

Exemple de configuration de génération et d'importation de LSC signés par une autorité de certification tierce CUCM

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Télécharger le certificat CA racine](#)

[Définir l'autorité de certification hors connexion pour le certificat sur Terminaux](#)

[Générer une demande de signature de certificat \(CSR\) pour les téléphones](#)

[Obtenir le CSR généré du CUCM au serveur FTP \(ou TFTP\)](#)

[Obtenir le certificat du téléphone](#)

[Convertir .cer au format .der](#)

[Compressez les certificats \(.der\) au format .tgz](#)

[Transférez le fichier .tgz vers le serveur SFTP](#)

[Importer le fichier .tgz sur le serveur CUCM](#)

[Signature du CSR avec l'autorité de certification Microsoft Windows 2003](#)

[Obtenir le certificat racine de l'autorité de certification](#)

[Vérifier](#)

[Dépannage](#)

Introduction

Les certificats LSC (Locally Significant Certificates) CAPF (Certificate Authority Proxy Function) sont signés localement. Cependant, vous pouvez exiger que les téléphones utilisent des LSC signés par une autorité de certification tierce. Ce document décrit une procédure qui vous aide à atteindre cet objectif.

Conditions préalables

Exigences

Cisco vous recommande de connaître Cisco Unified Communication Manager (CUCM).

Composants utilisés

Les informations contenues dans ce document sont basées sur CUCM version 10.5(2) ;

cependant, cette fonctionnalité fonctionne à partir de la version 10.0 et ultérieure.

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. If your network is live, make sure that you understand the potential impact of any command.

Configurer

Voici les étapes impliquées dans cette procédure, chacune d'entre elles étant détaillée dans sa propre section :

1. [Télécharger le certificat CA racine](#)
2. [Définir l'autorité de certification hors connexion pour le certificat sur Terminaux](#)
3. [Générer une demande de signature de certificat \(CSR\) pour les téléphones](#)
4. [Obtenez le CSR généré de Cisco Unified Communications Manager \(CUCM\) vers le serveur FTP](#)
5. [Obtenir le certificat de téléphone de CA](#)
6. [Convertir .cer au format .der](#)
7. [Compressez les certificats \(.der\) au format .tgz](#)
8. [Transférez le fichier .tgz vers le serveur FTP Secure Shell \(SFTP\)](#)
9. [Importer le fichier .tgz sur le serveur CUCM](#)
10. [Signature du CSR avec l'autorité de certification Microsoft Windows 2003](#)
11. [Obtenir le certificat racine de l'autorité de certification](#)

Télécharger le certificat CA racine

1. Connectez-vous à l'interface utilisateur graphique Web d'administration du système d'exploitation Cisco Unified.
2. Accédez à Gestion des certificats de sécurité.
3. Cliquez sur Upload Certificate/Certificate chain.
4. Choisissez CallManager-trust sous Certificate Purpose.
5. Accédez au certificat racine de l'autorité de certification et cliquez sur Upload.

Définir l'autorité de certification hors connexion pour le certificat sur Terminaux

1. Connectez-vous à l'interface utilisateur graphique Web Administration CUCM.
2. Accédez à System > Service Parameter.
3. Choisissez le serveur CUCM et sélectionnez Cisco Certificate Authority Proxy Function pour le service.

4. Sélectionnez Autorité de certification hors connexion pour l'émission du certificat au terminal.

Générer une demande de signature de certificat (CSR) pour les téléphones

1. Connectez-vous à l'interface utilisateur graphique Web Administration CUCM.
2. Accédez à Device Phones.
3. Sélectionnez le téléphone dont le LSC doit être signé par l'autorité de certification externe.
4. Remplacez le profil de sécurité du périphérique par un profil sécurisé (s'il n'est pas présent, ajoutez un système dans le profil Sécurité du téléphone).
5. Sur la page de configuration du téléphone, sous la section CAPF, choisissez Install/Upgrade for the Certification Operation. Effectuez cette étape pour tous les téléphones dont le LSC doit être signé par l'autorité de certification externe. Vous devriez voir Opération en attente pour l'état de l'opération de certificat.

Profil de sécurité du téléphone (modèle 7962).

Entrez la commande `utils capf csr count` dans la session Secure Shell (SSH) afin de confirmer si un CSR est généré. (Cette capture d'écran montre qu'un CSR a été généré pour trois téléphones.)



Remarque : l'état de l'opération de certificat sous la section CAPF du téléphone reste à l'état Opération en attente.

Obtenir le CSR généré du CUCM au serveur FTP (ou TFTP)

1. Envoyez SSH au serveur CUCM.
2. Exécutez la commande `utils capf csr dump`. Cette capture d'écran montre le vidage en cours de transfert vers le FTP.

3. Ouvrez le fichier de vidage avec WinRAR et extrayez le CSR sur votre ordinateur local.

Obtenir le certificat du téléphone

1. Envoyez les CSR du téléphone à l'autorité de certification.
2. L'autorité de certification vous fournit un certificat signé.



Remarque : vous pouvez utiliser un serveur Microsoft Windows 2003 comme autorité de certification. La procédure de signature du CSR avec une autorité de certification Microsoft Windows 2003 est expliquée plus loin dans ce document.

Convertir .cer au format .der

Si les certificats reçus sont au format .cer, renommez-les en .der.

Compressez les certificats (.der) au format .tgz

Vous pouvez utiliser la racine du serveur CUCM (Linux) afin de compresser le format du certificat. Vous pouvez également le faire dans un système Linux normal.

1. Transférez tous les certificats signés vers le système Linux avec le serveur SFTP.
2. Entrez cette commande afin de compresser tous les certificats .der dans un fichier .tgz.

```
<#root>
```

```
tar -zcvf
```

```
.tgz *.der
```

Transférez le fichier .tgz vers le serveur SFTP

Suivez les étapes indiquées dans la capture d'écran afin de transférer le fichier .tgz vers le serveur SFTP.

Importer le fichier .tgz sur le serveur CUCM

1. Envoyez SSH au serveur CUCM.
2. Exécutez la commande `utils capf cert import`.

Une fois les certificats importés avec succès, vous pouvez voir le nombre de CSR devenir zéro.

Signature du CSR avec l'autorité de certification Microsoft Windows 2003

Il s'agit d'informations facultatives pour Microsoft Windows 2003 - CA.

1. Autorité de certification ouverte.
2. Cliquez avec le bouton droit sur l'autorité de certification et accédez à Toutes les tâches > Soumettre une nouvelle demande...
3. Sélectionnez le CSR et cliquez sur Open. Faites-le pour tous les CSR.

Tous les CSR ouverts s'affichent dans le dossier Demandes en attente.

4. Cliquez avec le bouton droit sur chaque tâche et accédez à Toutes les tâches > Émettre afin d'émettre des certificats. Effectuez cette opération pour toutes les demandes en attente.

5. Afin de télécharger le certificat, choisissez Issued Certificate.
6. Cliquez avec le bouton droit sur le certificat et cliquez sur Ouvrir.
7. Vous pouvez voir les détails du certificat. Afin de télécharger le certificat, sélectionnez l'onglet Détails et choisissez Copier dans le fichier...
8. Dans l'Assistant Exportation de certificat, choisissez DER encoded binary X.509 (.CER).
9. Attribuez un nom approprié au fichier. Cet exemple utilise le format <MAC>.cer.
10. Obtenez les certificats des autres téléphones sous la section Issued Certificate avec cette procédure.

Obtenir le certificat racine de l'autorité de certification

1. Ouvrez Autorité de certification.
2. Suivez les étapes indiquées dans cette capture d'écran afin de télécharger l'autorité de certification racine.


Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

1. Accédez à la page de configuration du téléphone.
2. Dans la section CAPF, l'état de l'opération de certificat doit s'afficher comme réussite de la mise à niveau.



Remarque : reportez-vous à [Générer et importer des LSC signés par une autorité de](#)

 [certification tierce](#) pour plus d'informations.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

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.