# 排除CUCM中證書續訂的常見問題

## 簡介

本文說明在Cisco Unified Communications Manager(CUCM)中重新生成證書後的常見問題以及如何解決這些問題。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- CUCM證書續訂流程
- CUCM GUI介面
- Expressway伺服器
- 通過CUCM進程註冊裝置
- 證書頒發機構代理函式
- Cisco Unified Communications Manager安全指南

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- CUCM版本15

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。

### 業務影響

此表顯示操作中每次證書續訂的業務影響。請仔細閱讀此資訊。根據每個證書的風險級別，在數小時後或安靜期間續訂所需的證書。

Low Impact  Medium Impact.  High Impact.

| Type | Risk | Trust List | Impact | Phone Restart | Service Restart |
|---|---|---|---|---|---|
| Tomcat | | - | Web services, SSO, EM/EMCC Login | None | Tomcat |
| IPSec | | - | DRS, Ipsec Tunnels | None | DRF Master/Local |
| CAPF | | CTL + ITL | LSC must be updated, secure features | All | CAPF |
| Callmanager | | CTL + ITL | Registration, TL issues, Trunks, CTI | All | CM,CTI,TFTP |
| TVS | | ITL | Verification of TLs, CFG files, https connection | Some | TVS |
| ITLRecovery | | CTL + ITL | Signer or SAST backup for ITL/CTL | All | |

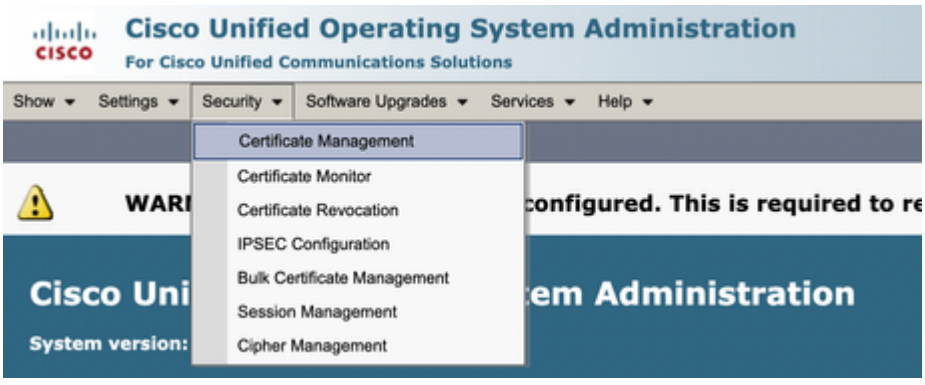
# 案例 1:電話在呼叫管理器、TVS和ITL證書續訂後未註冊

附註：此方案適用於CUCM混合模式和非安全集群下的部署，此外，它還適用於自簽名證書和CA證書。

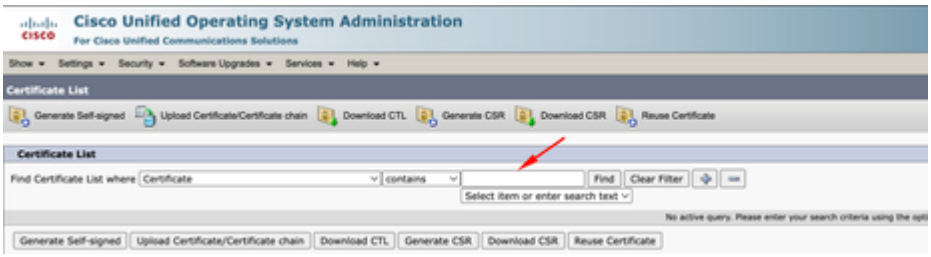
當Call Manager、TVS和ITL證書過期並同時續訂時，這會導致我們所有的電話都處於未註冊狀態，從而對系統造成重大影響，這是預期行為，因為我們將觸發電話不信任CUCM。

## 驗證

1.確保證書在Cisco Unified OS Administration > Security > Certificate Management下已過期

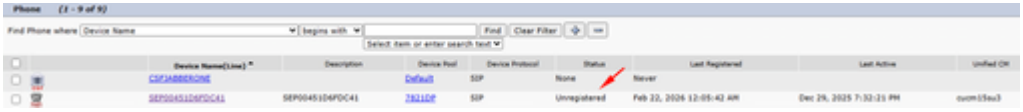



2.按頁面頂部過濾器下的Callmanager、TVS或ITL搜尋，並使用包含或開頭選項：




3.證書必須在到期列下顯示最新和詳細情況（TVS和ITL證書相同）

4.在證書續訂後，一旦驗證一切正常，電話將顯示為Unregistered狀態。



## 解決方案

有兩種方法可以解決此問題：

1. 對電話執行出廠重置，使電話刪除當前的安全設定並允許電話獲取新證書
2. 從發佈器節點上的CLI更新ITL和CTL證書，並使用命令 utils itl reset localkey。
   此步驟會影響所有電話（包括已註冊的電話），請確保在數小時後執行此操作。

High Impact.

---

# 場景2：在Tomcat證書續訂後，單一登入不起作用

---

附註：此方案可應用於使用集群範圍協定或每節點協定進行單點登入配置的部署

---

使用單點登入(SSO)在CUCM中登入時，它會顯示錯誤消息¨Error while processing saml

response¨或¨Error while processing saml response未能解密金鑰¨

## 驗證

1. 如果自簽名，請確保所有節點包含有效的tomcat證書，或者包含關聯的新多san tomcat證書。
2. 通過CLI在所有CUCM節點中使用set samltrace level debug，以便在調試級別啟用SSO日誌
3. 通過再次登入CUCM並使用SSO方法重新建立問題。
4. 在事件發生後收集Tomcat SSO日誌，並驗證您是否收到以下消息：
   -

```
2026-01-10 06:06:31,274 ERROR [http-nio-81-exec-157]  cpi.sso.saml.sp.security.authenticatio
com.sun.identity.saml2.common.SAML2Exception: Failed to decrypt the secret key.
              at com.sun.identity.saml2.xmlenc.FMEncProvider.getEncryptionKey(FMEncProvider.
              at com.sun.identity.saml2.xmlenc.FMEncProvider.decrypt(FMEncProvider.java:607)
              at com.sun.identity.saml2.assertion.impl.EncryptedAssertionImpl.decrypt(Encryp
...
```

## 解決方案

在Tomcat證書續訂後匯出CUCM後設資料並匯入到身份提供程式伺服器，以確保他們具有用於此通訊的新tomcat證書。

在啟用SSO部署的情況下續訂tomcat的過程：

---

⚠ 注意：技術協助中心(TAC)建議採取後續步驟，以便防止續訂Tomcat憑證後發生任何問題，並建議在數小時後執行此程式。

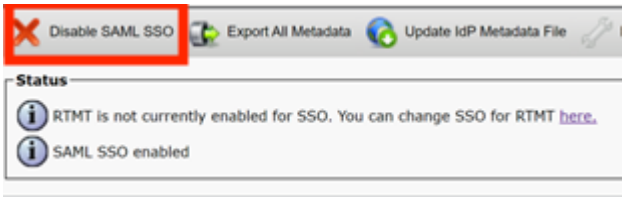
---

Low Impact

1.在所有CUCM節點中禁用SSO

- 訪問CM Administration > System > SAML Single Sign-on


- 選擇禁用SAML SSO

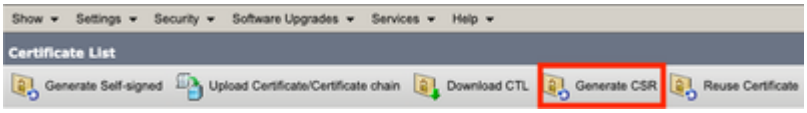



- 如果使用了每個節點的協定，則需要通過GUI在所有其餘節點中執行此過程。

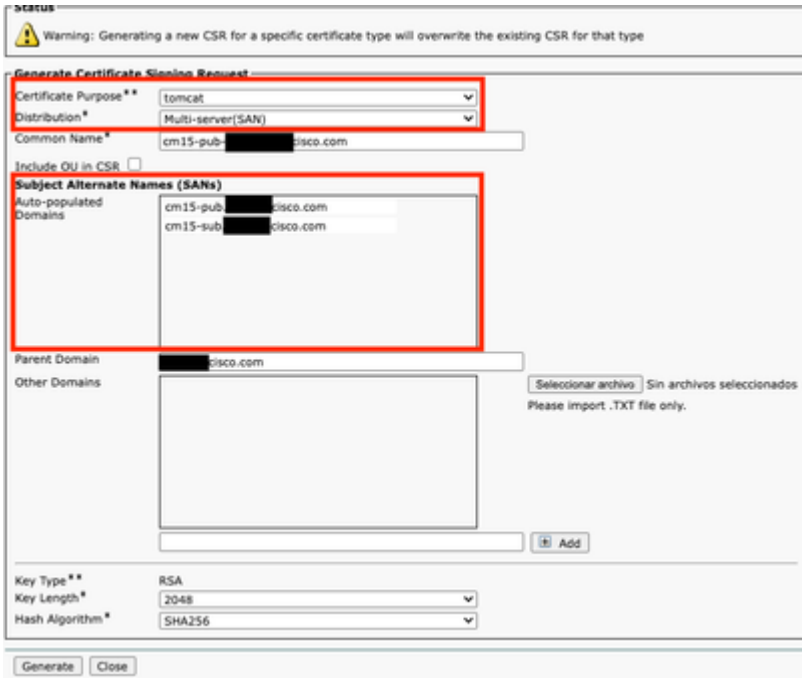
2.在CUCM群集中續訂Tomcat證書


在CUCM群集中續訂Tomcat多SAN證書的整體過程：

- 導航到OS administration > Security > Certificate management。
- 選擇產生CSR




- 在「Certificate Portuse」中選擇Tomcat。
- 選擇Multi-SAN in Distribution。
- 確保集群中的所有節點都列在自動填充域下。




- 選擇Generate。確保在群集中的所有節點中建立CSR。
- 從CUCM發佈伺服器下載生成的CSR，並使用證書頒發機構(CA)伺服器對其進行簽名。
- 轉到OS administration > Security > Certificate management。選擇Upload certificate/Certificate chain。
- 將CA憑證上傳為Tomcat-trust。
- 重複步驟6，現在將Tomcat簽名證書上傳為Tomcat。
- 完成並驗證所有節點都應用了新的tomcat證書後，使用此命令utils service restart Cisco Tomcat，在群集中的所有節點中通過CLI重新啟動Tomcat服務。

如需詳細資訊，請參閱以下檔案：

- 重新生成Tomcat自簽名證書
- 重新生成Tomcat CA簽名的證書。

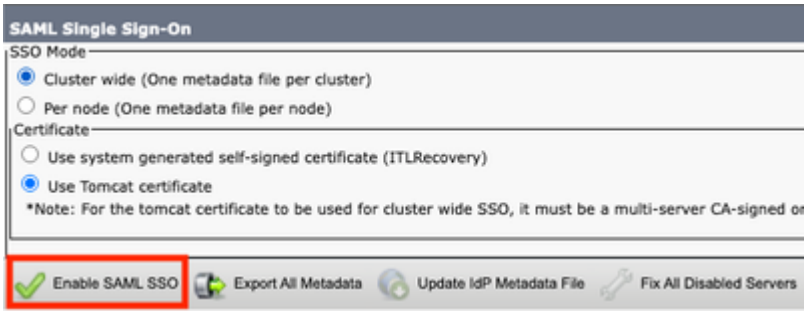
3.匯出服務提供商(SP)後設資料

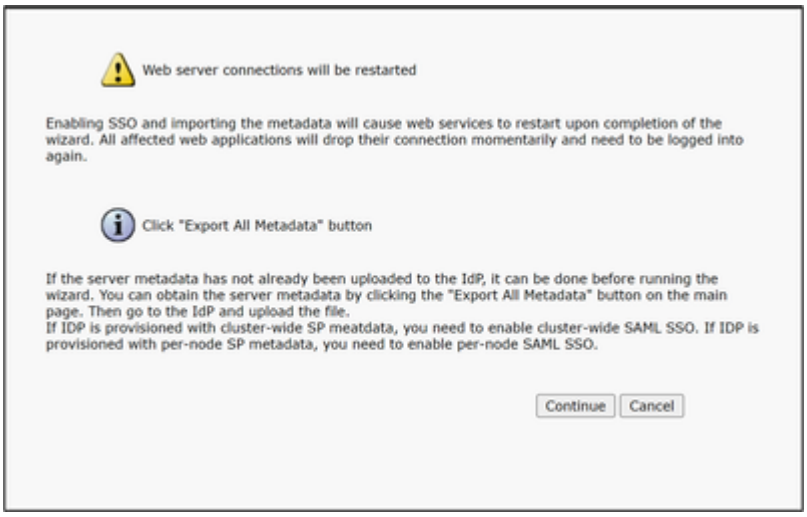

- 轉到CM Administration > System > Single Sign-On
- 配置SSO選項(在此示例中，在SSO模式上配置集群範圍並配置了在證書上使用tomcat certificate)，然後選擇匯出所有後設資料


- 將SP後設資料匯入到身份提供程式(IdP)伺服器。有關詳細資訊，請參閱在身份提供程式上配置SAML SSO

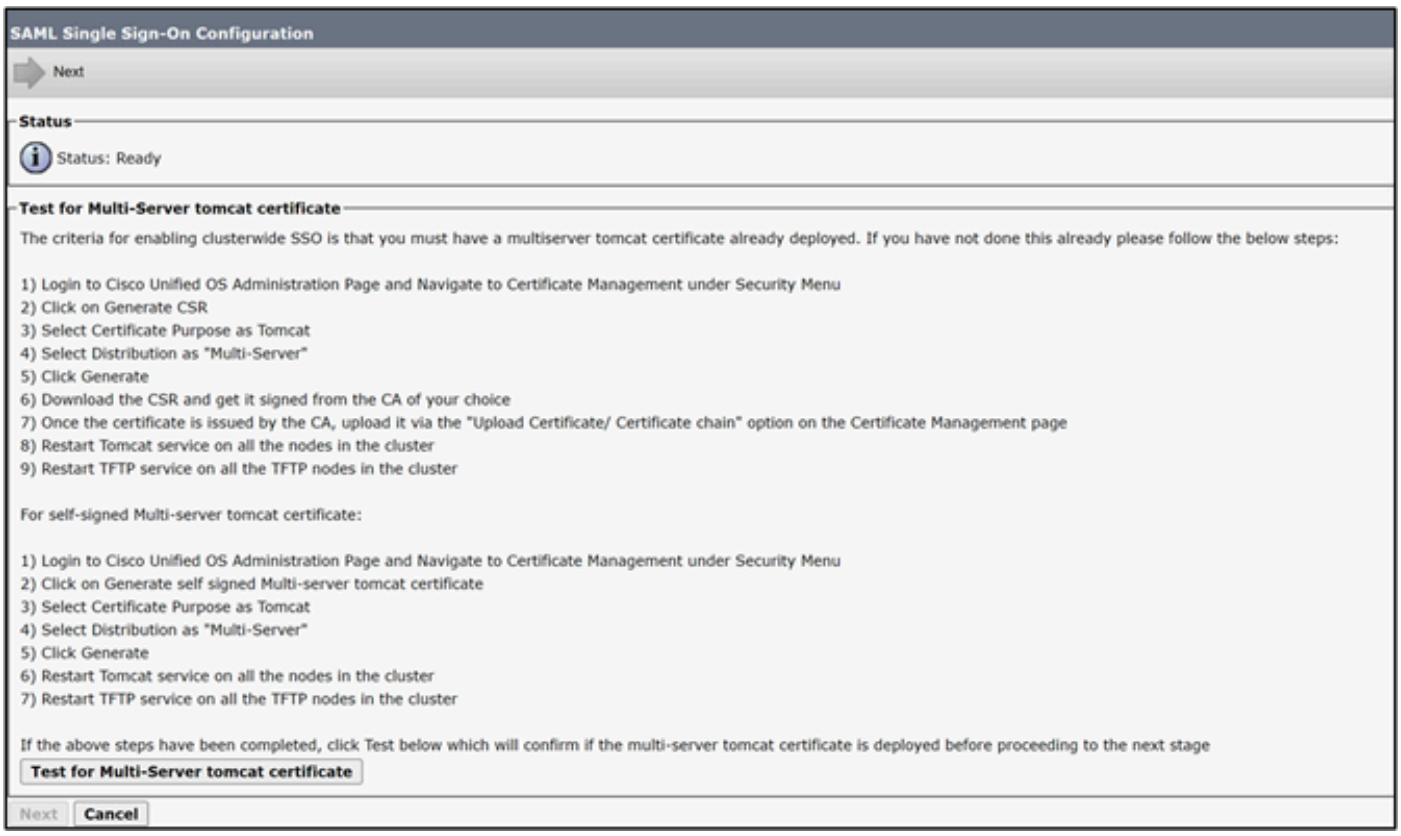
4.在CUCM群集中啟用SSO


- 轉到CM Administration > System > Single Sign-On
- 在匯出CUCM後設資料時選擇了相同的SSO選項，請選擇Enable SAML SSO並選擇繼續。

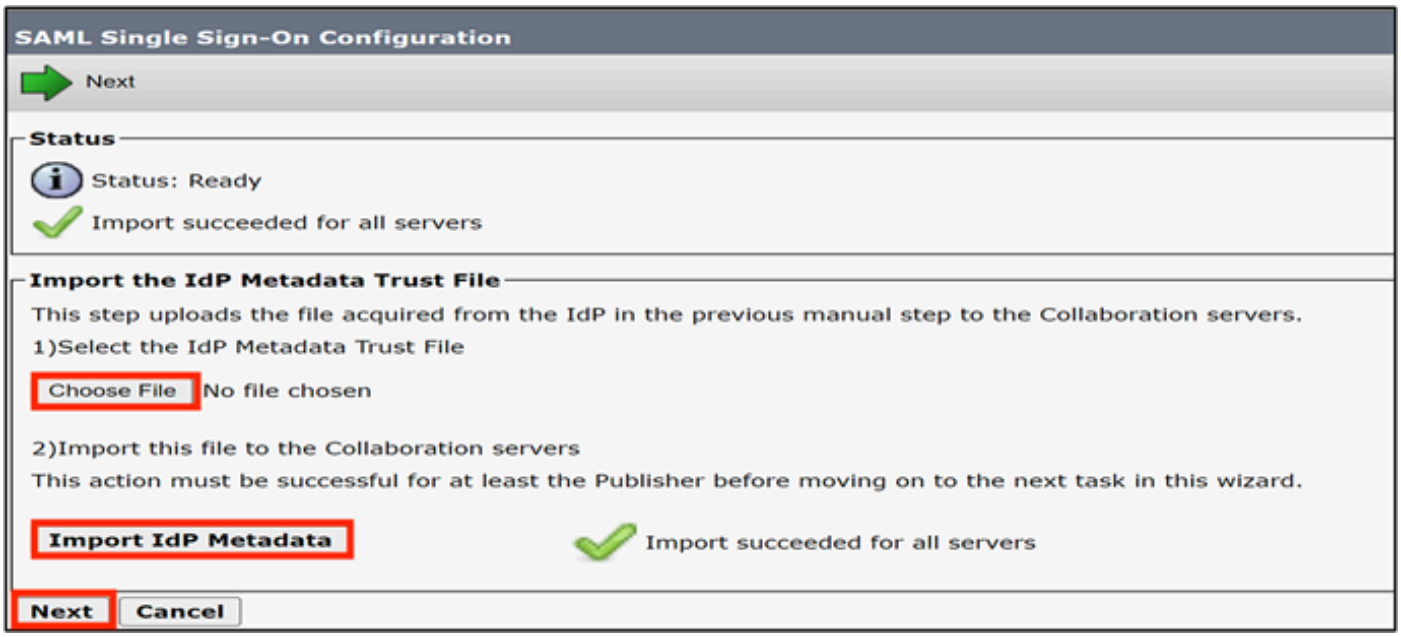




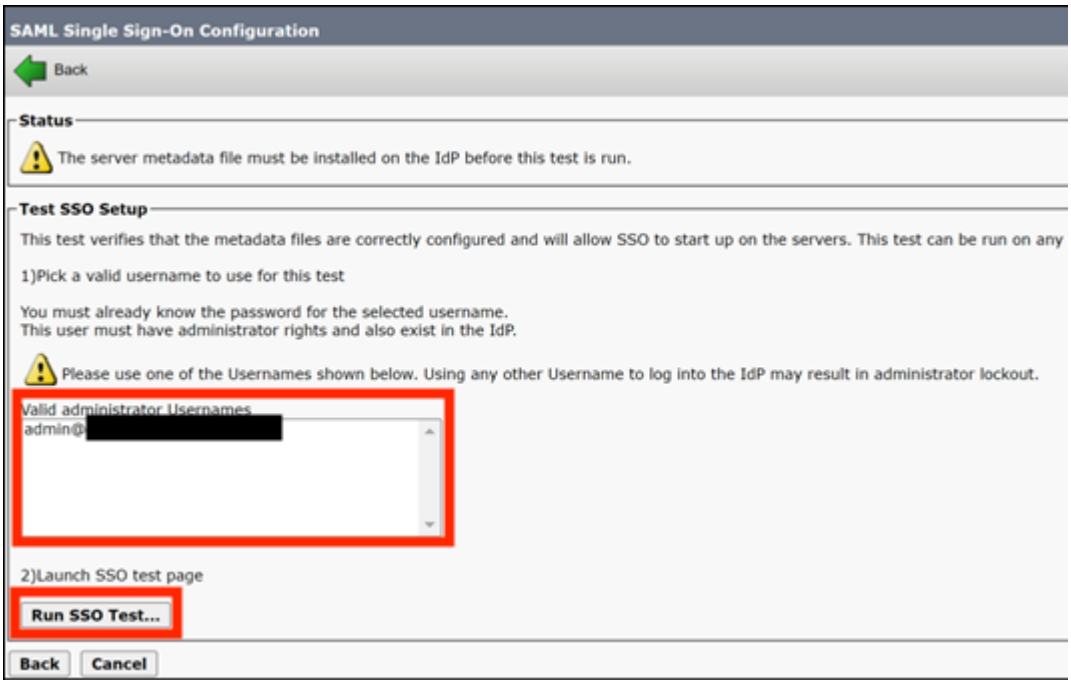

- 如果是在群集範圍內，此步驟可用於檢查所有節點中的多san證書，請選擇Test for multi-server tomcat certificate。完成後，選擇Next。

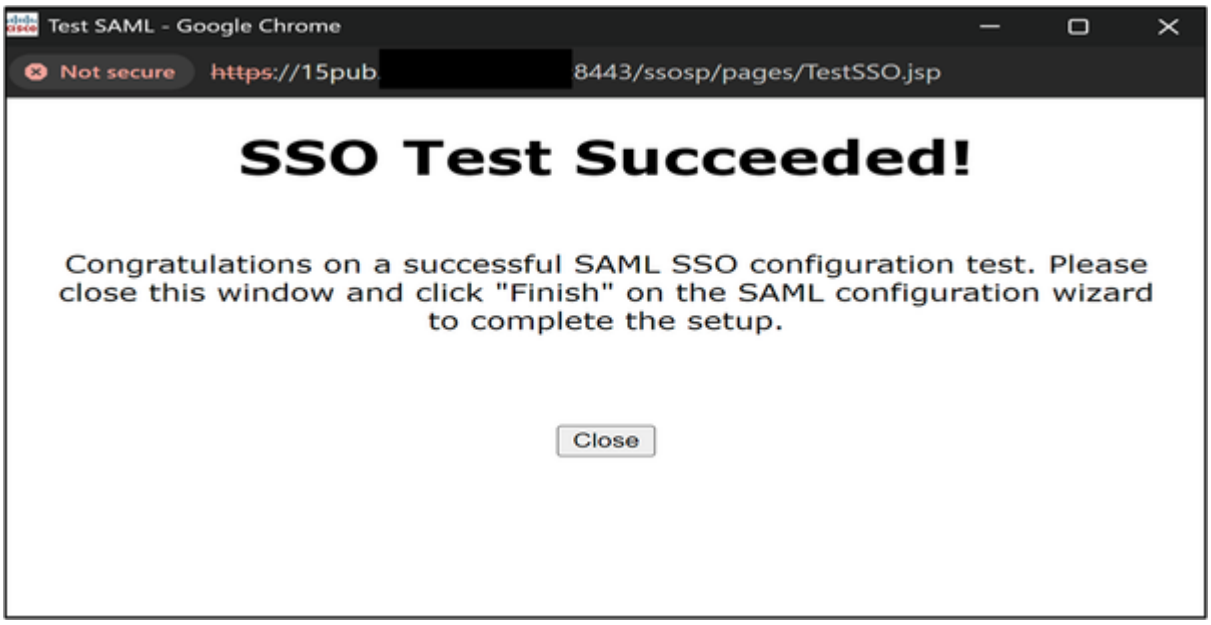



- 上傳IdP後設資料，選擇匯入IdP後設資料，完成後，選擇下一步



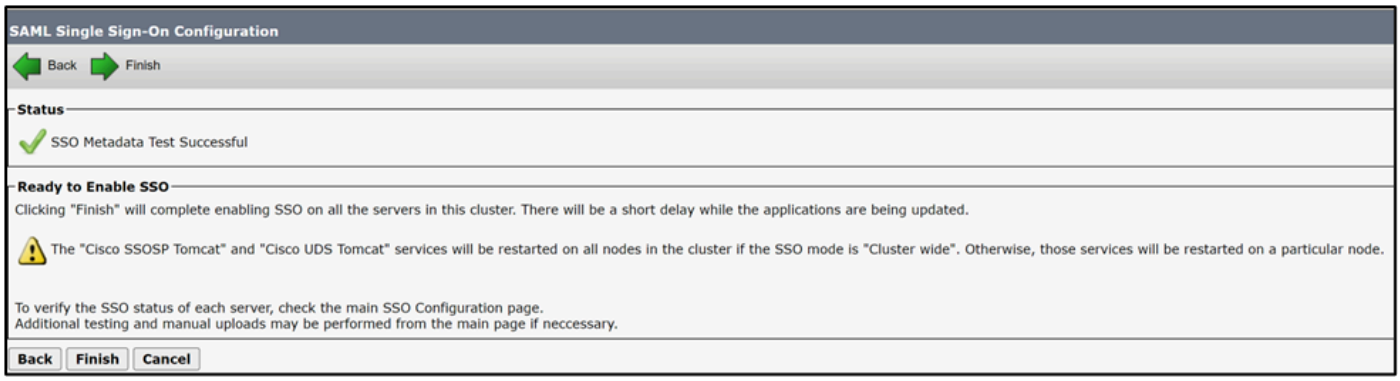

- 在「測試SSO設定」中，選擇分配了標準CCM超級使用者組的使用者，然後選擇運行SSO測試，直至成功。






4.啟用SSO後重新啟動所需的服務。


- 啟用SSO將重新啟動tomcat服務。




但是，TAC建議在SSO啟用流程後在所有節點中手動重新啟動Tomcat(utils service restart Cisco Tomcat)和UDS Tomcat(utils service restart CiscoUDSTomcat)服務。

---

## 案例 3:證書續訂後的移動和遠端訪問註冊問題

在混合模式部署中續訂Call manager、Tomcat和Expressway C證書後，Webex應用無法通過移動

和遠端訪問(MRA)向CUCM註冊。

## 驗證

1. CUCM Call manager和Tomcat證書是CA簽名的證書。
2. CUCM和Expressway部署在混合模式(TLS)上運行。
3. inspect Expressway-C日誌顯示「SSL常式：ssl3_read_bytes:tlsv1 alert unknown ca」。
   <#root>

```
2026-01-29T14:01:16.974-05:00 exp-c traffic_server[2030]: UTCTime="2026-01-29 19:01:16,974" Module
HTTPMSG:
|GET /CSFmarcoalh.cnf.xml HTTP/1.1
 Host: expc.cisco.com:6972
 Accept: */*
 Cookie:<CONCEALED>
 User-Agent: WebEx/0.0.0.0
 TrackingID: fxxxxxxx-86f6-4030-8259-0b768c07723e
 Client-ip: xxx.xxx.xxx.xxx
 X-Forwarded-For: xxx.xxx.xxx.xxx, 127.0.0.1
 Via: https/1.1 vcs[0fxxxxxx-c853-xxxx-aa16-0a290bf56fc8] (ATS), http/1.1 vcs[5xxxxxxx-7feb-4xxx-9

 |

2026-01-29T14:01:16.974-05:00 exp-c traffic_server[2030]:[ET_NET 1]ERROR:SSL connection failed for

SSL routines:ssl3_read_bytes:tlsv1 alert unknown ca
```

## 解決方案

在CUCM和Expressway-C之間匯出和匯入證書，以確保信任關係。

---

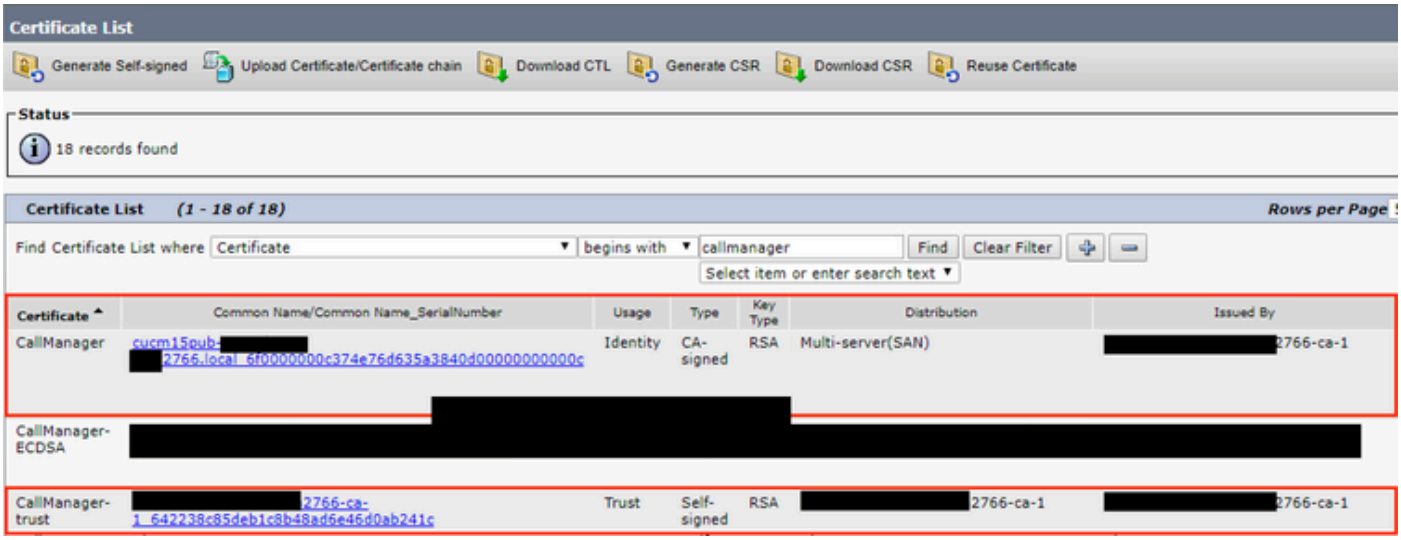
⚠ 注意：TAC建議在數小時後執行此操作，因為此過程要求重新啟動服務。業務影響是

---

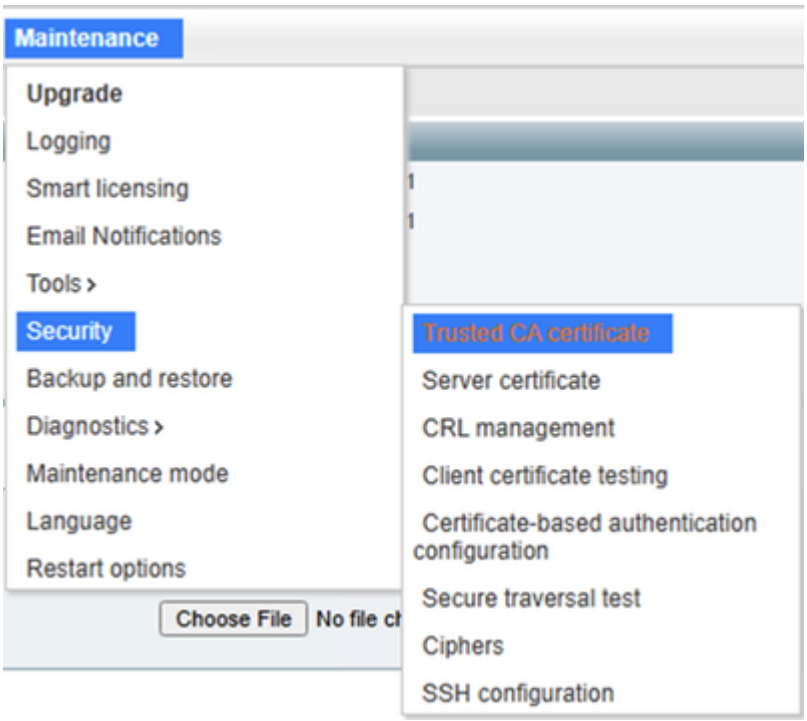
Medium Impact.

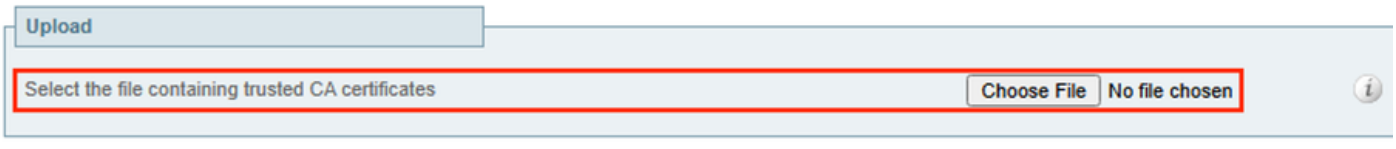
1. 使用CA簽名證書完成CUCM和Expressway之間的信任關係的過程

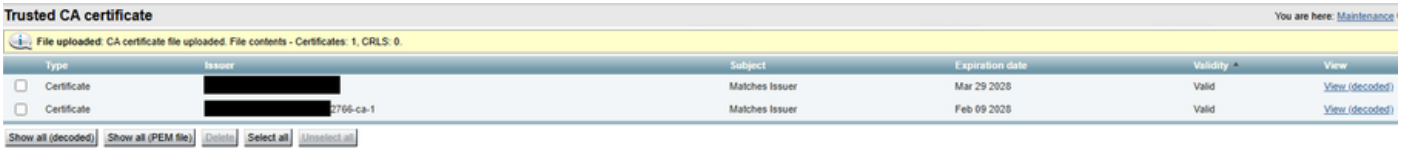
導覽至OS administration > Security > Certificate management，然後下載簽署Call Manager和Tomcat證書的根CA證書和中繼（如果有）。




然後導航到Expressway-C > Maintenance > Security > Trusted CA certificate，並上傳Call Manager和Tomcat證書的CA證書。

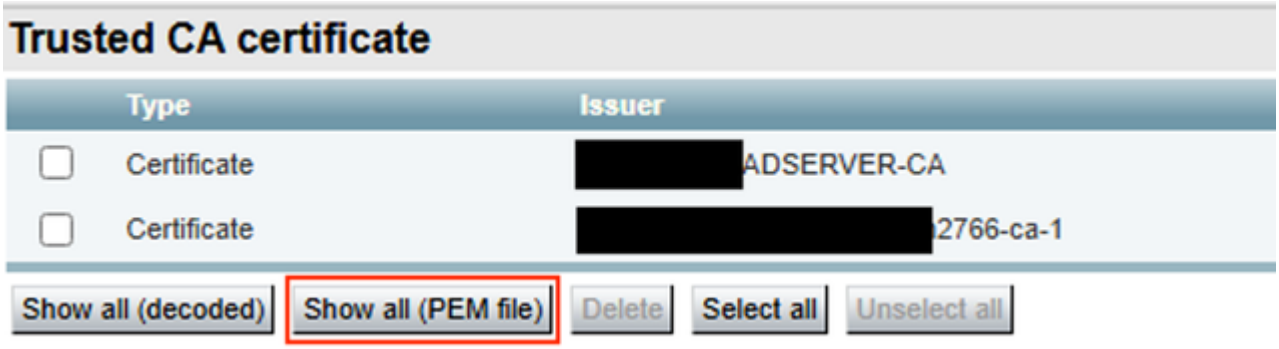


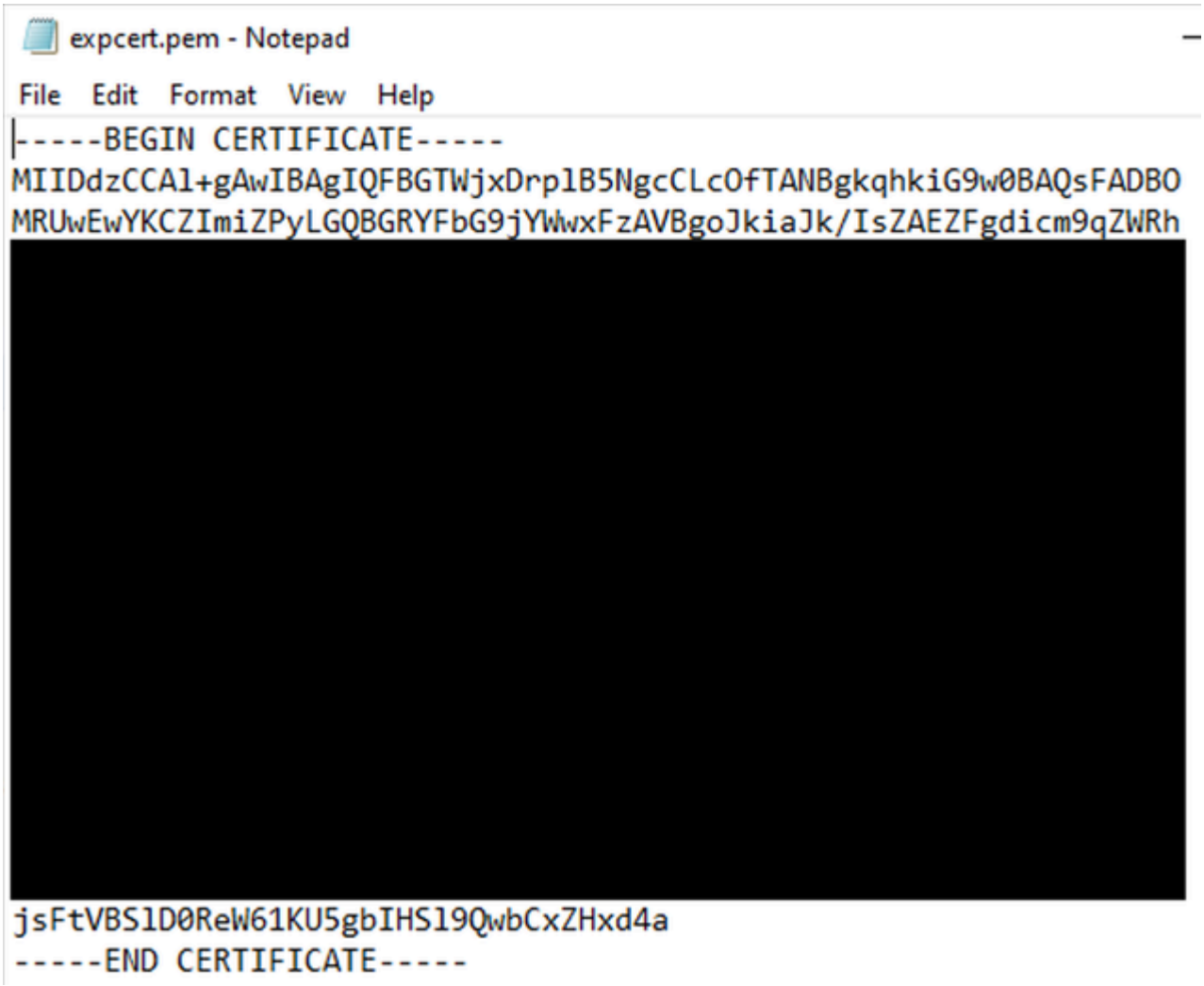



附註：在Call Manager和Tomcat證書為自簽名的場景中，下載實際的Call Manager和Tomcat證書並將其上傳到Expressway。

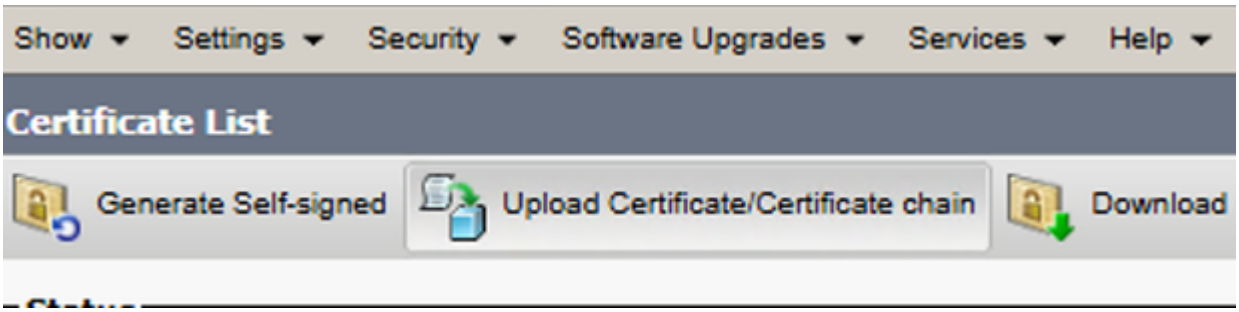

導航到Expressway-C >維護>安全>受信任CA證書>顯示全部（PEM檔案）

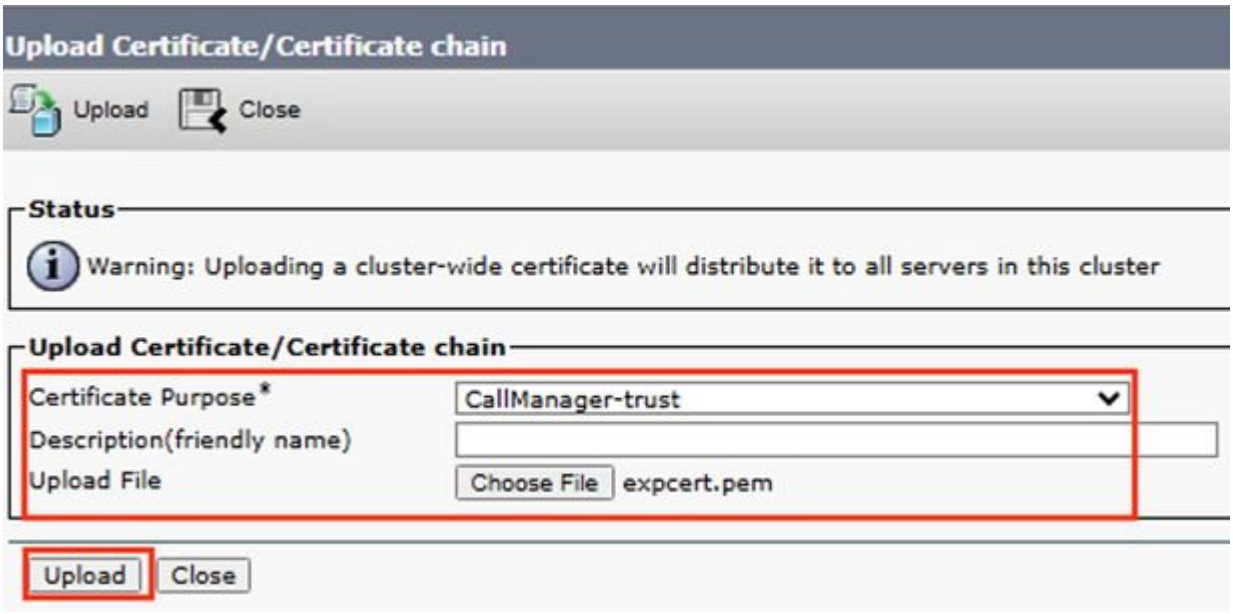



複製簽署Expressway-C的CA證書的PEM值，並將其儲存在txt檔案中。




導航到OS administration > Security > Certificate management，然後選擇Upload Certificate/Certificate Chain，並將expressway-C CA證書上傳為Tomcat-trust和Call Manager-trust







在CUCM群集中重新啟動所需的服務：

- 導航到Cisco Unified Serviceability > Tools > Control Center - Feature Services，並在運行該服務的所有節點中重新啟動Cisco CallManager服務。
- 導航到Cisco Unified Serviceability > Tools > Control Center - Feature Services，並在運行該服務的所有節點中重新啟動Cisco TFTP服務。
- 使用utils service restart Cisco Tomcat命令，通過CLI在群集中的所有節點中重新啟動Tomcat服務。
- 使用utils service restart Cisco HAProxy命令，通過CLI在群集中的所有節點中重新啟動Cisco HAproxy服務。

---

# 案例 4:證書頒發機構代理函式證書原因的續訂

## 案例 4.1:802.1x身份驗證失敗

在CUCM發佈伺服器上重新生成證書授權代理功能(CAPF)證書後，電話不與ASA進行身份驗證。

**驗證**

1. 電話狀態消息顯示「802.1x Authentication:失敗」


2. 檢查受影響伺服器的電話日誌並找到「SSL_ERROR_WANT_READ」

```
4592 NOT Feb 17 11:01:25.041733 (349-349) PAE: -Secure Connection Handshake in progress - status SSL_ER
4593 NOT Feb 17 11:01:25.041826 (349-349) PAE: -EV_REQUEST_REC, ST_AUTHENTICATING->ST_AUTHENTICATING
++ EAP-Failure
4594 NOT Feb 17 11:01:25.041898 (349-349) PAE: -send EAP-Resp/TLS - id 9
4595 NOT Feb 17 11:01:25.042032 (349-349) PAE: -authWhile timer set: 30 sec
4596 NOT Feb 17 11:01:27.061822 (349-349) PAE: -[0001-0] 08-cc-a7-1c-bb-ae vid=0xfff=4095 static=0 pri=
4597 NOT Feb 17 11:01:27.061950 (349-349) PAE: -port=0
4598 NOT Feb 17 11:01:27.062009 (349-349) PAE: -cprCdpGetPort address:  8:CC:A7:1C:BB:AE  Phyport=0 app
4599 NOT Feb 17 11:01:27.062068 (349-349) PAE: - >>>>>>>>>>>>>> port obtained = 0 for mac macAddress 08:
4600 NOT Feb 17 11:01:27.062134 (349-349) PAE: -rcvd EAP-Failure
4601 NOT Feb 17 11:01:27.062189 (349-349) PAE: -EV_FAILURE, ST_AUTHENTICATING->ST_HELD
4602 WRN Feb 17 11:01:27.062462 (349-349) PAE: -802.1X auth FAILED
4603 NOT Feb 17 11:01:27.062550 (349-349) PAE: -paeInfoToInetd: PAE info sent to NETSD
4604 NOT Feb 17 11:01:27.062717 (1786-1880) JAVA-Calling handleNetSDEvent
4605 WRN Feb 17 11:01:27.062953 (1786-1880) JAVA-Thread-11|cip.sec.Security:? - Security: Received a pr
4606 DEB Feb 17 11:01:27.063039 (1786-1880) JAVA-openQue(): que->/tmp/pae_msg_que, key->0x101019ab
4607 DEB Feb 17 11:01:27.063069 (1786-1880) JAVA-openQue(): que->/tmp/pae_rsp_que, key->0x10101c4c
4608 DEB Feb 17 11:01:27.063091 (1786-1880) JAVA-getpaeinfo: send pae info message paeCmd.mtype=1880, p
4609 DEB Feb 17 11:01:27.063121 (1786-1880) JAVA-getpaeinfo: recv pae info resp ret=-1, errno=No messag
4610 NOT Feb 17 11:01:27.063306 (349-349) PAE: -paeInfoToInetd: Netsd event NETSD_EV_PAE sent to NETSD
4611 NOT Feb 17 11:01:27.063370 (349-349) PAE: - PAE RE-AUTH, not sending SEC_DOWN Netsd event for CDP
4612 NOT Feb 17 11:01:27.063423 (349-349) PAE: -paeSetLastSupStatus: LastSupStatus 0
4613 NOT Feb 17 11:01:27.063475 (349-349) PAE: -heldWhile timer set: 60 sec
4614 NOT Feb 17 11:01:27.064074 (349-349) PAE: -paeNetsdRcvMsg(349): PAE event: status: FAIL : Resource
```

解決方案

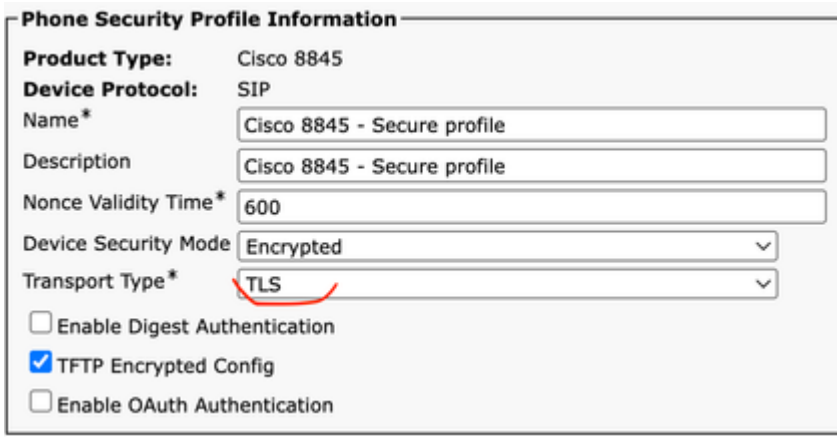
從CUCM發佈伺服器下載CAPF證書並上傳到身份驗證伺服器，繞過802.1x以允許註冊並在受影響的電話上安裝LSC證書。

## 案例 4.2:電話不註冊在TLS模式下使用安全配置檔案的CUCM。

在CUCM發佈伺服器上重新生成CAPF證書後，電話顯示「電話正在註冊」。

## 驗證

1. 受影響的電話包含啟用TLS模式的安全配置檔案。




2. 受影響的電話已安裝LSC證書。
3. 確保CAPF證書是最新的。


4. 登入到CUCM發佈器，然後使用顯示舊CAPF證書序列號的show ctl命令。
5. 然後將電話安全配置檔案更改為非安全。

## 解決方案

在CUCM上重新生成CTL檔案，並重新啟動所需的服務，以確保電話獲得帶CAPF檔案的新CTL檔案。

---

⚠ 注意：TAC建議在數小時後執行此操作，因為此過程要求重新啟動服務。業務影響是

---

Medium Impact.

確保成功續訂CAPF的程式。

```
admin:utils ctl update CTLFile
This operation will update the CTLFile. Do you want to continue? (y/n): y

Updating CTL file
CTL file Updated
Please reset all Encrypted and Authenticated phones for the CTL file updates to take effect.
```

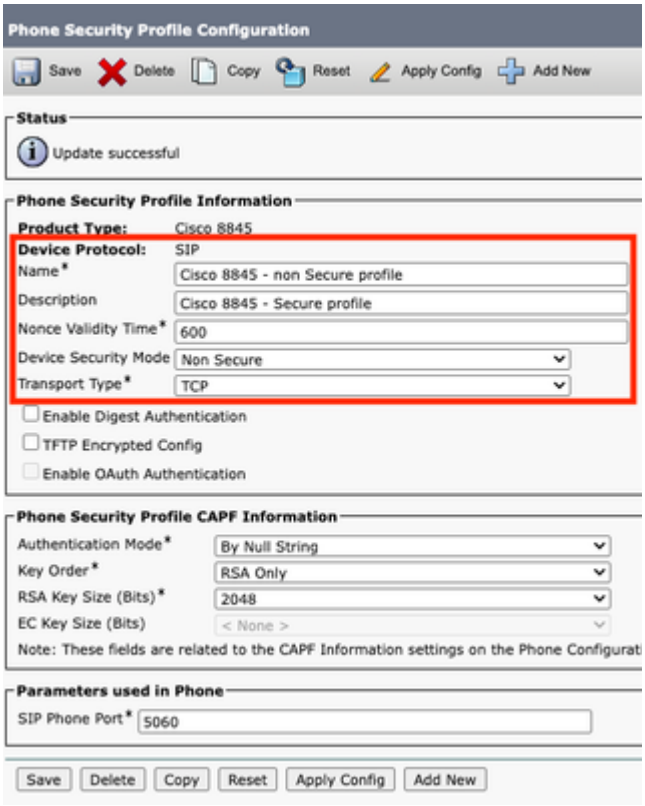
在CAPF再生後更新CTL檔案。登入到發布器的CLI並輸入命令以利用更新CTL檔案。


1. 在CUCM publisher中導航到Cisco Unified Serviceability > Tools > Control Center - Feature Services，然後重新啟動CAPF服務。
2. 導航到Cisco Unified Serviceability > Tools > Control Center - Network Services，並在運行該服務的所有節點中重新啟動Cisco Trust Verification Service。
3. 導航到Cisco Unified Serviceability > Tools > Control Center - Feature Services，並在運行該服務的所有節點中重新啟動Cisco TFTP Service

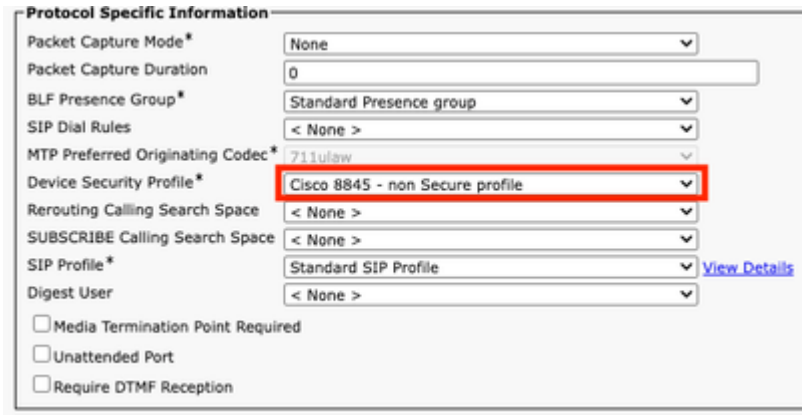

- 導航到CM Administration > System > Security > Phone Security Profile。

- 複製分配給所需電話的當前電話安全配置檔案。

- 將名稱和裝置安全模式更改為Non Secure，然後選擇Save and Apply Config，將此更改應用到所有所需的電話。

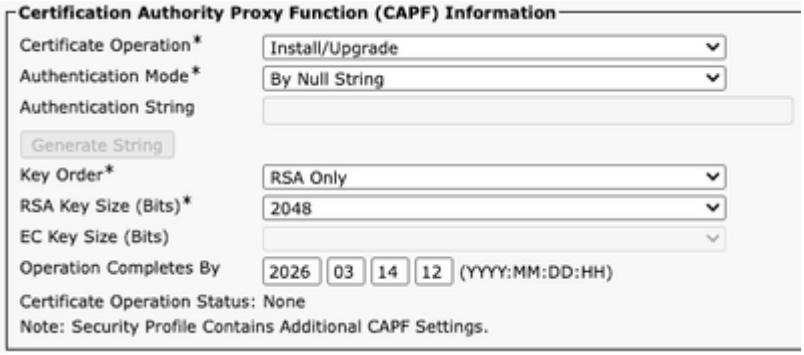



- 將建立的Device Security Profile應用到所需的電話配置，選擇Save and Apply Config。



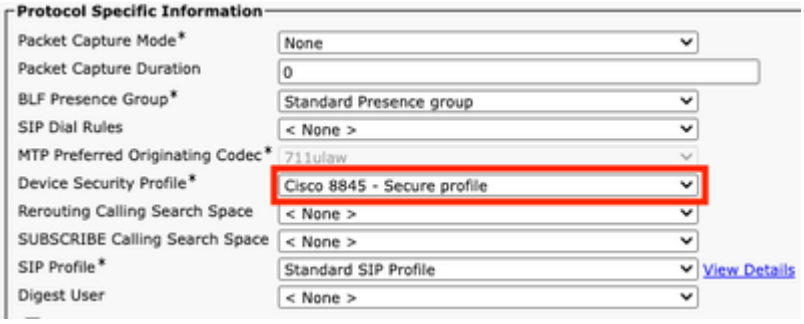

使用受影響電話的裝置配置中的CAPF資訊部分在所需電話中安裝LSC證書。

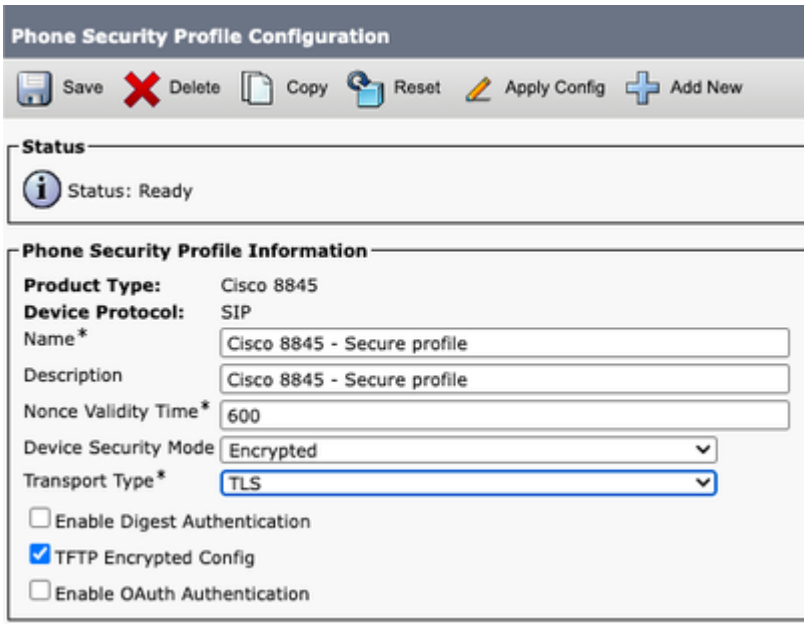
- 在CAPF資訊中，選擇Install/Upgrade in Certificate Operation。




- 選擇Save and Apply Config。
- 請等待「Certificate Operation Status（證書操作狀態）」顯示「Operation completed（操作已完成）」。


在電話配置的協定特定資訊部分，選擇已建立的啟用TLS的安全配置檔案。






## 相關資訊

- https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/214231-certificate-regeneration-process-for-cis.html
- https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/217138-regeneration-of-cucm-ca-signed-certifica.html
- https://www.cisco.com/c/en/us/support/docs/content-networking/certificates/213295-how-to-install-an-lsc-on-a-cisco-ip-phon.html
- https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X15-2/mra/exwy_b_mra-deployment-guide-x152.html

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）。