為CUCM 14中的CallManager配置Tomcat證書重複使用

目錄

簡介

必要條件

- 需求
- 採用元件

背景資訊

設定

- 1.將Tomcat證書設定為Multi-SAN
  - 自簽名
  - CA簽名
- 2.重用CallManager的Tomcat證書

驗證

相關資訊

簡介

本文檔介紹如何在Cisco Unified Communications Manager(CUCM)伺服器上為CallManager重複使用Multi-SAN Tomcat證書。

必要條件

需求

思科建議您瞭解以下主題：

- CUCM證書
- 即時監控工具(RTMT)
- 身份信任清單(ITL)

採用元件

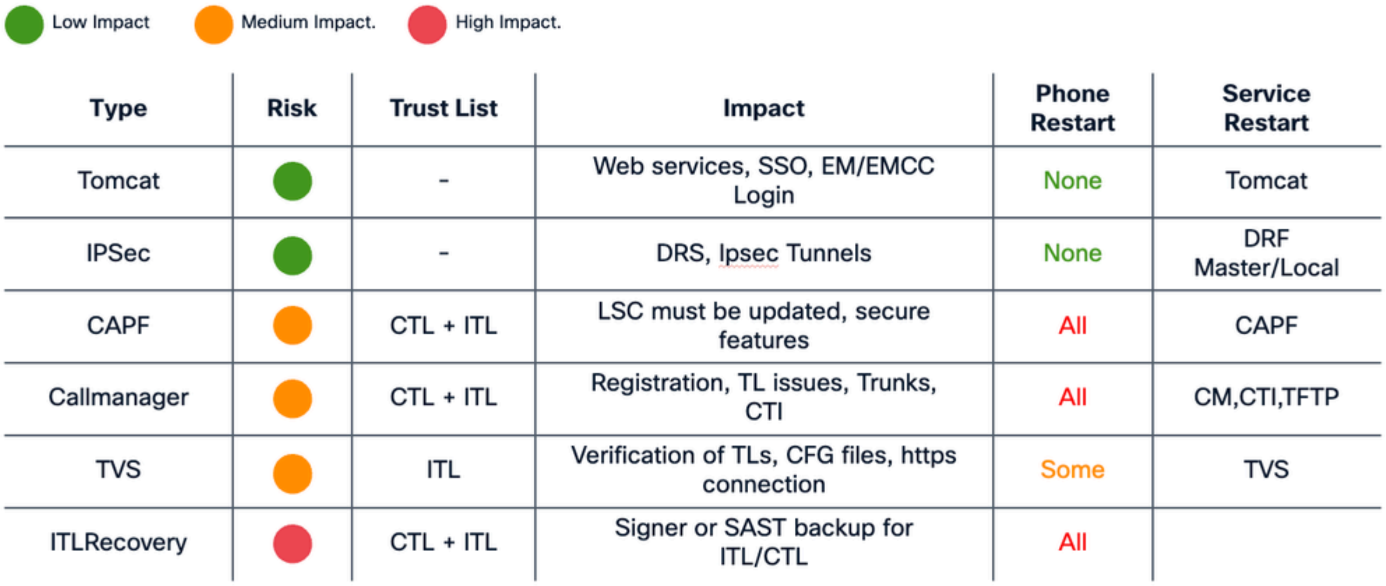
本文檔中的資訊基於CUCM 14.0.1.13900-155。

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

CUCM的兩個主要服務是Tomcat和CallManager。在早期版本中，每個服務都需要不同的證書才能完成整個群集。在CUCM版本14中，新增了一項新功能，以便對CallManager服務重新使用Multi-SAN Tomcat證書。使用此功能的優勢包括：

- 降低獲得由公共證書頒發機構(CA)簽名的證書集群的兩個證書的成本。
- 此功能可減小ITL檔案的大小，從而降低開銷。



🟢 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	

設定

⚠ 注意：上傳Tomcat證書之前，請驗證單一登入(SSO)是否已禁用。如果已啟用SSO，則在Tomcat證書再生過程完成之後，必須禁用並重新啟用SSO。

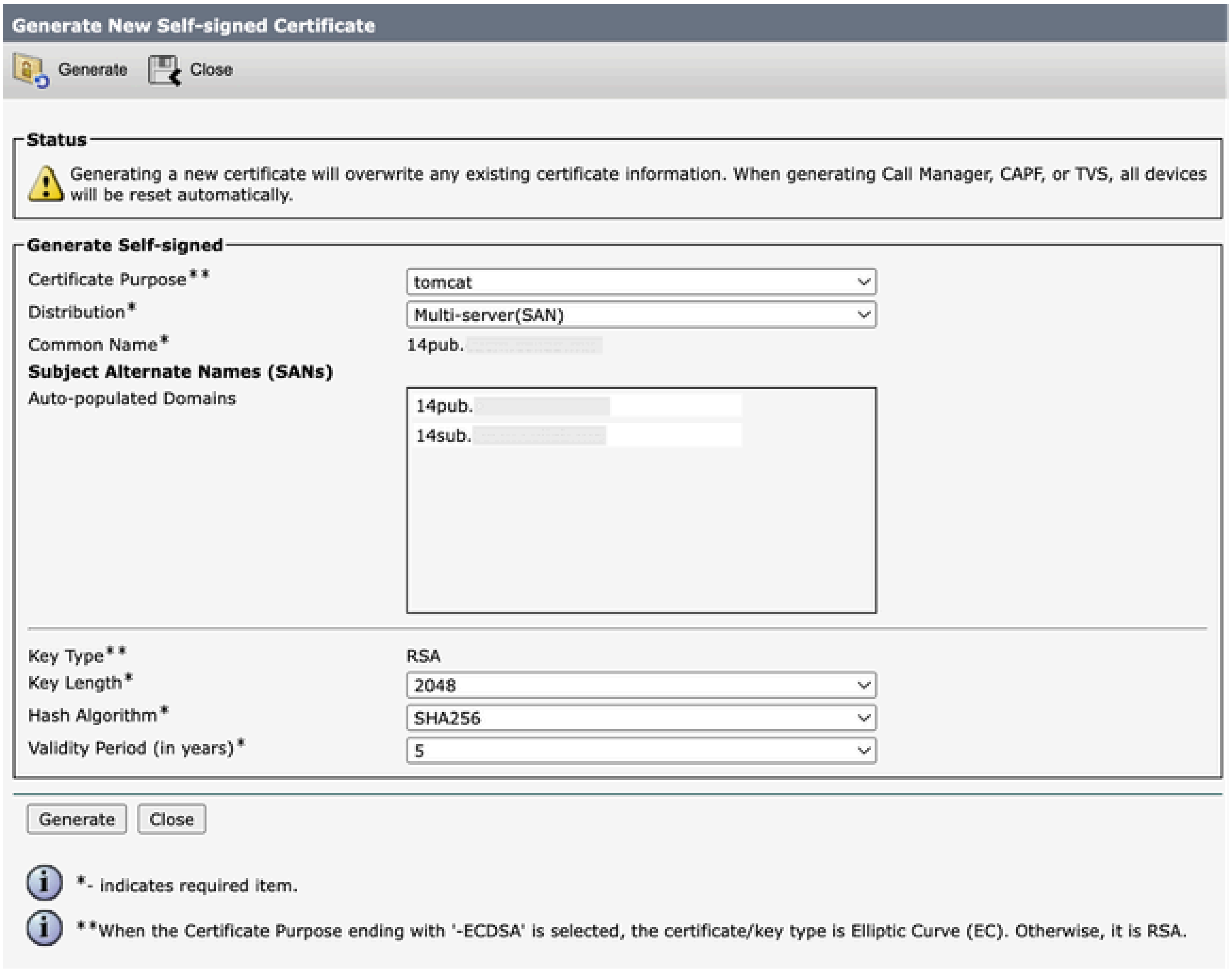
1.將Tomcat證書設定為Multi-SAN 🟢 Low Impact

在CUCM 14中，Tomcat Multi-SAN證書可以是自簽名或CA簽名。如果您的Tomcat證書已經是多SAN，請跳過此部分。

自簽名

步驟1.登入到Publisher > Operating System (OS) Administration，然後導航到Security > Certificate Management > Generate Self-Signed。

步驟2.選擇Certificate Purpose: tomcat > Distribution: Multi-Server SAN。它將自動填充SAN域和父域。



Generate New Self-signed Certificate

Status

⚠ Generating a new certificate will overwrite any existing certificate information. When generating Call Manager, CAPF, or TVS, all devices will be reset automatically.

Generate Self-signed

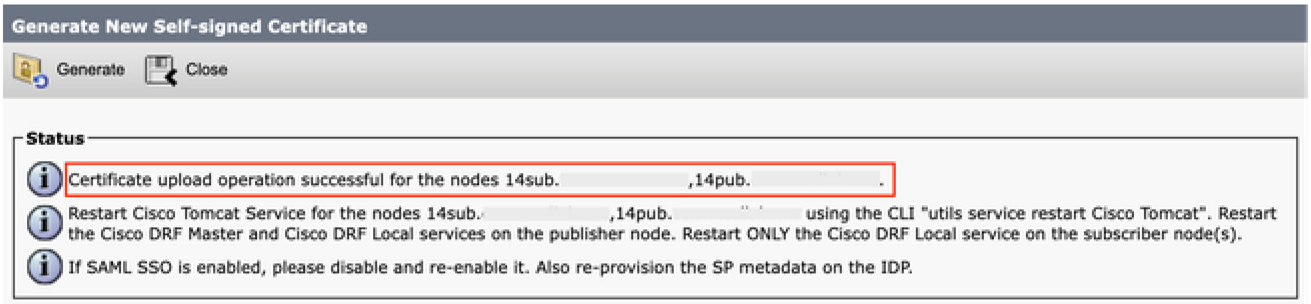
Certificate Purpose**	tomcat
Distribution*	Multi-server(SAN)
Common Name*	14pub.[redacted]
Subject Alternate Names (SANs)	
Auto-populated Domains	14pub.[redacted] 14sub.[redacted]
Key Type**	RSA
Key Length*	2048
Hash Algorithm*	SHA256
Validity Period (in years)*	5

*- indicates required item.

**When the Certificate Purpose ending with '-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it is RSA.

生成自簽名的多SAN Tomcat證書螢幕

步驟3.按一下Generate，並驗證消息下是否列出了所有節Certificate upload operation successful點。按一下Close。



Generate New Self-signed Certificate

Status

Certificate upload operation successful for the nodes 14sub.[redacted],14pub.[redacted].

Restart Cisco Tomcat Service for the nodes 14sub.[redacted],14pub.[redacted] using the CLI "utils service restart Cisco Tomcat". Restart the Cisco DRF Master and Cisco DRF Local services on the publisher node. Restart ONLY the Cisco DRF Local service on the subscriber node(s).

If SAML SSO is enabled, please disable and re-enable it. Also re-provision the SP metadata on the IDP.

生成自簽名多SAN Tomcat成功消息

步驟4.重新啟動Tomcat服務，開啟與群集所有節點的CLI會話，然後運行utils service restart Cisco Tomcat命令。

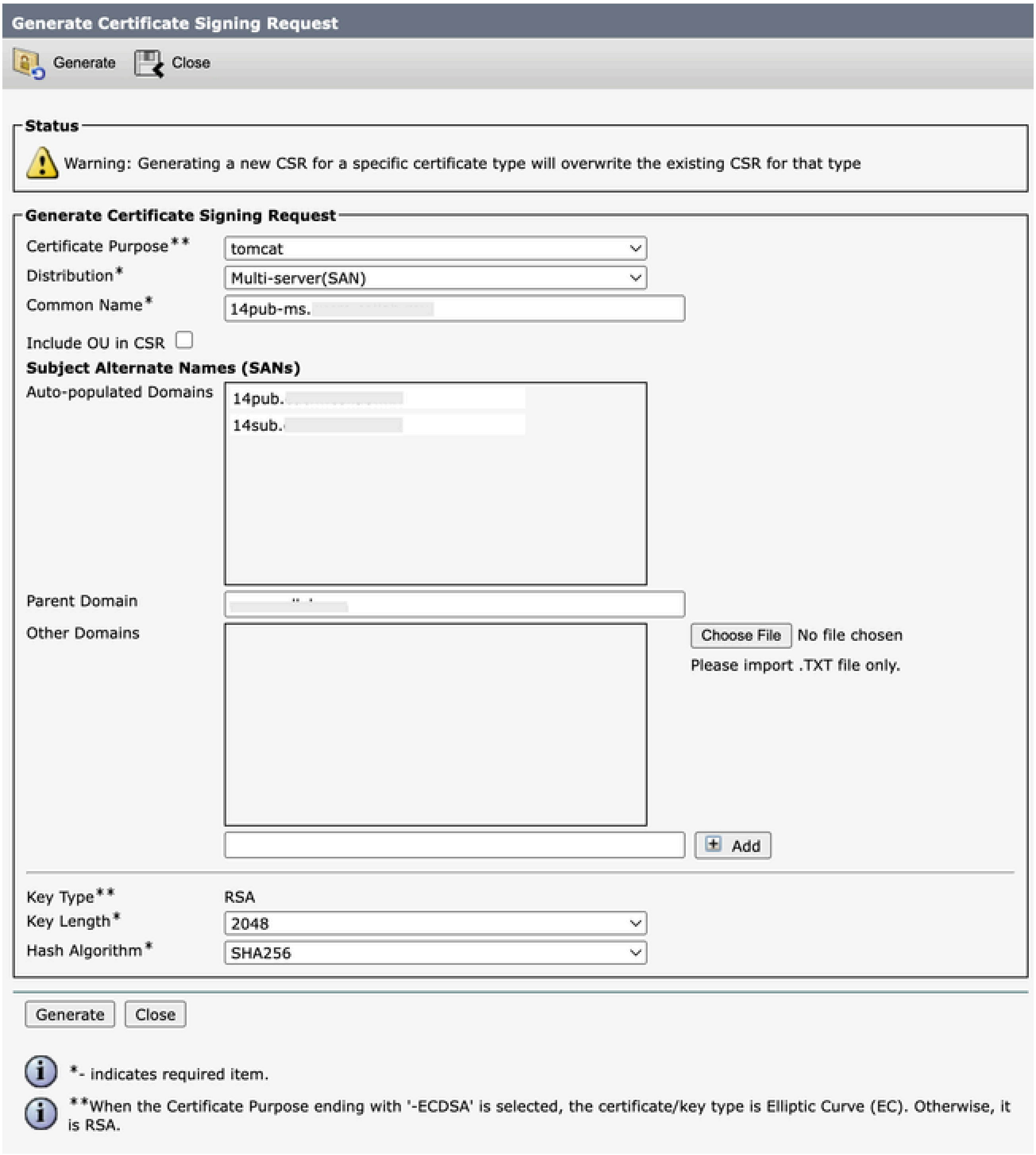
步驟5.導航至Publisher > Cisco Unified Serviceability > Tools > Control Center - Network Services，然後重新啟動Cisco DRF Master Service和Cisco DRF Local Service。

步驟6.定位至每個並重新啟Subscriber > Cisco Unified Serviceability > Tools > Control Center - Network Services動Cisco DRF Local Service。

CA簽名

步驟1.登入到Publisher > Operating System (OS) Administration，然後導航到Security > Certificate Management > Generate CSR。

步驟2.選擇Certificate Purpose: tomcat > Distribution: Multi-Server SAN。它將自動填充SAN域和父域。



Generate Certificate Signing Request

Status

Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose**	tomcat
Distribution*	Multi-server(SAN)
Common Name*	14pub-ms.[redacted]
Include OU in CSR	□

Subject Alternate Names (SANs)

Auto-populated Domains	14pub.[redacted] 14sub.[redacted]
Parent Domain	[redacted]
Other Domains	

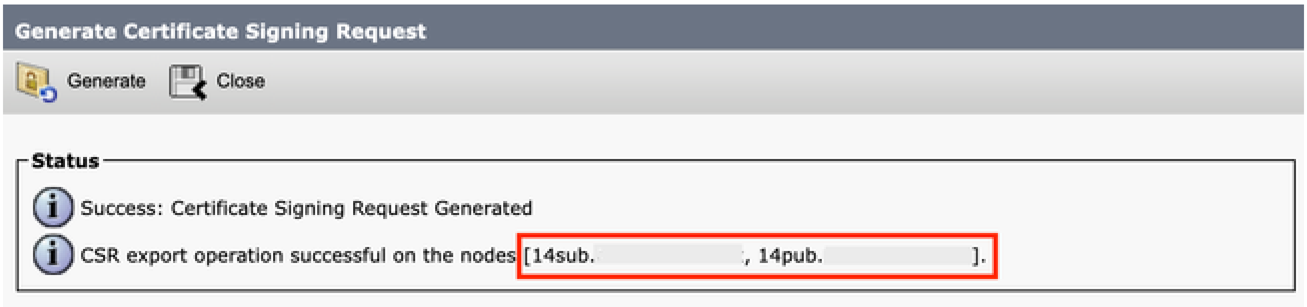
Key Type**	RSA
Key Length*	2048
Hash Algorithm*	SHA256

*- indicates required item.

**When the Certificate Purpose ending with '-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it is RSA.

Generate Multi-SAN CSR for Tomcat Certificate螢幕

步驟3.按一下Generate，並驗證消息下列出的所有節CSR export operation successful點。按一下Close。



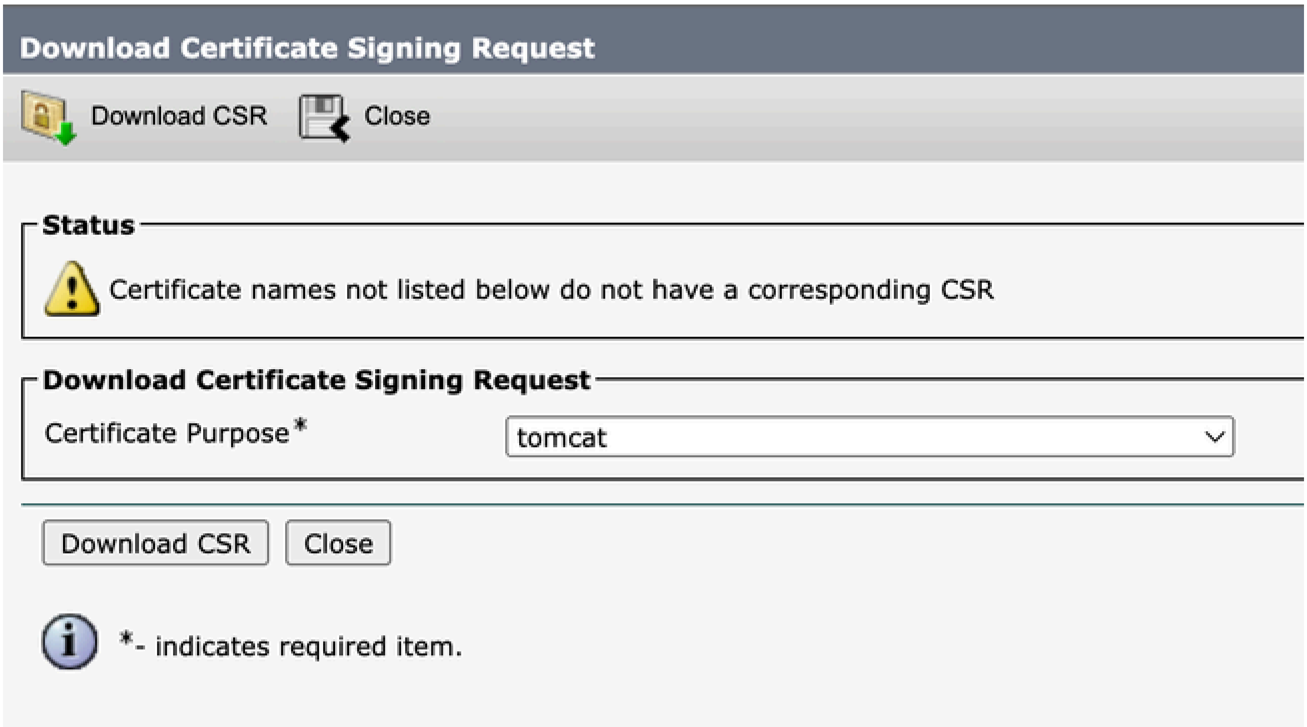
Status

Success: Certificate Signing Request Generated

CSR export operation successful on the nodes [14sub. , 14pub.].

生成多SAN CSR Tomcat成功消息

步驟4.按一下Download CSR > Certificate Purpose: tomcat > Download。



Status

Certificate names not listed below do not have a corresponding CSR

Download Certificate Signing Request

Certificate Purpose* tomcat

*- indicates required item.

下載Tomcat CSR螢幕

步驟5.將CSR傳送到您的CA進行簽名。

步驟6。若要上傳CA信任鏈，請導覽Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust。設定憑證的說明，並瀏覽信任鏈檔案。

步驟7.上傳CA簽名的證書，導航至Certificate Management > Upload certificate > Certificate Purpose: tomcat。設定證書描述並瀏覽CA簽名的證書檔案。

步驟8.重新啟動Tomcat服務，開啟與群集所有節點的CLI會話，然後運行該命令utils service restart Cisco Tomcat。

步驟9.導航至Publisher > Cisco Unified Serviceability > Tools > Control Center - Network Services，然後重新啟動Cisco DRF Master Service和Cisco DRF Local Service。

步驟10.導航到每個並重新啟Subscriber > Cisco Unified Serviceability > Tools > Control Center - Network Services動Cisco DRF Local Service。

2.重用CallManager的Tomcat證書 ● Medium Impact.

⚠

注意：針對CUCM 14，介紹了一種新的企業參Phone Interaction on Certificate Update數。使用此欄位可在更新其中一個TVS、CAPF或TFTP(CallManager/ITLRecovery)證書時手動或自動重置電話（如果適用）。此引數預設設定為reset the phones automatically。在重新生成、刪除和更新證書後，確保重新啟動適當的服務。

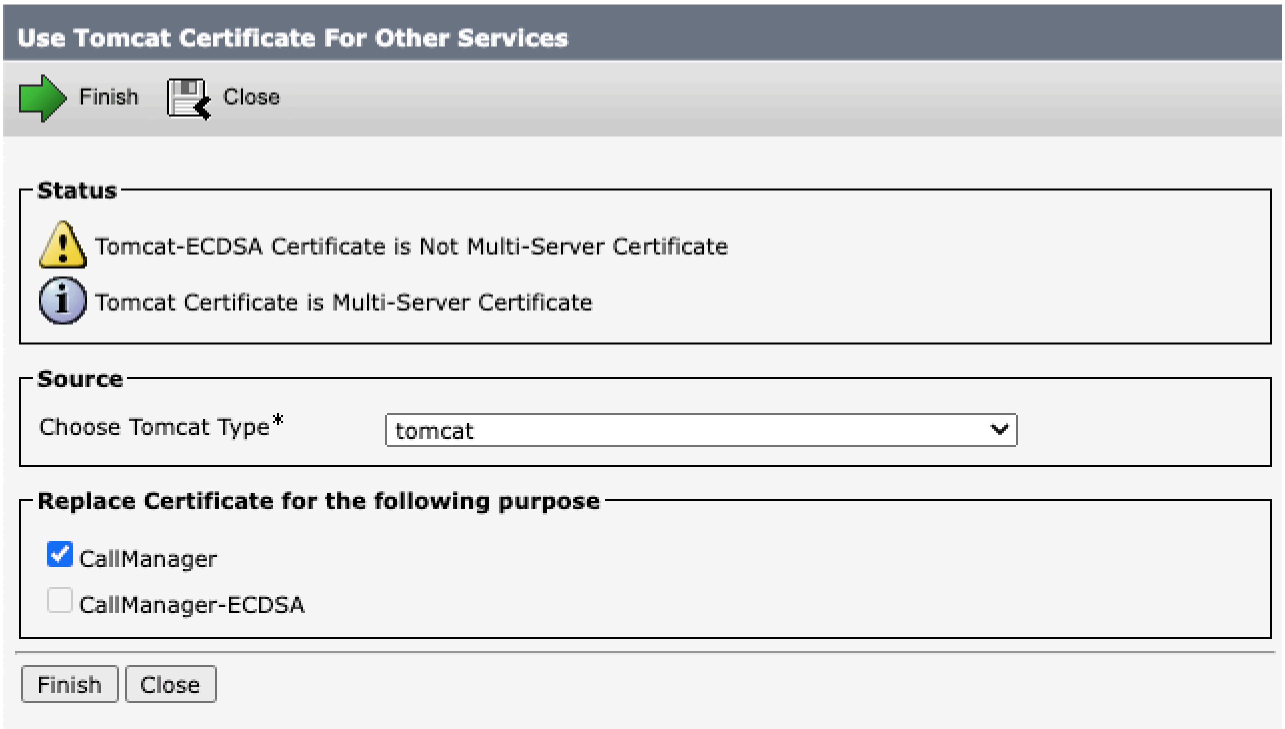
需要重新啟動服務才能進行正常的CallManager證書重新生成。選中Regenerate Certificates In Unified Communications Manager。

步驟1.導航到您的CUCM發佈者，然後導航到Cisco Unified OS Administration > Security > Certificate Management。

步驟2.按一下Reuse Certificate。

步驟3.從choose **Tomcat type**下拉式清單中選擇tomcat。

步驟4.在窗Replace Certificate for the following purpose格中，勾選CallManager覈取方塊。



Use Tomcat Certificate For Other Services

Status

⚠ Tomcat-ECDSA Certificate is Not Multi-Server Certificate

ⓘ Tomcat Certificate is Multi-Server Certificate

Source

Choose Tomcat Type* tomcat

Replace Certificate for the following purpose

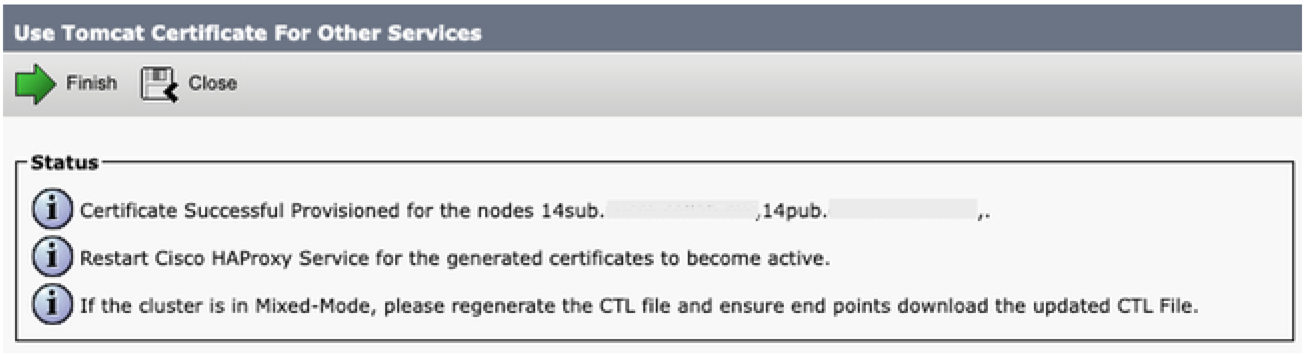
☑ CallManager

☐ CallManager-ECDSA

「為其他服務重複使用Tomcat證書」螢幕

附註：如果選擇Tomcat作為證書型別，則會啟用CallManager作為替代項。如果選擇tomcat-ECDSA作為證書型別，則會啟用CallManager-ECDSA作為替代項。

步驟5.按一下Finish，將CallManager證書替換為Tomcat Multi-SAN證書。



Use Tomcat Certificate For Other Services

Status

Certificate Successful Provisioned for the nodes 14sub. ,14pub. ,.

Restart Cisco HAProxy Service for the generated certificates to become active.

If the cluster is in Mixed-Mode, please regenerate the CTL file and ensure end points download the updated CTL File.

重新使用Tomcat證書成功消息

步驟6.重新啟動Cisco HAProxy服務，開啟到群集所有節點的CLI會話，然後運行該命令utils service restart Cisco HAProxy。

附註：要確定群集是否處於混合模式，請導航至Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode(0 == Non-Secure;1 ==混合模式)。

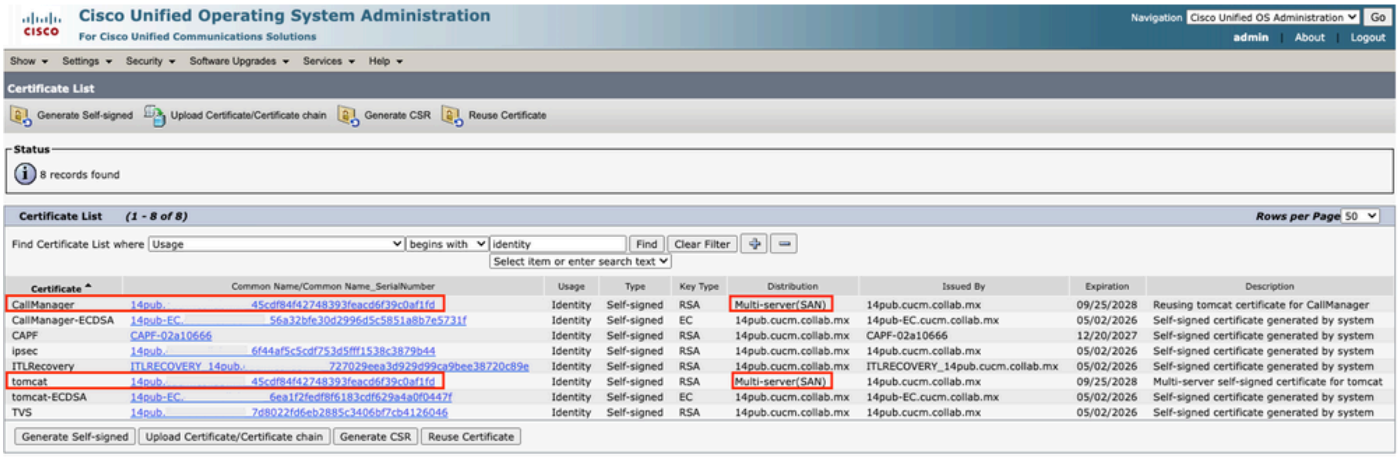
步驟7.如果群集處於混合模式，請開啟與發佈伺服器節點的CLI會話，然後運行命令，並重置群集的所有電話，使CTL檔案更新生效**utils ctl update CTLFile**。

驗證

步驟1.導航到您的CUCM發佈者，然後導航到Cisco Unified OS Administration > Security > Certificate Management。

步驟2.按篩選條件Find Certificate List where: Usage > begins with: identity，然後按一下Find。

步驟3. CallManager和Tomcat證書必須以相同的值結Common Name_Serial Number尾。



Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Navigation Cisco Unified OS Administration
Go
admin
About
Logout
Show
Settings
Security
Software Upgrades
Services
Help
Certificate List
Generate Self-signed
Upload Certificate/Certificate chain
Generate CSR
Reuse Certificate

Status

8 records found

Certificate List *(1 - 8 of 8)* — *Rows per Page* 50

Find Certificate List where Usage begins with identity Find Clear Filter

Select item or enter search text

Certificate	Common Name/Common Name_SerialNumber	Usage	Type	Key Type	Distribution	Issued By	Expiration	Description
CallManager	14pub. 45cdf84f42748393feacd6f39c0af1fd	Identity	Self-signed	RSA	Multi-server(SAN)	14pub.cucm.collab.mx	09/25/2028	Reusing tomcat certificate for CallManager
CallManager-ECDSA	14pub-EC. 56a32bfe30d2996d5c5851a8b7e5731f	Identity	Self-signed	EC	14pub.cucm.collab.mx	14pub-EC.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system
CAPF	CAPF-02a10666	Identity	Self-signed	RSA	14pub.cucm.collab.mx	CAPF-02a10666	12/20/2027	Self-signed certificate generated by system
ipsec	14pub. 6f44af5c5cdf753d5fff1538c3879b44	Identity	Self-signed	RSA	14pub.cucm.collab.mx	14pub.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system
ITLRecovery	ITLRECOVERY_14pub. 727029eea3d929d99ca9bee38720c89e	Identity	Self-signed	RSA	14pub.cucm.collab.mx	ITLRECOVERY_14pub.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system
tomcat	14pub. 45cdf84f42748393feacd6f39c0af1fd	Identity	Self-signed	RSA	Multi-server(SAN)	14pub.cucm.collab.mx	09/25/2028	Multi-server self-signed certificate for tomcat
tomcat-ECDSA	14pub-EC. 6ea1f2fedf8f6183cdf629a4a0f0447f	Identity	Self-signed	EC	14pub.cucm.collab.mx	14pub-EC.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system
TVS	14pub. 7d8022fd6eb2885c3406bf7cb4126046	Identity	Self-signed	RSA	14pub.cucm.collab.mx	14pub.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system

驗證CallManager的Tomcat證書重複使用

附註：從SU4開始，在啟用證書重用後，GUI上不顯示Call Manager證書，而兩個證書在SU2和SU3中均可見。

相關資訊

- 思科統一通訊管理器14安全指南
- 思科技術支援與下載

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）。