從簽名的CA證書建立新證書

目錄

簡介

本檔案介紹如何在Cisco Unified Communications Manager(CUCM)中重新產生憑證授權單位(CA)簽署的憑證。

必要條件

需求

思科建議您瞭解以下主題：

- 即時監控工具(RTMT)
- CUCM證書

採用元件

- CUCM版本10.x、11.x和12.x。

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。

預檢資訊

附註：有關自簽名證書再生的資訊，請參閱證書再生指南。有關CA簽名的多SAN證書再生的資訊，請參閱多SAN證書再生指南。

要瞭解每個證書及其再生的影響，請參閱自簽名再生指南。

每個證書簽名請求(CSR)型別具有不同的金鑰用法，簽名證書中需要使用這些金鑰。安全指南包括一個表，其中包含每種證書型別所需的金鑰用法。

要更改主題設定（位置、狀態、組織單元等），請運行以下命令：

- **set web-security** orgunit orgname locality state [country] [alternatehostname]

Tomcat證書將在您運行 set web-security 指令。除非重新啟動Tomcat服務，否則不會應用新的自簽名證書。如需此命令的詳細資訊，請參閱以下指南：

- 命令列參考指南
- 思科社群步驟連結
- 影片

配置和重新生成證書

針對每種型別的證書，列出了在由CA簽名的CUCM群集中重新生成單節點證書的步驟。如果群集中的所有證書尚未過期，則無需重新生成這些證書。

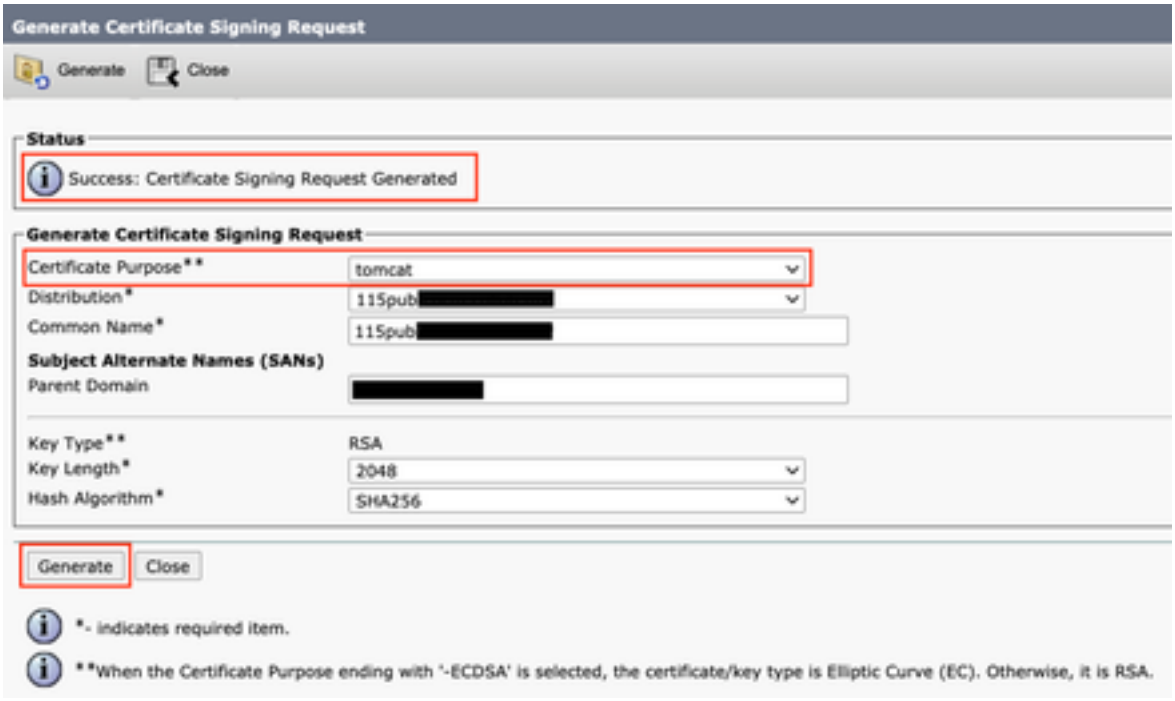
Tomcat證書

注意：驗證群集中的SSO是否已禁用(**CM Administration > System > SAML Single Sign-On**)。 如果啟用SSO，則必須禁用SSO，然後在Tomcat證書重新生成過程完成後啟用SSO。

在群集的所有節點（CallManager和IM&P）上：

步驟1.導航至 **Cisco Unified OS Administration > Security > Certificate Management > Find** 並驗證Tomcat證書的到期日期。

步驟2.按一下 Generate CSR > Certificate Purpose: tomcat.為證書選擇所需的設定，然後按一下 **Generate**.等待出現成功消息並按一下 Close.



步驟3.下載CSR。按一下 Download CSR ，選擇 **Certificate Purpose: tomcat**，然後按一下 Download.

步驟4.將CSR傳送到憑證授權單位。

步驟5.證書頒發機構為已簽名的證書鏈返回兩個或多個檔案。按以下順序上傳憑證：

- 作為tomcat-trust的根CA證書。導航至 **Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust**. 設定證書描述並瀏覽根證書檔案。
- 作為tomcat-trust的中間證書（可選）。 **導航至 Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust**.設定證書的描述並瀏覽中間證書檔案。

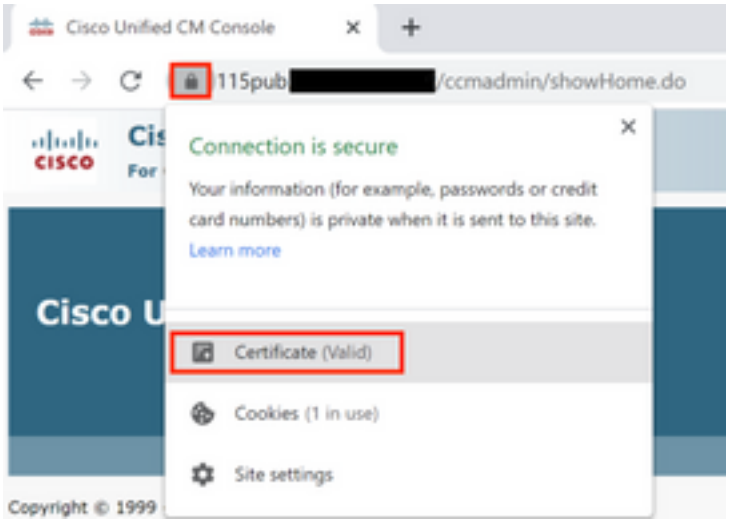
  附註：某些CA不提供中間憑證，如果只提供根憑證，則可以省略此步驟。

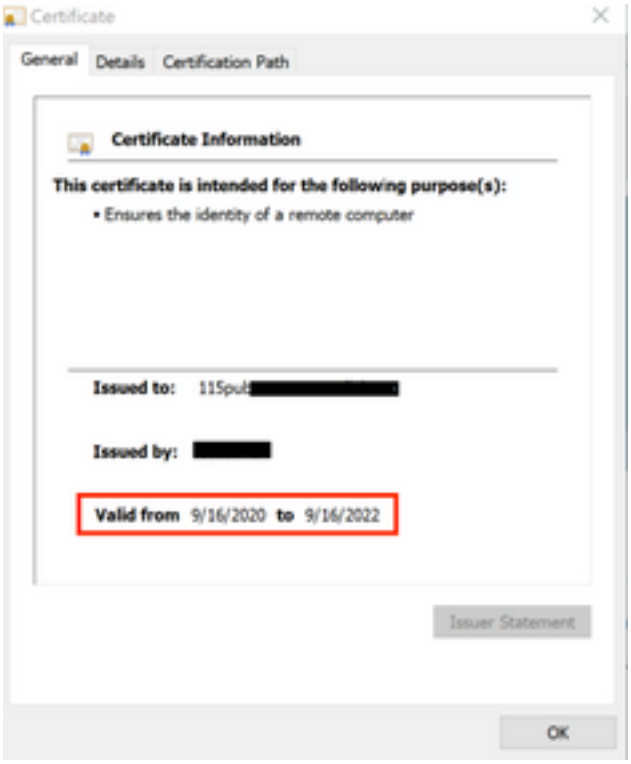
- CA簽名的證書作為tomcat。 **導航至 Certificate Management > Upload certificate > Certificate Purpose: tomcat**。設定證書描述並瀏覽當前CUCM節點的CA簽名證書檔案。

  附註：此時，CUCM會比較CSR和上傳的CA簽名證書。如果資訊相符，CSR就會消失，且系統會上傳新的CA簽名的憑證。如果您在上傳憑證後收到錯誤訊息，請參閱 Upload Certificate Common Error Messages 部分。

步驟6.若要將新證書應用到伺服器，需要通過CLI重新啟動Cisco Tomcat服務（先從Publisher啟動，再從訂閱伺服器啟動，一次一個啟動），請使用命令 utils service restart Cisco Tomcat.

驗證CUCM現在已使用Tomcat證書。導航到節點的網頁並選擇 Site Information （鎖定圖示）在瀏覽器中，按一下 certificate 選項，並驗證新證書的日期。





CallManager證書

> **注意**：請勿同時重新生成CallManager和TVS證書。這會導致終端上已安裝的ITL出現不可恢復的不匹配，這要求從集群中的所有終端上刪除ITL。完成CallManager的整個過程，並在電話註冊回後，啟動TVS的流程。

> **注意**：要確定集群是否處於混合模式，請導航至**Cisco Unified CM管理>系統>企業引數>集群安全模式(0 == Non-Secure;1 == Mixed Mode)**。

對於群集的所有CallManager節點：

步驟1.導航至 Cisco Unified OS Administration > Security > Certificate Management > Find 並驗證CallManager證書的到期日期。

步驟2.按一下 Generate CSR > Certificate Purpose: CallManager.為證書選擇所需的設定，然後按一下 Generate.等待出現成功消息並按一下 Close.

步驟3.下載CSR。按一下 **Download CSR**. Select **Certificate Purpose: CallManager** and click **Download**.

步驟4.將CSR傳送到 Certificate Authority .

步驟5.證書頒發機構為已簽名的證書鏈返回兩個或多個檔案。按以下順序上傳憑證：

- 作為CallManager-trust的根CA證書。導航至 Certificate Management > Upload certificate > Certificate Purpose: CallManager-trust.設定證書描述並瀏覽根證書檔案。
- 作為CallManager-trust的中間證書（可選）。 導航至 Certificate Management > Upload certificate > Certificate Purpose: CallManager-trust.設定證書的描述並瀏覽中間證書檔案。

附註：某些CA不提供中間憑證，如果只提供根憑證，則可以省略此步驟。

- CA簽名的證書作為CallManager。導航至 Certificate Management > Upload certificate > Certificate Purpose: CallManager.設定證書描述並瀏覽當前CUCM節點的CA簽名證書檔案。

附註：此時，CUCM會比較CSR和上傳的CA簽名證書。如果資訊相符，CSR就會消失，且系統會上傳新的CA簽名的憑證。如果您在上傳憑證後收到錯誤訊息，請參閱**上傳憑證常見錯誤訊息**一節。

步驟6.如果群集處於混合模式，請在服務重新啟動之前更新CTL:Token或Tokenless。如果群集處於非安全模式，請跳過此步驟並繼續服務重新啟動。

步驟7.要將新證書應用到伺服器，必須重新啟動所需的服務（僅當服務運行且處於活動狀態時）。導覽至：

- Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco Trust Verification Service
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco TFTP
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco CallManager
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco CTIManager

步驟8.重置所有電話：

- 導航至 Cisco Unified CM Administration > System > Enterprise Parameters > Reset.系統將顯示一個彈出視窗，其中顯示「You are about to reset all devices in the system（您即將重置系統中的所有裝置）」語句。此操作無法撤消。是否繼續？選擇 OK 然後按一下 Reset .

附註：通過RTMT監控裝置註冊。所有電話重新註冊後，您可以繼續使用下一個證書型別。

IPSec憑證

注意：重新生成IPSec證書時，備份或還原任務不得處於活動狀態。

對於群集的所有節點（CallManager和IM&P）：

步驟1.導航至 Cisco Unified OS Administration > Security > Certificate Management > Find 並驗證ipsec證書的到期日

期。

步驟2.按一下**「產生CSR」>「憑證用途」：ipsec。選擇證書的所需設定，然後按一下生成。**等待出現成功消息，然後按一下**Close**。

步驟3.下載CSR。按一下「**Download CSR**」。選擇Certificate Purpose ipsec並按一下**Download**。

步驟4.將CSR傳送到憑證授權單位。

步驟5.證書頒發機構為已簽名的證書鏈返回兩個或多個檔案。按以下順序上傳憑證：

- 作為ipsec-trust的根CA證書。導覽至**Certificate Management > Upload certificate > Certificate Purpose:ipsec-trust。**設定證書描述並瀏覽根證書檔案。
- 作為ipsec-trust的中間證書（可選）。 導覽至**Certificate Management > Upload certificate > Certificate Purpose:tomcat-trust**。設定證書的描述並瀏覽中間證書檔案。

  附註：某些CA不提供中間憑證，如果只提供根憑證，則可以省略此步驟。

  - CA簽名的證書作為ipsec。導覽至**Certificate Management > Upload certificate > Certificate Purpose:ipsec**。設定證書描述並瀏覽當前CUCM節點的CA簽名證書檔案。

  附註：此時，CUCM會比較CSR和上傳的CA簽名證書。如果資訊相符，則CSR會消失，且已上傳新的CA簽署的憑證。如果您在上傳憑證後收到錯誤訊息，請參閱**上傳憑證常見錯誤訊息一節。**

步驟6.要將新證書應用到伺服器，必須重新啟動所需的服務（僅當服務運行且處於活動狀態時）。導覽至：

- **Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco DRF Master**（發佈者）
- **Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco DRF Local**（發佈者和訂戶）

CAPF證書

注意：要確定集群是否處於混合模式，請轉至**Cisco Unified CM管理>系統>企業引數>集群安全模式(0 == Non-Secure;1 == Mixed Mode)。**

注意:CAPF服務僅在發佈伺服器上運行，這是唯一使用的證書。不需要獲取CA簽名的訂閱伺服器節點，因為它們未被使用。如果證書在訂閱器中已過期，並且希望避免出現過期證書的警報，則可以重新生成訂閱器CAPF證書作為自簽名。有關詳細資訊，請參閱CAPF Certificate as Self-Signed。

在發佈伺服器中：

步驟1.導航到**Cisco Unified OS Administration > Security > Certificate Management > Find**，然後驗證CAPF證書的到期日期。

步驟2.按一下**「產生CSR」>「憑證用途」：CAPF。為證書選擇所需的設定，然後按一下**

Generate。等待出現成功消息，然後按一下**Close**。

步驟3.下載CSR。按一下「**Download CSR**」。選擇Certificate Purpose CAPF，然後按一下**Download**。

步驟4.將CSR傳送到憑證授權單位。

步驟5.證書頒發機構為已簽名的證書鏈返回兩個或多個檔案。按以下順序上傳憑證：

- 作為CAPF-trust的根CA證書。導覽至**Certificate Management > Upload certificate > Certificate Purpose:CAPF-trust**。設定證書描述並瀏覽根證書檔案。
- 作為CAPF-trust的中間證書（可選）。 導覽至**Certificate Management > Upload certificate > Certificate Purpose:CAPF-trust**。設定證書的描述並瀏覽中間證書檔案。

附註：某些CA不提供中間憑證，如果只提供根憑證，則可以省略此步驟。

- CA簽名的證書作為CAPF。導覽至**Certificate Management > Upload certificate > Certificate Purpose:CAPF**。設定證書描述並瀏覽當前CUCM節點的CA簽名證書檔案。

附註：此時，CUCM會比較CSR和上傳的CA簽名證書。如果資訊相符，則CSR會消失，且已上傳新的CA簽署的憑證。如果您在上傳憑證後收到錯誤訊息，請參閱**上傳憑證常見錯誤訊息**一節。

步驟6.如果群集處於混合模式，請在服務重新啟動之前更新CTL:Token或Tokenless。如果群集處於非安全模式，請跳過此步驟並繼續服務重新啟動。

步驟7.要將新證書應用到伺服器，必須重新啟動所需的服務（僅當服務運行且處於活動狀態時）。導覽至：

- **Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco Trust Verification Service**（運行服務的所有節點）
- **Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco TFTP**（運行服務的所有節點）
- **Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco Certificate Authority Proxy Function**(Publisher)

步驟8.重置所有電話：

- 導航至**Cisco Unified CM管理>系統>企業引數>重置**。系統將顯示一個彈出視窗，其中顯示「You are about to reset all devices in the system（您即將重置系統中的所有裝置）」語句。此操作無法撤消。是否繼續？選擇**OK**，然後按一下**Reset**。

附註：通過RTMT監控裝置註冊。所有電話重新註冊後，您可以繼續使用下一個證書型別。

TVS證書

注意：請勿同時重新生成CallManager和TVS證書。這會導致終端上已安裝的ITL出現不可恢復的不匹配，這要求從集群中的所有終端上刪除ITL。完成CallManager的整個過程，並在電話註冊回後，啟動TVS的流程。

對於群集的所有TVS節點：

步驟1.導航到**Cisco Unified OS Administration > Security > Certificate Management > Find**，然後驗證TVS證書的到期日期。

步驟2.按一下**「產生CSR」>「憑證用途」：電視**。為證書選擇所需的設定，然後按一下**Generate**。等待出現成功消息，然後按一下**Close**。

步驟3.下載CSR。按一下「**Download CSR**」。選擇**Certificate Purpose TVS**，然後按一下**Download**。

步驟4.將CSR傳送到憑證授權單位。

步驟5.證書頒發機構為已簽名的證書鏈返回兩個或多個檔案。按以下順序上傳憑證：

- 作為TVS-trust的根CA證書。導覽至**Certificate Management > Upload certificate > Certificate Purpose:TVS信任**。設定證書描述並瀏覽根證書檔案。
- 作為TVS-trust的中間證書（可選）。 導覽至**Certificate Management > Upload certificate > Certificate Purpose:TVS信任**。設定證書的描述並瀏覽中間證書檔案。

  附註：某些CA不提供中間憑證，如果只提供根憑證，則可以省略此步驟。

- CA簽名的證書作為TVS。導覽至**Certificate Management > Upload certificate > Certificate Purpose:電視**。設定證書描述並瀏覽當前CUCM節點的CA簽名證書檔案。

  附註：此時，CUCM會比較CSR和上傳的CA簽名證書。如果資訊相符，CSR就會消失，且系統會上傳新的CA簽名的憑證。如果您在上傳憑證後收到錯誤訊息，請參閱**上傳憑證常見錯誤訊息**一節。

步驟6.要將新證書應用到伺服器，必須重新啟動所需的服務（僅當服務運行且處於活動狀態時）。導覽至：

- **Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco TFTP**（運行服務的所有節點）
- **Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco Trust Verification Service**（運行服務的所有節點）

步驟7.重置所有電話：

- 導航至**Cisco Unified CM管理>系統>企業引數>重置**。系統將顯示一個彈出視窗，其中顯示「You are about to reset all devices in the system（您即將重置系統中的所有裝置）」語句。此操作無法撤消。是否繼續？選擇**OK**，然後按一下**Reset**。

  附註：通過RTMT監控裝置註冊。所有電話重新註冊後，您可以繼續使用下一個證書型別。

常見上傳證書錯誤消息疑難解答

本節列出了上傳CA簽名證書時的一些最常見錯誤消息。

CA證書在信任儲存中不可用

此錯誤表示根憑證或中間憑證未上傳到CUCM。在上傳服務證書之前，驗證這兩個證書是否已作為信任儲存上傳。

檔案/usr/local/platform/.security/tomcat/keys/tomcat.csr不存在

當證書(tomcat、callmanager、ipsec、capf、tvs)的CSR不存在時，將出現此錯誤。 確認之前已建立CSR，且憑證已根據該CSR建立。要牢記的要點：

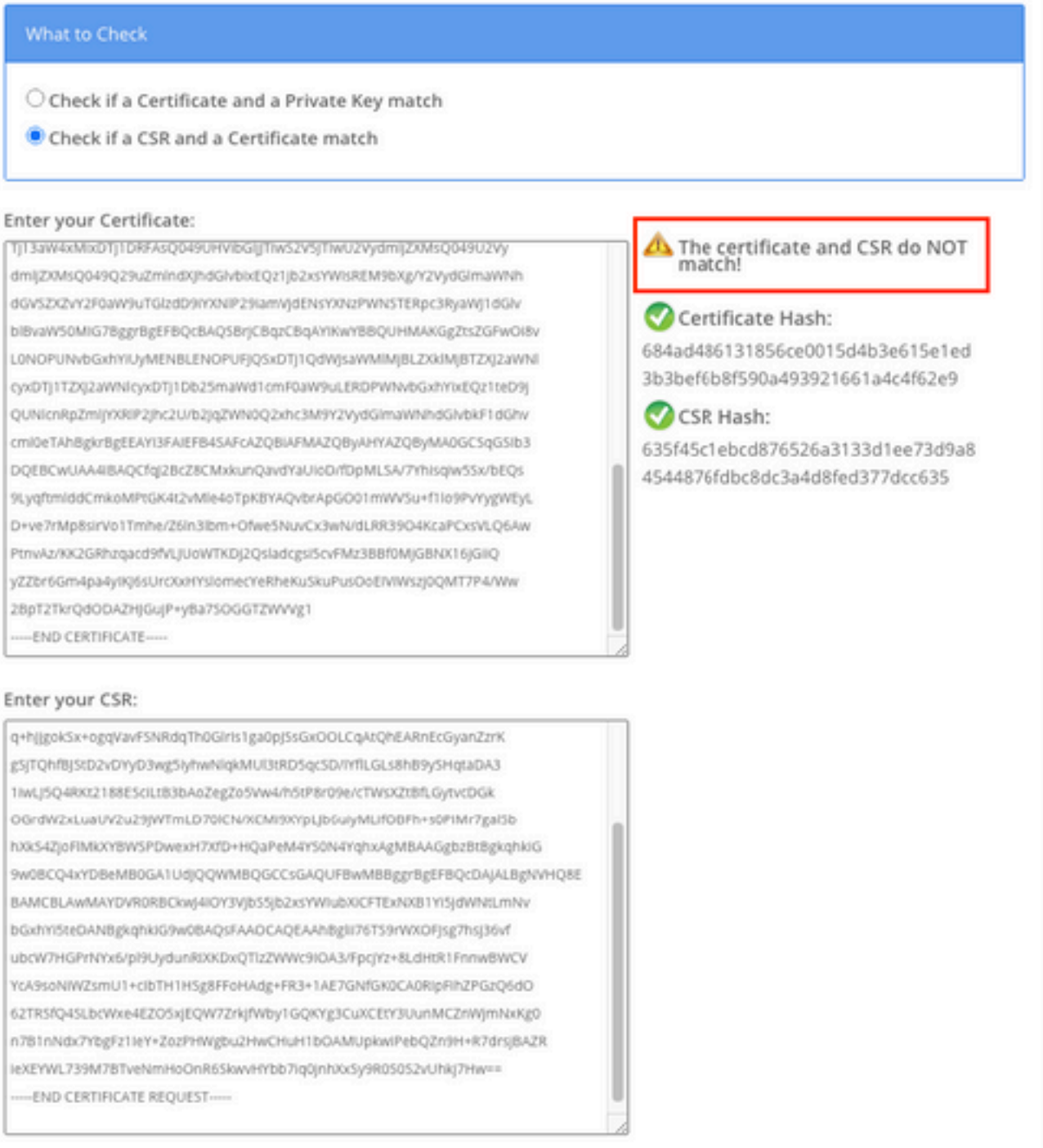
- 每個伺服器和證書型別只能存在1個CSR。這表示如果建立了新的CSR，則會替換舊的CSR。
- CUCM不支援萬用字元證書。
- 如果沒有新的CSR，則無法替換當前存在的服務證書。
- 同一問題的另一個可能的錯誤是「無法上載檔案/usr/local/platform/upload/certs//tomcat.der。」 這取決於CUCM版本。

CSR公鑰和證書公鑰不匹配

當CA提供的憑證與CSR檔案中傳送的憑證具有不同的公鑰時，系統會顯示此錯誤。可能的原因包括：

- 上傳了不正確的證書（可能來自另一個節點）。
- CA證書是使用不同的CSR生成的。
- 已重新產生CSR，並取代用於取得簽署憑證的舊CSR。

若要確認CSR和憑證公鑰是否相符，有多個工具線上，例如SSL。



同一問題的另一個可能的錯誤是「無法上載檔案/usr/local/platform/upload/certs//tomcat.der。」 這取決於CUCM版本。

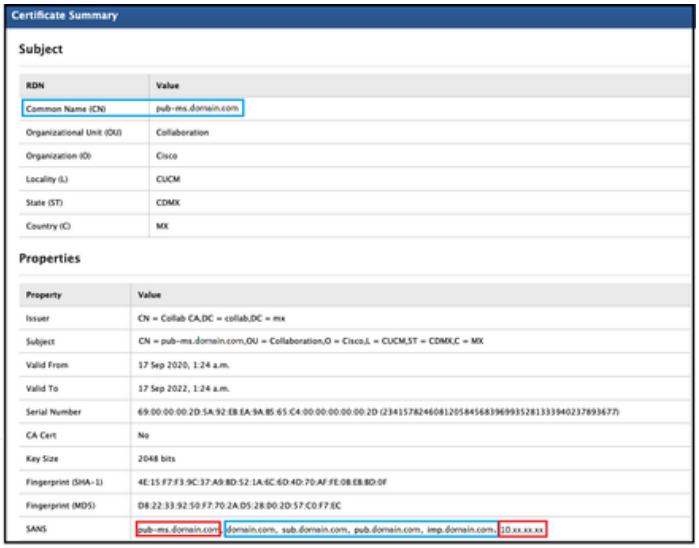
CSR使用者替代名稱(SAN)和憑證SAN不匹配

CSR和憑證之間的SAN必須相同。這將阻止對不允許的域進行認證。要驗證SAN不匹配，請執行以下步驟：

1.解碼CSR和證書（基礎64）。 線上提供不同的解碼器，例如Decoder。

2.比較SAN條目並驗證它們是否全部匹配。順序並不重要，但是CSR中的所有專案在憑證中必須相同。

例如，CA簽名的證書新增了兩個額外的SAN條目：證書的公用名和一個額外的IP地址。

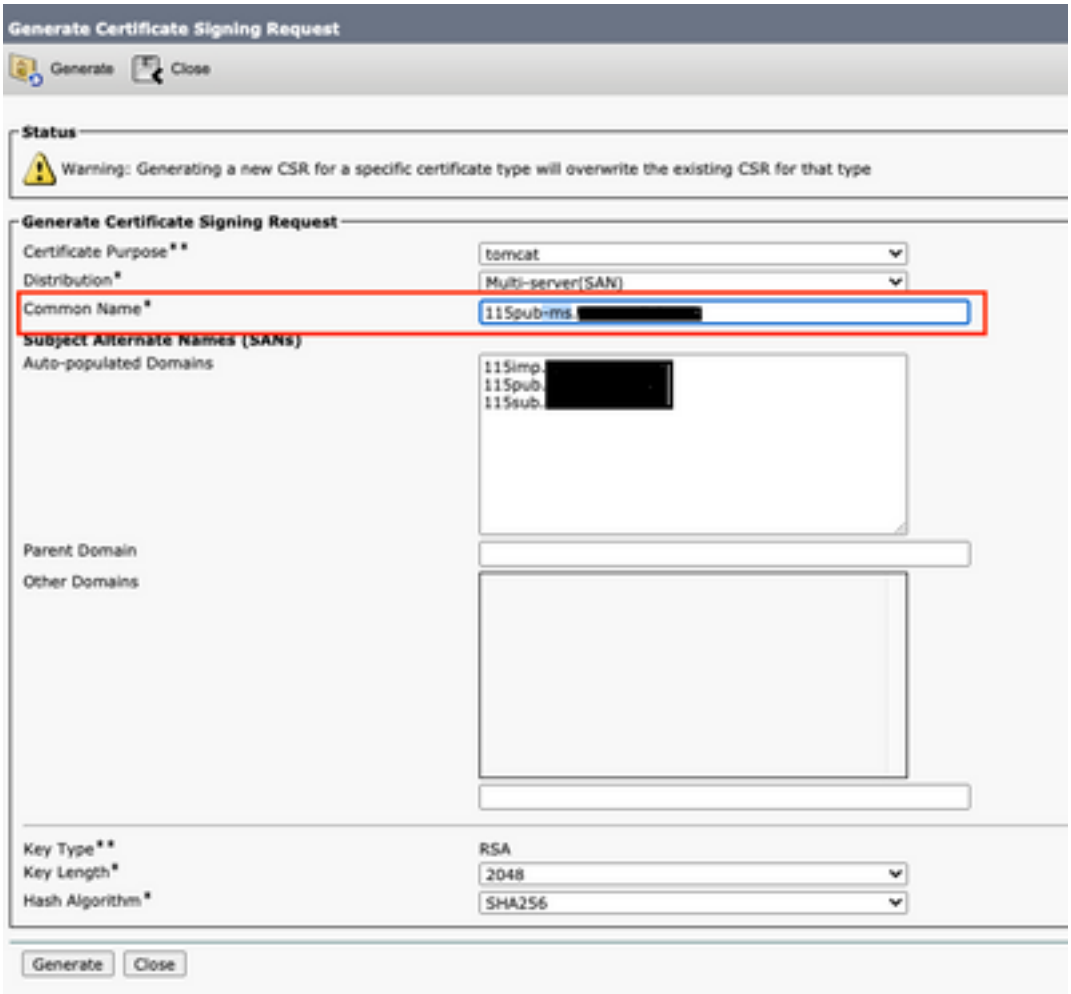


3.一旦您確定SAN不匹配，有兩種方法可以解決此問題：

1. 請您的CA管理員頒發一個證書，該證書與CSR中傳送的SAN條目完全相同。
2. 在CUCM中建立符合CA要求的CSR。

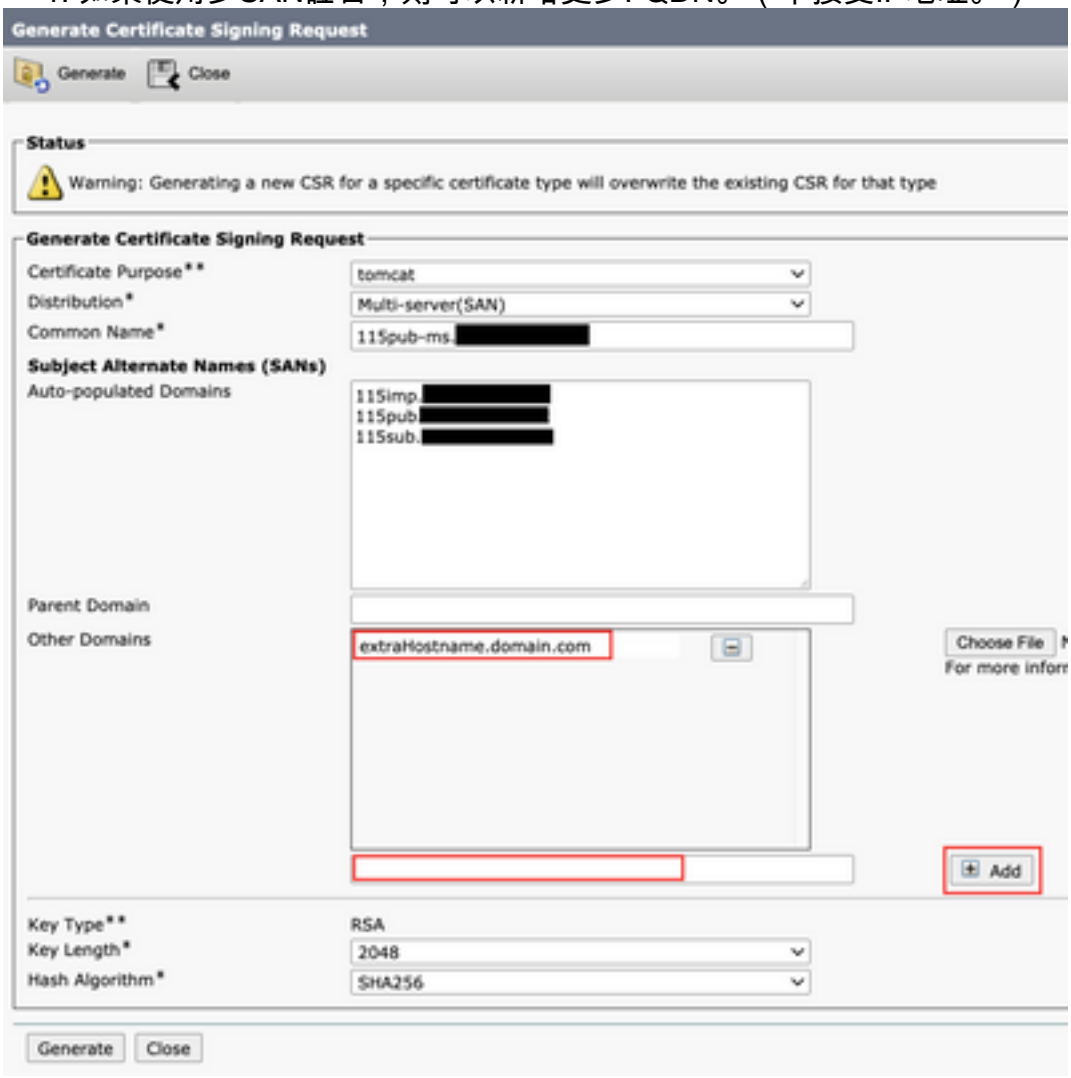
修改由CUCM建立的CSR:

1. 如果CA刪除域，則無需域即可在CUCM中建立CSR。建立CSR時，刪除預設填充的域。
2. 如果建立多SAN憑證，則有些CA不會接受公用名稱中的「 — ms」。建立CSR時，可以將「 — ms」從CSR中移除。



3.新增除CUCM自動完成的名稱以外的替代名稱：

1. 如果使用多SAN證書，則可以新增更多FQDN。（不接受IP地址。）



b.如果證書為單節點，請使用 set web-security 指令。此命令甚至適用於多SAN證書。（可以新增任何型別的域，也允許IP地址。）

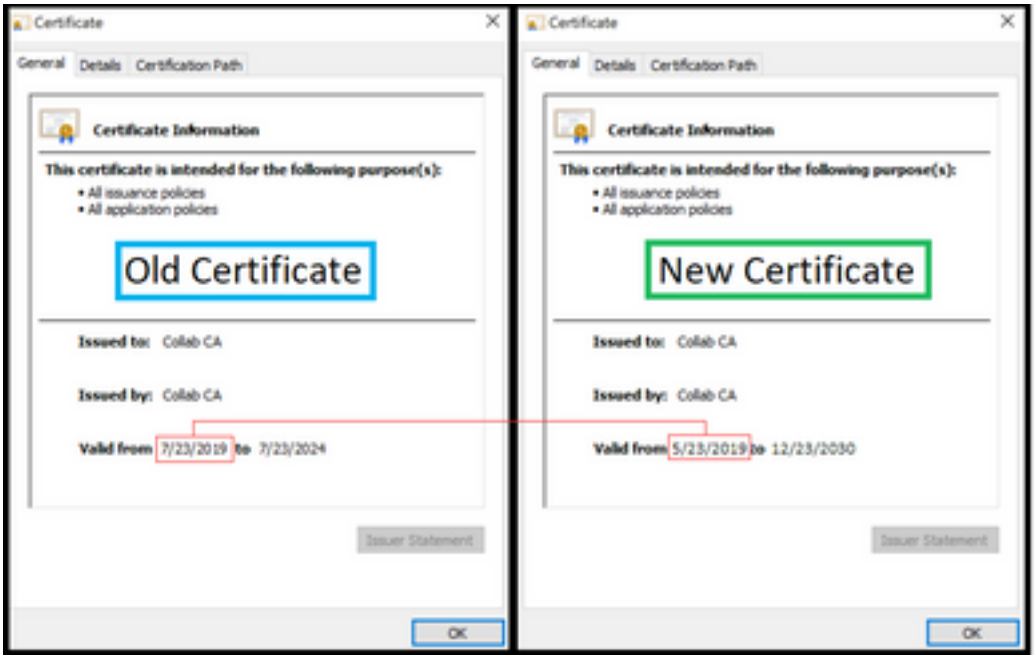
有關詳細資訊，請參閱命令列參考指南。

不會更換具有相同CN的信任證書

CUCM設計為僅儲存一個具有相同公用名稱和相同證書型別的證書。這意味著，如果資料庫中已經存在tomcat-trust證書，並且需要用具有相同CN的最近證書替換該證書，則CUCM將刪除舊證書，並用新證書替換。

在某些情況下，CUCM不替換舊證書：

1. 上傳的證書已過期：CUCM不允許上傳過期的證書。
2. 舊證書的「FROM」日期比新證書的日期更近。CUCM保留最新的證書，並且使用較舊的「FROM」日期將其目錄為較舊的。在此案例中，必須刪除不需要的憑證，然後上傳新憑證。


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All issuance policies
• All application policies
Old Certificate
Issued to: Collab CA
Issued by: Collab CA
Valid from 7/23/2019 to 7/23/2024
Issuer Statement
OK
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All issuance policies
• All application policies
New Certificate
Issued to: Collab CA
Issued by: Collab CA
Valid from 5/23/2019 to 12/23/2030
Issuer Statement
OK

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）。