# 设置统一通信集群

## 目录



## 简介

本文档介绍如何使用证书颁发机构(CA)签名的多服务器SAN证书设置统一通信集群。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 思科统一通信管理器 (CUCM)
- CUCM IM and Presence版本10.5

在尝试此配置之前，请确保这些服务已启用且运行正常：

- 思科平台管理Web服务
- Cisco Tomcat 服务

要在Web界面上验证这些服务，请导航到**Cisco Unified Serviceability Page Services > Network Service > Select a server**。要在CLI上验证它们，请输入**utils service list**命令。

如果在CUCM集群中启用了SSO，则需要禁用并重新启用它。

### 使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 背景信息

在CUCM版本10.5及更高版本中，此信任存储证书签名请求(CSR)可以包括使用者备用名(SAN)和备用域。

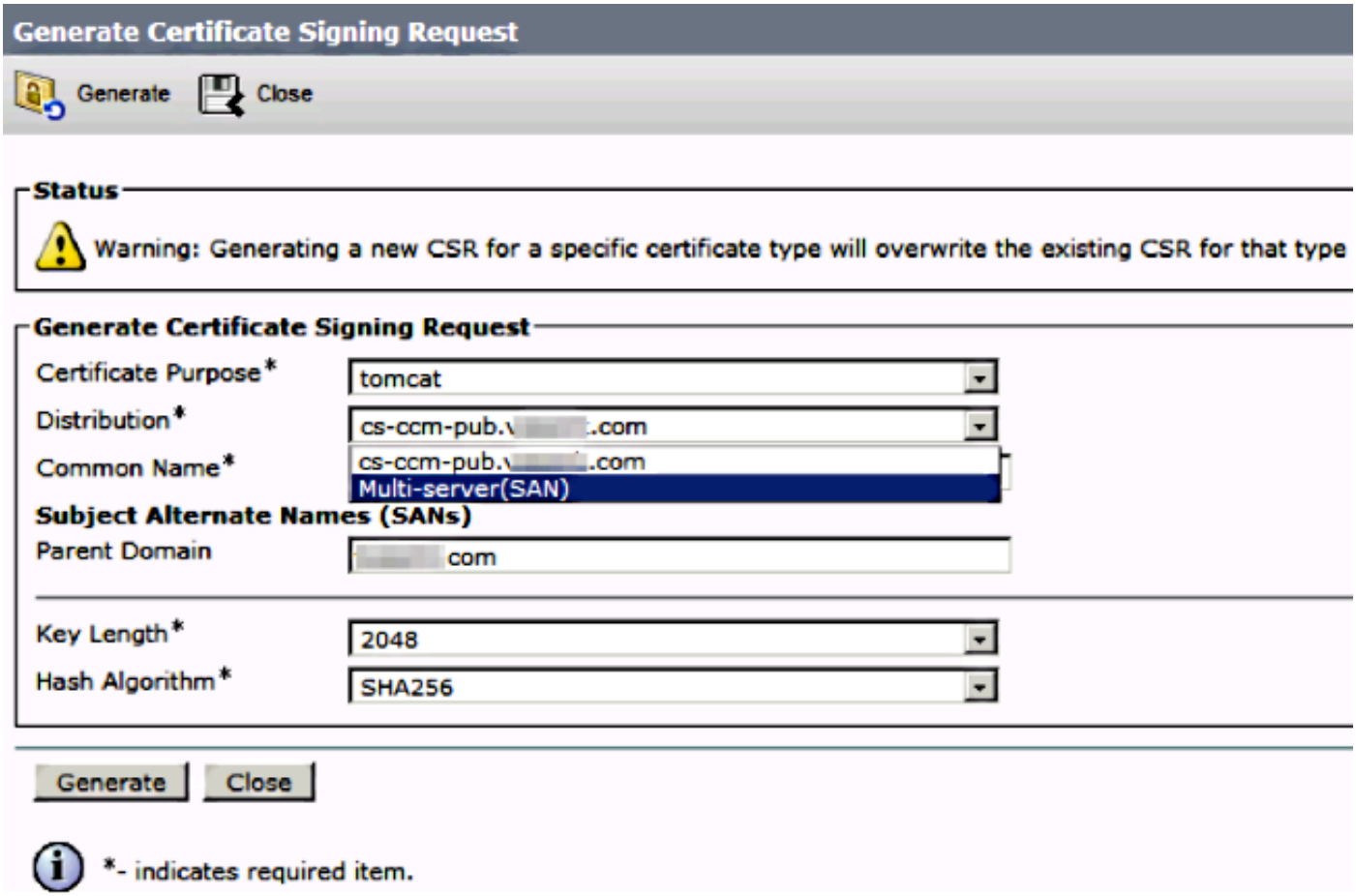
1. Tomcat - CUCM和IM&P
2. Cisco CallManager — 仅CUCM
3. Cisco Unified Presence — 可扩展消息传送和在线状态协议(CUP-XMPP) — 仅IM&P
4. CUP-XMPP服务器到服务器(S2S) — 仅IM&P

在此版本中获取CA签名的证书更简单。只需一个CSR由CA签署，而不需要从每个服务器节点获取CSR，然后为每个CSR获取CA签署的证书并单独管理它们。

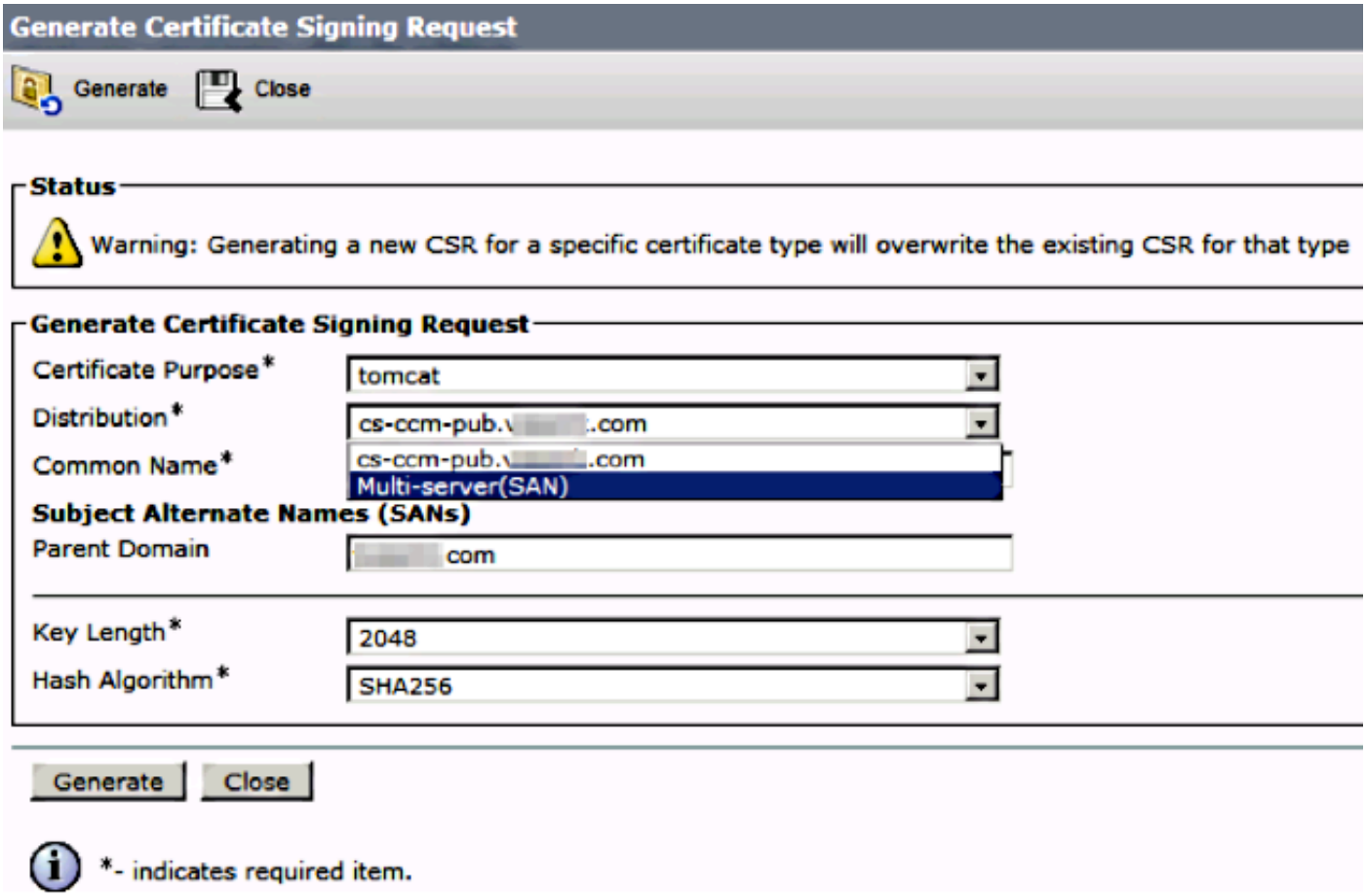
# 配置

**步骤1:**

登录到Publisher的操作系统(OS)管理，然后导航到**安全>证书管理>生成CSR**。

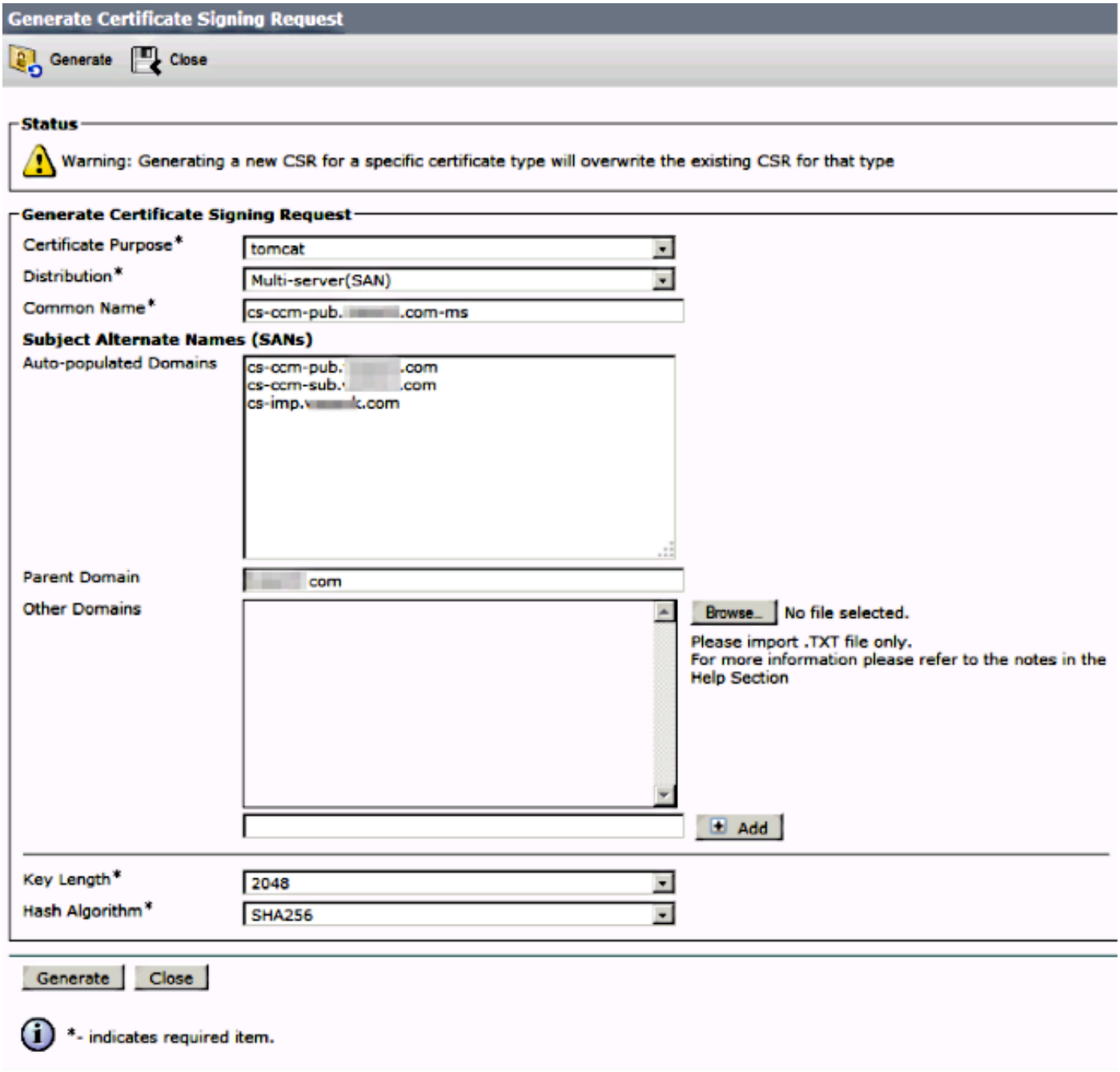



**第二步：**
选择**Multi-Server SAN** in Distribution。



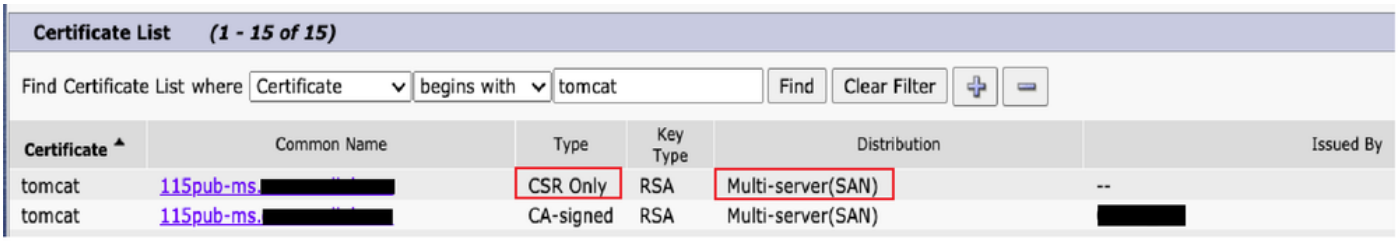

它会自动填充SAN域和父域。

验证Tomcat是否列出了集群的所有节点：CallManager的所有CUCM和IM&P节点均列出：仅列出了CUCM节点。



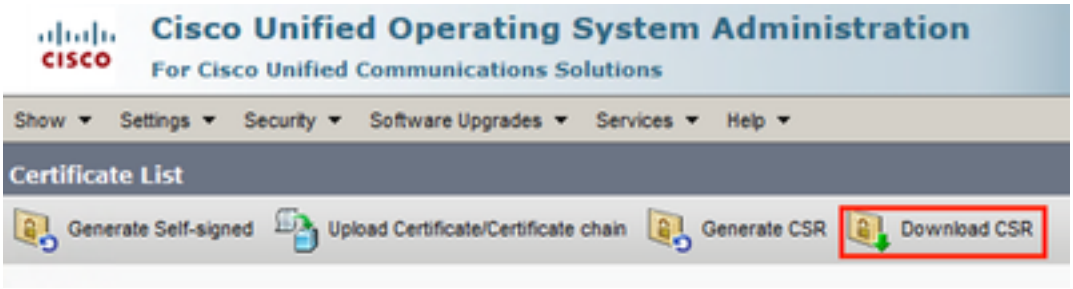

**第三步：**
点击generate，在生成CSR后，验证CSR中列出的所有节点是否也显示在Successful CSR exported列表中。


在证书管理中，会生成SAN请求：




**第四步：**

单击**Download CSR**，然后选择证书用途，然后单击**Download CSR**。

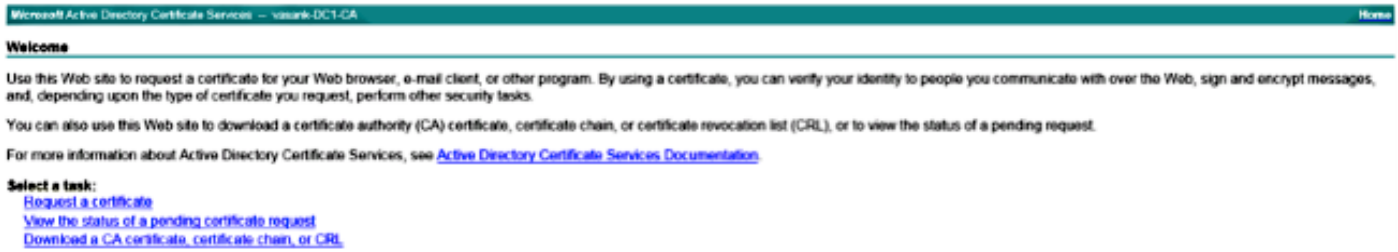




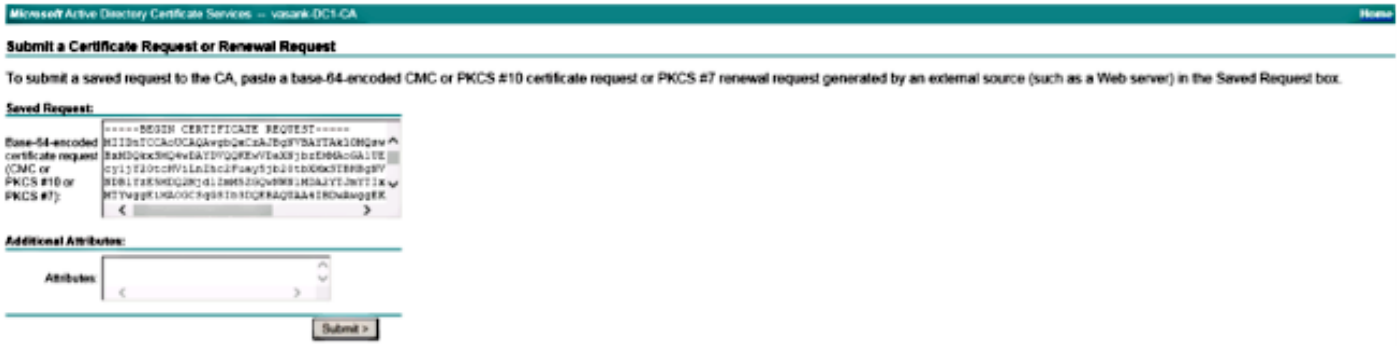
可以使用本地CA或类似VeriSign的外部CA对CSR（在上一步中下载的文件）进行签名。

此示例显示基于Microsoft Windows Server的CA的配置步骤。如果使用不同的CA或外部CA，请转至步骤5。

登录https://<windowsserveripaddress>/certsrv/
选择**Request a Certificate > Advanced Certificate Request。**
将CSR文件的内容复制到Base-64编码的证书请求字段，然后点击**Submit。**



按如下所示提交CSR请求。

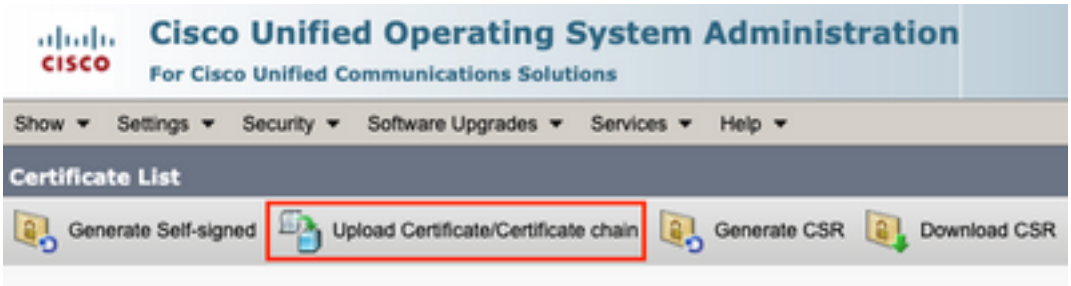


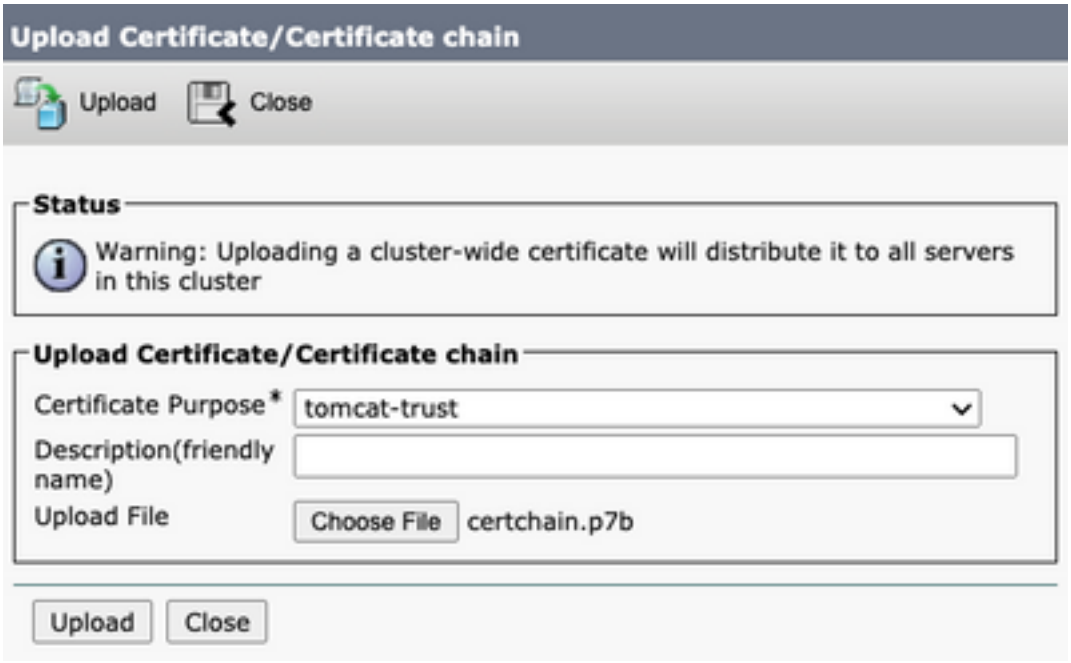


**第五步：**

> **注**：上传Tomcat证书之前，请验证SSO是否已禁用。如果启用SSO，则必须在所有Tomcat证书再生过程完成后禁用并重新启用SSO。

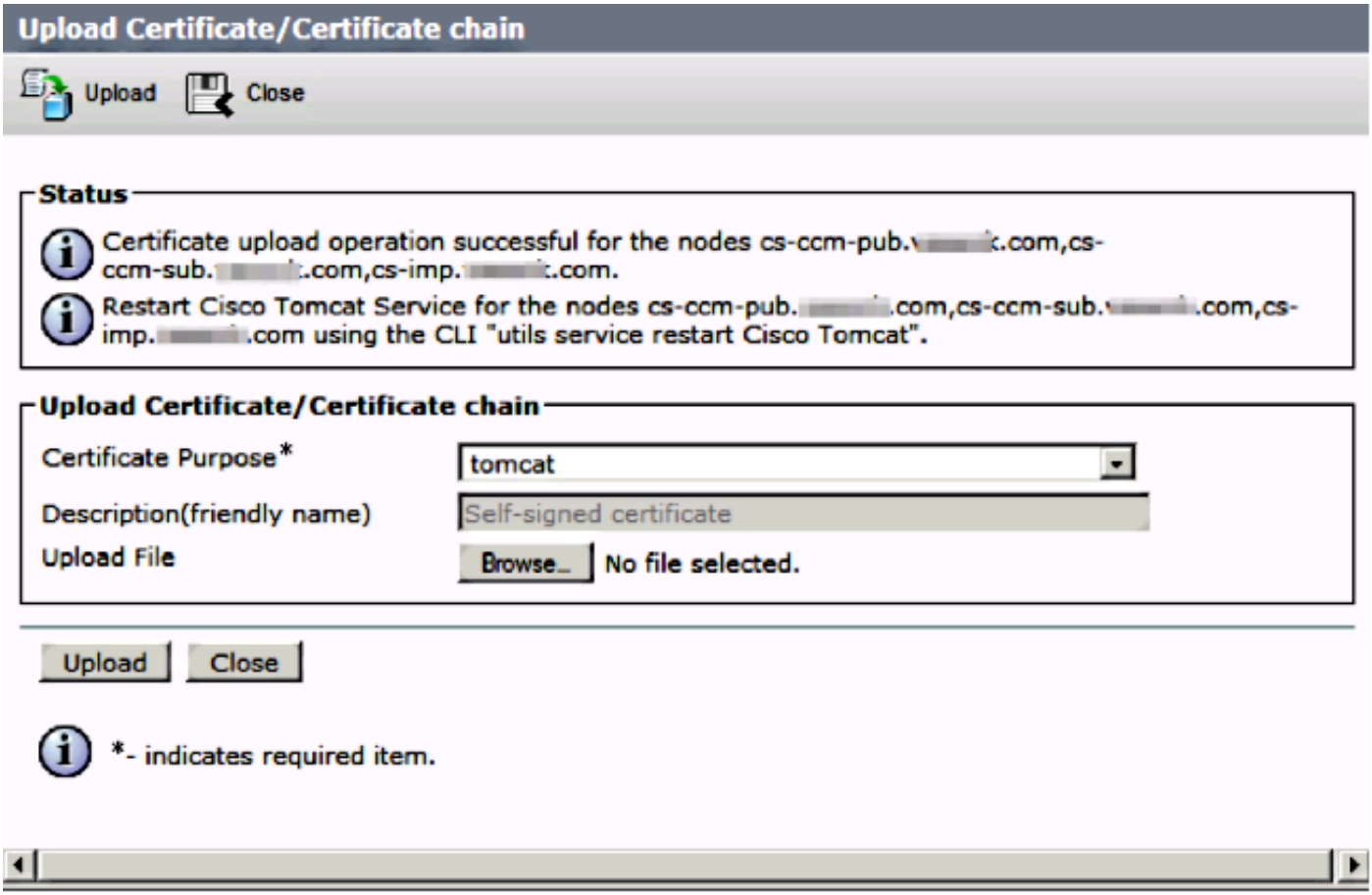
使用签名证书上传CA证书作为tomcat-trust。首先配置根证书，然后配置中间证书（如果存在）。






**第六步：**

现在将CUCM签名证书上传为Tomcat，并验证集群的所有节点是否列在“证书上传操作成功”(Certificate upload operation successful)中，如图所示：




“证书管理”中列出了多服务器SAN，如图所示：

| | | | | | | |
|---|---|---|---|---|---|---|
| ipsec-trust | cs-ccm-pub.[redacted].com | Self-signed | cs-ccm-pub.[redacted].com | cs-ccm-pub.[redacted].com | 04/18/2019 | Trust Certificate |
| ITLRecovery | ITLRECOVERY_cs-ccm-pub.vasank.com | Self-signed | ITLRECOVERY_cs-ccm-pub.[redacted].com | ITLRECOVERY_cs-ccm-pub.[redacted].com | 04/18/2019 | Self-signed certificate generated by system |
| tomcat | cs-ccm-pub.[redacted].com-ms | CA-signed | Multi-server(SAN) | [redacted]-DC1-CA | 12/19/2015 | Certificate Signed by [redacted]-DC1-CA |
| tomcat-trust | cs-ccm-pub.[redacted].com-ms | CA-signed | Multi-server(SAN) | [redacted]-DC1-CA | 12/19/2015 | Trust Certificate |
| tomcat-trust | cs-ccm-pub.[redacted].com | Self-signed | cs-ccm-pub.[redacted].com | cs-ccm-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-ccm-pub.[redacted].com | Self-signed | dc1-ccm-pub.[redacted].com | dc1-ccm-pub.[redacted].com | 04/17/2019 | Trust Certificate |
| tomcat-trust | dc1-ccm-sub.[redacted].com | Self-signed | dc1-ccm-sub.[redacted].com | dc1-ccm-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-ccm-pub.vasank.com | Self-signed | cs-ccm-pub.[redacted].com | cs-ccm-pub.[redacted].com | 04/18/2019 | Self-signed certificate generated by system |

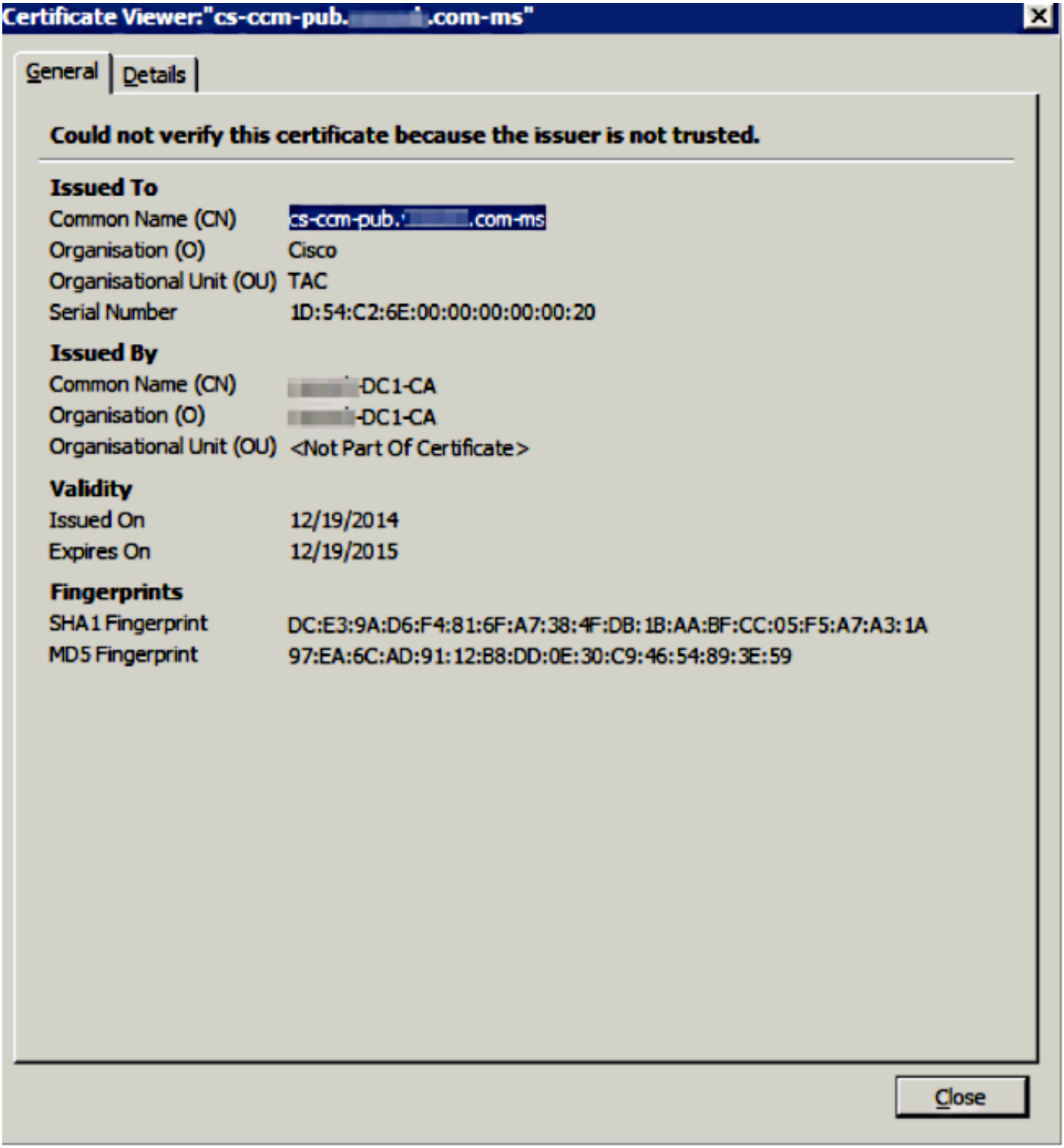
**步骤 7.**

使用命令**utils service restart Cisco Tomcat**，通过CLI在SAN列表中的所有节点（首先是发布服务器，然后是订用服务器）上重新启动Tomcat服务。

```
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:
```

# 验证

登录http://<fqdnofccm>:8443/ccmadmin以确保使用新证书。




## CallManager多服务器SAN证书

对于CallManager证书，可遵循类似的过程。在这种情况下，自动填充的域仅是CallManager节点。如果Cisco CallManager服务未运行，您可以选择将其保留在SAN列表中或将其删除。

> **警告**：此过程会影响电话注册和呼叫处理。确保为CUCM/TVS/ITL/CAPF证书的任何工作安排维护窗口。

在CUCM的CA签名的SAN证书之前，请确保：

- IP电话可以信任信任信任验证服务(TVS)。这可以通过从电话访问任何HTTPS服务进行验证。

例如，如果公司目录访问有效，则表示电话信任TVS服务。

- 验证集群是否处于非安全模式或混合模式。

要确定它是否为混合模式集群，请选择 **Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode(0 == Non-Secure; 1 == Mixed Mode)**.

**警告**：如果在服务重新启动之前处于混合模式集群，则必须更新CTL:令牌或无令牌的。

安装由CA颁发的证书后，必须在已启用的节点中重新启动下一个服务列表：

- 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 — 网络服务> Cisco Trust Verification Service

# 故障排除

这些日志可帮助思科技术支持中心确定与多服务器SAN CSR生成和上传CA签名证书相关的所有问题。

- 思科统一操作系统平台API
- Cisco Tomcat
- IPT平台证书管理器日志
- 证书更新过程

## 已知问题说明

·Cisco Bug ID CSCur97909 — 上传多服务器证书不会删除数据库中的自签名证书
·思科漏洞ID CSCus47235 - CUCM 10.5.2 CN未复制到CSR的SAN
·Cisco Bug ID CSCup28852 — 由于使用多服务器证书进行证书更新，每7分钟重置一次电话

如果现有多服务器证书，建议在以下情况下重新生成：

- 主机名或域更改。执行主机名或域更改时，证书将自动重新生成为自签名。要将其更改为CA签名，必须遵循之前的步骤。
- 如果向集群中添加了新节点，则必须生成包含新节点的新CSR。
- 当用户恢复且未使用备份时，节点可以拥有新的自签名证书。可能需要整个集群的新CSR才能包括用户。(存在增强请求Cisco bug ID CSCuv75957 添加此功能。)

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。