Créer de nouveaux certificats à partir de certificats CA signés

Table des matières

Introduction

Ce document décrit comment régénérer les certificats signés par une autorité de certification (CA) dans Cisco Unified Communications Manager (CUCM).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Outil de surveillance en temps réel (RTMT)
- Certificats CUCM

Composants utilisés

- CUCM versions 10.x, 11.x et 12.x.

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 de pré-vérification

Remarque : pour la régénération des certificats auto-signés, reportez-vous au Guide de régénération des certificats. Pour la régénération de certificat multi-SAN signé par l'autorité de certification, reportez-vous au Guide de régénération de certificat multi-SAN

Pour comprendre l'impact de chaque certificat et sa régénération, reportez-vous au Guide de régénération auto-signé.

Chaque type de demande de signature de certificat (CSR) a différentes utilisations de clé et celles-ci sont requises dans le certificat signé. Le Guide de sécurité inclut un tableau avec les utilisations de clés requises pour chaque type de certificat.

Pour modifier les paramètres d'objet (emplacement, état, unité d'organisation, etc.), exécutez cette commande :

- **set web-security** orgunit orgname locality state [country] [alternatehostname]

Le certificat Tomcat est régénéré automatiquement après l'exécution de la commande Tomcat`set web-security`. Le nouveau certificat auto-signé n'est pas appliqué, sauf si le service Tomcat est redémarré. Reportez-vous à ces guides pour plus d'informations sur cette commande :

- Guide de référence de la ligne de commande
- Lien vers les étapes de la communauté Cisco
- Vidéo

Configuration et régénération des certificats

Les étapes de régénération des certificats de noeud unique dans un cluster CUCM signé par une autorité de certification sont répertoriées pour chaque type de certificat. Il n'est pas nécessaire de régénérer tous les certificats du cluster s'ils n'ont pas expiré.

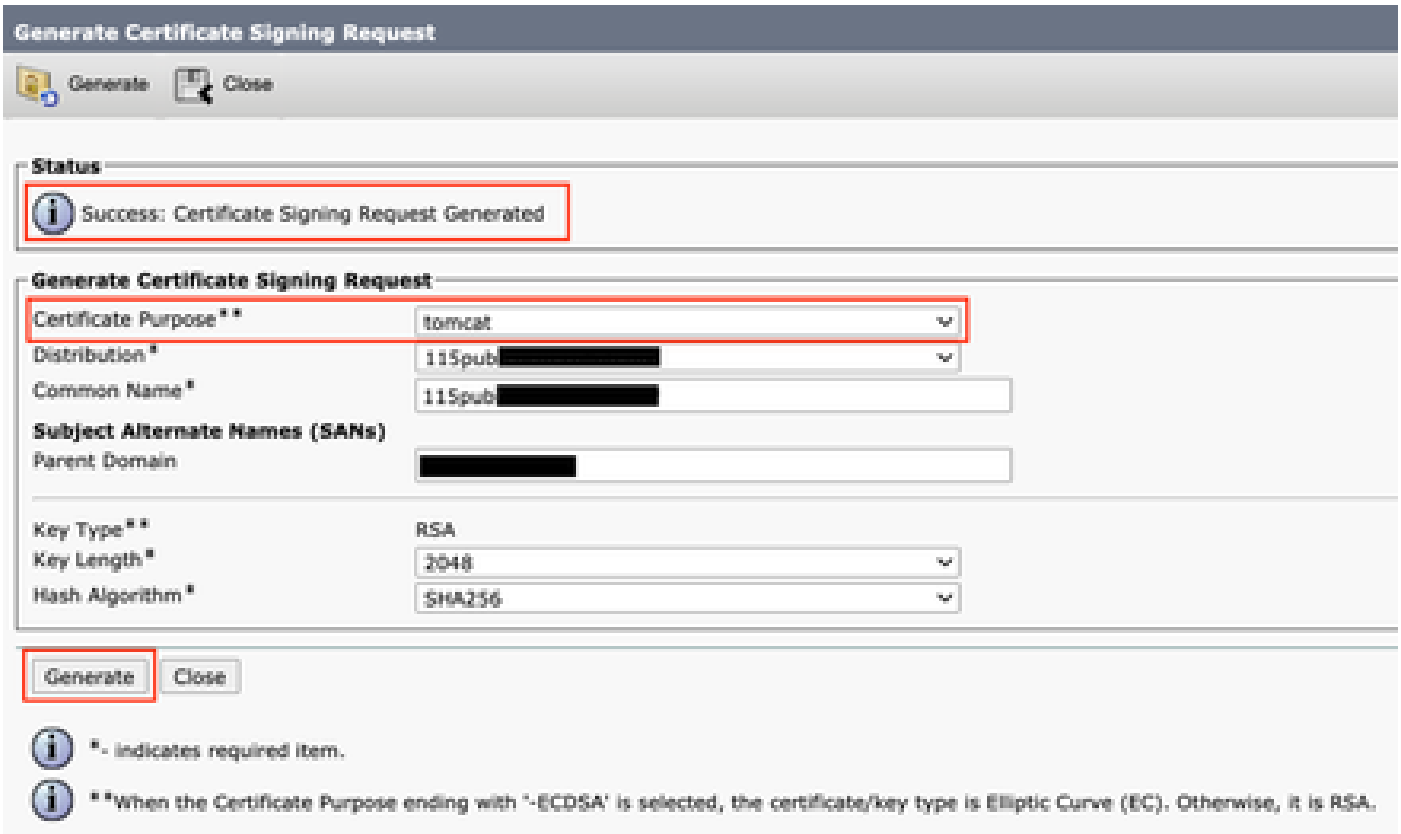
Certificat Tomcat

Attention : vérifiez que l'authentification unique est désactivée dans le cluster (**CM Administration > System > SAML Single Sign-On**). Si l'authentification unique est activée, elle doit être désactivée, puis activée une fois le processus de régénération de certificat Tomcat terminé.

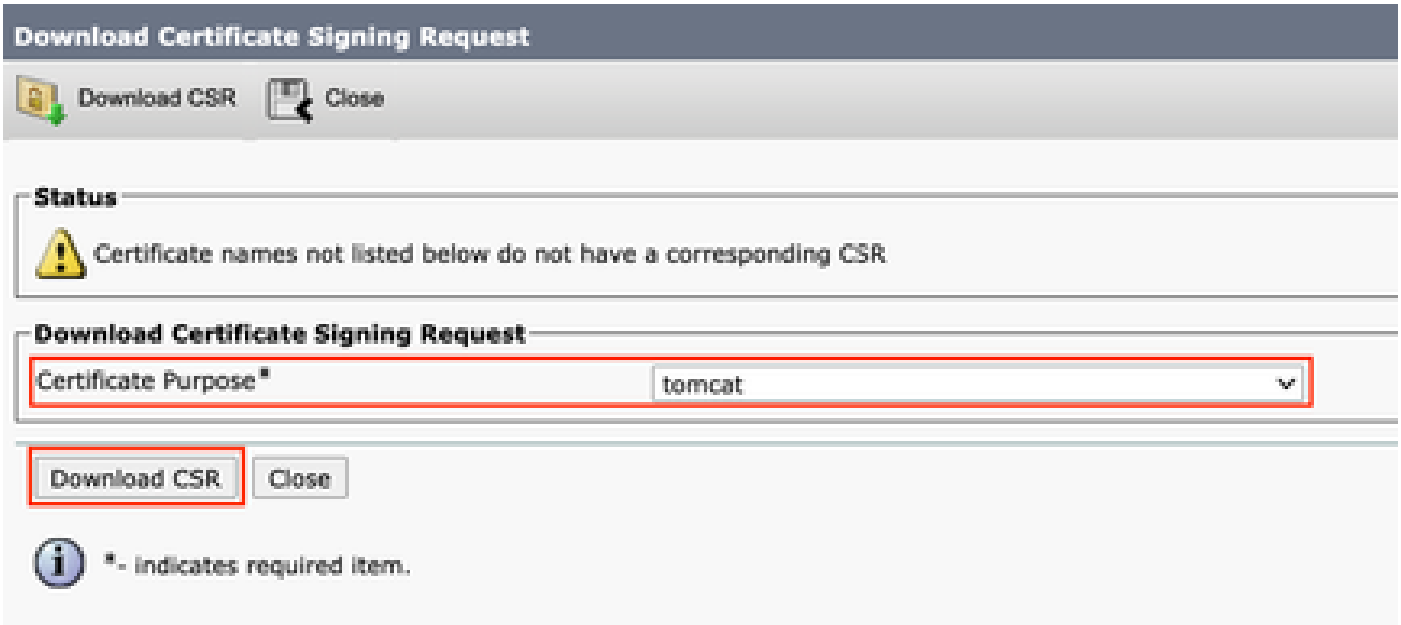
Sur tous les noeuds (CallManager et IM&P) du cluster :

Étape 1. Naviguez jusqu'à la date d'expiration du certificat Tomcat, **Cisco Unified OS Administration > Security > Certificate Management > Find** puis vérifiez-la.

Étape 2. Cliquez surGenerate CSR > Certificate Purpose: tomcat. Sélectionnez les paramètres souhaités pour le certificat, puis cliquez surGenerate. Attendez que le message de réussite s'affiche et cliquez surClose.



Étape 3. Téléchargez le CSR. Cliquez surDownload CSR, sélectionnez **Certificate Purpose: tomcat**, et cliquez surDownload.



Étape 4. Envoyez le CSR à l'autorité de certification.

Étape 5. L'autorité de certification renvoie au moins deux fichiers pour la chaîne de certificats signés. Téléchargez les certificats dans l'ordre suivant :

- Certificat d'autorité de certification racine comme tomcat-trust. Naviguez jusqu'à **Certificate Management** > **Upload certificate** > **Certificate Purpose: tomcat-trust**. Définir la description du certificat et parcourez le fichier de certificat racine.
- Certificat intermédiaire comme tomcat-trust (facultatif). Accédez à **Certificate Management** > **Upload certificate** > **Certificate Purpose: tomcat-trust**. Définissez la description du certificat et parcourez le fichier de certificat intermédiaire.

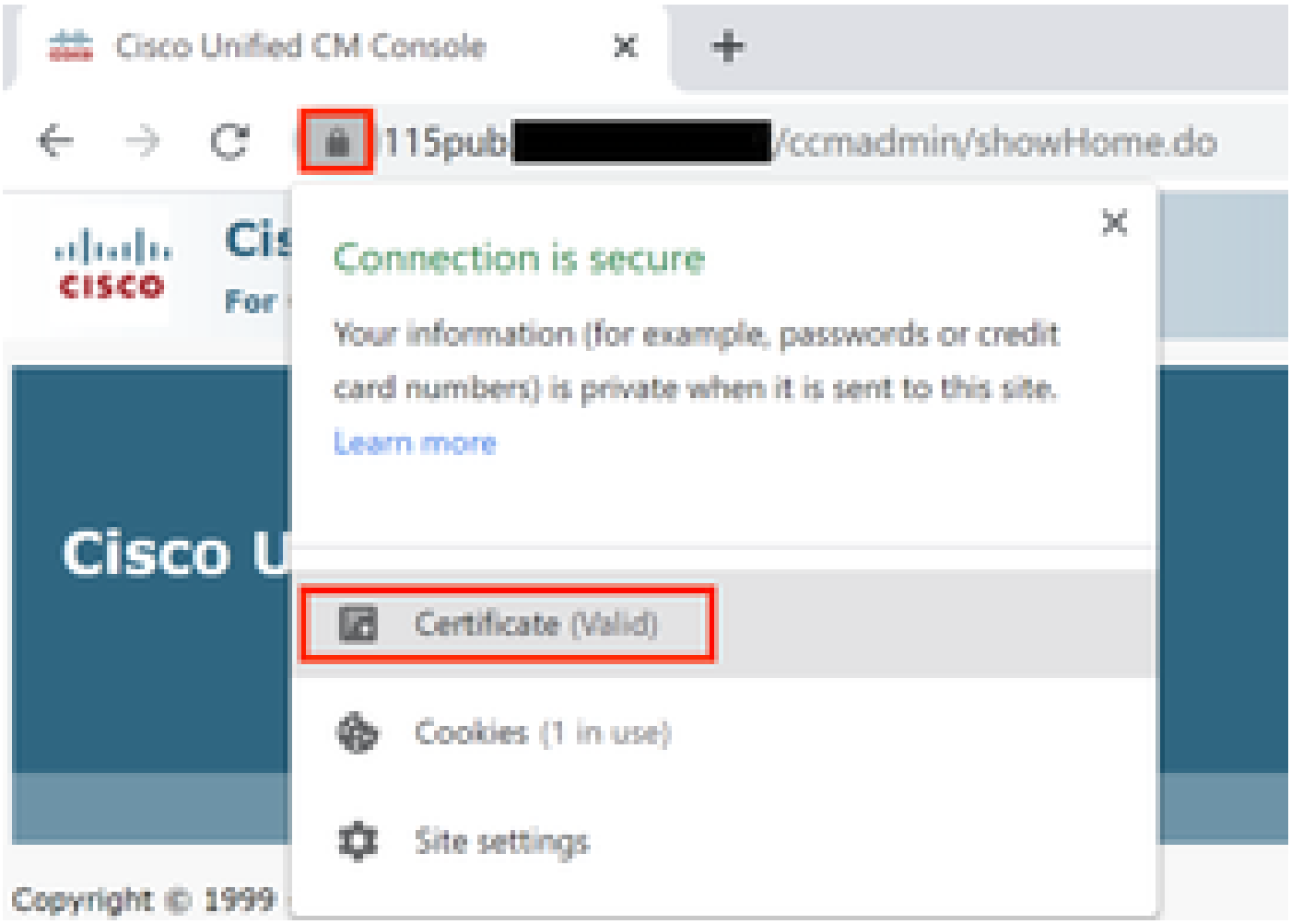
Remarque : certaines autorités de certification ne fournissent pas de certificat intermédiaire. Si seul le certificat racine a été fourni, cette étape peut être omise.

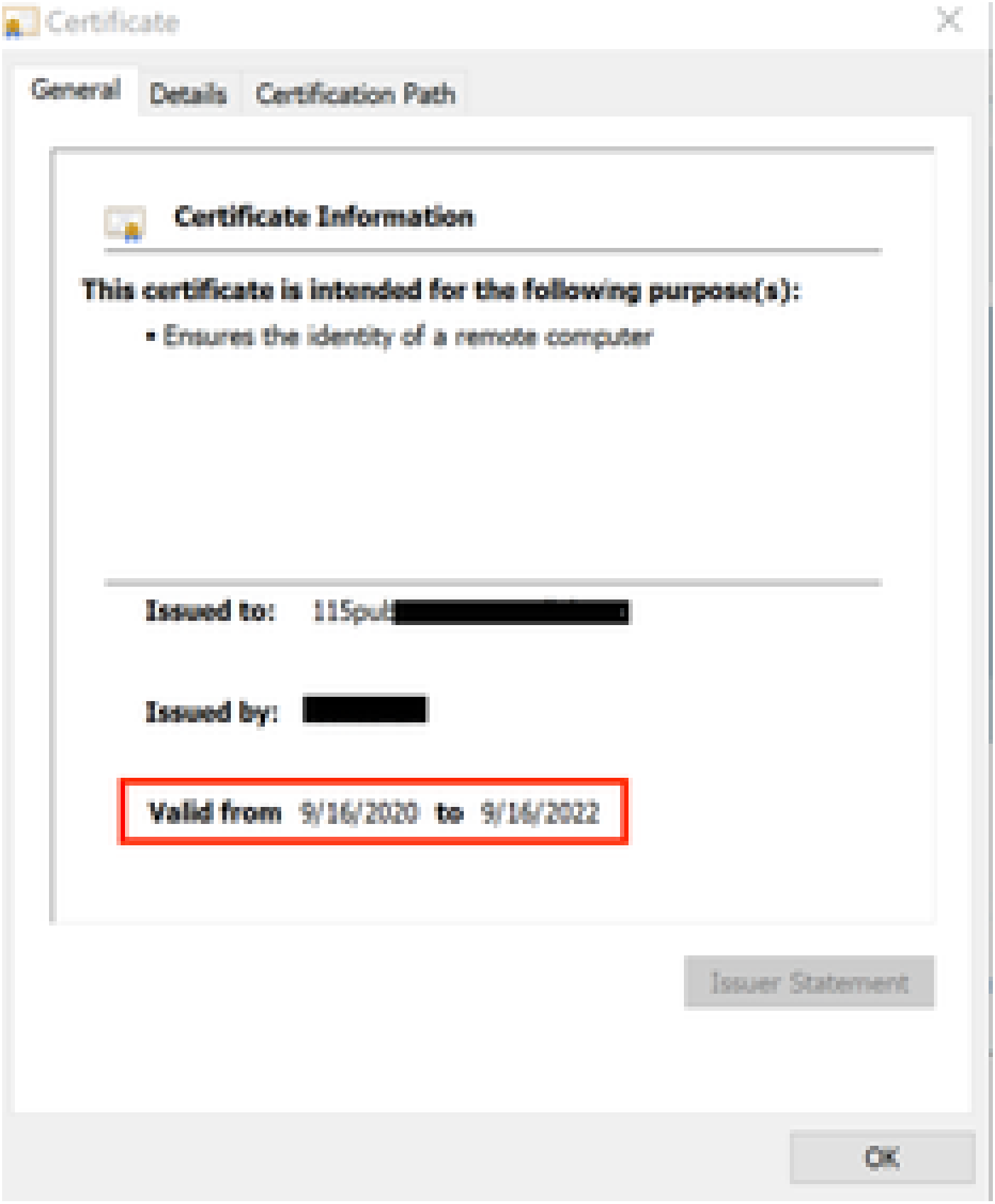
- Certificat CA signé en tant que tomcat. Accédez àCertificate Management > Upload certificate > Certificate Purpose: tomcat. Définissez la description du certificat et parcourez le fichier de certificat signé par l'autorité de certification pour le noeud CUCM actuel.

Remarque : à ce stade, CUCM compare le CSR et le certificat CA signé chargé. Si les informations correspondent, le CSR disparaît et le nouveau certificat signé par l'autorité de certification est téléchargé. Upload Certificate Common Error Messages Si vous recevez un message d'erreur après le téléchargement du certificat, reportez-vous à la section .

Étape 6. Pour que le nouveau certificat soit appliqué au serveur, le service Cisco Tomcat doit être redémarré via l'interface de ligne de commande (en commençant par Publisher, puis les abonnés, un par un), utilisez la commande utils service restart Cisco Tomcat.

Pour valider que le certificat Tomcat est maintenant utilisé par CUCM, accédez à la page Web du noeud et sélectionnez Site Information(Icône de verrouillage) dans le navigateur. Cliquez sur cette certificateoption et vérifiez la date du nouveau certificat.


Cisco Unified CM Console
115pub[redacted]/ccmadmin/showHome.do
Connection is secure
Your information (for example, passwords or credit card numbers) is private when it is sent to this site.
Learn more
Certificate (Valid)
Cookies (1 in use)
Site settings
Copyright © 1999



Certificat CallManager

⚠ Attention : ne régénérez pas les certificats CallManager et TVS en même temps. Cela entraîne une non-correspondance irrécupérable avec l'ITL installé sur les points d'extrémité, ce qui nécessite la suppression de l'ITL de TOUS les points d'extrémité du cluster. Terminez

⚠ le processus complet pour CallManager et, une fois les téléphones réenregistrés, démarrez le processus pour le TVS.

Remarque : pour déterminer si le cluster est en mode mixte, accédez à Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode (0 == Non-Secure ; 1 == Mixed Mode).

Pour tous les noeuds CallManager du cluster :

Étape 1. Naviguez Cisco Unified OS Administration > Security > Certificate Management > Find jusqu'à la date d'expiration du certificat CallManager et vérifiez-la.

Étape 2. Cliquez surGenerate CSR > Certificate Purpose: CallManager. Sélectionnez les paramètres souhaités pour le certificat, puis cliquez surGenerate. Attendez que le message de réussite s'affiche et cliquez surClose.

Étape 3. Téléchargez le CSR. Cliquez sur **Download CSR**. Select **Certificate Purpose: CallManager** and click **Download**.

Étape 4. Envoyez le CSR à l' Certificate Authority .

Étape 5. L'autorité de certification renvoie au moins deux fichiers pour la chaîne de certificats signés. Téléchargez les certificats dans l'ordre suivant :

- Certificat d'autorité de certification racine comme CallManager-trust. Accédez àCertificate Management > Upload certificate > Certificate Purpose: CallManager-trust. Définissez la description du certificat et parcourez le fichier de certificat racine.
- Certificat intermédiaire en tant que CallManager-trust (facultatif). Accédez àCertificate Management > Upload certificate > Certificate Purpose: CallManager-trust. Définissez la description du certificat et parcourez le fichier de certificat intermédiaire.

Remarque : certaines autorités de certification ne fournissent pas de certificat intermédiaire. Si seul le certificat racine a été fourni, cette étape peut être omise.

- Certificat signé par l'autorité de certification comme CallManager. Accédez àCertificate Management > Upload certificate > Certificate Purpose: CallManager. Définissez la description du certificat et parcourez le fichier de certificat signé par l'autorité de certification pour le noeud CUCM actuel.

Remarque : à ce stade, CUCM compare le CSR et le certificat CA signé chargé. Si les informations correspondent, le CSR disparaît et le nouveau certificat signé par l'autorité de certification est téléchargé. Si vous recevez un message d'erreur après le téléchargement du certificat, reportez-vous à la section Messages d'erreur courants du téléchargement du certificat.

Étape 6. Si le cluster est en mode mixte, mettez à jour la CTL avant le redémarrage des services :

Token ou Tokenless. Si le cluster est en mode non sécurisé, ignorez cette étape et redémarrez les services.

Étape 7. Pour que le nouveau certificat soit appliqué au serveur, les services requis doivent être redémarrés (uniquement si le service s'exécute et est actif). Naviguez jusqu'à l'adresse :

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

Étape 8. Réinitialisez tous les téléphones :

- Accédez àCisco Unified CM Administration > System > Enterprise Parameters > Reset. Une fenêtre contextuelle s'affiche avec l'instruction « Vous êtes sur le point de réinitialiser tous les périphériques du système ». Cette action ne peut pas être annulée. Continuer ? sélectionnez OK , puis cliquez sur Reset .

Remarque : surveillez l'enregistrement des périphériques via RTMT. Une fois que tous les téléphones se sont réinscrits, vous pouvez passer au type de certificat suivant.

Certificat IPSec

Attention : une tâche de sauvegarde ou de restauration ne doit pas être active lors de la régénération du certificat IPSec.

Pour tous les noeuds (CallManager et IM&P) du cluster :

Étape 1. Accédez àCisco Unified OS Administration > Security > Certificate Management > Findet vérifiez la date d'expiration du certificat ipsec.

Étape 2. Cliquez sur Generate CSR > Certificate Purpose : ipsec. Sélectionnez les paramètres souhaités pour le certificat, puis cliquez sur Générer. Attendez que le message de réussite s'affiche, puis cliquez sur Fermer.

Étape 3. Téléchargez le CSR. Cliquez sur Download CSR. Sélectionnez Certificate Purpose ipsec et cliquez sur Download.

Étape 4. Envoyez le CSR à l'autorité de certification.

Étape 5. L'autorité de certification renvoie au moins deux fichiers pour la chaîne de certificats signés. Téléchargez les certificats dans l'ordre suivant :

- Certificat d'autorité de certification racine comme ipsec-trust. Accédez à Certificate Management > Upload certificate > Certificate Purpose : ipsec-trust. Définissez la description du certificat et parcourez le fichier de certificat racine.
- Certificat intermédiaire comme ipsec-trust (facultatif). Accédez à Certificate Management >

Upload certificate > Certificate Purpose : tomcat-trust. Définissez la description du certificat et parcourez le fichier de certificat intermédiaire.

Remarque : certaines autorités de certification ne fournissent pas de certificat intermédiaire. Si seul le certificat racine a été fourni, cette étape peut être omise.

- Certificat signé par l'autorité de certification en tant qu'ipsec. Accédez à Certificate Management > Upload certificate > Certificate Purpose : ipsec. Définissez la description du certificat et parcourez le fichier de certificat signé par l'autorité de certification pour le noeud CUCM actuel.

Remarque : à ce stade, CUCM compare le CSR et le certificat CA signé chargé. Si les informations correspondent, le CSR disparaît et le nouveau certificat signé par l'autorité de certification est téléchargé. Si vous recevez un message d'erreur après le téléchargement du certificat, reportez-vous à la section Messages d'erreur communs de téléchargement du certificat< /strong>.

Étape 6. Pour que le nouveau certificat soit appliqué au serveur, les services requis doivent être redémarrés (uniquement si le service s'exécute et est actif). Naviguez jusqu'à l'adresse :

- Cisco Unified Serviceability > Outils > Control Center - Services réseau > Cisco DRF Master(Publisher)
- Cisco Unified Serviceability > Outils > Control Center - Services réseau > Cisco DRF Local (Éditeur et Abonnés)

Certificat CAPF

Remarque : pour déterminer si le cluster est en mode mixte, accédez à Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode (0 == Non-Secure ; 1 == Mixed Mode).

Remarque : le service CAPF s'exécute uniquement dans le serveur de publication et c'est le seul certificat utilisé. Il n'est pas nécessaire d'obtenir les noeuds d'abonné signés par une autorité de certification, car ils ne sont pas utilisés. Si le certificat a expiré dans les Abonnés et que vous souhaitez éviter les alertes de certificats expirés, vous pouvez régénérer les certificats CAPF des abonnés en tant que certificats auto-signés. Pour plus d'informations, consultez Certificat CAPF auto-signé.

Dans l'éditeur :

Étape 1. Accédez à Cisco Unified OS Administration > Security > Certificate Management > Find and verify the expiration date of the CAPF certificate.

Étape 2. Cliquez sur Generate CSR > Certificate Purpose : CAPF. Sélectionnez les paramètres

souhaités pour le certificat, puis cliquez sur Generate. Attendez que le message de réussite s'affiche et cliquez sur Close.

Étape 3. Téléchargez le CSR. Cliquez sur Download CSR. Sélectionnez Certificate Purpose CAPF et cliquez sur Download.

Étape 4. Envoyez le CSR à l'autorité de certification.

Étape 5. L'autorité de certification renvoie au moins deux fichiers pour la chaîne de certificats signés. Téléchargez les certificats dans l'ordre suivant :

- Certificat d'autorité de certification racine comme CAPF-trust. Accédez à Certificate Management > Upload certificate > Certificate Purpose : CAPF-trust. Définissez la description du certificat et parcourez le fichier de certificat racine.
- Certificat intermédiaire en tant que CAPF-trust (facultatif). Accédez à Certificate Management > Upload certificate > Certificate Purpose : CAPF-trust. Définissez la description du certificat et parcourez le fichier de certificat intermédiaire.

Remarque : certaines autorités de certification ne fournissent pas de certificat intermédiaire. Si seul le certificat racine a été fourni, cette étape peut être omise.

- Certificat CA signé en tant que CAPF. Accédez à Certificate Management > Upload certificate > Certificate Purpose : CAPF. Définissez la description du certificat et parcourez le fichier de certificat signé par l'autorité de certification pour le noeud CUCM actuel.

Remarque : à ce stade, CUCM compare le CSR et le certificat CA signé chargé. Si les informations correspondent, le CSR disparaît et le nouveau certificat signé par l'autorité de certification est téléchargé. Si vous recevez un message d'erreur après le téléchargement du certificat, reportez-vous à la section Messages d'erreur communs de téléchargement du certificat.

Étape 6. Si le cluster est en mode mixte, mettez à jour la CTL avant le redémarrage des services : Token ou Tokenless. Si le cluster est en mode non sécurisé, ignorez cette étape et redémarrez le service.

Étape 7. Pour que le nouveau certificat soit appliqué au serveur, les services requis doivent être redémarrés (uniquement si le service s'exécute et est actif). Naviguez jusqu'à l'adresse :

- Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco Trust Verification Service (Tous les noeuds où le service s'exécute.)
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco TFTP (Tous les noeuds où le service s'exécute.)
- Cisco Unified Serviceability > Outils > Control Center - Services de fonctionnalités > Fonction Cisco Certificate Authority Proxy (Publisher)

Étape 8. Réinitialisez tous les téléphones :

- Accédez à Cisco Unified CM Administration > System > Enterprise Parameters > Reset. Une fenêtre contextuelle s'affiche avec l'instruction « Vous êtes sur le point de réinitialiser tous les périphériques du système ». Cette action ne peut pas être annulée. Continuer ? sélectionnez OK, puis cliquez sur Réinitialiser.

Remarque : surveillez l'enregistrement des périphériques via RTMT. Une fois que tous les téléphones se sont réinscrits, vous pouvez passer au type de certificat suivant.

Certificat TVS

Attention : ne régénérez pas les certificats CallManager et TVS en même temps. Cela entraîne une non-correspondance irrécupérable avec l'ITL installé sur les points d'extrémité, ce qui nécessite la suppression de l'ITL de TOUS les points d'extrémité du cluster. Terminez le processus complet pour CallManager et, une fois les téléphones réenregistrés, démarrez le processus pour le TVS.

Pour tous les noeuds TVS du cluster :

Étape 1. Accédez à Cisco Unified OS Administration > Security > Certificate Management > Find et vérifiez la date d'expiration du certificat TVS.

Étape 2. Cliquez sur Generate CSR > Certificate Purpose : TVS. Sélectionnez les paramètres souhaités pour le certificat, puis cliquez sur Generate. Attendez que le message de réussite s'affiche et cliquez sur Close.

Étape 3. Téléchargez le CSR. Cliquez sur Download CSR. Sélectionnez Certificate Purpose TVS et cliquez sur Download.

Étape 4. Envoyez le CSR à l'autorité de certification.

Étape 5. L'autorité de certification renvoie au moins deux fichiers pour la chaîne de certificats signés. Téléchargez les certificats dans l'ordre suivant :

- Certificat d'autorité de certification racine comme TVS-trust. Accédez à Certificate Management > Upload certificate > Certificate Purpose : TVS-trust. Définissez la description du certificat et parcourez le fichier de certificat racine.
- Certificat intermédiaire de confiance TVS (facultatif). Accédez à Certificate Management > Upload certificate > Certificate Purpose : TVS-trust. Définissez la description du certificat et parcourez le fichier de certificat intermédiaire.

Remarque : certaines autorités de certification ne fournissent pas de certificat intermédiaire. Si seul le certificat racine a été fourni, cette étape peut être omise.

- Certificat CA signé comme TVS. Accédez à Certificate Management > Upload certificate > Certificate Purpose : TVS. Définissez la description du certificat et parcourez le fichier de

certificat signé par l'autorité de certification pour le noeud CUCM actuel.

Remarque : à ce stade, CUCM compare le CSR et le certificat CA signé chargé. Si les informations correspondent, le CSR disparaît et le nouveau certificat signé par l'autorité de certification est téléchargé. Si vous recevez un message d'erreur après le téléchargement du certificat, reportez-vous à la section Messages d'erreur courants du téléchargement du certificat.

Étape 6. Pour que le nouveau certificat soit appliqué au serveur, les services requis doivent être redémarrés (uniquement si le service s'exécute et est actif). Naviguez jusqu'à l'adresse :

- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco TFTP (Tous les noeuds où le service s'exécute.)
- Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco Trust Verification Service (Tous les noeuds où le service s'exécute.)

Étape 7. Réinitialisez tous les téléphones :

- Accédez à Cisco Unified CM Administration > System > Enterprise Parameters > Reset. Une fenêtre contextuelle s'affiche avec l'instruction « Vous êtes sur le point de réinitialiser tous les périphériques du système ». Cette action ne peut pas être annulée. Continuer ? sélectionnez OK, puis cliquez sur Réinitialiser.

Remarque : surveillez l'enregistrement des périphériques via RTMT. Une fois que tous les téléphones se sont réinscrits, vous pouvez passer au type de certificat suivant.

Dépanner les messages d'erreur de certificat téléchargés courants

Cette section répertorie certains des messages d'erreur les plus courants lors du téléchargement d'un certificat signé par une autorité de certification.

Le certificat CA n'est pas disponible dans le Trust-Store

Cette erreur signifie que le certificat racine ou intermédiaire n'a pas été téléchargé sur le CUCM. Vérifiez que ces deux certificats ont été téléchargés en tant que trust-store avant le téléchargement du certificat de service.

Le fichier /usr/local/platform/.security/tomcat/keys/tomcat.csr n'existe pas

Cette erreur apparaît lorsqu'il n'existe pas de CSR pour le certificat (tomcat, callmanager, ipsec, capf, tvs). Vérifiez que le CSR a été créé avant et que le certificat a été créé en fonction de ce CSR. Points importants à garder à l'esprit :

- Un seul CSR par serveur et type de certificat peut exister. Cela signifie que si une nouvelle

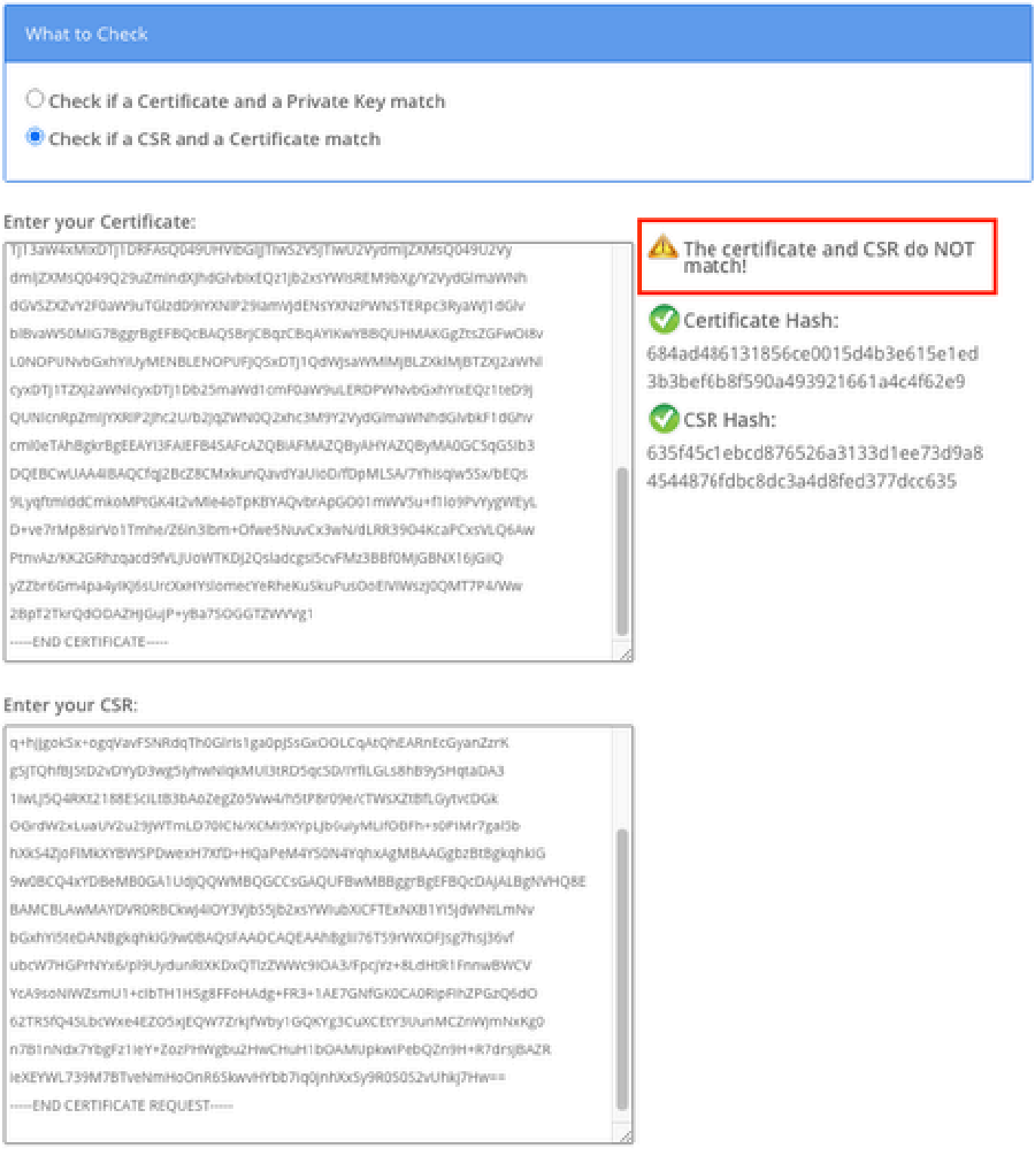
RSE est créée, l'ancienne est remplacée.
- CUCM ne prend pas en charge les certificats génériques.
- Il n'est pas possible de remplacer un certificat de service actuellement en place sans un nouveau CSR.
- Une autre erreur possible pour le même problème est « Le fichier /usr/local/platform/upload/certs//tomcat.der n'a pas pu être chargé. » Cela dépend de la version de CUCM.

Clé publique CSR et clé publique de certificat ne correspondent pas

Cette erreur apparaît lorsque le certificat fourni par l'autorité de certification a une clé publique différente de celle envoyée dans le fichier CSR. Les raisons possibles sont :

- Le certificat incorrect (provenant peut-être d'un autre noeud) est chargé.
- Le certificat CA a été généré avec un CSR différent.
- Le CSR a été régénéré et a remplacé l'ancien CSR utilisé pour obtenir le certificat signé.

Pour vérifier la correspondance entre le CSR et la clé publique de certificat, plusieurs outils sont disponibles en ligne, tels que SSL.



Une autre erreur possible pour le même problème est « Le fichier /usr/local/platform/upload/certs//tomcat.der n'a pas pu être chargé. » Cela dépend de la version de CUCM.

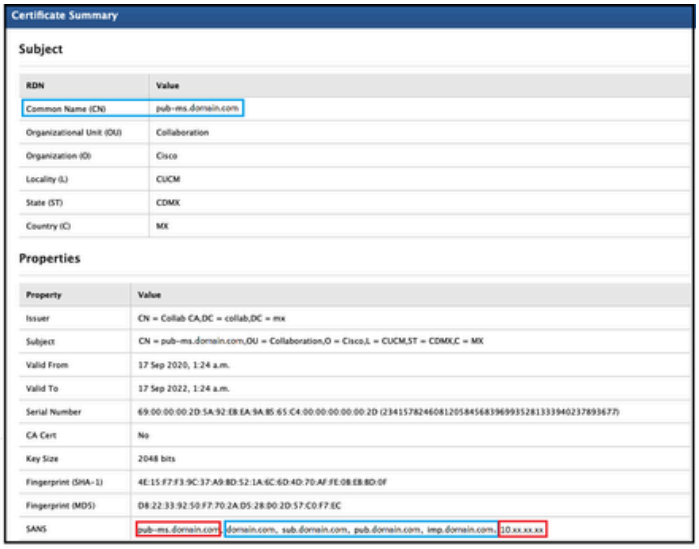
Le nom alternatif de l'objet CSR (SAN) et le certificat SAN ne correspondent pas

Les SAN entre le CSR et le certificat doivent être identiques. Cela empêche la certification pour les domaines qui ne sont pas autorisés. Pour vérifier la non-concordance du SAN, procédez comme suit :

1. Décoder le CSR et le certificat (base 64). Différents décodeurs sont disponibles en ligne, tels que le Decoder.

2. Comparez les entrées SAN et vérifiez qu'elles correspondent toutes. L'ordre n'est pas important, mais toutes les entrées du CSR doivent être identiques dans le certificat.

Par exemple, le certificat signé par une autorité de certification comporte deux entrées SAN supplémentaires, le nom commun du certificat et une adresse IP supplémentaire.

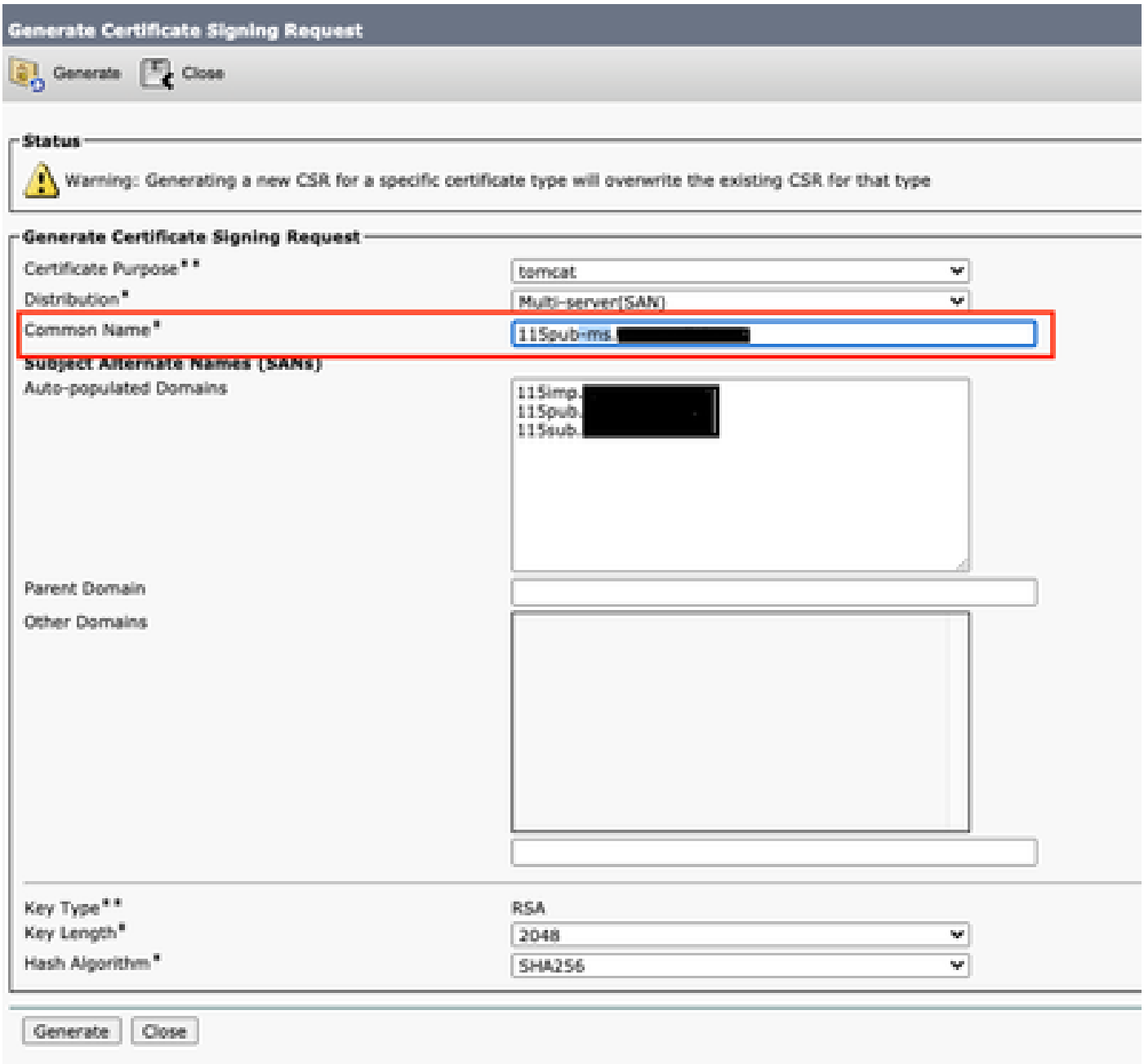


3. Une fois que vous avez identifié que le réseau SAN ne correspond pas, vous avez deux options pour résoudre ce problème :

1. Demandez à votre administrateur CA d'émettre un certificat avec les mêmes entrées SAN que celles envoyées dans le CSR.
2. Créez un CSR dans CUCM qui correspond aux exigences de l'autorité de certification.

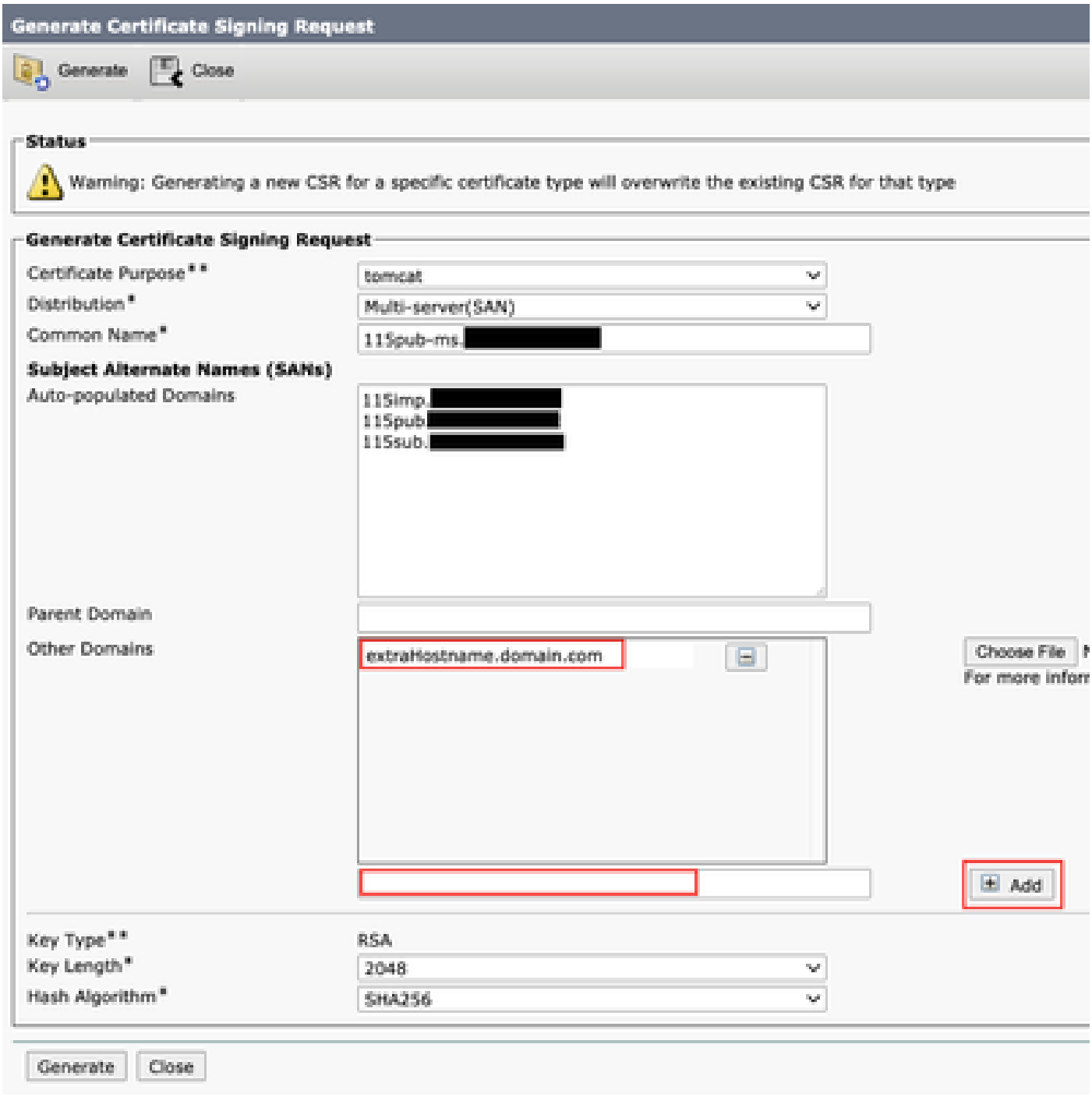
Pour modifier le CSR créé par CUCM :

1. Si l'autorité de certification supprime le domaine, un CSR dans CUCM peut être créé sans le domaine. Lors de la création de CSR, supprimez le domaine qui est renseigné par défaut.
2. Si un certificat Multi-SAN est créé, il y a des CA qui n'acceptent pas les -ms dans le nom commun. L'option -ms peut être supprimée de la CSR lors de sa création.



3. Pour ajouter un autre nom en plus de ceux remplis automatiquement par CUCM :

    1. Si le certificat Multi-SAN est utilisé, d'autres noms de domaine complets peuvent être ajoutés. (Les adresses IP ne sont pas acceptées.)



set web-securityb. Si le certificat est un noeud unique, utilisez la commande . Cette commande s'applique même aux certificats multi-SAN. (Tout type de domaine peut être ajouté, les adresses IP sont également autorisées.)

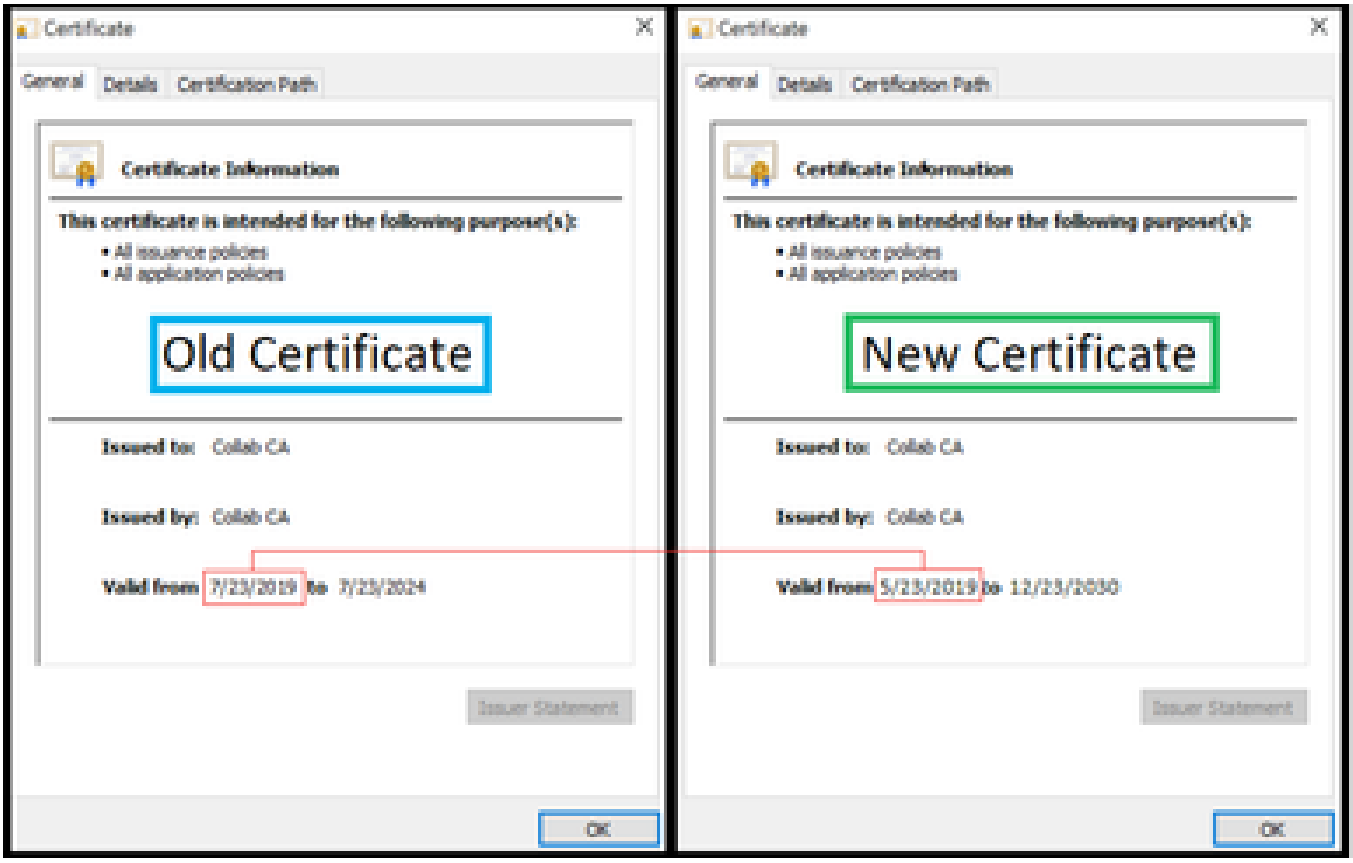
Pour plus d'informations, consultez le Guide de référence de la ligne de commande.

Les certificats de confiance avec le même CN ne sont pas remplacés

CUCM a été conçu pour stocker un seul certificat avec le même nom commun et le même type de certificat. Cela signifie que si un certificat tomcat-trust existe déjà dans la base de données et doit être remplacé par un certificat récent avec le même CN, CUCM supprime l'ancien certificat et le remplace par le nouveau.

Dans certains cas, CUCM ne remplace pas l'ancien certificat :

1. Le certificat téléchargé a expiré : CUCM ne vous permet pas de télécharger un certificat expiré.
2. L'ancien certificat a une date FROM plus récente que le nouveau certificat. CUCM conserve le certificat le plus récent, et la date FROM plus ancienne est cataloguée comme plus ancienne. Pour ce scénario, il est nécessaire de supprimer le certificat indésirable, puis de télécharger le nouveau.



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.