瞭解移動和遠端訪問證書要求和ATS歷史記錄

目錄

簡介

本檔案介紹適用於行動及遠端存取的CUCM上的憑證上傳要求。

背景資訊

Cisco Expressway使用Apache Traffic Server(ATS)。流量伺服器是遍歷解決方案中非常重要的元件，主要用於以下功能：

- 證書驗證：它對Cisco Unified Communications Manager(CUCM)、即時消息和線上狀態以及Unity伺服器節點執行MRA服務的證書驗證。
- 代理和快取：它充當HTTP/HTTPS流量的快速、可擴展快取代理伺服器。

Expressway版本14.0.2

流量伺服器(ATS)在MRA調配期間與CUCM協商時，會開始看到「證書驗證」的輕微實施。

要求記錄在CSCvz45074下，其中簽署Expressway核心伺服器證書的根證書必須作為Tomcat-Trust和Callmanager Trust上載到CUCM:https://cdetsng.cisco.com/summary/#/defect/CSCvz45074。

- 流量伺服器實施證書驗證。
- 升級到X14.0.2版本之前，請確保符合此證書要求。

要求 — 必須向CUCM的tomcat-trust和CallManager-trust清單中新增簽署Expressway-C證書的證書頒發機構(CA)鏈（根+中介），即使Unified Communications Manager(UCM)處於非安全模式也是如此。

原因 — 每當伺服器UCM請求證書時，Expressway中的流量伺服器服務都會傳送其證書。這些請求

適用於在8443以外的埠（例如埠6971、6972等）上運行的服務。 即使UCM處於非安全模式，這也會強制進行證書驗證。有關詳細資訊，請參閱通過Expressway進行移動和遠端訪問部署指南。

早於14.0.8版本的行為

處理Expressway-C和統一通訊節點之間的安全HTTPS雙向連線的Expressway-C上的流量伺服器未驗證遠端端提供的證書。在MRA配置下，在Configuration > Unified Communications > Unified CM servers/IM and Presence Service nodes/Unity Connection servers下新增CUCM、IM&P或Unity伺服器時，可以選擇將TLS驗證模式配置為「On」，以驗證TLS證書。配置選項顯示在下一個螢幕截圖中，指示它驗證SAN中的FQDN或IP、證書的有效性以及證書是否由受信任的CA簽名。

還存在一個已知問題，即無法將兩個具有相同CN名稱的證書載入到Expressway信任儲存上。此限制導致了兩個問題：

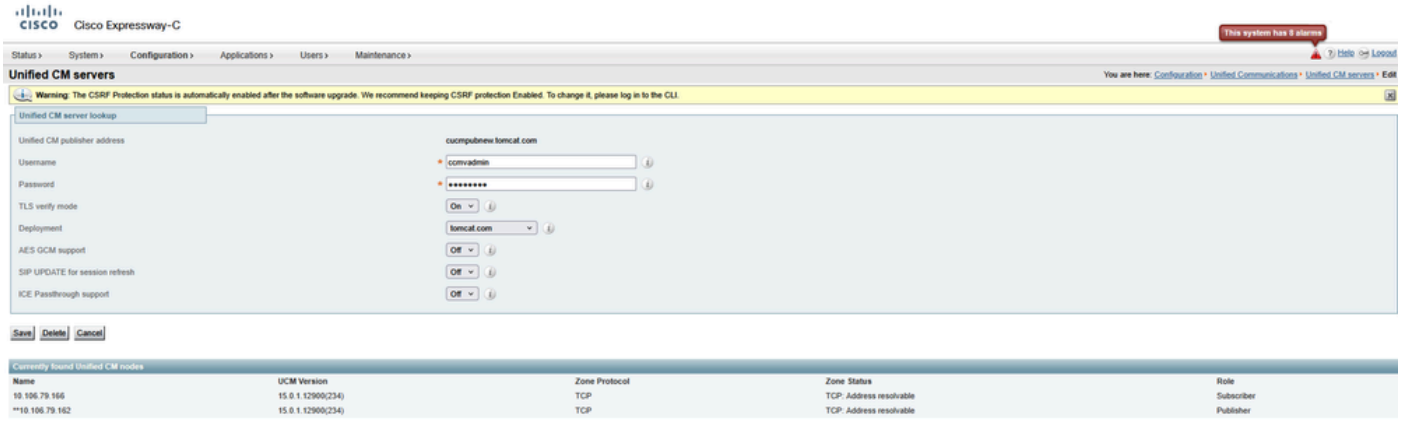
1.如果選擇在Expressway信任儲存上載入呼叫管理器證書，則新增CUCM時，TLS驗證「開啟」將失敗。

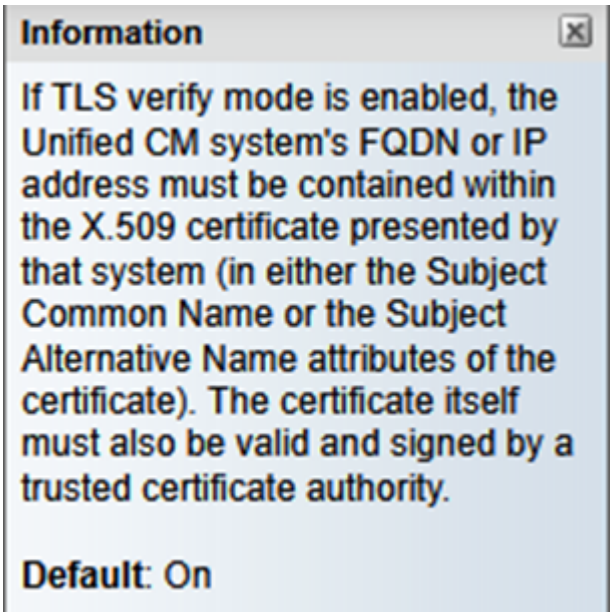
2:如果選擇在Expressway信任儲存上載入Tomcat證書，則在5061上安全sip註冊將失敗。

此行為記錄在CSCwa12894中。

此外，此TLS證書驗證檢查僅在發現CUCM/IM&P/Unity伺服器時進行，而不是在MRA客戶端調配期間進行。

此配置的缺點在於它只針對您新增的發佈伺服器地址進行驗證。在從發佈伺服器節點的資料庫中檢索訂閱伺服器節點資訊（FQDN或IP）時，不會驗證訂閱伺服器節點上的證書是否設定正確。





版本14.0.8及更高版本上的行為

從X14.0.8版本開始，Expressway伺服器對通過流量伺服器發出的每個HTTPS請求執行TLS證書驗證。這意味著，在發現CUCM/IM&P/Unity節點期間，當TLS驗證模式設定為「關閉」時，它也會執行此操作。如果驗證未成功，則TLS握手不會完成，並且請求失敗，這會導致功能丟失（例如，冗餘、故障切換問題或完全登入失敗）。此外，如果將「TLS驗證模式」設定為「開」，則不能保證所有連線都能正常運行（如後面的示例所述）。

Expressway向CUCM/IM&P/Unity節點檢查的確切證書如MRA指南一節所示。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X15-0/mra/exwy_b_mra-deployment-guide-x150.pdf

截面

Certificate Requirements > Certificate Exchange Requirements

由於Expressway-Core和CUCM之間的通訊方式發生了這些變化，必須確保：

1.建議對移動和遠端訪問使用CA簽名的證書。

2.每個Unified CM集群必須信任Expressway-C證書。對於每個群集，請確保：

- 如果啟用混合模式 — 必須將Expressway-C證書安裝到Unified CM上的CallManager-trust和Tomcat-trust儲存區。
- 如果禁用混合模式 — 必須將Expressway-C證書的根CA證書安裝到Unified CM上的CallManager-trust和Tomcat-trust儲存區。然後重新啟動以下專案：· Tomcat服務· CallManager服務· HA代理服務（如果在Tomcat上使用TLS）。

在Expressway-Core上，確保採取以下措施：

- Expressway-C必須信任每個Unified CM和IM and Presence Service群集提供的證書。

Expressway-C的信任儲存必須包括根CA證書，該證書用於為所有UC群集簽署Unified CM和IM and Presence Service證書。

附註：確保將所有用於簽署Expressway-C證書的根和中間CA證書或完整CA鏈新增到Cisco Unified Communications Manager(UCM)的Tomcat-trust和CallManager-trust清單中，即使UCM在非安全模式下運行。

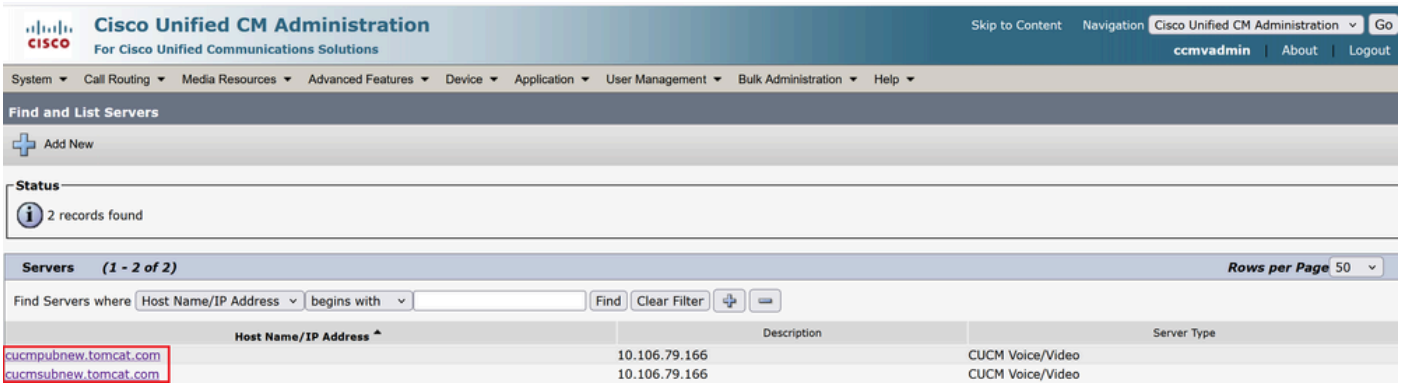
原因 — 每當伺服器(UCM)請求證書時，Expressway中的流量伺服器服務都會傳送其證書。這些請求適用於在8443以外的埠（例如埠6971、6972等）上運行的服務。 即使UCM處於非安全模式，這也會強制進行證書驗證。

在System > Server下新增CUCM地址的方式在Configuration > Unified Communications > Unified CM servers/IM and Presence Service nodes下新增Expressway核心上的CUCM/IMP時起著非常重要的作用。

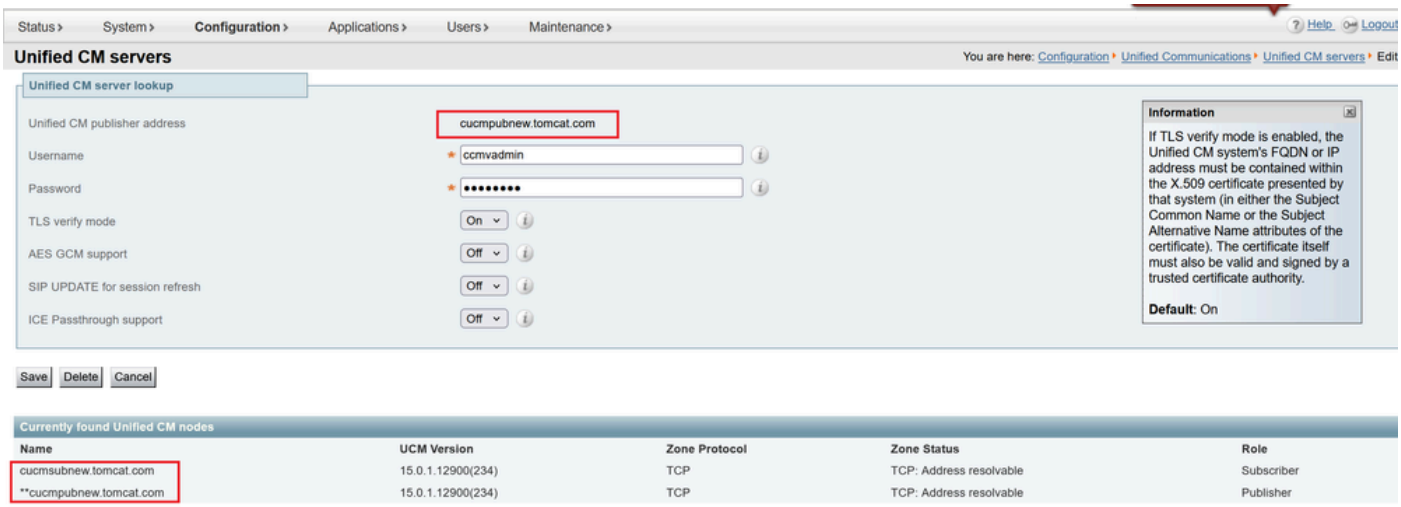
必須始終使用FQDN新增CUCM，而不是使用主機名或IP地址。如果發現CUCM在System > Server下新增為主機名/IP地址

在TLS握手期間，TLS驗證「開啟」將失敗，並且不會在Expressway-Core上新增CUCM集群。

下圖顯示新增為主機名的CUCM:



下圖顯示使用FQDN和TLS驗證模式=ON在Expressway-Core上新增的CUCM:

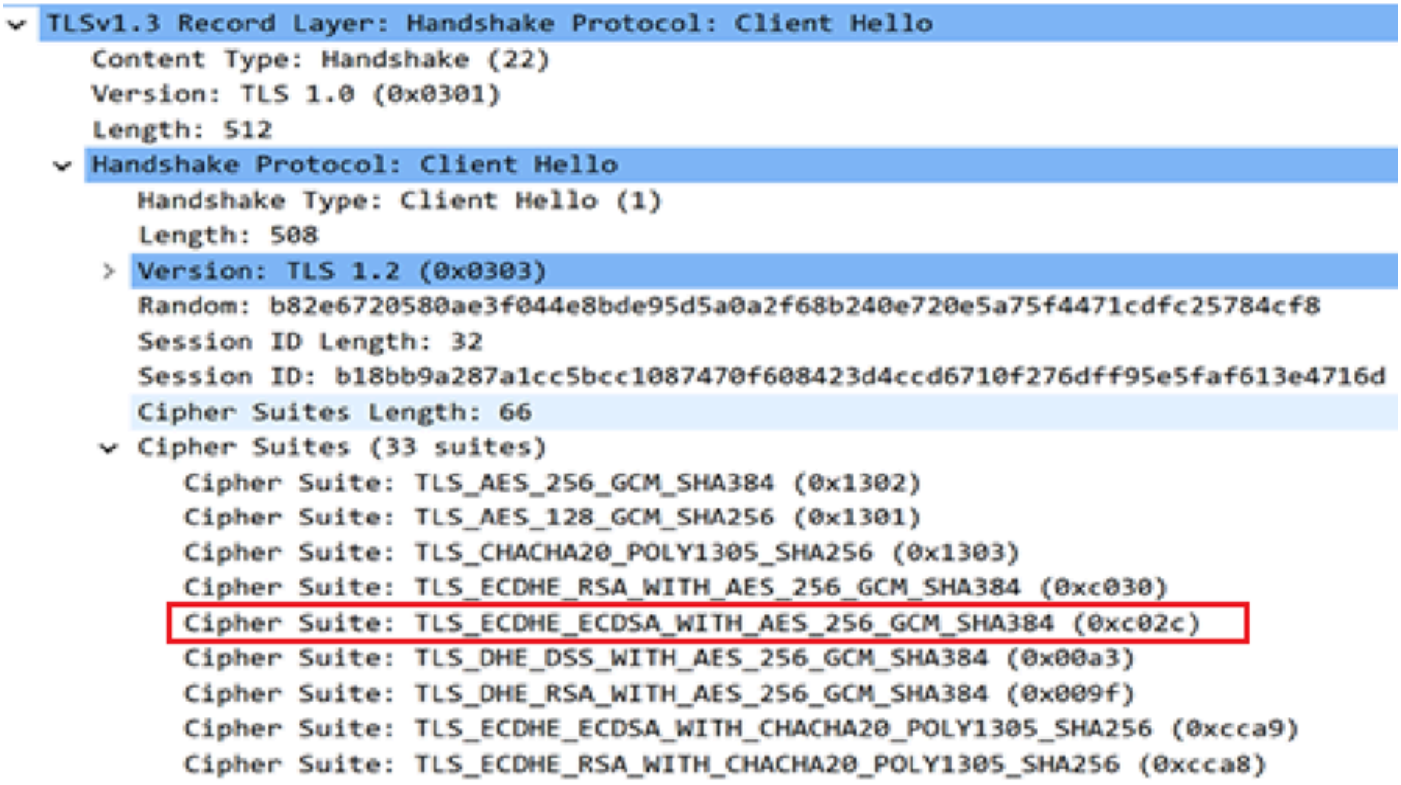


X14.2中還引入了一個更改，該更改將在TLS握手（客戶端問候）期間以不同的優先順序顯示密碼。這取決於升級路徑，並在軟體升級後導致意外的TLS連線。可能是，在TLS握手期間升級之前，它請求從CUCM獲得Cisco Tomcat或Cisco CallManager證書。但在升級後，它請求使用ECDSA變體（比RSA更安全的密碼變體）。 Cisco Tomcat-ECDSA或Cisco CallManager-ECDSA證書可以由其他CA簽名，也可以僅由自簽名證書簽名（預設）。

此密碼首選項順序的更改並非始終與您相關，因為它取決於升級路徑，如Expressway X14.2.1版本說明所示。簡而言之，您可以從維護>安全性>密碼中檢視每個密碼清單是否預置ECDHE-RSA-AES256-GCM-SHA384。如果沒有，則它會優先使用較新的ECDSA密碼而非RSA密碼。如果是，則您有與之前的RSA相同的行為，其優先順序別較高。

下一個螢幕截圖顯示在客戶端hello中TLS協商消息期間Expressway核心通告的ECDSA密碼的紅色方框中，#IF TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384由伺服器hello中的遠端響應方(CUCM)選擇，則TLS協商將失敗，如果：

根CA證書或來自Responder的實際ECDSA證書，即在此案例中，CUCM未安裝在Expressway信任儲存上。



或者，您也可以修改Expressway密碼，使ECDSA不優先。

1.通過附加GCM-Sha384開放式SSL字串修改SIP密碼。

"ECDHE-RSA-AES256-GCM-SHA384:EECDH:EDH:HIGH:.....:!MD5:!PSK:!eNULL:!aNULL:!aDH"

2.添加+以最後移動密碼，或新增!以永久禁用ECDSA。

密碼："EECDH:EDH:HIGH:-

AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL:!aDH:+ECDSA"

3.在CUCM上新增簽署ECDSA證書的根和中間CA證書，或在Expressway信任儲存上新增Tomcat-ECDSA證書（在某些情況下）。

但是，由於密碼優先順序的變更、升級後，MRA部署可能會中斷，因此TAC必須執行前面提到的解決方法，才能使工作重新正常。

隨著TLS 1.3的引入，在Wireshark中檢查交換的證書變得更為困難。

x15.3版本上的行為

僅對於SIP介面，您可以選擇使用RSA或ECDSA密碼。

X15.x TLS 1.3已實施。從欄位上看，RSA演算法大多優於ECDSA。現在升級到x15.2的客戶可以選擇

RSA和ECDSA演算法之間的連線：

xConfiguration SIP Advanced TlsSignatureAlgoPrefRsa:開/關

TlssignatureAlgoPrefRSA僅在SIP介面具有TLS 1.3時有效

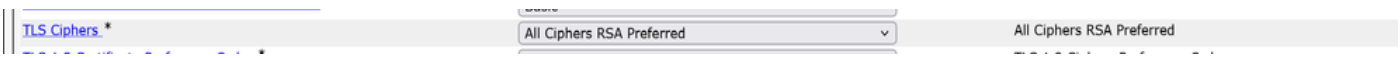
xConfiguration SIP Advanced SipTlsVersions:"TLSv1.3"

附註：目前這僅適用於SIP介面。8443上的Traffic Server和Tomcat注意事項保持不變，如前文所述。

選擇RSA後，Expressway向CUCM傳送的「客戶端問候」期間傳送的密碼套餐將顯示如下。

- 簽名演算法：rsa_pss_rsae_sha512(0x0806)
- 簽名演算法：rsa_pss_rsae_sha384(0x0805)
- 簽名演算法：rsa_pss_rsae_sha256(0x0804)
- 簽名演算法：ecdsa_secp521r1_sha512(0x0603)
- 簽名演算法：ecdsa_secp384r1_sha384(0x0503)
- 簽名演算法：ecdsa_secp256r1_sha256(0x0403)

在Enterprise Parameters > Security Parameters下，早期的配置將在您在CUCM到TLS密碼上選擇的配置上協同工作。



此外，必須注意的是，在Expressway-C和CUCM之間通過TLS 1.3進行斷開的TLS握手期間，診斷日誌或PCAP中列印的錯誤不會非常有用。在使用TAC時啟用這些調試是值得的，以便元件可以列印清楚的錯誤以進行故障排除。

xConfiguration Logger Developer developer.trafficserver.http級別："調試"
xConfiguration Logger Developer developer.trafficserver.http_trans級別："調試"
xConfiguration Logger Developer .trafficserver.iocore級別："調試"
xConfiguration Logger Developer developer.trafficserver.ssl級別："調試"

當Callmanager與多個服務共用一個證書時的期望值

在CUCM上重複使用證書後，情況略有變化。

從CUCM 14.0開始，您可以重複使用Tomcat和Tomcat ECDSA證書作為Call manager和Call manager ECDSA。

Tomcat證書可以作為Callmanager證書重新使用。

Tomcat-ECDSA證書可以重用為Callmanager-ECDSA證書。

這讓生活變得輕鬆。

1. CUCM上的多個服務現在使用一個證書，從而降低了證書的成本。

2.證書管理減少。

3.如果您需要在Expressway-Core信任儲存上上傳Tomcat/Callmanager或Tomcat-ECDSA/Callmanager-ECDSA證書（出於任何原因），則只需上傳一個證書。不存在相同的CN名稱問題（本文檔前面已討論）。

附註：只有當Tomcat和Tomcat-ECDSA是多SAN證書時，才會重複使用證書。

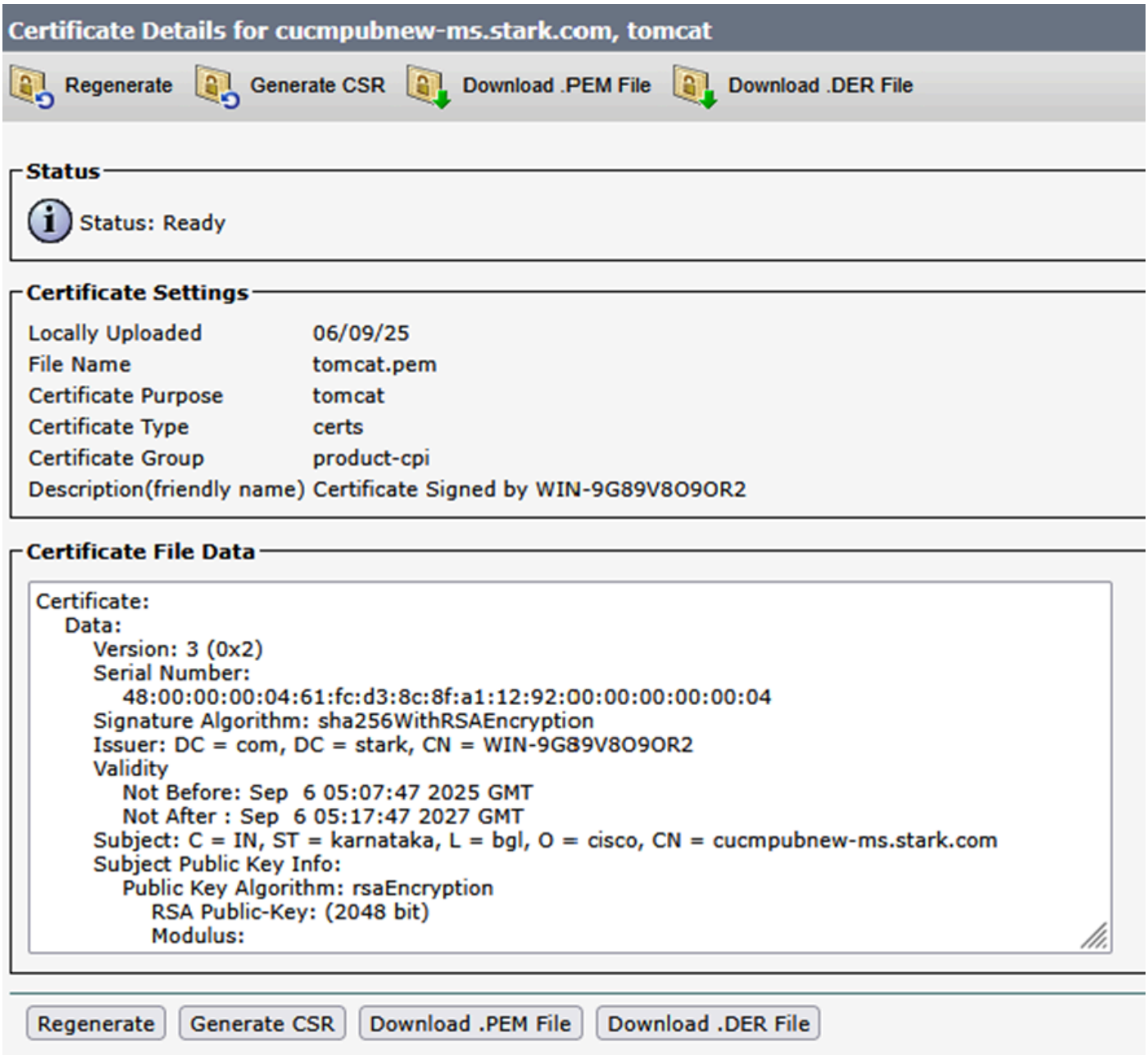
Post Reuse、Callmanager和Callmanager ECDSA伺服器證書在CUCM信任儲存上不可見。您可以通過運行以下命令從CLI驗證證書重複使用：

show cert own CallManager

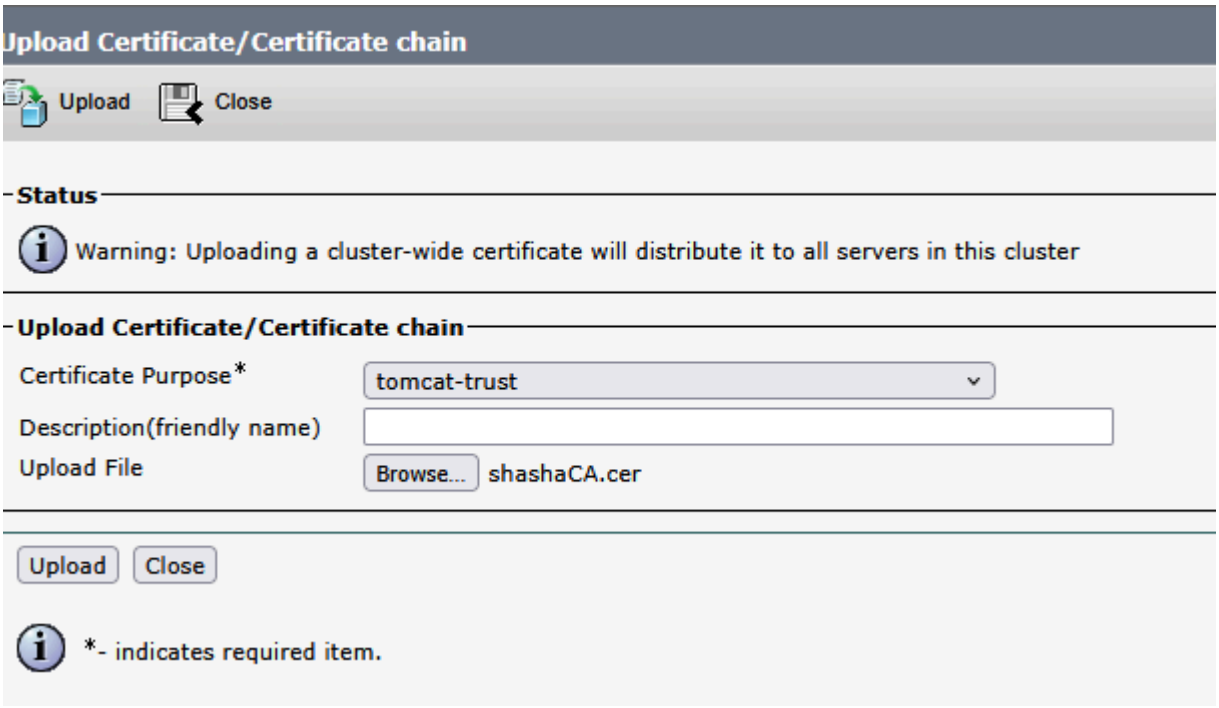
show cert own tomcat

重新使用證書的步驟

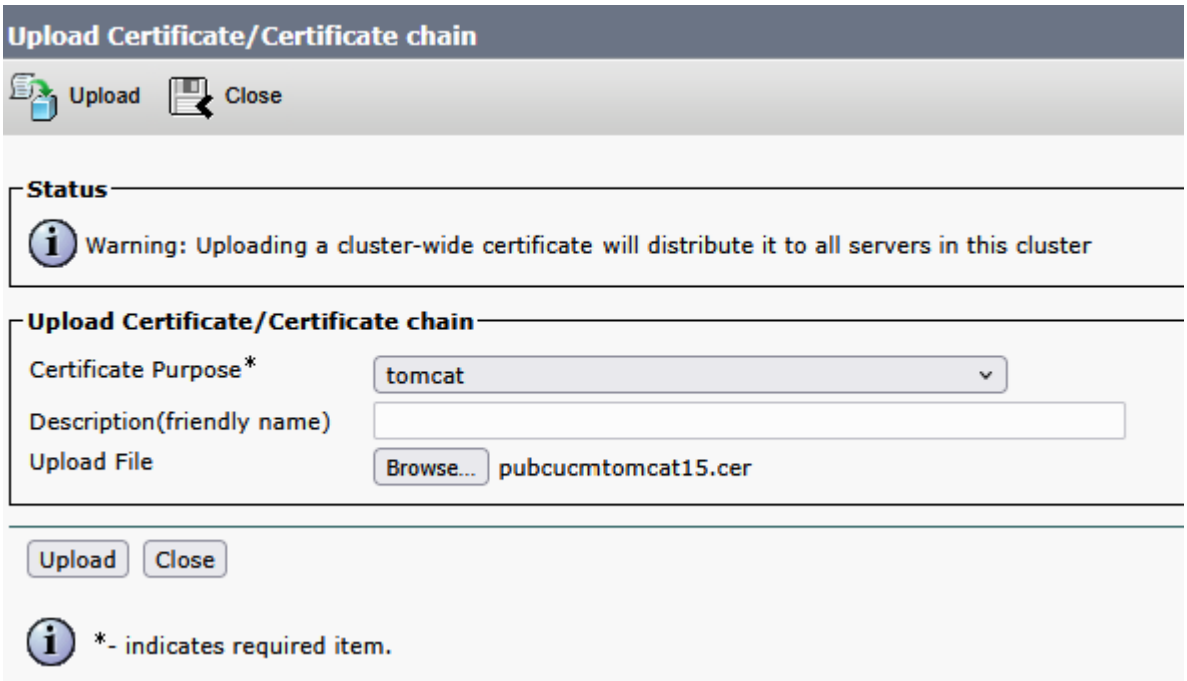
正在生成Tomcat CSR pub add。



上傳CA證書，該證書將作為Tomcat-trust在CUCM上簽署Tomcat證書。



簽署Tomcat證書後，即可上傳到發佈伺服器上。根據提示重新啟動相關服務。



簽署Tomcat證書後，即可上傳到發佈伺服器上。根據提示重新啟動相關服務。

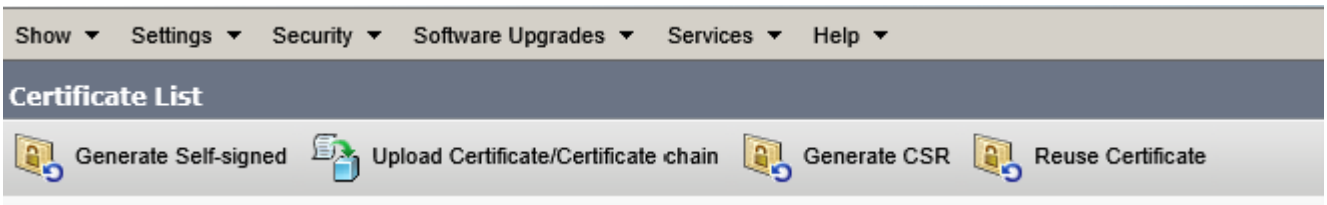
成功：證書已上載。執行災難恢復備份，以便最新備份包含上傳的證書。
在所有群集節點(UCM/IMP)上使用CLI「utils service restart Cisco Tomcat」重新啟動Cisco Tomcat Web服務。 在所有UCM群集節點上使用CLI「utils service restart Cisco UDS Tomcat and utils service restart Cisco AXL Tomcat」重新啟動Cisco UDS Tomcat和Cisco AXL Tomcat Web服務。此外，在發佈器節點上重新啟動Cisco DRF Master和Cisco DRF Local服務。僅重啟使用者節點上的Cisco DRF本地服務。

Tomcat證書現在由CA簽名。

tomcat	cucmpubnew-ms.stark.com_51dc40f400000000000b	signed IdentityCA-signed	RSA	Multi-server(SAN)	RICKY200-TMS-CA	10/23/2027	Certificate Signed by RICKY200-TMS-CA

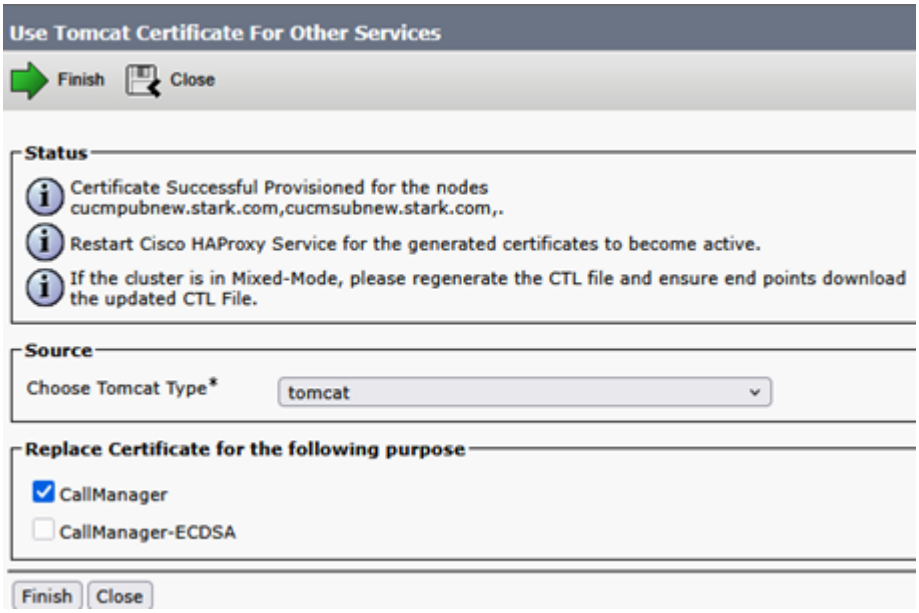
以便立即將Tomcat證書重新用作Callmanager證書。

按一下「Reuse Certificate」。



在下拉選單中選擇Tomcat並檢查Callmanager證書。

按一下「Finish」（結束）。



Tomcat證書現在被重用為Callmanager證書。這可通過CLI進行驗證。

Callmanager證書序列號(SN):56:ff:6c:71:00:00:00:00:00:00:0d

```
admin:show cert own CallManager
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            56:ff:6c:71:00:00:00:00:00:0d
        Signature Algorithm: sha384WithRSAEncryption
        Issuer: DC = com, DC = RICKY200, CN = RICKY200-TMS-CA
        Validity
            Not Before: Oct 24 08:44:34 2025 GMT
            Not After : Oct 24 08:54:34 2027 GMT
        Subject: C = IN, ST = karnataka, L = bgl, O = cisco, CN = cucmpubnew-ms.
tomcat.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:b4:a6:fa:8f:9a:c3:32:02:74:fa:e9:92:30:de:
                    6e:3b:70:cd:d7:4e:64:e4:71:04:fe:17:80:0d:5b:
                    44:d1:7f:00:63:69:4a:5c:1a:1b:75:0c:1a:d6:ce:
                    10:3f:01:e2:d0:f1:75:33:57:b7:0a:71:e1:60:d1:
                    89:3c:e8:a4:8c:3e:30:69:4d:4e:98:da:b8:5d:dd:
                    23:8c:4d:69:90:69:9d:43:74:84:20:a8:9f:45:dc:
                    5a:aa:7b:c8:d1:d0:6f:05:13:d8:99:58:0e:49:7b:
Press <enter> for 1 line, <space> for one page, or <q> to quit
```

Tomcat certificate SN:56:ff:6c:71:00:00:00:00:00:00:0d

```
admin:show cert own tomcat
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            56:ff:6c:71:00:00:00:00:00:0d
        Signature Algorithm: sha384WithRSAEncryption
        Issuer: DC = com, DC = RICKY200, CN = RICKY200-TMS-CA
        Validity
            Not Before: Oct 24 08:44:34 2025 GMT
            Not After : Oct 24 08:54:34 2027 GMT
        Subject: C = IN, ST = karnataka, L = bgl, O = cisco, CN = cucmpubnew-ms.tomcat.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:b4:a6:fa:8f:9a:c3:32:02:74:fa:e9:92:30:de:
                    6e:3b:70:cd:d7:4e:64:e4:71:04:fe:17:80:0d:5b:
                    44:d1:7f:00:63:69:4a:5c:1a:1b:75:0c:1a:d6:ce:
                    10:3f:01:e2:d0:f1:75:33:57:b7:0a:71:e1:60:d1:
                    89:3c:e8:a4:8c:3e:30:69:4d:4e:98:da:b8:5d:dd:
                    23:8c:4d:69:90:69:9d:43:74:84:20:a8:9f:45:dc:
                    5a:aa:7b:c8:d1:d0:6f:05:13:d8:99:58:0e:49:7b:
Press <enter> for 1 line, <space> for one page, or <q> to quit
```

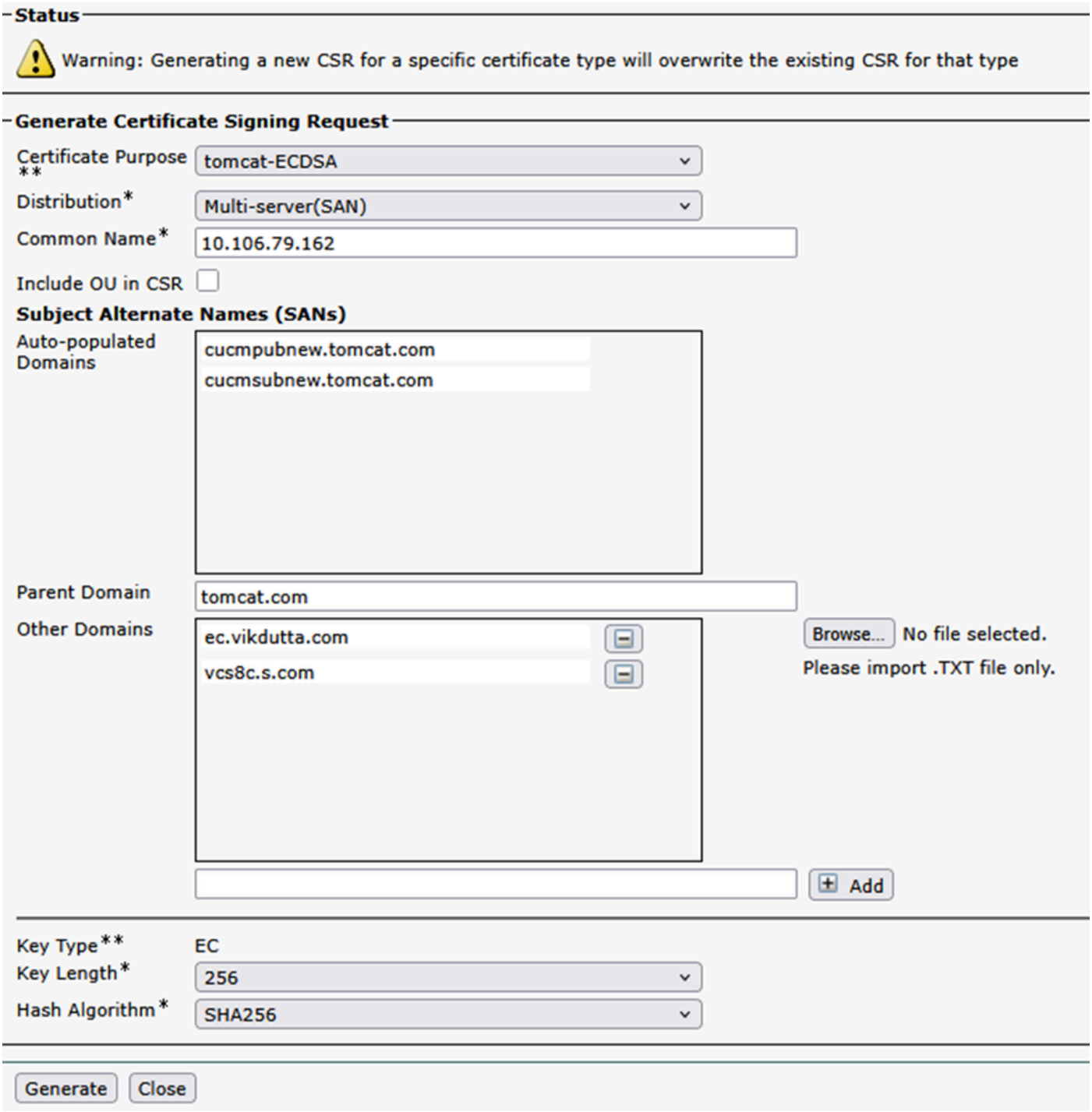
對訂閱伺服器執行相同步驟。

允許立即對ECDSA證書簽名，以便它可以作為Callmanager-ECDSA重複使用。

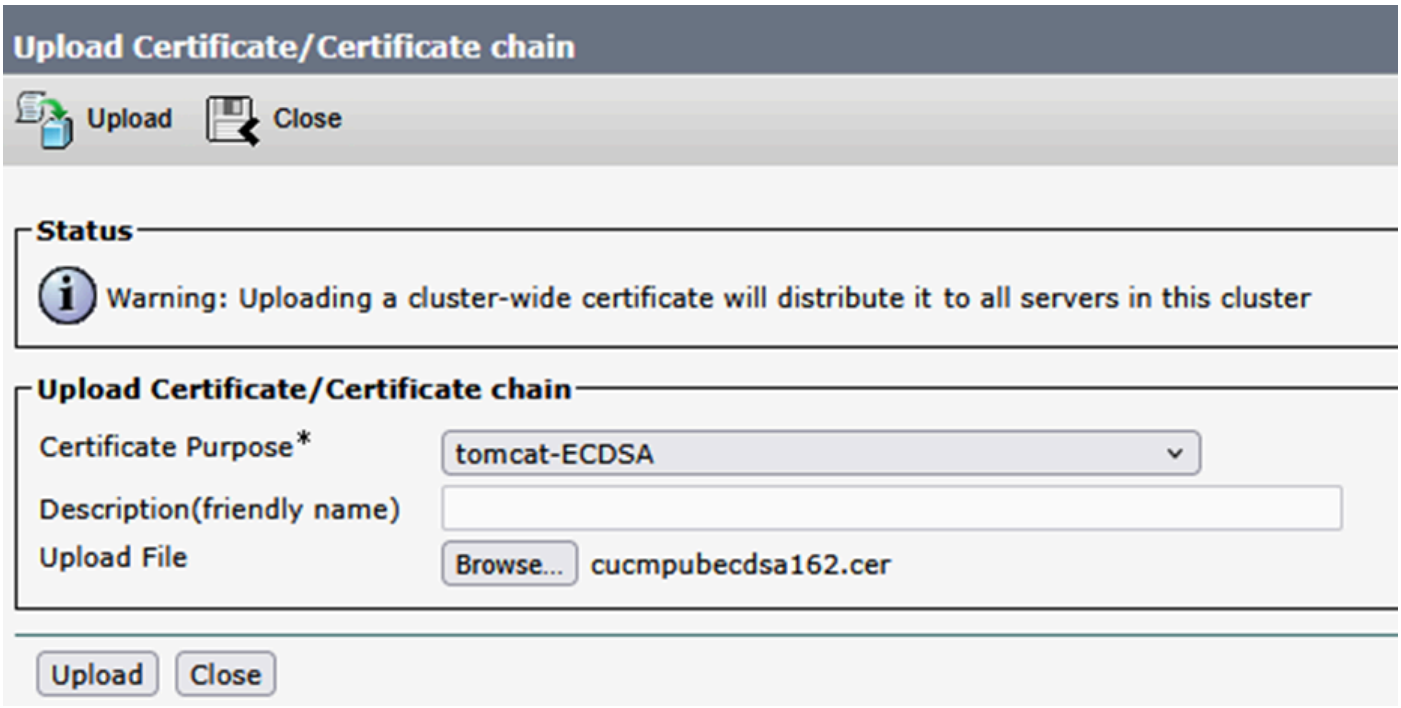
當前的Tomcat-ECDSA證書是自簽名的。

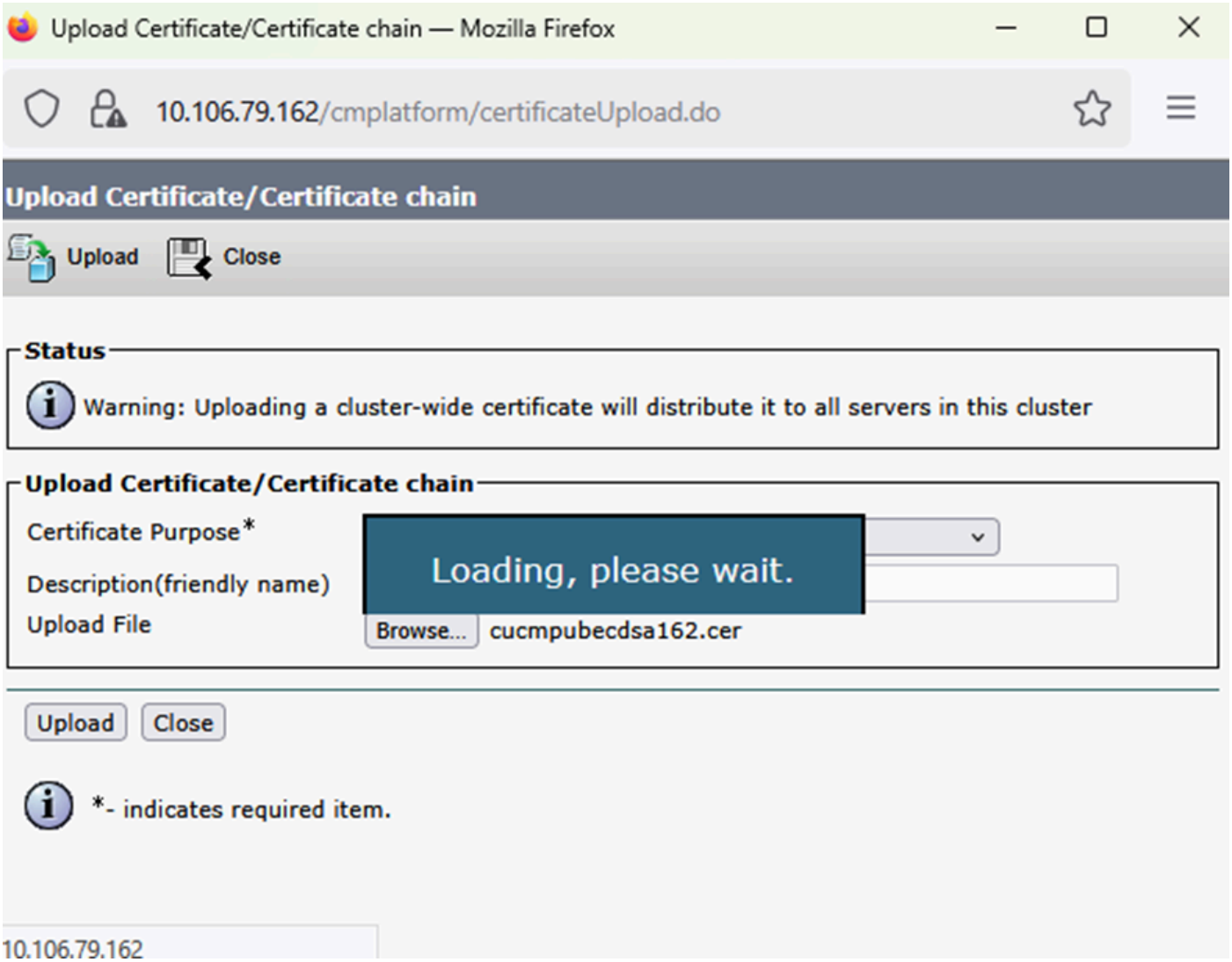
tomcat	10.106.79.162_5aceb67f00000000000f	Identity	CA-signed	RSA	Multi-server(SAN)	RICKY200-TMS-CA	10/25/2027	Certificate Signed by RICKY200-TMS-CA
tomcat-ECDSA	cucmpubnew-EC.tomcat.com_4b404cd202f54fcabf8a8db78c715d4b	Identity	self-signed	EC	cucmpubnew.tomcat.com	cucmpubnew-EC.tomcat.com	10/23/2030	Self-signed certificate generated by system

為Tomcat-ECDSA證書簽署多san CSR。

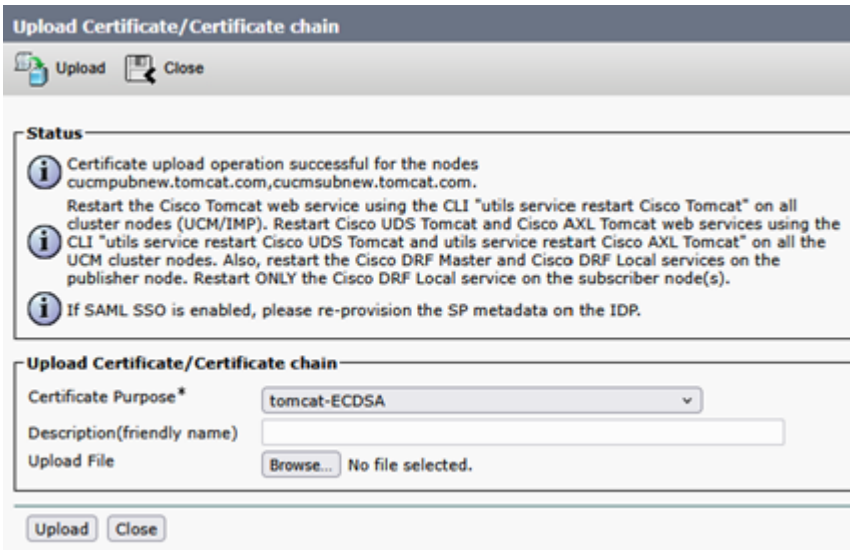


使用CSR簽署憑證並上傳。



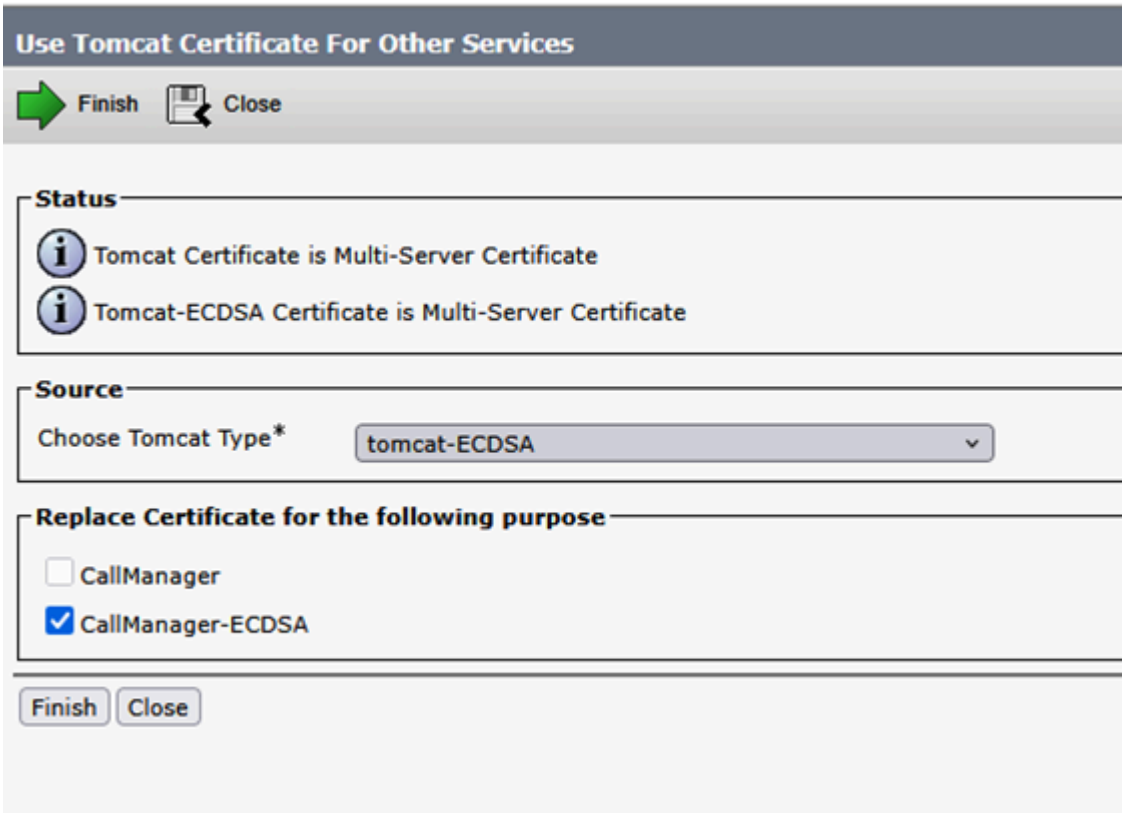


上傳成功。根據提示重新啟動相關服務。

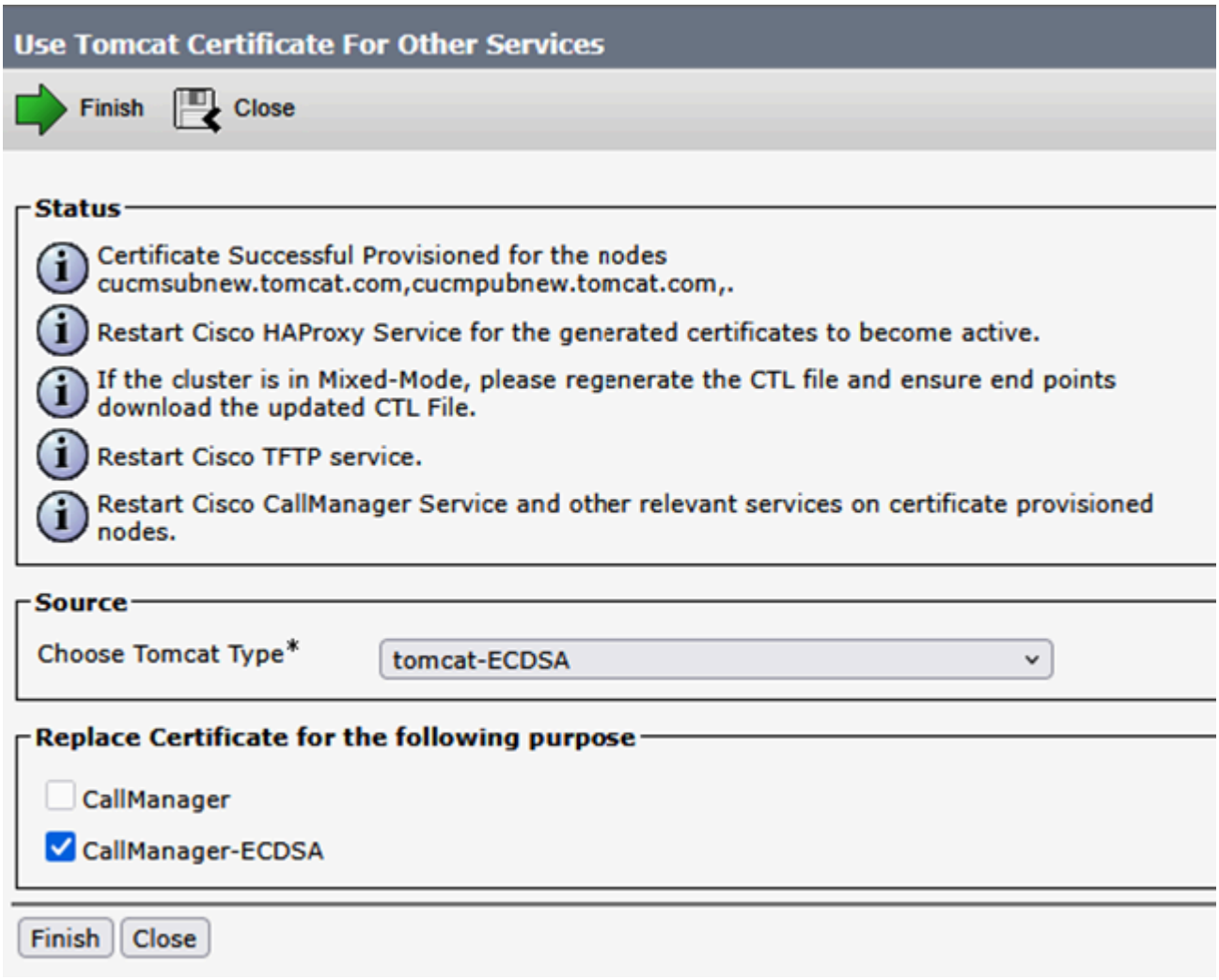


由CA簽名的Tomcat和Tomcat-ECDSA。

現在將Tomcat-ECDSA重用為Callmanager-ECDSA證書。



上傳成功。根據提示重新啟動相關服務。



從CLI驗證憑證。

Callmanager-ECDSA證書SN:2f:00:00:00:38:80:be:cc:a8:a1:8e:8f:23:00:00:00:00:00:38

```
admin:show cert own CallManager-ecdsa
Invalid Certificate Name. Certificate Not Found.

admin:show cert own CallManager-Ecdsa
Invalid Certificate Name. Certificate Not Found.

admin:show cert own tomcat-ECDSA
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            2f:00:00:00:38:80:be:cc:a8:a1:8e:8f:23:00:00:00:00:00:38
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC = com, DC = bgluclab, CN = bgluclab-WIN-DC-01-CA
        Validity
            Not Before: Oct 25 06:46:37 2025 GMT
            Not After : Oct 25 06:46:37 2026 GMT
```

Tomcat-ECDSA證書SN:2f:00:00:00:38:80:be:cc:a8:a1:8e:8f:23:00:00:00:00:00:38。

```
admin:show cert own tomcat-ECDSA
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            2f:00:00:00:38:80:be:cc:a8:a1:8e:8f:23:00:00:00:00:00:38
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: DC = com, DC = bgluclab, CN = bgluclab-WIN-DC-01-CA
        Validity
            Not Before: Oct 25 06:46:37 2025 GMT
            Not After : Oct 25 06:46:37 2026 GMT
        Subject: C = IN, ST = karnataka, L = bgl, O = cisco, CN = cucmpubnew-EC-ms.tomcat.com
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
```

由於您現在對兩個服務使用了一個證書，即，用於Tomcat和Callmanager服務的Tomcat證書，以及用於Tomcat-ECDSA和Callmanager-ECDSA服務的Tomcat-ECDSA，因此在Expressway信任儲存上上傳證書變得不那麼麻煩（如果需要上傳）。

在用於MRA的expressway-core上新增UCM時，讓TLS驗證「開啟」比以往任何時候都更加容易。只需新增一個Tomcat證書CA或伺服器證書即可完成該作業（因為證書現在在Callmanager和Tomcat服務之間共用）。

如果升級到x14.2或更高版本導致了移動遠端訪問的中斷，則還可以參考本綜合文檔來排查問題。

Apache流量伺服器版本歷史記錄

若要檢查伺服器上的版本，請登入到root並運行~ # /apache2/bin/httpd -v。

Expressway x8.11.4
伺服器版本：Apache/2.4.34(Unix)
已構建伺服器：2018年11月12日19:04:23

Expressway x12.6

伺服器版本：Apache/2.4.43(Unix)
已構建伺服器：2020年5月26日18:27:21

Expressway x14.0.8

伺服器版本：Apache/2.4.53(Unix)
已構建伺服器：2022年5月4日08:52:57

Expressway x15.3

伺服器版本：Apache/2.4.62(Unix)
已構建伺服器：2025年7月16日12:10:19

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）。