設定統一通訊群集

目錄

簡介

本文檔介紹如何使用證書頒發機構(CA)簽名的多伺服器SAN證書來設定統一通訊群集。

必要條件

需求

思科建議您瞭解以下主題：

- 思科整合通訊管理員(CUCM)
- CUCM IM和狀態版本10.5

嘗試此組態之前，請確保這些服務已啟動且功能正常：

- Cisco平台管理Web服務
- Cisco Tomcat服務

要在Web介面上驗證這些服務，請導航至**Cisco Unified Serviceability Page Services > Network Service > Select a server**。若要在CLI上驗證它們，請輸入**utils service list**命令。

如果在CUCM群集中啟用了SSO，則需要禁用並再次啟用SSO。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

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

在CUCM版本10.5及更高版本中，此信任儲存證書簽名請求(CSR)可以包括使用者備用名稱(SAN)和備用域。

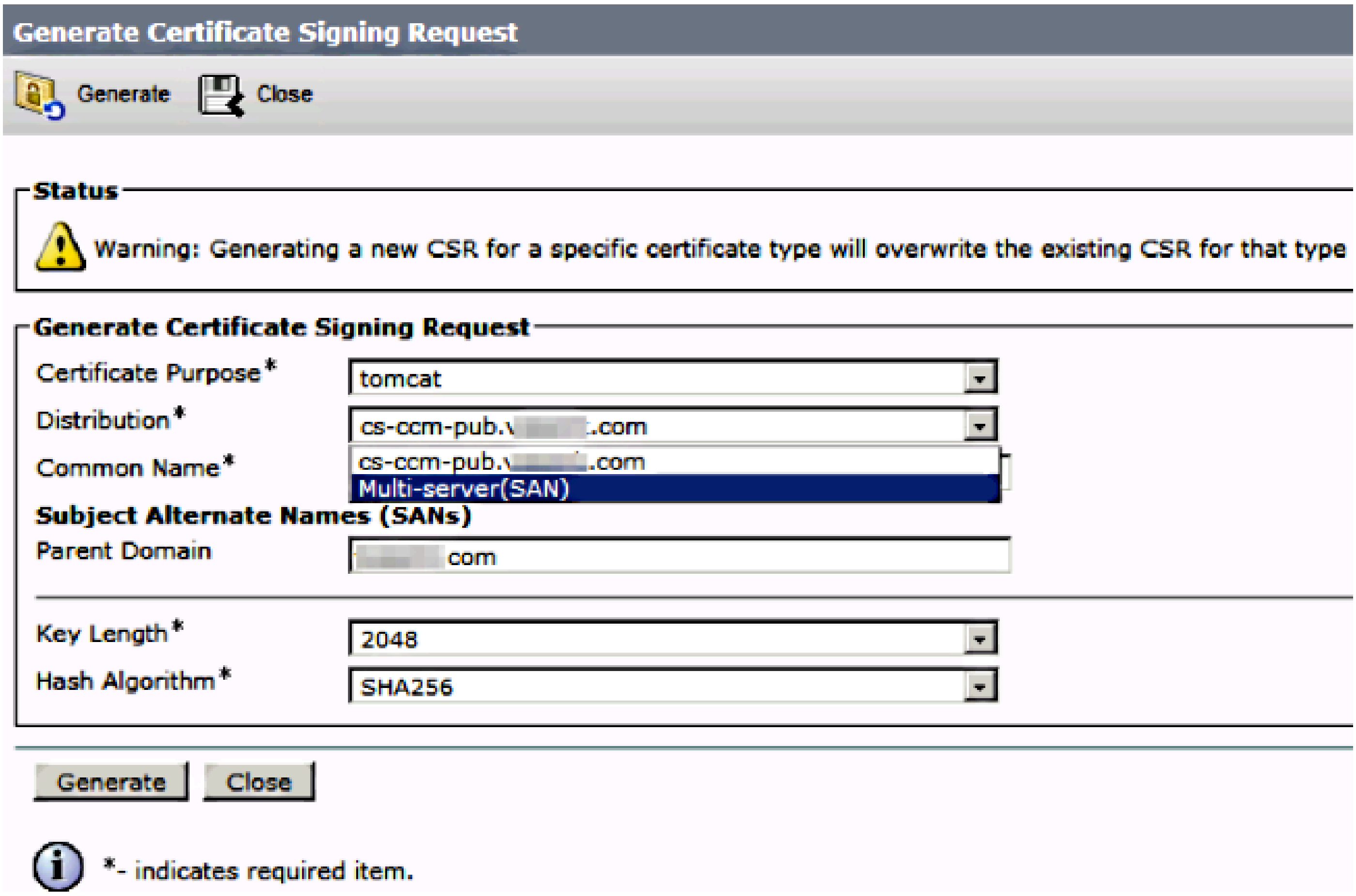
1. Tomcat - CUCM和IM&P
2. Cisco CallManager — 僅CUCM
3. Cisco Unified Presence — 可擴充訊息和狀態通訊協定(CUP-XMPP) — 僅限IM&P
4. CUP-XMPP伺服器到伺服器(S2S) — 僅限IM&P

在此版本中獲取CA簽名的證書更簡單。只需一個CSR由CA簽署，而不是要求從每個伺服器節點取得CSR，然後為每個CSR取得一個CA簽署的憑證並個別管理。

設定

步驟1.

登入到Publisher的作業系統(OS)管理，然後導航到**安全>證書管理>生成CSR**。



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* cs-ccm-pub.[redacted].com

cs-ccm-pub.[redacted].com

Multi-server(SAN)

Common Name*

Subject Alternate Names (SANs)

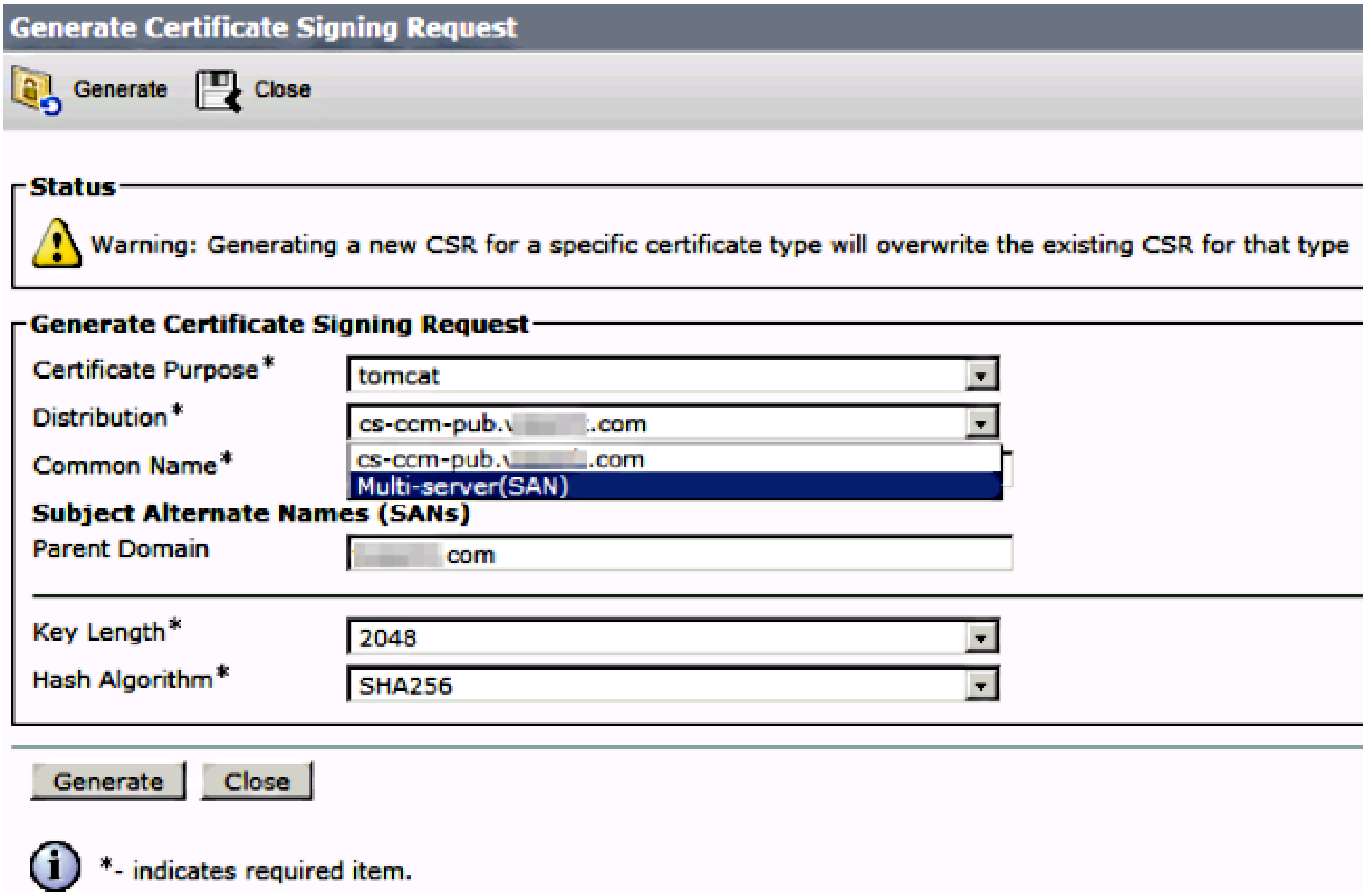
Parent Domain [redacted]com

Key Length* 2048

Hash Algorithm* SHA256

*- indicates required item.

步驟2.
選擇**Multi-Server SAN** in Distribution。



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*	cs-ccm-pub.[redacted].com
Common Name*	cs-ccm-pub.[redacted].com Multi-server(SAN)

Subject Alternate Names (SANs)

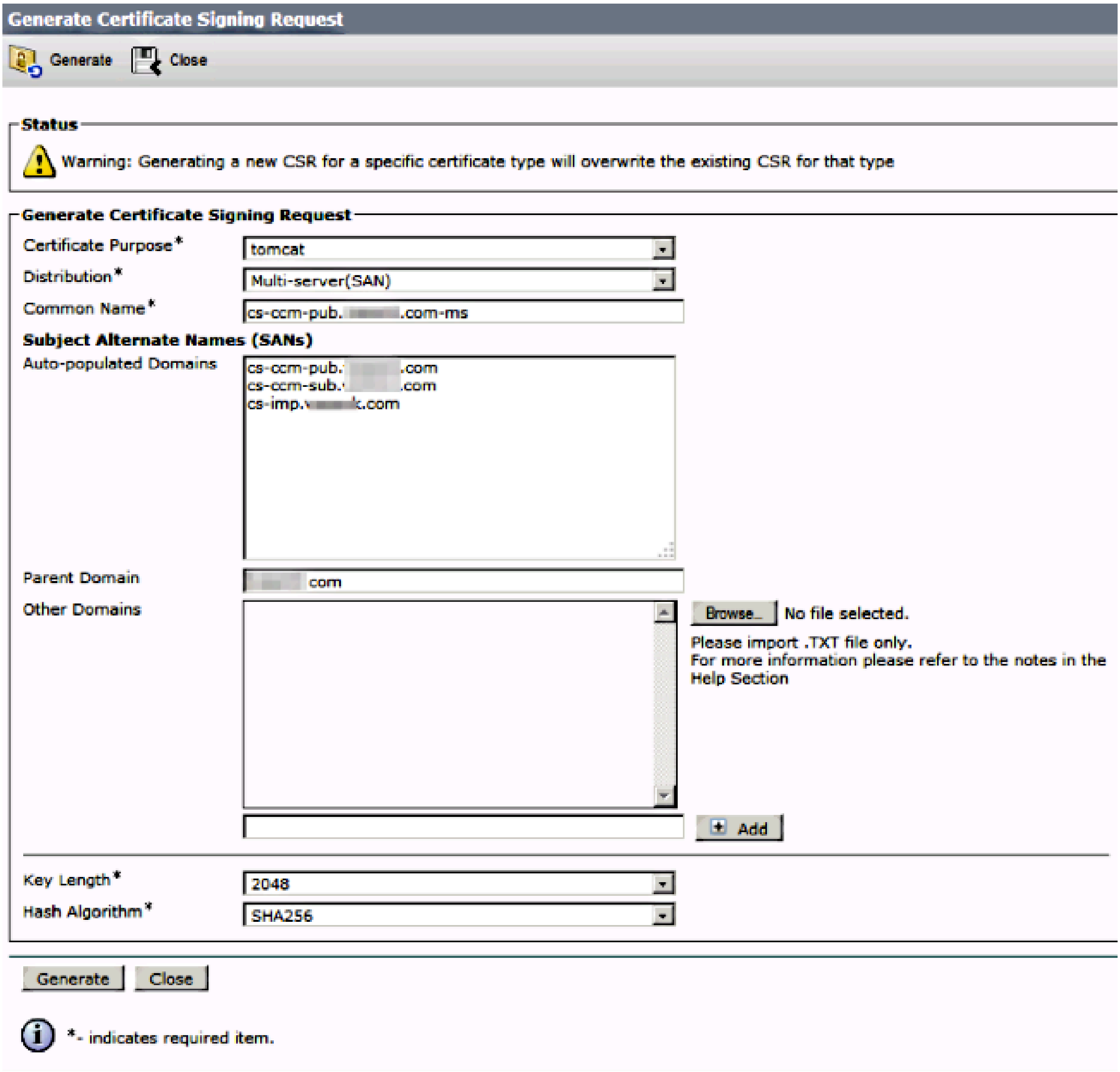
Parent Domain	[redacted] com

Key Length*	2048
Hash Algorithm*	SHA256

ⓘ *- indicates required item.

它會自動填充SAN域和父域。

驗證Tomcat是否列出了集群的所有節點：CallManager的所有CUCM和IM&P節點均列出：僅列出了CUCM節點。



Generate Certificate Signing Request

Generate Close

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* cs-ccm-pub.[redacted].com-ms

Subject Alternate Names (SANs)

Auto-populated Domains
cs-ccm-pub.[redacted].com
cs-ccm-sub.[redacted].com
cs-imp.[redacted].com

Parent Domain [redacted] com

Other Domains

Browse... No file selected.

Please import .TXT file only.
For more information please refer to the notes in the Help Section

Add

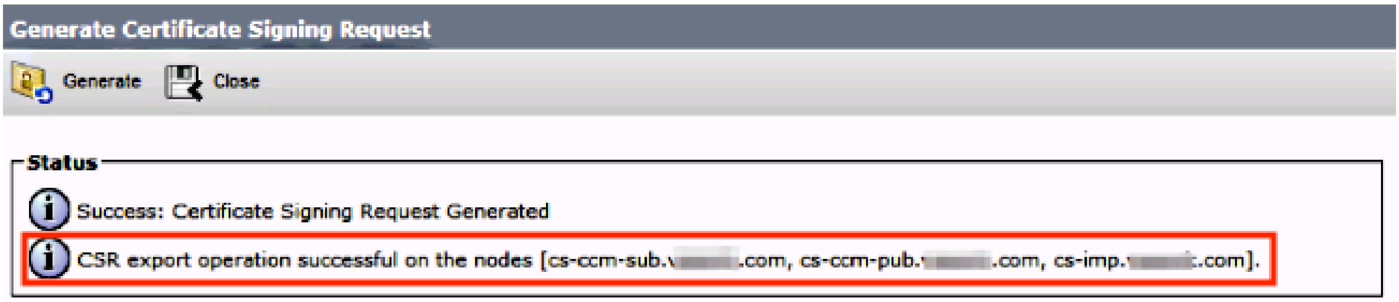
Key Length* 2048

Hash Algorithm* SHA256

Generate Close

ⓘ *- indicates required item.

步驟3.
按一下「generate」，一旦CSR產生，請確認CSR中列出的所有節點也會顯示在「Successful CSR exported」清單中。



Generate Certificate Signing Request

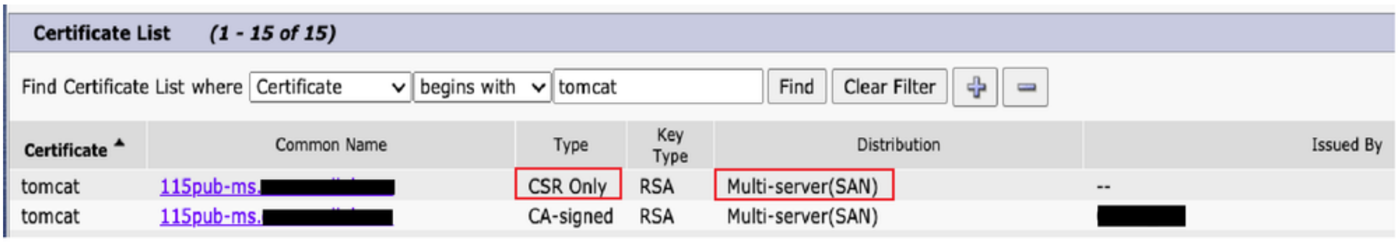
Generate Close

Status

ⓘ Success: Certificate Signing Request Generated

ⓘ CSR export operation successful on the nodes [cs-ccm-sub.[redacted].com, cs-ccm-pub.[redacted].com, cs-imp.[redacted].com].

在證書管理中，生成SAN請求：



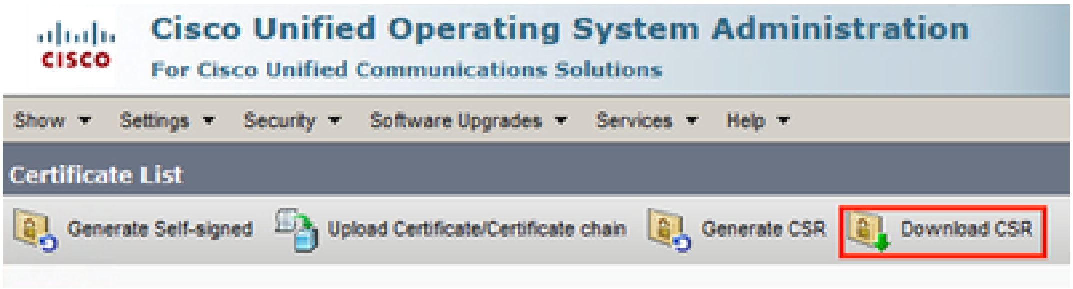
Certificate List (1 - 15 of 15)

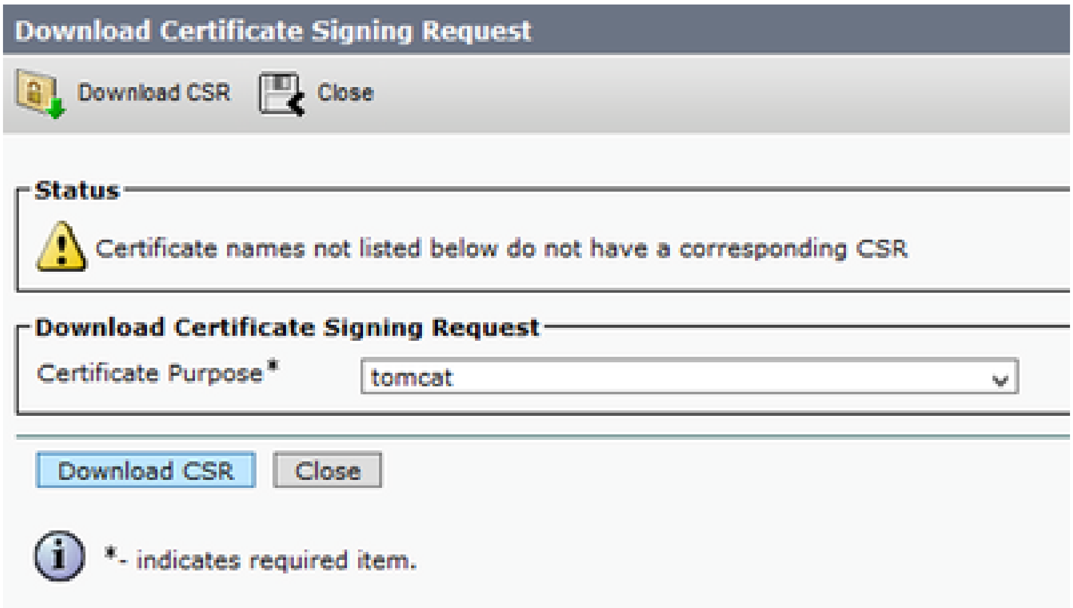
Find Certificate List where Certificate begins with tomcat Find Clear Filter

Certificate ▲	Common Name	Type	Key Type	Distribution	Issued By
tomcat	115pub-ms.[redacted]	CSR Only	RSA	Multi-server(SAN)	--
tomcat	115pub-ms.[redacted]	CA-signed	RSA	Multi-server(SAN)	[redacted]

步驟4.

按一下「**Download CSR**」，然後選擇憑證用途，然後按一下「**Download CSR**」。


Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Show
Settings
Security
Software Upgrades
Services
Help
Certificate List
Generate Self-signed
Upload Certificate/Certificate chain
Generate CSR
Download CSR



Status

Certificate names not listed below do not have a corresponding CSR

Download Certificate Signing Request

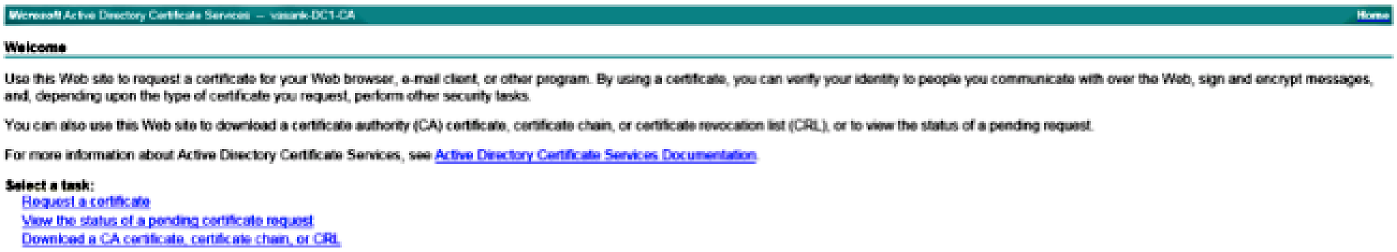
Certificate Purpose* tomcat

*- indicates required item.

可以使用本地CA或外部CA（例如VeriSign）來簽署CSR（在上一步中下載的檔案）。

此示例顯示基於Microsoft Windows Server的CA的配置步驟。如果您使用不同的CA或外部CA，請前往步驟5。

登入https://<windowsserveripaddress>/certsrv/
選擇**Request a Certificate > Advanced Certificate Request。**
將CSR檔案的內容複製到Base-64編碼憑證要求欄位，然後按一下**Submit。**


Microsoft Active Directory Certificate Services -- vasank-DC1-CA
Home

Welcome

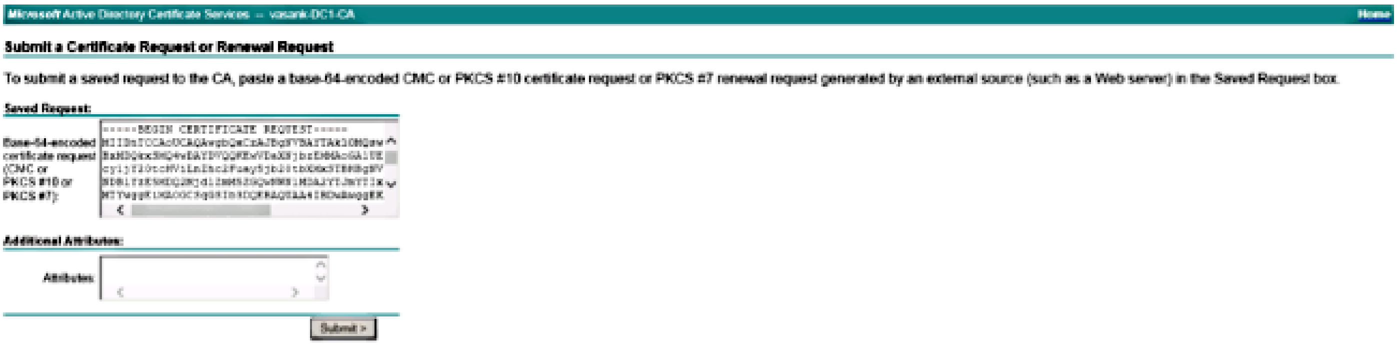
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

按此處所示提交CSR請求。


Microsoft Active Directory Certificate Services -- vasank-DC1-CA
Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

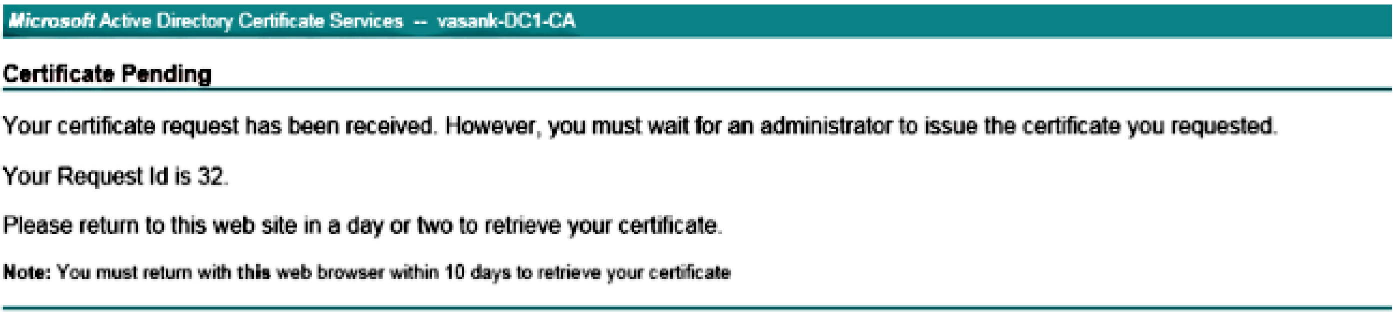
Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDnTCCAoUCAQAwgbQxCzAJBgNVBAYTAkl0MQsw
EsMDQxxSHQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UE
[illegible]
[illegible]
[illegible]
```

Additional Attributes:

Attributes:


Microsoft Active Directory Certificate Services -- vasank-DC1-CA

Certificate Pending

Your certificate request has been received. However, you must wait for an administrator to issue the certificate you requested.

Your Request Id is 32.

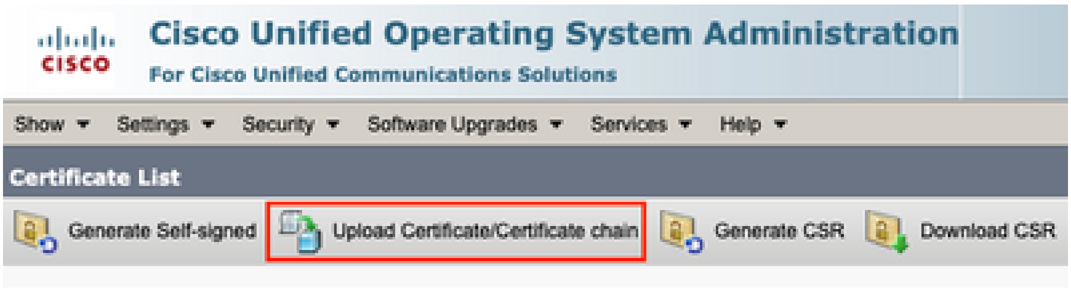
Please return to this web site in a day or two to retrieve your certificate.

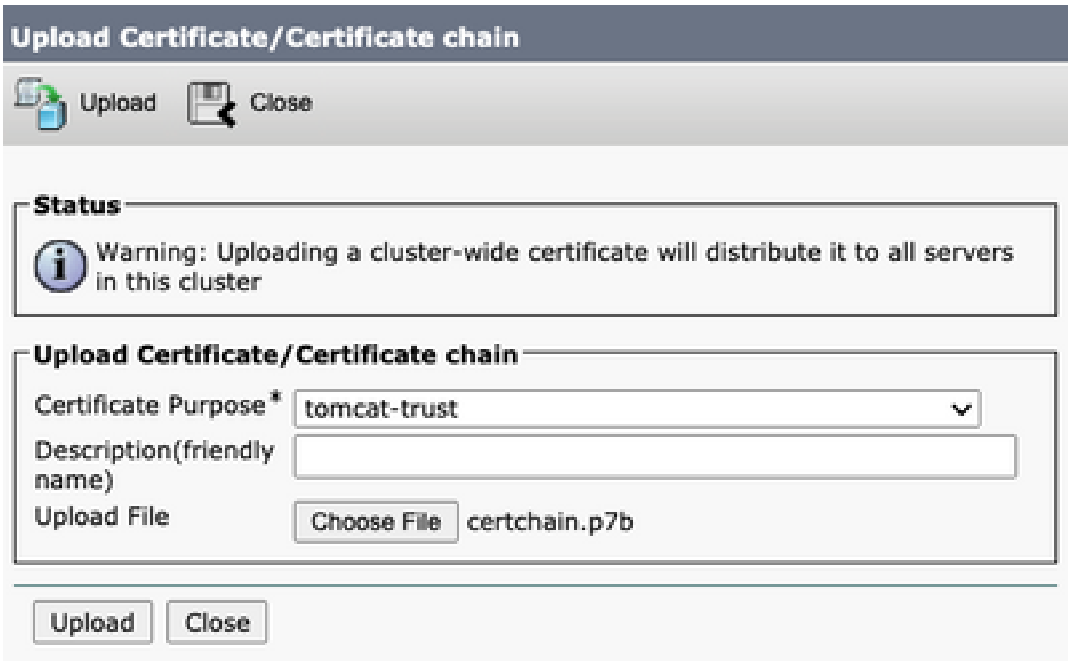
Note: You must return with this web browser within 10 days to retrieve your certificate

步驟5.

> **注意**：上傳Tomcat證書之前，請驗證SSO是否已禁用。如果已啟用SSO，則必須在所有Tomcat證書再生過程完成後禁用並重新啟用SSO。

簽署憑證後，將CA憑證上傳為tomcat-trust。首先獲取根證書，然後獲取中間證書（如果存在）。


cisco
Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions
Show
Settings
Security
Software Upgrades
Services
Help
Certificate List
Generate Self-signed
Upload Certificate/Certificate chain
Generate CSR
Download CSR



Upload Certificate/Certificate chain

Status

Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

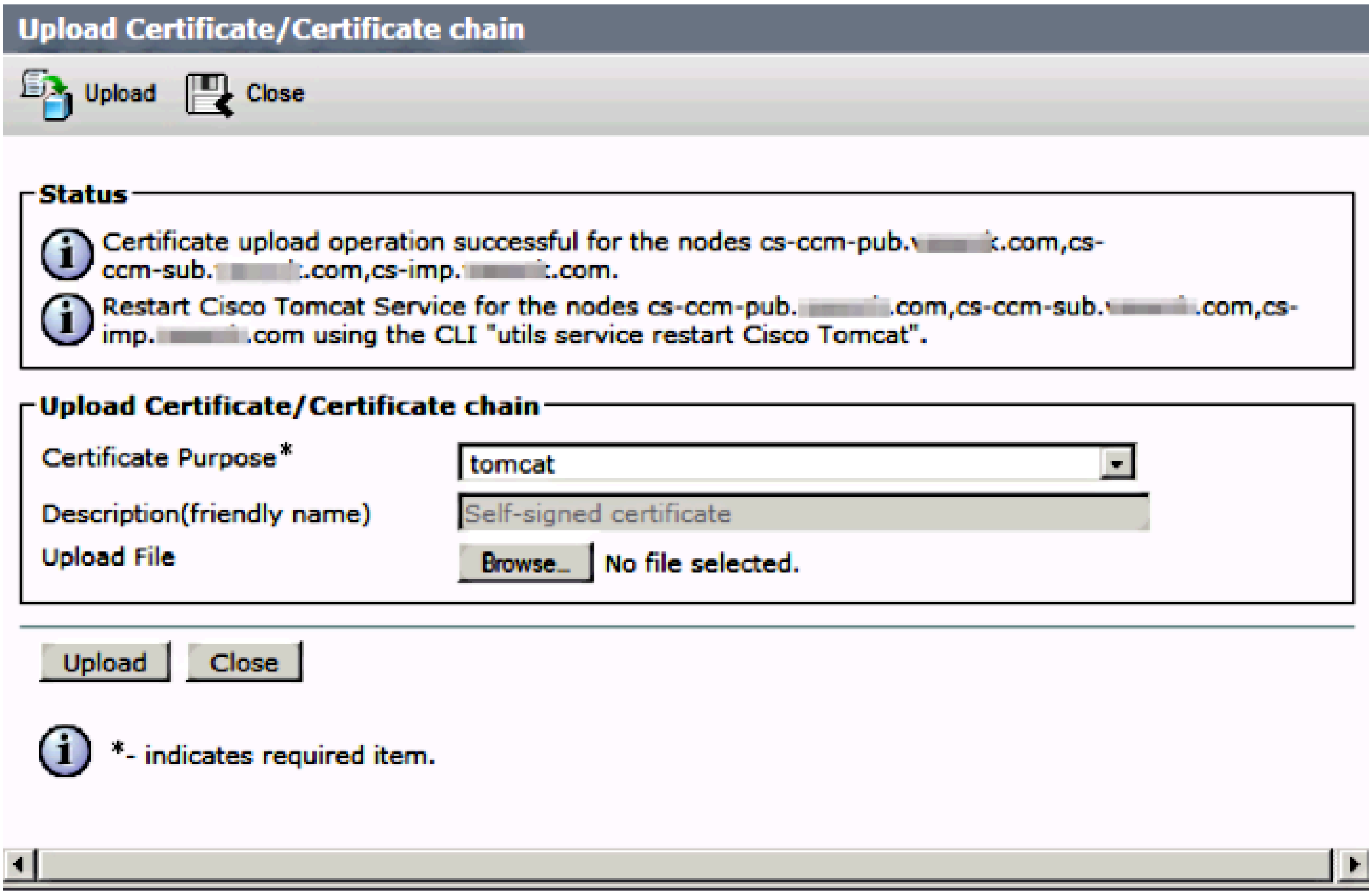
Certificate Purpose* tomcat-trust

Description(friendly name)

Upload File Choose File certchain.p7b

步驟6.

現在，將CUCM簽名的證書上傳為Tomcat，並驗證集群的所有節點是否列在「Certificate upload operation successful」中，如下圖所示：



Upload Certificate/Certificate chain

Status

Certificate upload operation successful for the nodes cs-ccm-pub.[redacted].com,cs-ccm-sub.[redacted].com,cs-imp.[redacted].com.

Restart Cisco Tomcat Service for the nodes cs-ccm-pub.[redacted].com,cs-ccm-sub.[redacted].com,cs-imp.[redacted].com using the CLI "utils service restart Cisco Tomcat".

Upload Certificate/Certificate chain

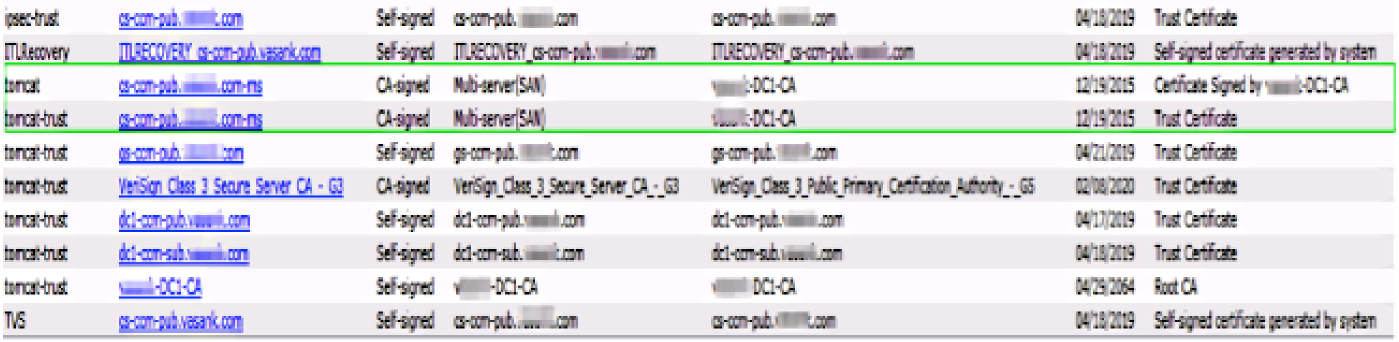
Certificate Purpose* tomcat

Description(friendly name) Self-signed certificate

Upload File Browse... No file selected.

*- indicates required item.

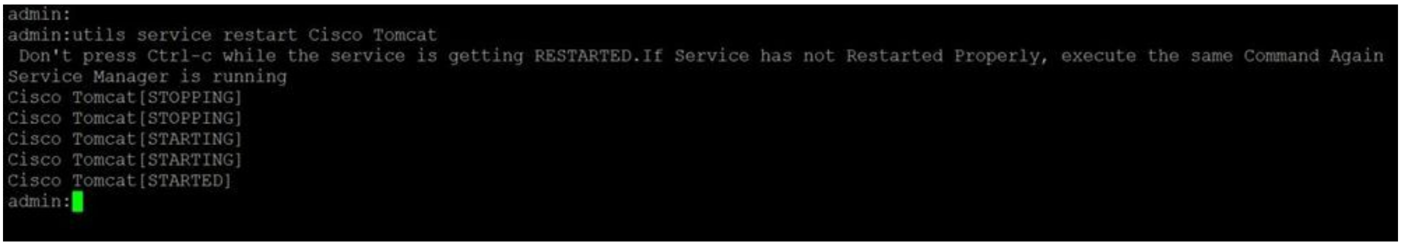
「Certificate Management」中列出了多伺服器SAN，如下圖所示：



ipsec-trust	cs-com-pub.[redacted].com	Self-signed	cs-com-pub.[redacted].com	cs-com-pub.[redacted].com	04/18/2019	Trust Certificate
ITLRecovery	ITLRECOVERY_cs-com-pub.vasank.com	Self-signed	ITLRECOVERY_cs-com-pub.[redacted].com	ITLRECOVERY_cs-com-pub.[redacted].com	04/18/2019	Self-signed certificate generated by system
tomcat	cs-com-pub.[redacted].com-ms	CA-signed	Multi-server(SAN)	[redacted]-DC1-CA	12/19/2015	Certificate Signed by [redacted]-DC1-CA
tomcat-trust	cs-com-pub.[redacted].com-ms	CA-signed	Multi-server(SAN)	[redacted]-DC1-CA	12/19/2015	Trust Certificate
tomcat-trust	gs-com-pub.[redacted].com	Self-signed	gs-com-pub.[redacted].com	gs-com-pub.[redacted].com	04/21/2019	Trust Certificate
tomcat-trust	VeriSign Class 3 Secure Server CA - G3	CA-signed	VeriSign_Class_3_Secure_Server_CA_-_G3	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5	02/08/2020	Trust Certificate
tomcat-trust	dc1-com-pub.[redacted].com	Self-signed	dc1-com-pub.[redacted].com	dc1-com-pub.[redacted].com	04/17/2019	Trust Certificate
tomcat-trust	dc1-com-sub.[redacted].com	Self-signed	dc1-com-sub.[redacted].com	dc1-com-sub.[redacted].com	04/18/2019	Trust Certificate
tomcat-trust	[redacted]-DC1-CA	Self-signed	[redacted]-DC1-CA	[redacted]-DC1-CA	04/29/2064	Root CA
TVS	cs-com-pub.vasank.com	Self-signed	cs-com-pub.[redacted].com	cs-com-pub.[redacted].com	04/18/2019	Self-signed certificate generated by system

步驟7.

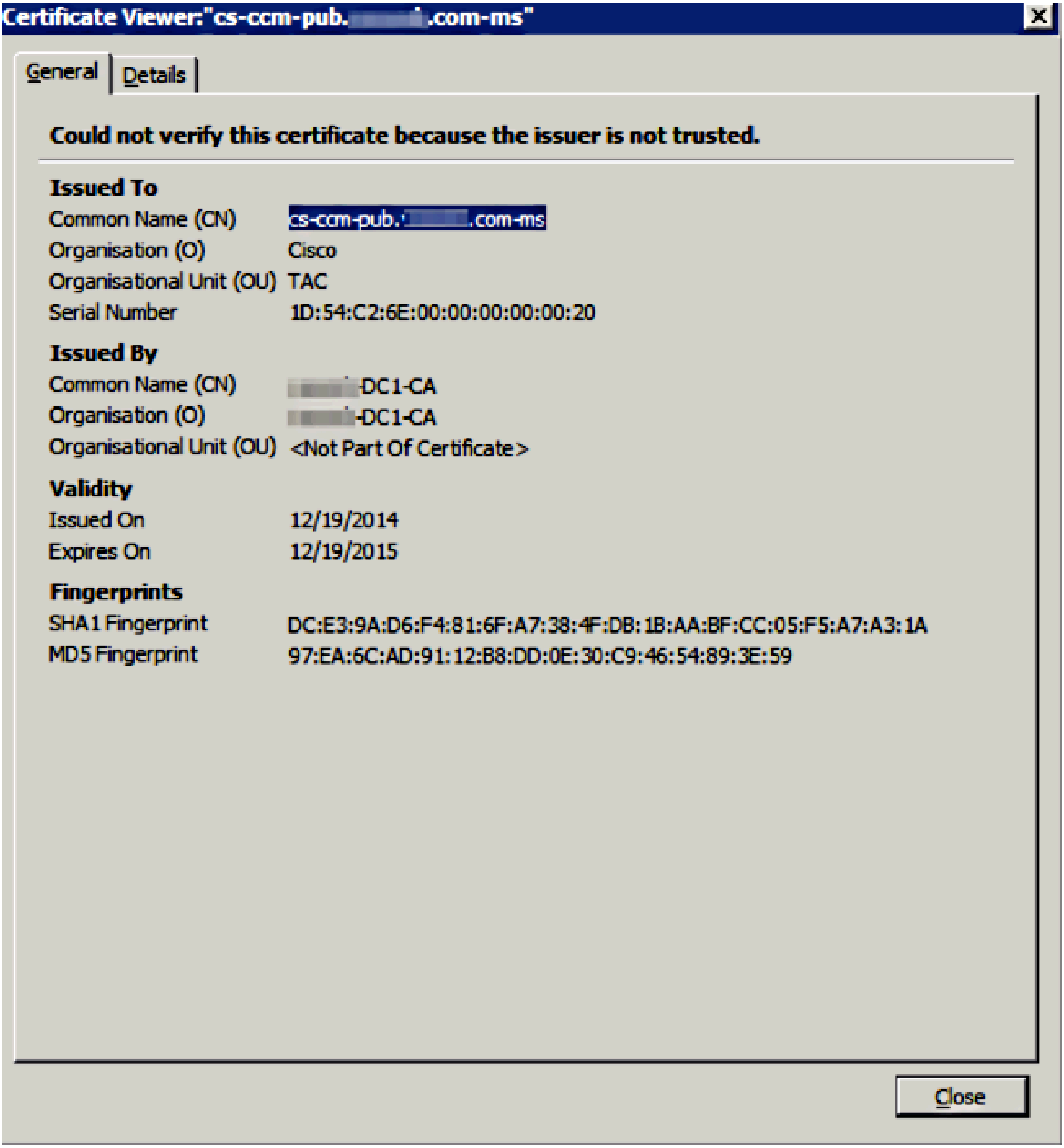
使用**utils service restart Cisco Tomcat** 命令，通過CLI在SAN清單中的所有節點（首先是發佈伺服器，然後是訂閱伺服器）上重新啟動Tomcat服務。



```
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:
```

驗證

登入http://<fqdnofccm>:8443/ccmadmin以確保使用新證書。



Certificate Viewer:"cs-ccm-pub.[redacted].com-ms"

Could not verify this certificate because the issuer is not trusted.

Issued To

Common Name (CN)	cs-ccm-pub.[redacted].com-ms
Organisation (O)	Cisco
Organisational Unit (OU)	TAC
Serial Number	1D:54:C2:6E:00:00:00:00:00:20

Issued By

Common Name (CN)	[redacted]-DC1-CA
Organisation (O)	[redacted]-DC1-CA
Organisational Unit (OU)	<Not Part Of Certificate>

Validity

Issued On	12/19/2014
Expires On	12/19/2015

Fingerprints

SHA1 Fingerprint	DC:E3:9A:D6:F4:81:6F:A7:38:4F:DB:1B:AA:BF:CC:05:F5:A7:A3:1A
MD5 Fingerprint	97:EA:6C:AD:91:12:B8:DD:0E:30:C9:46:54:89:3E:59

CallManager多伺服器SAN證書

對於CallManager證書，可以執行類似的過程。在這種情況下，自動填充的域僅是CallManager節點。如果Cisco CallManager服務沒有運行，您可以選擇將其保留在SAN清單中或將其刪除。

> **警告**：此過程會影響電話註冊和呼叫處理。確保為使用CUCM/TVS/ITL/CAPF證書的任何工作安排維護視窗。

在CA簽名的CUCM SAN證書之前，請確保：

- IP電話能夠信任信任信任驗證服務(TVS)。這可以通過從電話訪問任何HTTPS服務來驗證。例

如，如果公司目錄訪問有效，則表示電話信任TVS服務。

- 驗證群集是否處於非安全模式或混合模式。

要確定它是否為混合模式集群，請選擇 **Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode(0 == Non-Secure; 1 == Mixed Mode)**.

警告：如果在服務重新啟動之前處於混合模式集群，則必須更新CTL:Token或Tokenless。

安裝由CA頒發的證書後，必須在已啟用的節點中重新啟動下一個服務清單：

- 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
- Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco Trust Verification Service

疑難排解

這些日誌可幫助思科技術支援中心識別與多伺服器SAN CSR生成和上傳CA簽名證書相關的任何問題。

- Cisco整合OS平台API
- Cisco Tomcat
- IPT平台CertMgr日誌
- 證書續訂流程

已知警告

·思科錯誤ID CSCur97909 — 上傳多伺服器證書不會刪除資料庫中的自簽名證書
·Cisco錯誤ID CSCus47235 - CUCM 10.5.2 CN未複製到SAN中用於CSR
·思科錯誤ID CSCup28852 — 使用多伺服器證書時，由於證書更新，每7分鐘重置一次電話

如果存在現有的多伺服器證書，建議在以下情況下重新生成：

- 主機名或域更改。執行主機名或域更改時，證書將自動重新生成為自簽名。若要將其更改為CA簽名，必須遵循前面的步驟。
- 如果向群集中新增了新節點，則必須生成包含新節點的新CSR。
- 當訂閱伺服器還原且未使用備份時，節點可以擁有新的自簽名證書。可能需要整個群集的新CSR以包含訂閱伺服器。(存在增強請求思科錯誤ID CSCuv75957 新增此功能。)

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）。