# Configurer le cluster de communications unifiées

## Table des matières



## Introduction

Ce document décrit comment configurer un cluster de communications unifiées avec l'utilisation de certificats SAN multiserveurs signés par l'autorité de certification (CA).

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Gestionnaire de communications unifiées de Cisco (version CUCM)
- CUCM IM and Presence version 10.5

Avant d'essayer cette configuration, assurez-vous que ces services sont opérationnels :

- Service Web d'administration de plate-forme Cisco
- Service Cisco Tomcat

Afin de vérifier ces services sur une interface Web, naviguez vers **Cisco Unified Serviceability Page Services > Network Service > Select a server**. Afin de les vérifier sur la CLI, entrez la commande **utils service list**.

Si l'authentification unique est activée dans le cluster CUCM, elle doit être désactivée et réactivée.

### Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

# Informations générales

Dans CUCM version 10.5 et ultérieure, cette demande de signature de certificat (CSR) de magasin de confiance peut inclure un nom de remplacement de sujet (SAN) et d'autres domaines.

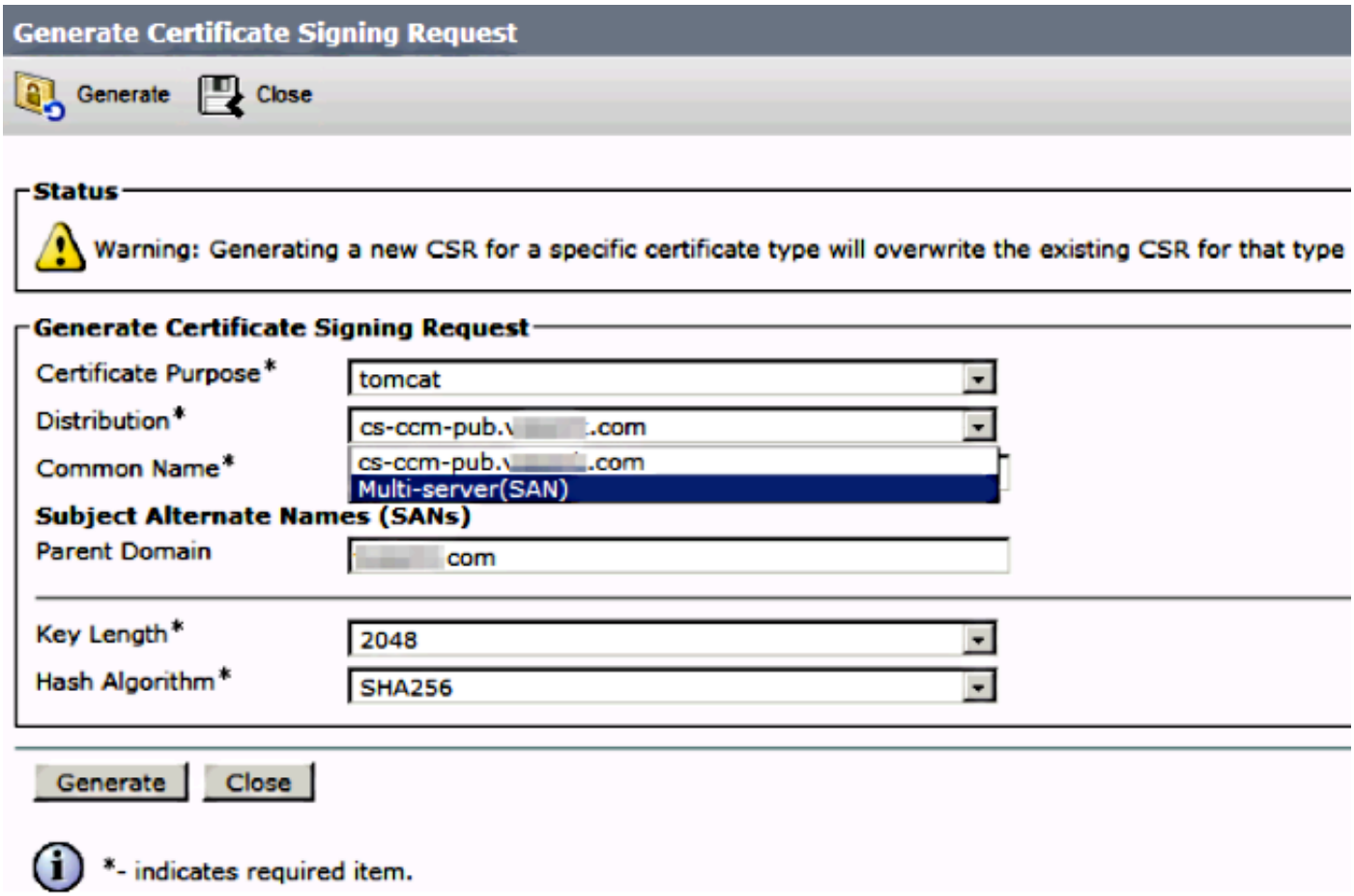
1. Tomcat - CUCM et IM&P
2. Cisco CallManager - CUCM uniquement
3. Cisco Unified Presence-Extensible Messaging and Presence Protocol (CUP-XMPP) - Uniquement IM&P
4. CUP-XMPP de serveur à serveur (S2S) - Uniquement IM&P

Il est plus simple d'obtenir un certificat signé par une autorité de certification dans cette version. Une seule autorité de certification doit être signée par une seule autorité de certification plutôt que d'obtenir une autorité de certification de chaque noeud de serveur, puis d'obtenir un certificat signé par une autorité de certification pour chaque autorité de certification et de les gérer individuellement.

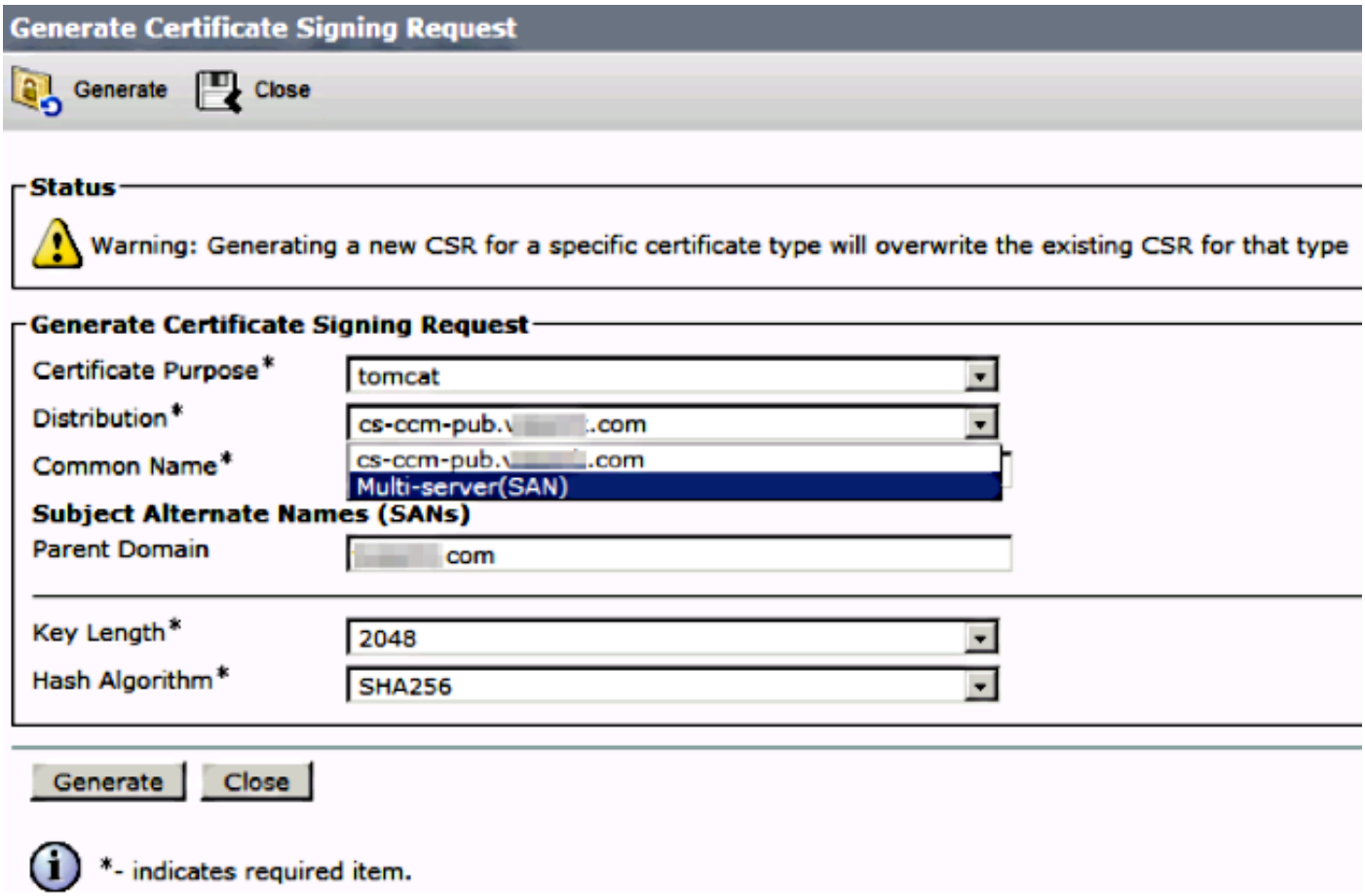
# Configurer

**Étape 1.**

Connectez-vous à l'Administration du système d'exploitation de Publisher et accédez à **Sécurité > Gestion des certificats > Générer CSR**.

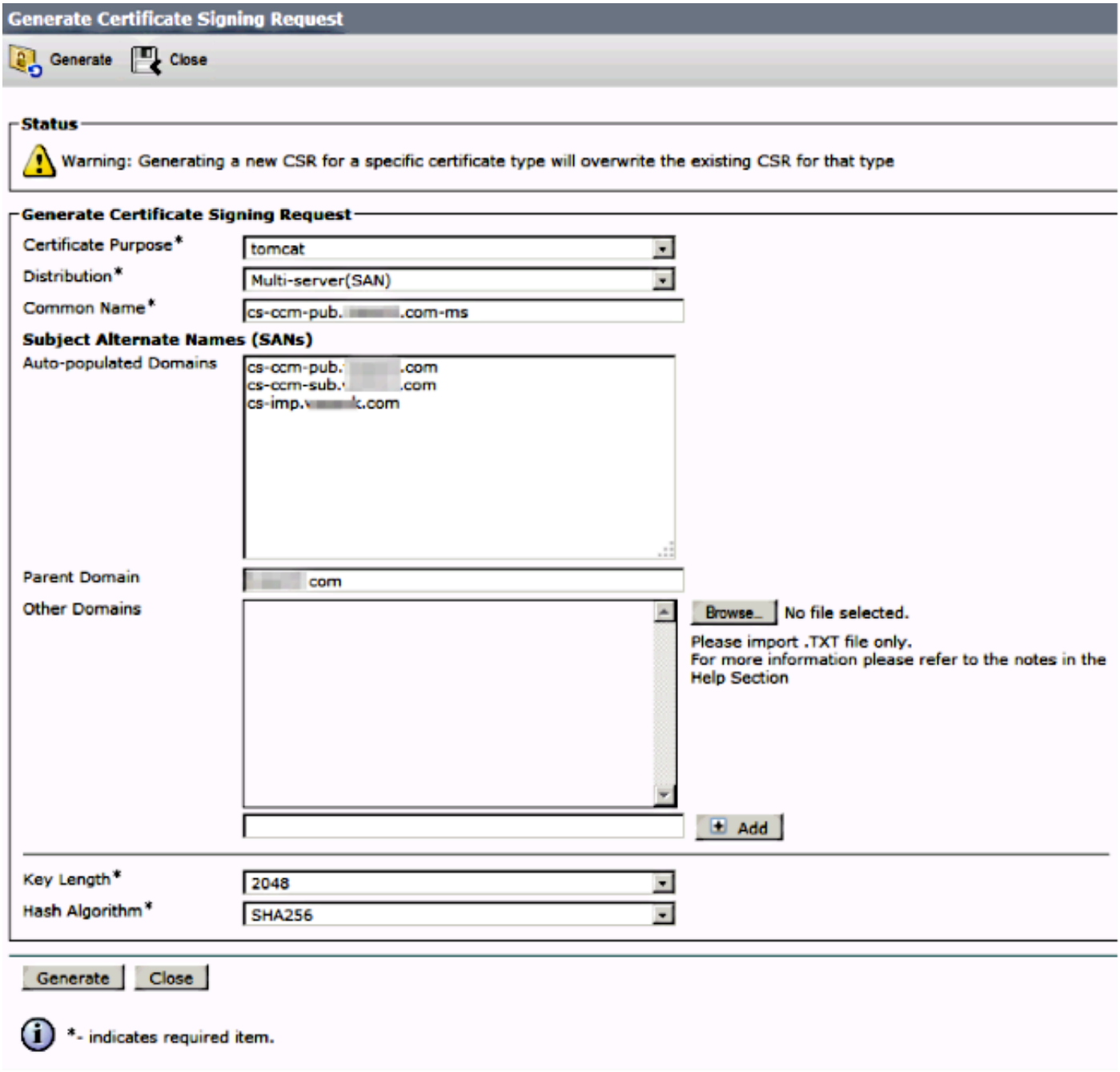



**Étape 2.**
Sélectionnez **Multi-Server SAN** dans Distribution.




Il remplit automatiquement les domaines SAN et le domaine parent.

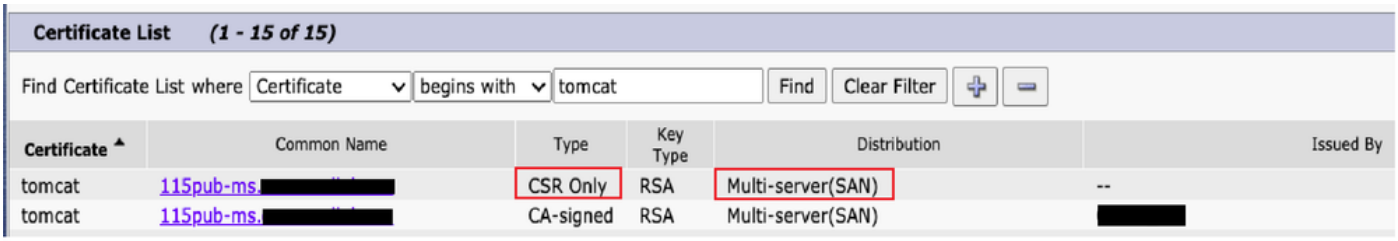
Vérifiez que tous les noeuds de votre cluster sont répertoriés pour Tomcat : tous les noeuds CUCM et IM&P pour CallManager : seuls les noeuds CUCM sont répertoriés.




## Étape 3.

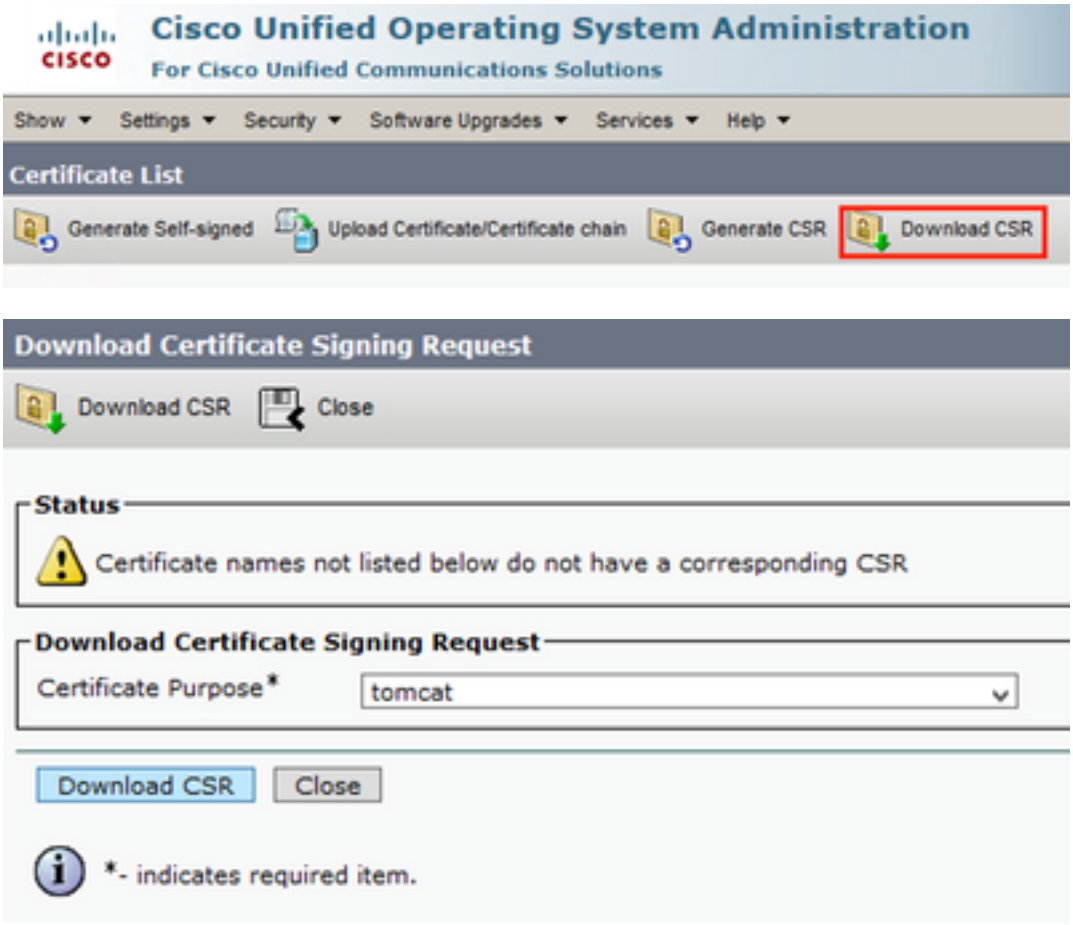
Cliquez sur Generate (Générer) et une fois que le CSR est généré, vérifiez que tous les noeuds répertoriés dans le CSR sont également affichés dans la liste des CSR exportés avec succès.


Dans Certificate Management, la requête SAN est générée :




### Étape 4.

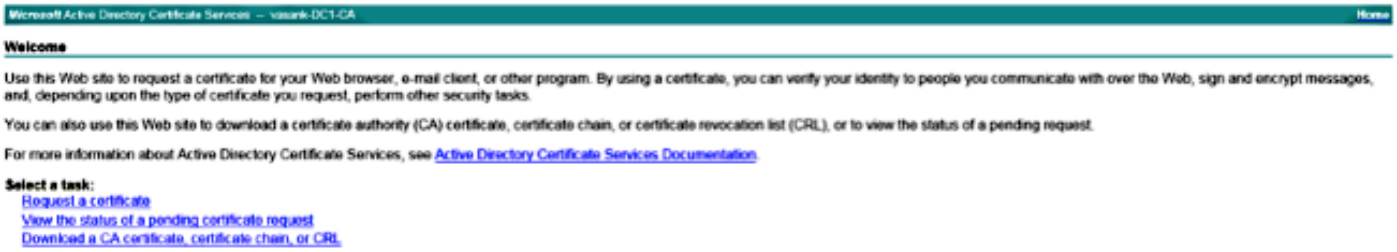
Cliquez sur **Download CSR** puis choisissez le rôle du certificat et cliquez sur **Download CSR**.



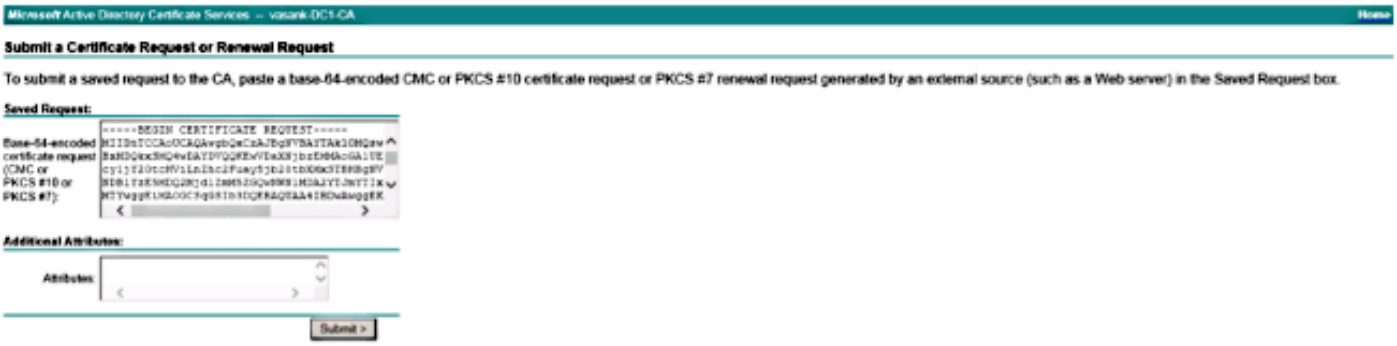

Il est possible d'utiliser l'autorité de certification locale ou une autorité de certification externe comme VeriSign afin de faire signer le CSR (fichier téléchargé à l'étape précédente).

Cet exemple montre les étapes de configuration d'une autorité de certification basée sur Microsoft Windows Server. Si vous utilisez une autre autorité de certification ou une autorité de certification externe, passez à l'étape 5.

Connectez-vous à https://<adresse_serveursde Windows>/certsrv/
Choisissez **Request a Certificate > Advanced Certificate Request.**
Copiez le contenu du fichier CSR dans le champ de demande de certificat codé en base 64, puis cliquez sur **Submit**.




Envoyez la demande de CSR comme indiqué ici.

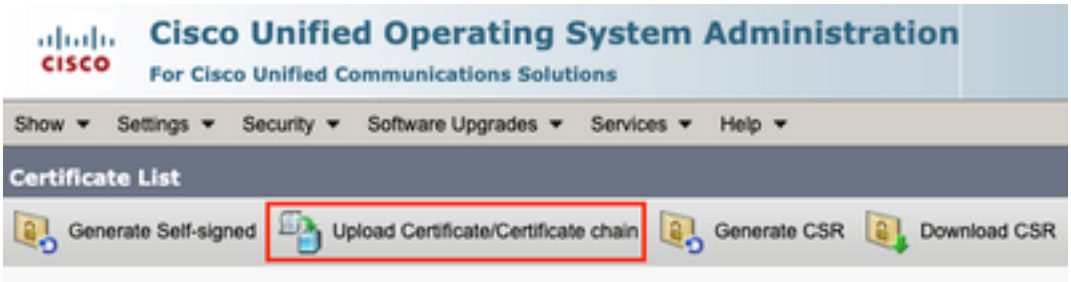


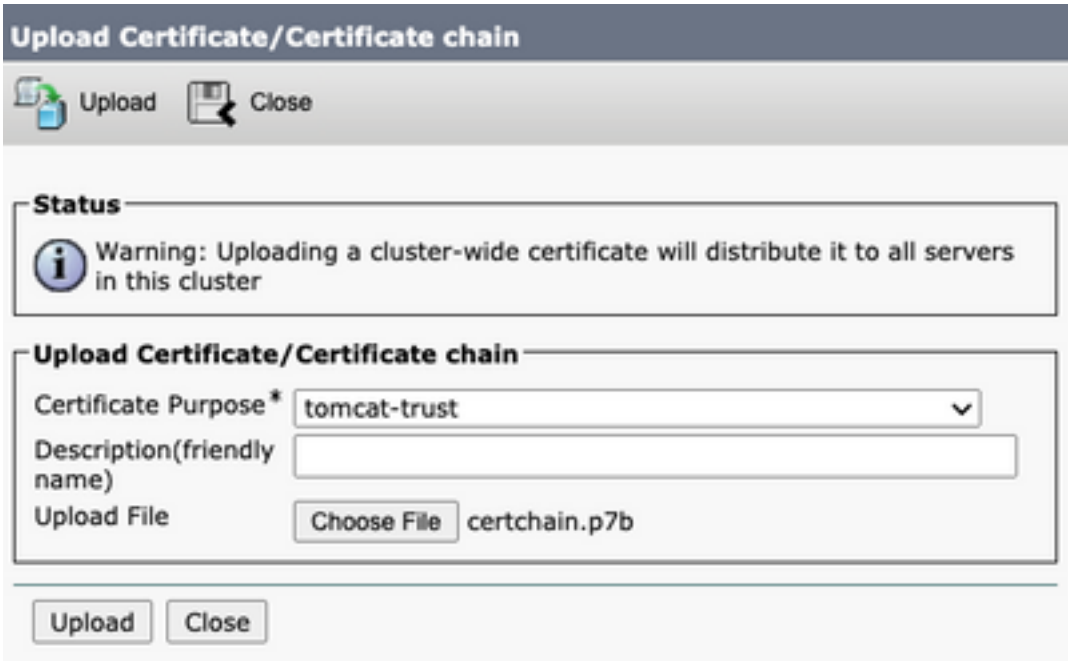


## Étape 5.

> **Remarque** : avant de télécharger un certificat Tomcat, vérifiez que l'authentification unique est désactivée. Dans le cas où il est activé, SSO doit être désactivé et réactivé une fois que tout le processus de régénération de certificat Tomcat est terminé.

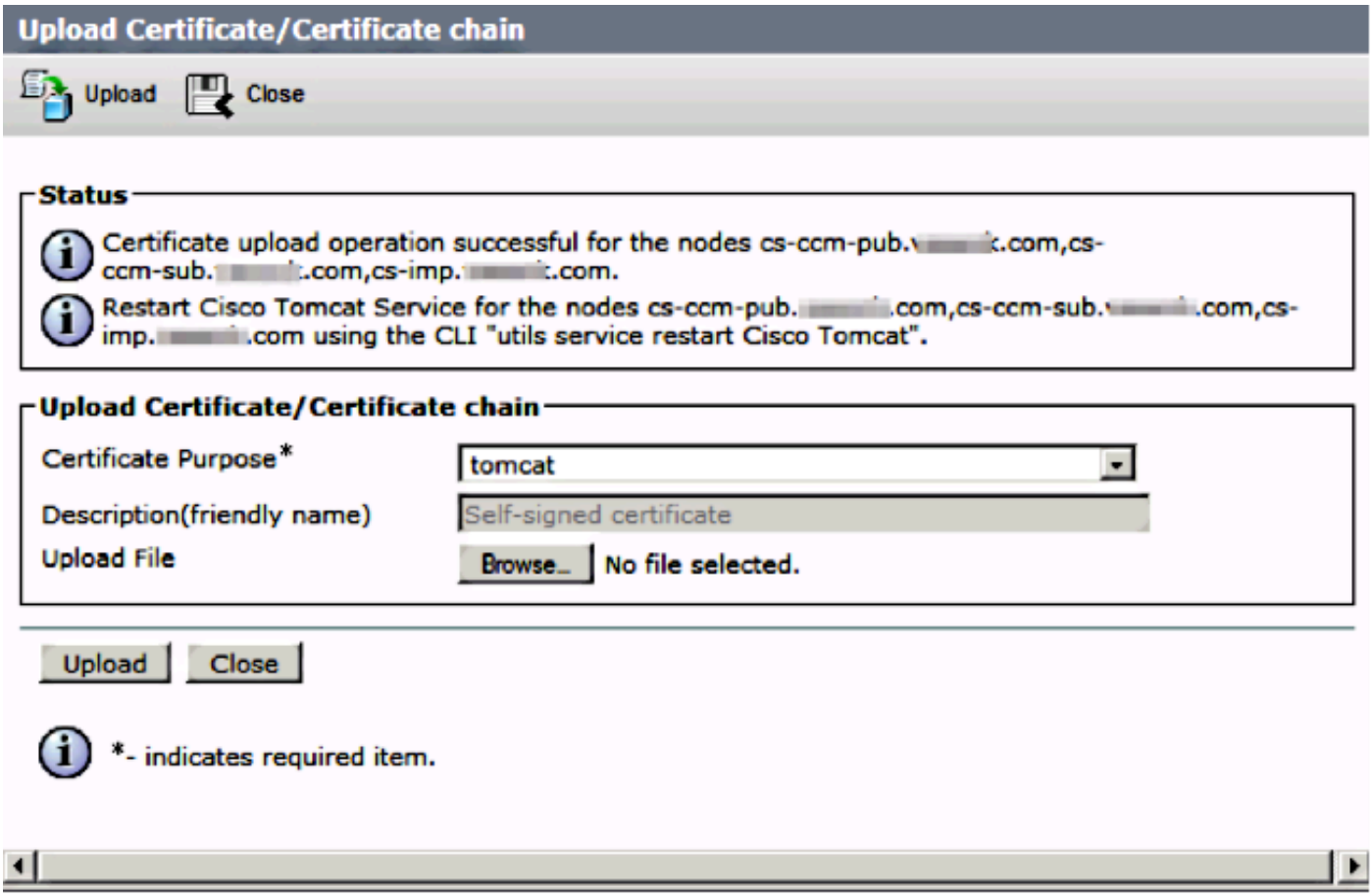
Une fois le certificat signé, téléchargez les certificats d'autorité de certification en tant que tomcat-trust. Commencez par le certificat racine, puis le certificat intermédiaire s'il existe.






### Étape 6.

Téléchargez maintenant le certificat signé CUCM en tant que Tomcat et vérifiez que tous les noeuds de votre cluster sont répertoriés dans la section « Opération de téléchargement de certificat réussie », comme illustré dans l'image :




Le SAN multiserveur est répertorié dans la section Certificate Management, comme illustré dans l'image :

| | | | | | | |
|---|---|---|---|---|---|---|
| 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 |

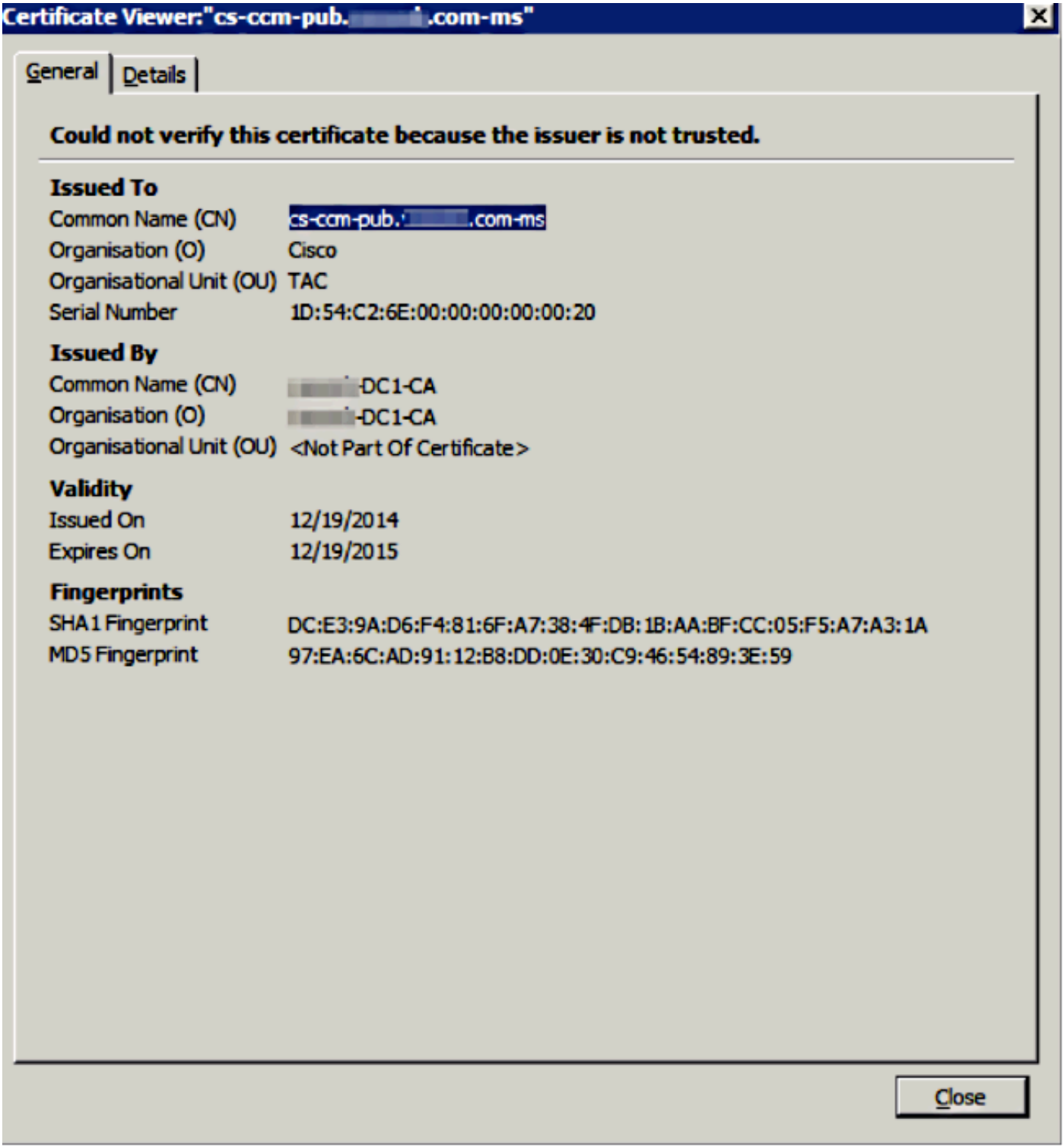
### Étape 7.

Redémarrez le service Tomcat sur tous les noeuds de la liste SAN (d'abord le serveur de publication, puis les abonnés) via l'interface de ligne de commande à l'aide de la commande : **utils service restart Cisco Tomcat**.

```
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:
```

## Vérifier

Connectez-vous à http://<fqdnofccm>:8443/ccmadmin afin de vous assurer que le nouveau certificat est utilisé.




## Certificat SAN multiserveur CallManager

Une procédure similaire peut être suivie pour le certificat CallManager. Dans ce cas, les domaines remplis automatiquement ne sont que des noeuds CallManager. Si le service Cisco CallManager n'est pas en cours d'exécution, vous pouvez choisir de le conserver dans la liste SAN ou de le supprimer.

> **Avertissement** : ce processus affecte l'enregistrement des téléphones et le traitement des appels. Assurez-vous de planifier une fenêtre de maintenance pour tout travail avec les certificats CUCM/TVS/ITL/CAPF.

Avant de signer le certificat SAN pour CUCM, assurez-vous que :

- Le téléphone IP peut faire confiance au service de vérification de la confiance (TVS). Cela peut être vérifié avec l'accès à n'importe quel service HTTPS à partir du téléphone. Par exemple, si l'accès au répertoire d'entreprise fonctionne, cela signifie que le téléphone fait confiance au service TVS.
- Vérifiez si le cluster est en mode non sécurisé ou en mode mixte.

Pour déterminer s'il s'agit d'un cluster en mode mixte, sélectionnez **Administration de Cisco Unified CM > Système > Paramètres d'entreprise > Mode de sécurité du cluster (0 == Non sécurisé ; 1 == Mode mixte)**.

> **Avertissement** : si vous êtes dans un cluster en mode mixte avant le redémarrage des services, la CTL doit être mise à jour : Token ou Tokenless.

Après avoir installé le certificat émis par l'autorité de certification, la liste suivante de services doit être redémarrée dans les noeuds activés :

- Cisco Unified Serviceability > Outils > Control Center - Services de fonctionnalités > Cisco TFTP
- Cisco Unified Serviceability > Outils > Control Center - Services de fonctionnalités > Cisco CallManager
- Facilité de maintenance unifiée Cisco > Outils > Centre de contrôle - Services de fonctionnalités > Cisco TIManager
- Cisco Unified Serviceability > Outils > Centre de contrôle - Services réseau > Service de vérification de la confiance Cisco

# Dépannage

Ces journaux peuvent aider le centre d'assistance technique Cisco à identifier tout problème lié à la génération de CSR SAN multiserveur et au téléchargement du certificat CA-Signed.

- API de la plate-forme Cisco Unified OS
- Cisco Tomcat
- Journaux CertMgr de la plateforme IPT
- Processus de renouvellement de certificat

## Avertissements connus

·ID de bogue Cisco CSCur97909 - Le téléchargement de certificats multiserveurs ne supprime pas les certificats auto-signés dans la base de données
·ID de bogue Cisco CSCus47235 - CUCM 10.5.2 CN non dupliqué dans SAN pour CSR
·ID de bogue Cisco CSCup2852 - réinitialisation du téléphone toutes les 7 minutes en raison d'une mise à jour du certificat lorsque vous utilisez le certificat multiserveur

S'il existe un certificat multiserveur existant, la régénération est recommandée dans les scénarios suivants :

- Changement de nom d'hôte ou de domaine. Lorsqu'un changement de nom d'hôte ou de

domaine est effectué, les certificats sont automatiquement régénérés comme étant auto-signés. Pour le remplacer par un certificat CA-Signed, vous devez suivre les étapes précédentes.

- Si un nouveau noeud a été ajouté au cluster, un nouveau CSR doit être généré pour inclure le nouveau noeud.
- Lorsqu'un abonné est restauré et qu'aucune sauvegarde n'a été utilisée, le noeud peut avoir de nouveaux certificats auto-signés. Un nouveau CSR pour la grappe complète peut être requis pour inclure l'abonné. (Il y a une demande d'amélioration ID de bogue Cisco CSCuv75957 pour ajouter cette fonctionnalité.)

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.