Processus de régénération/renouvellement du certificat CUCM

Contenu

Introduction

Ce document décrit comment régénérer les certificats utilisés dans Cisco Unified Communications Manager (CUCM) version 8.x et ultérieure. La liste d'approbation d'identité (ITL) activée par la fonction de sécurité par défaut (SBD) et la liste d'approbation de certificat (CTL) pour les environnements en mode mixte sont également couvertes dans ce document afin d'éviter toute interruption indésirable. Par exemple, comment éviter les problèmes d'enregistrement des téléphones ou les téléphones qui n'acceptent pas les modifications de configuration ou de micrologiciel.

> **Attention** : Il est toujours recommandé de terminer la régénération du certificat durant une période de maintenance.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- CallManager
- CAPF (Certificate Authority Proxy Function)
- IPsec
- Tomcat
- TVS (Trust Verification Service)
- ITLRecovery (seulement pour CUCM 10.X et versions ultérieures)
- phone-vpn-trust
- phone-sast-trust
- phone-trust
- phone-ctl-trust
- LSC (Locally Significant Certificates)
- MIC (Manufacturer Installed Certificates)

Components Used

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- CUCM version 9.1(2)SU2a,
- CUCM version 8.x 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Quand régénérer les certificats ?

La plupart des certificats utilisés dans CUCM après une nouvelle installation sont des certificats autosignés émis, par défaut, pour cinq ans. Notez que l'intervalle de cinq ans ne peut pas être modifié pour être plus court sur CUCM. Toutefois, une autorité de certification (AC) peut délivrer des certificats pour presque n’importe quel intervalle de temps.

Les certificats de CUCM sont classés en deux rôles :

- Certificats de service : Il est possible de les régénérer et ne sont PAS étiquetés avec le mot -trust. Chaque noeud possède ses propres certificats de service, ce qui signifie que chaque pub et chaque sous-groupe possède un certificat CallManager, Tomcat, IPsec, TVS et CAPF.

- Certificats de confiance : Il n'est PAS possible de les régénérer et sont étiquetés avec le mot -trust. Ces certificats peuvent être des copies de certificats de service, de certificats installés par défaut ou de certificats d'autres serveurs.

Il existe également des certificats de confiance (tels que CAPF-trust et CallManager-trust) qui sont préchargés et ont une période de validité plus longue. Par exemple, le certificat CA de fabrication Cisco est fourni sur les magasins d'approbation CUCM pour des fonctionnalités spécifiques et

n'expire pas avant 2029.

Les certificats doivent être régénérés avant leur expiration. Lorsque les certificats sont sur le point d'expirer, vous recevez des avertissements dans RTMT (Visionneuse Syslog) et un e-mail avec la notification est envoyé si configuré.

Un exemple de notification d'expiration de certificat qui détaille le certificat **CUCM01.der** expire le **lundi 19 mai 14:46** sur le serveur CUCM02 sur le magasin de confiance **tomcat-trust** est montré ici :

```
At Fri Sep 05 02:00:56 CEST 2014 on node 192.168.1.2, the following
SyslogSeverityMatchFound events generated:

SeverityMatch : Critical

MatchedEvent : Sep 5 02:00:06 CUCM02 local7 2 : 864: CUCM02.localdomain:
Sep 05 2014 00:00:06.433 UTC : %UC_CERT-2-CertValidfor7days:
%[Message=Certificate expiration Notification. Certificate name:CUCM01.der
Unit:tomcat-trust Type:own-cert Expiration:Mon May 19 14:46:]
[AppID=Cisco Certificate Monitor][ClusterID=][NodeID=CUCM02]:
Alarm to indicate that Certificate has Expired or Expires in less than seven days

AppID : Cisco Syslog Agent

ClusterID :

NodeID : CUCM02

TimeStamp : Fri Sep 05 02:00:16 CEST 2014
```

Gardez à l'esprit que les certificats expirés peuvent avoir un impact sur votre fonctionnalité CUCM, selon la configuration de la grappe. Les aspects à considérer sont abordés dans les sections suivantes.

Impact du service par le magasin de certificats

Il est essentiel pour la bonne fonctionnalité du système que tous les certificats soient mis à jour dans la grappe CUCM. Si vos certificats sont expirés ou invalides, ils peuvent affecter de manière significative le fonctionnement normal du système. Une liste des problèmes potentiels que vous pourriez rencontrer lorsque l'un des certificats spécifiques n'est pas valide ou a expiré est affichée ici. La différence d'impact peut dépendre de la configuration de votre système.

CallManager.pem

- TFTP n'est pas fiable (les téléphones n'acceptent pas les fichiers de configuration signés ou les fichiers ITL).
- Les services téléphoniques pourraient être touchés.
- Les liaisons SIP (Secure Session Initiation Protocol) ou les ressources multimédias (ponts de conférence, point de terminaison de support (MTP), codeurs Xcoders, etc.) ne s'enregistrent pas ou ne fonctionnent pas.
- La requête AXL échoue.

Tomcat.pem

- Les téléphones ne peuvent pas accéder aux services HTTP hébergés sur le nœud CUCM,

tels que l’annuaire d’entreprise.
- Problèmes liés à l’interface graphique Web du CUCM, comme l’impossibilité d’accéder aux pages de service à partir d’autres nœuds de la grappe.
- Problèmes avec Extension Mobility ou Extension Mobility Cross Cluster.
- Si UCCX (Unified Contact Center Express) est intégré, en raison d'un changement de sécurité par rapport à CCX 12.5, il est nécessaire de télécharger le certificat Tomcat CUCM (autosigné) ou le certificat racine et intermédiaire Tomcat (pour CA signé) dans le magasin UCCX tomcat-trust car il affecte les connexions de bureau Finesse

CAPF.pem

- Les téléphones ne s’authentifient pas pour les services « Phone VPN », « 802.1x » ou « Phone Proxy ».
- Échec de livraison de certificats LSC pour les téléphones.
- Les fichiers de configuration cryptés ne fonctionnent pas.

IPSec.pem

- Le système ou cadre de reprise après sinistre (DRS ou DRF) ne fonctionne pas correctement.
- Les tunnels IPsec vers d’autres grappes CUCM ne fonctionnent pas.

Service de vérification de la confiance (TVS)

Le téléphone ne peut pas authentifier le service HTTPS. Le téléphone ne peut pas authentifier les fichiers de configuration (cela peut toucher presque tout sur CUCM).

phone-vpn-trust

Le VPN du téléphone ne fonctionne pas, car l'URL HTTPS du VPN ne peut pas être authentifiée.

> **Note**: Si cela n’existe pas, ne vous inquiétez pas; ceci n’est valable que pour des configurations particulières.

phone-sast-trust

Les CTL/eTokens précédents ne peuvent pas mettre à jour ou modifier CTL.

> **Note**: Si cela n’existe pas, ne vous inquiétez pas; ceci n’est valable que pour des configurations particulières.

phone-trust and phone-ctl-trust

La messagerie vocale visuelle avec Unity ou Unity Connection ne fonctionne pas.

> **Note**: Si cela n’existe pas, ne vous inquiétez pas; ceci n’est valable que pour des configurations particulières.

LSC et MIC

Les téléphones ne s'enregistrent pas, le téléphone ne s'authentifie pas sur Phone VPN, Phone Proxy ou 802.1x.

Note: Par défaut, les MIC sont sur la plupart des modèles de téléphone. Les LSC sont signés par le CAPF et durent cinq ans par défaut. Les logiciels clients tels que CIPC (Cisco IP Communicator) et Jabber n'ont pas de MIC installé.

Créer une sauvegarde DRS

Il est recommandé de créer une sauvegarde DRS avant d'effectuer des modifications majeures comme celle-ci. Le fichier de sauvegarde DRF CUCM sauvegarde tous les certificats du cluster. Toutes les procédures de sauvegarde/restauration DRS se trouvent dans le *Guide d'administration du système de reprise après sinistre de* Cisco *pour Cisco Unified Communications Manager.*

Attention : Gardez à l'esprit l'ID de bogue Cisco CSCtn50405, CUCM DRF Backup ne sauvegarde pas les certificats.

Déterminer le mode mixte

Pour déterminer si vous utilisez une grappe CTL/sécurisée/mode mixte, choisissez **Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode (0 === Non-Secure ; 1 == Mixed Mode)**.

Si la grappe est en mode mixte

Si vous exécutez une grappe CUCM en mode mixte, cela signifie que le fichier CTL doit être mis à jour après tous les changements de certificat. La procédure à suivre se trouve dans le Guide de sécurité de Cisco. Cependant, assurez-vous que vous disposez d'au moins un eToken à partir du lancement initial de la fonction Mixed-Mode et que le mot de passe eToken est connu.

Note: Une mise à jour de la CTL n'est pas automatique (comme dans le cas du fichier ITL). Il doit être complété manuellement par l'administrateur avec la commande CTL Client ou par l'interface de ligne de commande.

Dans CUCM 10.X et les versions ultérieures, vous pouvez mettre la grappe en mode mixte de deux façons :

- Interface de ligne de commande – si cette méthode est utilisée, votre fichier CTL est signé avec le certificat CallManager.pem du serveur Publisher.

```
admin:show ctl
The checksum value of the CTL file:
0c05655de63fe2a042cf252d96c6d609(MD5)
8c92d1a569f7263cf4485812366e66e3b503a2f5(SHA1)

Length of CTL file: 4947
The CTL File was last modified on Fri Mar 06 19:45:13 CET 2015

[...]

CTL Record #:1
----
BYTEPOS TAG LENGTH VALUE
```

```
------- --- ------ -----
1 RECORDLENGTH 2 1156
2 DNSNAME 16 cucm-1051-a-pub
3 SUBJECTNAME 62 CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 62 CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL
6 SERIALNUMBER 16 70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB
7 PUBLICKEY 140
8 SIGNATURE 128
9 CERTIFICATE 694 E9 D4 33 64 5B C8 8C ED 51 4D 8F E5 EA 5B 6D 21
A5 A3 8C 9C (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

- Client CTL – si cette méthode est utilisée, votre fichier CTL est signé avec l'un des eTokens matériels.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Remarque : vous pouvez passer de la méthode utilisée avec le mode mixte CUCM avec CTL sans jeton.

Selon la méthode utilisée pour sécuriser votre grappe, une procédure de mise à jour CTL appropriée doit être utilisée. Relancez le client CTL ou entrez la commande **utils ctl update CTLfile depuis la ligne de commande.**

Vérifier la sécurité par défaut de la grappe

Il est important d'éviter les problèmes liés à l'ITL, car cela peut entraîner l'échec de nombreuses fonctionnalités ou le téléphone refuse de se conformer à toute modification de configuration. Les problèmes d'ITL peuvent être évités de ces deux manières.

Utilisation de la fonction Préparer le cluster pour la restauration vers la version antérieure à 8.0

Cette fonctionnalité occulte les entrées ITL dans le fichier ITL, de sorte que les téléphones font confiance à tout serveur TFTP. Toute demande HTTPS de/vers les téléphones échoue alors que ce paramètre est défini sur True. Il n'est pas recommandé de l'activer car il limite les fonctionnalités téléphoniques telles que la substitution de poste, le répertoire d'entreprise, etc. Cependant, vous pouvez passer et recevoir des appels téléphoniques de base.

> **Note**: Cette fonctionnalité ne fonctionne pas pour les clusters en mode mixte, car ce paramètre efface uniquement ITL et non les entrées CTL.

> **Note**: Cette fonctionnalité empêche mais ne résout pas les problèmes ITL, si le problème est déjà dans le téléphone, elle ne supprime pas le ITL et le retrait ITL doit être manuel.

> **Remarque** : si vous modifiez ce paramètre, TOUS LES TÉLÉPHONES SONT RÉINITIALISÉS.

Une fois cette fonctionnalité définie, tous les serveurs TFTP doivent être redémarrés (afin de fournir le nouveau RIT) et tous les téléphones doivent être réinitialisés afin de les forcer à demander le nouveau RIT **vide**. Une fois les modifications de certificat terminées et tous les services nécessaires redémarrés, cette fonctionnalité peut être rétablie sur **False**, le service TFTP redémarré et la réinitialisation du téléphone (afin que le téléphone puisse obtenir le fichier ITL valide). Ensuite, toutes les fonctionnalités continuent de fonctionner comme auparavant.

Régénérer les certificats dans un ordre particulier

Cette procédure fournit au serveur TFTP un fichier ITL valide/mis à jour provenant d'un serveur TFTP de confiance et disponible.

1. Arrêtez le service TFTP sur le serveur TFTP primaire.
2. Apportez les modifications nécessaires aux certificats du serveur TFTP principal.
3. Réinitialisez les téléphones (afin d'obtenir un nouveau fichier ITL à partir du serveur TFTP secondaire) – en fonction des certificats qui sont régénérés, cela peut se produire automatiquement.
4. Une fois que les téléphones ont été réinitialisés, démarrez le service TFTP du serveur TFTP primaire.
5. Modifiez les certificats sur le serveur TFTP secondaire.
6. Réinitialisez les téléphones (afin d'obtenir un nouveau fichier ITL à partir du serveur TFTP primaire).

> **Attention** : NE MODIFIEZ PAS les certificats sur les deux serveurs TFTP en même temps. Il n'y aurait alors aucun serveur TFTP de confiance et exigerait de l'administrateur local qu'il retire manuellement l'ITL de tous les téléphones.

Régénérer un type de certificat à la fois

Il s'agit de la procédure la plus utilisée et recommandée car elle empêche les téléphones de perdre confiance. Le processus est décrit dans la section

Procédure de régénération des certificats pour le guide Cisco Unified Communications Manager

(CUCM).

Supprimer et régénérer des certificats dans CUCM

Seuls les certificats de service (magasins de certificats qui ne sont pas étiquetés avec -trust) peuvent être régénérés. Les certificats des magasins d'approbation (magasins de certificats étiquetés avec -trust) doivent être supprimés, car ils ne peuvent pas être régénérés.

> **Attention** : Attention au bogue CSCut58407 - Les périphériques ne devraient pas redémarrer lorsque CAPF / CallManager / TVS-trust est supprimé.

Une fois un certificat modifié, le service visé doit être redémarré pour recevoir les modifications. La section « Après la régénération/suppression de certificats » aborde ce sujet plus en détail.

> **Attention** : soyez conscient de l'ID de bogue Cisco CSCto86463 - Les certificats supprimés réapparaissent, impossible de supprimer les certificats de CUCM. Il s'agit d'un problème où les certificats supprimés continuent de réapparaître après la suppression. Suivez la solution de contournement dans la fiche du bogue.

Régénérer les certificats avec l'interface de ligne de commande

> **Attention** : La régénération des certificats déclenche une mise à jour automatique des fichiers ITL au sein du cluster, ce qui déclenche une réinitialisation logicielle à l'échelle du cluster pour permettre aux téléphones de déclencher une mise à jour de leur ITL local. Cette opération est centrée sur les régénérations de certificats CAPF et CallManager, mais peut se produire avec d'autres magasins de certificats dans CUCM, comme Tomcat.

Régénérer CAPF : Lors de la régénération, le certificat CAPF se télécharge automatiquement dans CAPF-trust et CallManager-trust. De plus, CAPF a toujours un en-tête de nom de sujet unique, de sorte que les certificats CAPF précédemment utilisés sont conservés et utilisés pour l'authentification.

```
set cert regen CAPF
```

> **Remarque** : si un certificat CAPF expire, les téléphones qui utilisent LSC ne peuvent pas s'enregistrer auprès de CUCM car CUCM rejette leur certificat. Toutefois, vous pouvez toujours générer un nouveau LSC pour un téléphone avec le nouveau certificat CAPF. Lorsque vous redémarrerez le téléphone, il téléchargera la configuration et contactera ensuite CAPF afin de mettre à jour le LSC. Après la mise à jour du LSC, le téléphone s'enregistrera comme il se doit. Cela fonctionne tant qu'un nouveau certificat CAPF se trouve dans le fichier ITL et que le téléphone a téléchargé et fait confiance au certificat qui l'a signé (callmanager.pem).

Régénérer CallManager : Lors de la régénération, le CallManager se télécharge automatiquement vers CallManager-trust.

```
set cert regen CallManager
```

Régénérer IPsec : Lors de la régénération, le certificat IPsec se télécharge automatiquement vers ipsec-trust.

```
set cert regen ipsec
```

Régénérer Tomcat : Lors de la régénération, le certificat Tomcat se télécharge automatiquement vers tomcat-trust.

```
set cert regen tomcat
```

Régénérer TVS :

```
set cert regen TVS
```

Àquoi s'attendre ?

Lorsque vous régénérez des certificats via l’interface de ligne de commande, vous êtes invité à vérifier les modifications effectuées. Saisissez yes, puis sélectionnez Enter.

```
admin:set cert regen CAPF

WARNING: This operation will overwrite any CA signed certificate previously imported
for CAPF

Proceed with regeneration (yes|no)? yes

Successfully Regenerated Certificate for CAPF.

You must restart services related to CAPF for the regenerated certificates to become active.
```

Supprimer des certificats avec l’interface de ligne de commande

Suppression des certificats CAPF-trust

```
set cert delete CAPF <name of certificate>.pem
```

Suppression des certificats CallManager-trust

```
set cert delete CallManager <name of certificate>.pem
```

Suppression des certificats ipsec-trust

```
set cert delete ipsec <name of certificate>.pem
```

Enlever les certificats Tomcat-trust

```
set cert delete tomcat <name of certificate>.pem
```

Suppression des certificats TVS-trust

```
set cert delete TVS <name of certificate>.pem
```

Régénérer les certificats avec l’interface graphique Web

Régénérer CAPF :

Lors de la régénération, le certificat CAPF se télécharge automatiquement dans CAPF-trust et CallManager-trust. De plus, le certificat CAPF a toujours un nom unique, de sorte que les certificats du CAPF utilisés précédemment seront conservés et utilisés pour l’authentification.

```
OS Admin > Security > Certificate Management > Find > Click CAPF certificate > Regenerate
```

Régénérer CallManager :

Lors de la régénération, le certificat CallManager se télécharge automatiquement vers CallManager-trust.

```
OS Admin > Security > Certificate Management > Find > Click CallManager certificate > Regenerate
```

Régénérer IPsec :

Lors de la régénération, le certificat IPsec se télécharge automatiquement vers ipsec-trust.

```
OS Admin > Security > Certificate Management > Find > Click ipsec certificate > Regenerate
```

Régénérer Tomcat :

Lors de la régénération, le certificat Tomcat se télécharge automatiquement vers tomcat-trust.

```
OS Admin > Security > Certificate Management > Find > Click tomcat certificate > Regenerate
```

Régénérer TVS :

```
OS Admin > Security > Certificate Management > Find > Click TVS certificate > Regenerate
```

Supprimer des certificats avec l’interface graphique Web

```
OS Admin > Security > Certificate Management > Find > Click X certificate within the
'-trust' store > Remove/Delete
```

Après la régénération/suppression de certificats

Une fois qu’un certificat a été régénéré d’un magasin ou supprimé, le service visé doit être redémarré pour recevoir les modifications.

Magasin	Service à redémarrer	Comment
Tomcat	Tomcat	CLI : utils service restart Cisco Tomcat Suivez les étapes requises de l'environnement CCX, le cas échéant https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-co https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_c
CallManager	CallManager; TFTP;	GUI Web: Accédez à **Cisco Unified Serviceability > Tools > Control Center - F** Interface utilisateur Web : Accédez à **Cisco Unified Serviceability > Tools > Co**

	CTIManager	Interface utilisateur Web : Accédez à **Cisco Unified Serviceability > Tools > Co**
CAPF	CAPF (seulement sur le serveur diffuseur)	GUI Web: Accédez à **Cisco Unified Serviceability > Tools > Control Center - F**
TVS	Service de vérification de confiance (sur le serveur concerné)	GUI Web: Accédez à **Cisco Unified Serviceability > Tools > Control Center - N**
ipsec	Cisco DRF Local (sur tous les nœuds); Cisco DRF Master (sur le serveur diffuseur)	CLI : **utils service restart Cisco DRF Local** CLI : **utils service restart Cisco DRF Master**

Comment identifier les certificats de confiance non utilisés ?

Avant de supprimer des certificats expirés dans le magasin d'approbation, il est important d'identifier ceux qui sont utilisés et ceux qui ne le sont pas. Gardez à l'esprit les points suivants pour sélectionner les certificats qui doivent être supprimés :

- La plupart des certificats de confiance sont des copies des certificats de service utilisés. Il est recommandé de régénérer d'abord tous les certificats de service expirés dans tous les noeuds, et CUCM met automatiquement à jour la copie -trust.
- Le VeriSign_Class_3_Secure_Server_CA_-_G3 de la confiance tomcat n'est plus utilisé. Si la fonction Smart Call Home est utilisée, suivez le guide suivant pour télécharger le nouveau certificat : https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/smart-call-home/215210-troubleshooting-certficate-exipry-alert.html
- Les certificats de confiance de fabrication sont préchargés sur n'importe quel CUCM pendant l'installation et ils sont utilisés pour que CUCM fasse confiance à n'importe quel téléphone IP Cisco par défaut. Il n'est pas recommandé de supprimer ces certificats :

CAP-RTP-001

CAP-RTP-002

CA racine Cisco 2048

CA racine M2 Cisco

ACT2_SUDI_CA

CA_Fabrication_Cisco

Cisco_Manufacturing_CA_SHA2

- Si le domaine ou le nom d'hôte a été modifié, les anciens certificats avec un ancien domaine ou nom d'hôte sont répertoriés comme « trust ». Si ces noms d'hôte et domaines ne sont plus utilisés, ces certificats ne sont plus utilisés et peuvent être supprimés.
- Si le nom commun du certificat provient d'un autre serveur (et non d'un cluster CUCM), vérifiez que le certificat de l'autre serveur est valide. Étant donné que CUCM ne peut pas régénérer le certificat, cela doit être fait sur l'autre serveur, puis importer le certificat en tant que -trust dans CUCM.

Installer/mettre à jour LSC sur les téléphones

Si le certificat CAPF a été régénéré, les certificats LSC pour tous les téléphones de la grappe doivent être mis à jour avec un LSC signé par le nouveau certificat CAPF.

1. Accédez à **Serviceability > Service Activation de CUCM**. Activez la fonction « Cisco CTL Provider » et « Cisco Certificate Authority Proxy Function » sur le serveur diffuseur.

2. Sous **CUCM CCMAdmin**, accédez à **Device > Phone.** Choisissez le téléphone IP sur lequel vous voulez verser un LSC.

3. Dans la page Configuration du périphérique sous Opération de certificat, accédez à **Installer / Mettre à niveau > Par chaîne nulle**.

4. Sauvegardez la configuration du téléphone dans CCMAdmin et choisissez « **Apply Config** ».

Si le téléphone a des problèmes avec l'installation du LSC, effectuez ces actions sur le téléphone :

Lorsque le téléphone se réinitialise, sous le téléphone physique, accédez à **Paramètres > (6) Configuration de la sécurité > (4) LSC > **#** (cette opération déverrouille l'interface utilisateur graphique et nous permet de passer à l'étape suivante) **> Mise à jour** (la mise à jour n'est visible que lorsque vous exécutez l'étape précédente). Cliquez maintenant sur **Soumettre**.

N'assignez aucun certificat à un téléphone, sauf s'il s'agit d'un téléphone sans fil (7921/25). Les téléphones sans fil utilisent des autorités de certification tierces pour s'authentifier.

Processus de renouvellement des autres certificats

Processus De Régénération Des Certificats Pour Cisco Unified Communications Manager (CUCM) : le guide décrit le processus de régénération des certificats par type. il s'agit du processus le plus utilisé et recommandé.

Processus de régénération des certificats pour ITLRecovery sur CUCM 12.x et versions ultérieures : le guide décrit le processus de régénération du certificat ITLRecovery sur un cluster CUCM 12.x.

Régénération des certificats signés CA CUCM : le guide décrit le processus des certificats signés CA dans CUCM et les erreurs les plus courantes affichées lors du téléchargement d'un certificat.

Exemple de configuration de cluster de communications unifiées avec un sujet multiserveur signé par l'autorité de certification Autre nom : le guide fournit un exemple de régénération de certificat Tomcat Multi-san.

Régénérer les certificats auto-signés du service de messagerie instantanée et de présence Unified Communications Manager : le guide fournit le processus et les services de régénération à redémarrer pour les noeuds IM&P.

Guide de gestion des certificats de solution UCCX : le guide décrit les exigences d'intégration des certificats dans UCCX et le processus de régénération.

Le processus de régénération d'Expressway C et E est décrit dans les vidéos suivantes :

Installation d'un certificat de serveur sur un Expressway

Génération de CSR pour MRA/Clustering Expressways

Comment configurer la confiance des certificats entre Expressway-C et Expressway-E

Conclusion

Si vous rencontrez un problème ou avez besoin d'aide avec cette procédure, communiquez avec le Centre d'assistance technique Cisco (TAC). Dans ce cas, gardez votre sauvegarde DRF disponible car elle est utilisée en dernier recours afin de restaurer le service si le TAC ne peut pas le faire par d'autres méthodes.