Exemple de configuration de génération Ca-signé par tierce partie et d'importation CUCM LSC

Contenu

Introduction

Fonction de proxy d'autorité de certification (CAPF) localement - les Certificats significatifs (LSC) local-sont signés. Cependant, vous pourriez exiger des téléphones pour utiliser le tiers Autorité de certification (CA) - des LSC signés. Ce document décrit une procédure qui vous aide à réaliser ceci.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance du gestionnaire de Cisco Unified Communications (CUCM).

Composants utilisés

Les informations dans ce document sont basées sur la version 10.5(2) CUCM ; cependant, cette caractéristique fonctionne de la version 10.0 et ultérieures.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Voici les étapes impliquées dans cette procédure, qui est détaillée dans sa propre section :

1. Téléchargez le certificat de Ca-racine
2. Placez le CA hors ligne pour la question de certificat au point final
3. Générez une demande de signature de certificat (CSR) des téléphones
4. Obtenez le CSR généré de Cisco Unified Communications Manager (CUCM) au ftp server
5. Obtenez le certificat de téléphone du CA
6. Conversion .cer au format .der
7. Compressez les Certificats (.der) au format .tgz
8. Virez le fichier .tgz sur le serveur sécurisé de FTP de shell (SFTP)
9. Importez le fichier .tgz au serveur CUCM
10. Signez le CSR avec l'autorité de certification de Microsoft Windows 2003
11. Obtenez le certificat racine du CA

Téléchargez le certificat de Ca-racine

1. Connectez-vous dans le GUI du système d'exploitation de Web de gestion de Cisco Unified (SYSTÈME D'EXPLOITATION).

2. Naviguez vers la **Gestion de Security Certificate**.

3. Cliquez sur Upload la **chaîne de certificat/certificat**.

4. Choisissez la CallManager-**confiance** sous le but de certificat.

5. Parcourez au certificat racine du Ca et cliquez sur Upload.

Placez le CA hors ligne pour la question de certificat au point final

1. Connectez-vous dans le GUI de Web de gestion CUCM.

2. Naviguez vers le **système > le paramètre de service**.

3. Choisissez le serveur CUCM et sélectionnez la **fonction de proxy d'autorité de certification de**

Cisco pour le service.

4. **CA hors ligne** choisi pour la question de certificat au point final.

Générez une demande de signature de certificat (CSR) des téléphones

1. Connectez-vous dans le GUI de Web de gestion CUCM.
2. Naviguez vers des **téléphones de périphérique**.
3. Choisissez le téléphone dont le LSC doit être signé par le CA externe.
4. Changez le profil de sécurité des périphériques à sécurisé (sinon le présent, ajoutent un système sur le profil de degré de sécurité de téléphone de Sécurité).
5. Àla page de configuration de téléphone, sous la section CAPF, choisissez **installent/mises à jour** pour l'exécution de certification. Terminez-vous cette étape pour tous les téléphones dont le LSC doit être signé par le CA externe. Vous devriez voir l'**exécution en suspens** pour l'état d'exécution de certificat.

   Profil de degré de sécurité de téléphone (modèle 7962).

   Sélectionnez la commande de **compte csr de capf d'utils** en session de Protocole Secure Shell (SSH) afin de confirmer si un CSR est généré. (Cette copie d'écran prouve qu'un CSR a été généré pour trois téléphones.)

   Remarque: L'état d'exécution de certificat sous la section CAPF du téléphone demeure dans l'**état Pending d'exécution**.

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

1. SSH dans le serveur CUCM.
2. Exécutez la commande de **vidage mémoire csr de capf d'utils**. Cette copie d'écran affiche le vidage mémoire étant transféré vers le FTP.
3. Ouvrez le fichier de vidage mémoire avec WinRAR et extrayez le CSR à votre ordinateur local.

Obtenez le certificat de téléphone

1. Envoyez CSRs du téléphone au CA.

2. Le CA te fournit un certificat signé.

   Remarque: Vous pouvez utiliser un serveur de Microsoft Windows 2003 comme CA. La procédure pour signer le CSR avec un Microsft Windows 2003 CA est expliquée plus tard dans ce document.

Conversion .cer au format .der

Si les Certificats reçus sont dans le format de .cer, alors renommez-les à .der.

Compressez les Certificats (.der) au format .tgz

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

1. Transférez tous les Certificats signés vers le système Linux avec le serveur de SFTP.

2. Sélectionnez cette commande afin de compresser tous les Certificats .der dans un fichier .tgz.

   ```
   tar -zcvf <file_name>.tgz    *.der
   ```

Virez le fichier .tgz sur le serveur de SFTP

Terminez-vous les étapes affichées dans la copie d'écran afin de virer le fichier .tgz sur le serveur de SFTP.

Importez le fichier .tgz au serveur CUCM

1. SSH dans le serveur CUCM.

2. Exécutez la commande d'**importation de CERT de capf d'utils**.

   Une fois que les Certificats sont importés avec succès, puis vous pouvez voir que le CSR compter deviennent zéro.

Signez le CSR avec l'autorité de certification de Microsoft Windows 2003

C'est les informations facultatives pour le Microsoft Windows 2003 - CA.

1. Ouvrez l'autorité de certification.

2. Cliquez avec le bouton droit le CA et naviguez vers **toutes les tâches > soumettent la nouvelle demande…**

3. Sélectionnez le CSR et cliquez sur **ouvert**. Faites ceci pour tout le CSRs.

   Tout les affichage ouvert CSR dans le répertoire en attente de demandes.

4. Cliquez avec le bouton droit chacun et naviguez vers **toutes les tâches > question** afin de délivrer des Certificats. Faites ceci pour toutes les demandes en suspens.

5. Afin de télécharger le certificat, choisissez le **certificat délivré**.

6. Cliquez avec le bouton droit le certificat et cliquez sur **ouvert**.

7. Vous pouvez voir les détails de certificat. Afin de télécharger le certificat, sélectionner les détails tabulent et choisissent la **copie pour classer…**

8. Dans l'assistant d'exportation de certificat, choisissez **DER la binaire encodée X.509 (.CER)**.

9. Nommez le fichier quelque chose appropriée. Cet exemple utilise le format <MAC>.cer.

10. Obtenez les Certificats pour d'autres téléphones sous la section émise de certificat avec cette procédure.

Obtenez le certificat racine du CA

1. Ouvrez l'**autorité de certification**.

2. Terminez-vous les étapes affichées dans cette copie d'écran afin de télécharger le racine-CA.

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

1. Allez à la page de configuration de téléphone.

2. Sous la section CAPF, l'état d'exécution de certificat devrait afficher comme **succès de mise à jour**.

   Remarque: Référez-vous génèrent et importent le pour en savoir plus LSC Ca-signé par tiers.

Dépannez

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