cisco Unified OS Administration > Security > Certificate Management。

步驟 2. 從發佈伺服器GUI開始，選擇Find 顯示所有證書。

· 在tomcat.pem證書的「型別」列中，確定證書是自簽名還是CA簽名。

· 如果tomcat.pem證書是第三方簽名的（型別CA簽名的）分散式多SAN，請檢視此有關如何生成多SAN Tomcat CSR的連結並向CA提交用於CA簽名的Tomcat證書，[統一通訊集群使用CA簽名的多伺服器主題備用名稱配置示例](#)



**注意：**多SAN Tomcat CSR在CUCM發佈伺服器上生成，並分發到集群中的所有CUCM和IM/P節點。

---

· 如果證 tomcat.pem 書是第三方簽署的 ( 型別CA簽署 ) 分發單節點 ( 分發名稱等於證書的公用名稱 ) , 請查閱此連結以生成單節點 CUP-XMPP CSR , 並將其提交給CA以獲取CA簽署的CUP-XMPP證書 , [Jabber完成證書驗證操作指南](#)

· 如果 tomcat.pem 證書是自簽名證書 , 請繼續步驟3

步驟 3.選擇Find以顯示所有證書 :

- 選擇tomcat.pem證書。
- 打開後 , 選擇Regenerate並等待 , 直到您看到成功彈出窗口 , 然後關閉彈出窗口。


步驟 4.繼續處理每個後續訂戶 , 參閱步驟2中的過程 , 並完成集群中的所有訂戶。

步驟 5.在所有節點重新生成Tomcat證書後 , Restart將在所有節點上使用Tomcat服務。首先從發佈伺服器開始 , 然後是訂閱伺服器。  
Restart · 要使用Tomcat服務 , 您必須為每個節點打開一個CLI會話 , 並運行命令 , 直到服務重新啟動Cisco Tomcat為止 , 如圖所示 :


```
admin:
admin:utils service restart Cisco Tomcat
Don't press Ctrl-c while the service is getting RESTARTED.If Service has not Restarted Properly, execute the same Command Again
Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
admin: █
```

刪除過期的信任憑證

---

 **注意 :** 可在適當時候刪除信任證書 ( 以-trust結尾 ) 。可以刪除的信任證書是不再需要、已過期或已過時的信任證書。請勿刪除五個身份證書 : cup.pem 、 cup-xmpp.pem 、 cup-xmpp-s2s.pem 、 ipsec.pem 和 tomcat.pem 證書。如圖所示 , 服務重新啟動的目的是清除這些服務中這些舊證書的任何記憶體資訊。

---

 **注意 :** 如果線上狀態冗餘組配置選中了「啟用高可用性」 , 則Uncheck在服務處於Stopped/Started 或Restarted狀態之前會出現這種情況。可以透過CUCM Pub Administration > System > Presence Redundancy Group訪問線上狀態冗餘組配置。如圖所示 , 重新啟動某些服務會導致IM/P臨時中斷 , 必須在生產時間以外完成。

---

步驟 1.導覽至 : Cisco Unified Serviceability > Tools > Control Center - Network Services

- 從下拉選單中選擇IM/P發佈者 , 然後從Cisco Certificate Expiry Monitor中選擇Stop , 接著在Cisco Intercluster Sync Agent中選擇Stop。
- 對集群中的每個IM/P節點重複Stop這些服務。



**注意：**如果必須刪除Tomcat-trust證書，請導航到CUCM發佈伺服器的Cisco Unified Serviceability > Tools > Control Center - Network Services。

- 
- 從下拉選單中選擇CUCM發佈伺服器。
  - 選擇Stop from Cisco Certificate Expiry Monitor，然後在Cisco Certificate Change Notification中選擇Stop。
  - 對集群中的每個CUCM節點重複上述步驟。

步驟 2. 導航到Cisco Unified OS Administration > Security > Certificate Management > Find。

- 查詢過期的信任證書(對於版本10.x及更高版本，您可以按到期進行過濾。從10.0之前的版本中，您必須手動辨識特定證書，或者透過RTMT警報(如果收到)。



- 相同的信任憑證可以出現在多個節點中，必須從每個節點個別刪除。
- 選擇要刪除的信任憑證（根據版本，您會收到快顯視窗，或是導覽至相同頁面上的憑證）。
- 選擇Delete(您將看到以「您將永久刪除此證書.....」(you are about to permanent delete this certificate...)開頭的彈出窗口。)
- 點選 OK.

步驟 3.對每個要刪除的信任證書重複此過程。

步驟 4.完成後，必須重新啟動與已刪除的證書直接相關的服務。

- CUP-trust：Cisco SIP代理、Cisco Presence Engine，如果配置用於SIP聯合，則使用Cisco XCP SIP聯合連線管理器（請參閱CUP證書部分）
- CUP-XMPP-trust：Cisco XCP路由器（請參閱CUP-XMPP certificate部分）
- CUP-XMPP-S2S-trust：Cisco XCP路由器和Cisco XCP XMPP聯合連線管理器
- IPSec-trust：DRF源/DRF本地（請參閱IPSec證書部分）
- Tomcat-trust：透過命令列重新啟動Tomcat服務（請參閱Tomcat certificate部分）

步驟 5.重新啟動服務已在步驟1中停止。

## 驗證

目前沒有適用於此組態的驗證程序。

## 疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。