Batterie CUCM changée de l'exemple Non-sécurisé de configuration de mode de mode mixte

Contenu

Introduction

Le document décrit l'étape nécessaire afin de changer la security mode de Cisco Unified Communications Manager (CUCM) du mode Non-sécurisé de mode mixte. Il affiche également comment le contenu d'un fichier de la liste de confiance de certificat (CTL) est changé quand ce mouvement est terminé.

Il y a trois parties principales pour changer la security mode CUCM :

1a. Exécutez le client CTL et sélectionnez la variante désirée de la security mode.
1b. Sélectionnez la commande CLI afin de sélectionner la variante désirée de la security mode.
2. Redémarrez le Cisco CallManager et les services TFTP de Cisco sur tous les serveurs CUCM qui dirigent ces services.
3. Redémarrez tous les Téléphones IP de sorte qu'ils puissent télécharger la version mise à jour du fichier CTL.

> Remarque: Si la security mode de batterie est changée du mode Non-sécurisé de mode mixte le fichier CTL existe toujours sur les serveurs et aux téléphones, mais le fichier CTL ne contient aucun Certificats CCM+TFTP (serveur). Puisque les Certificats CCM+TFTP (serveur) n'existent pas dans le fichier CTL, ceci force le téléphone pour s'enregistrer comme Non-sécurisé avec CUCM.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de la version 10.0(1) ou ultérieures CUCM. Supplémentaire, assurez cela :

- Le service de fournisseur CTL est en hausse et fonctionne sur tous les serveurs actifs TFTP dans la batterie. Par défaut le service fonctionne sur le port TCP 2444, mais ceci peut être modifié dans la configuration de paramètre de service CUCM.
- Les services de la fonction de proxy d'autorité de certification (CAPF) sont hauts et fonctionnent sur le noeud de Publisher.
- La réplication de base de données (DB) dans la batterie fonctionne correctement et les données repliées de serveurs en temps réel.

Composants utilisés

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

- Batterie de la version 10.0.1.11900-2 CUCM de deux Noeuds
- Téléphone IP de Cisco 7975 (inscrit à Protocole SCCP (Skinny Call Control Protocol), à version de firmware SCCP75.9-3-1SR3-1S)
- Deux jetons de sécurité Cisco sont nécessaires afin de placer la batterie au mode mixte
- Un des jetons de Sécurité répertoriés précédemment est nécessaire afin de placer le mode Non-sécurisé de batterie

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.

Informations générales

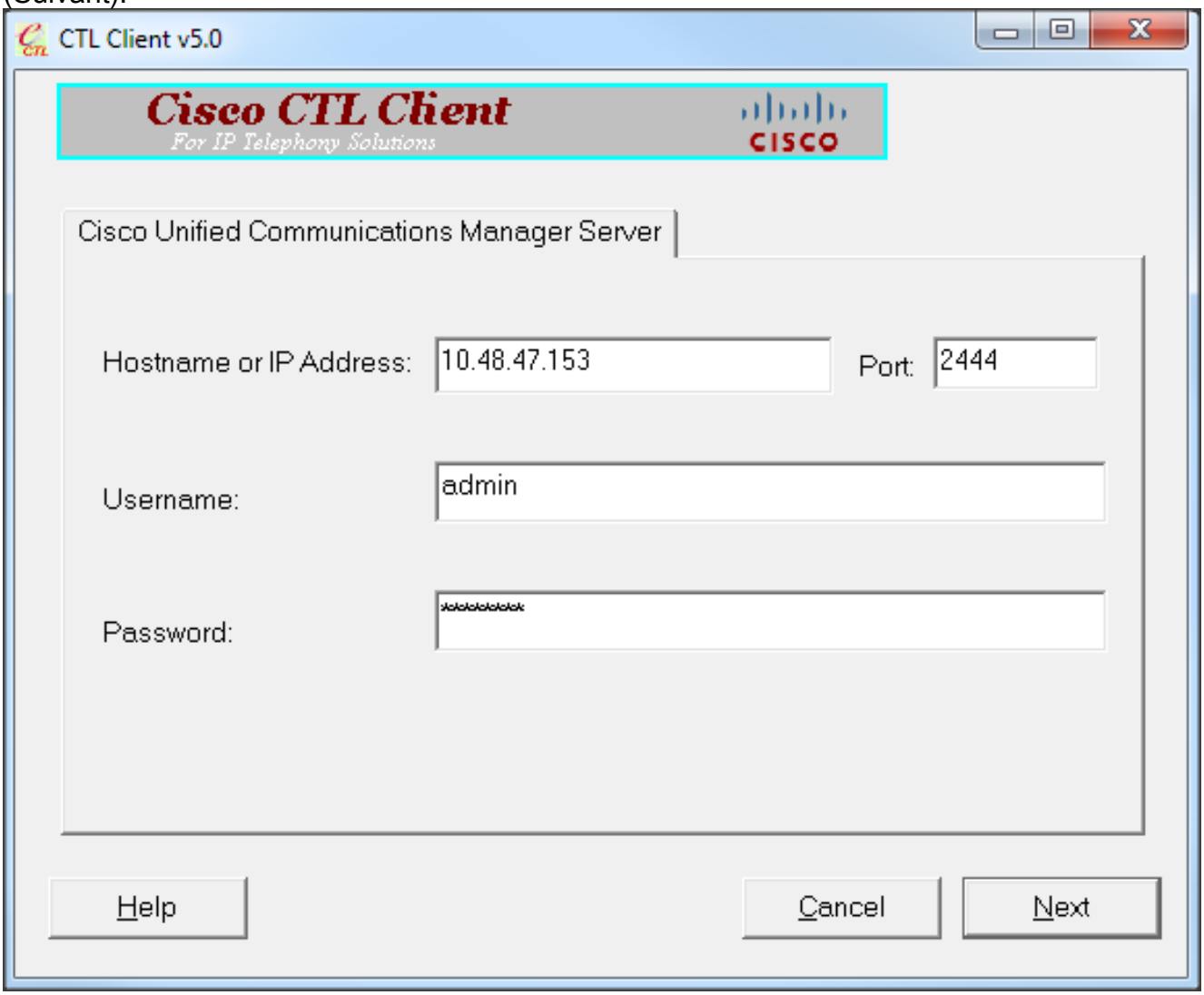
Afin d'exécuter le module d'extension de client CTL on l'exige pour avoir accès au moins à un jeton de Sécurité qui a été inséré afin de créer ou mettre le plus défunt fichier CTL à jour existe sur le serveur CUCM Publisher. En d'autres termes, au moins un des Certificats d'eToken qui existe dans le fichier CTL en cours sur CUCM doit être sur le jeton de Sécurité qui est utilisé pour changer la security mode.

Configurez

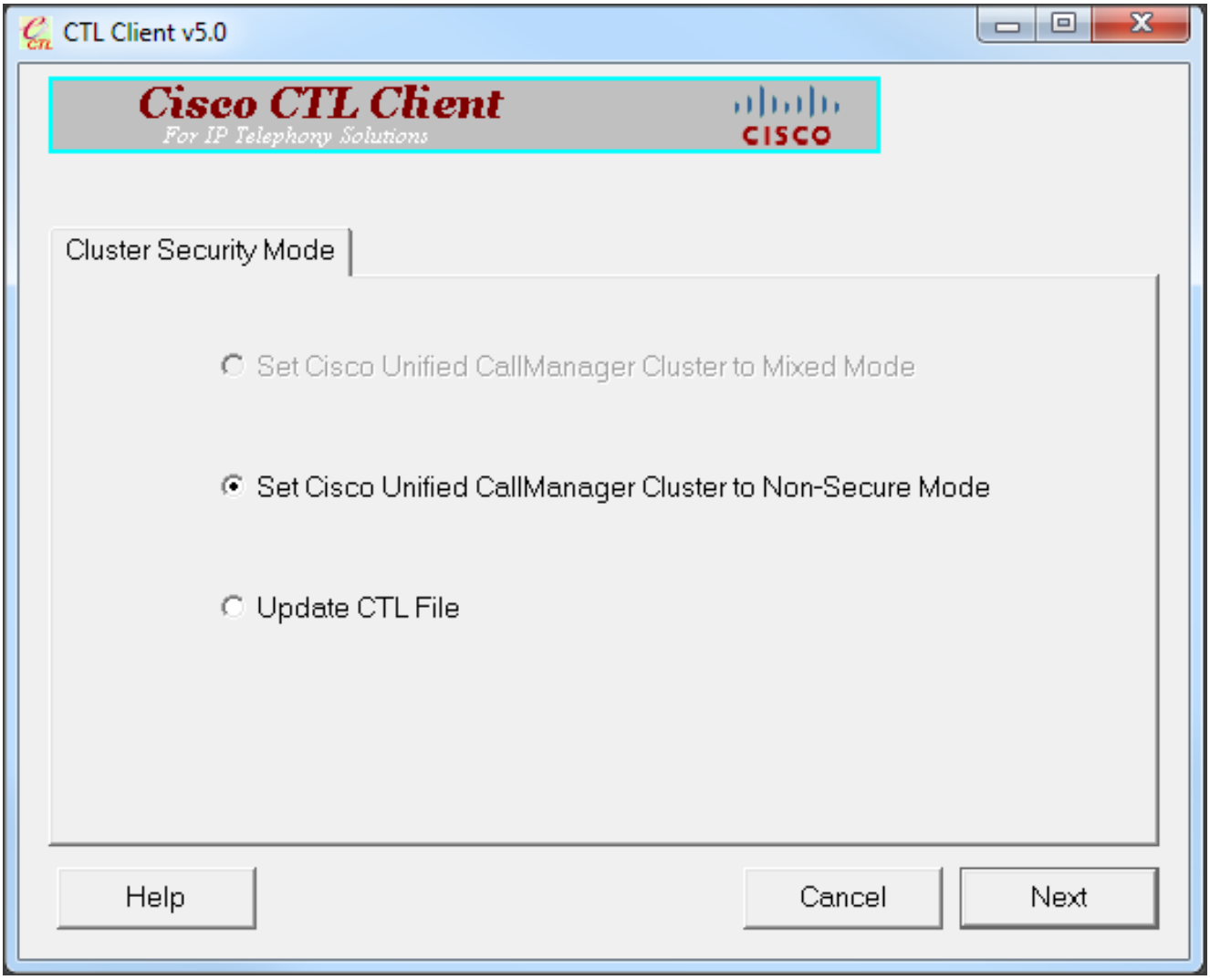
Changez la Sécurité de batterie CUCM du mode Non-sécurisé de mode mixte avec le client CTL

Terminez-vous ces étapes afin de changer la Sécurité de batterie CUCM du mode Non-sécurisé de mode mixte avec le client CTL :

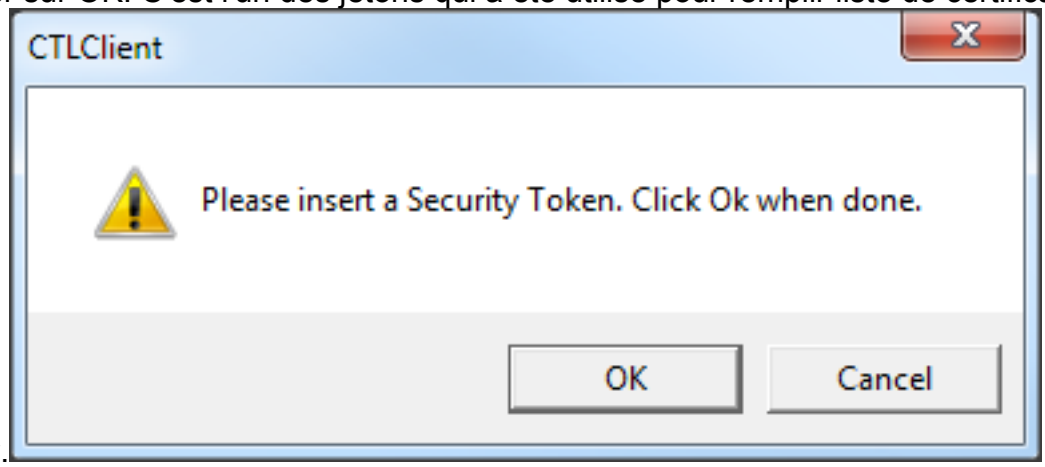
1. Obtenez un jeton de Sécurité que vous vous êtes inséré pour configurer le plus défunt fichier CTL.
2. Exécutez le client CTL. Fournissez l'adresse Internet IP/adresse du bar CUCM et des qualifications de l'administrateur CCM. Cliquez sur **Next** (Suivant).



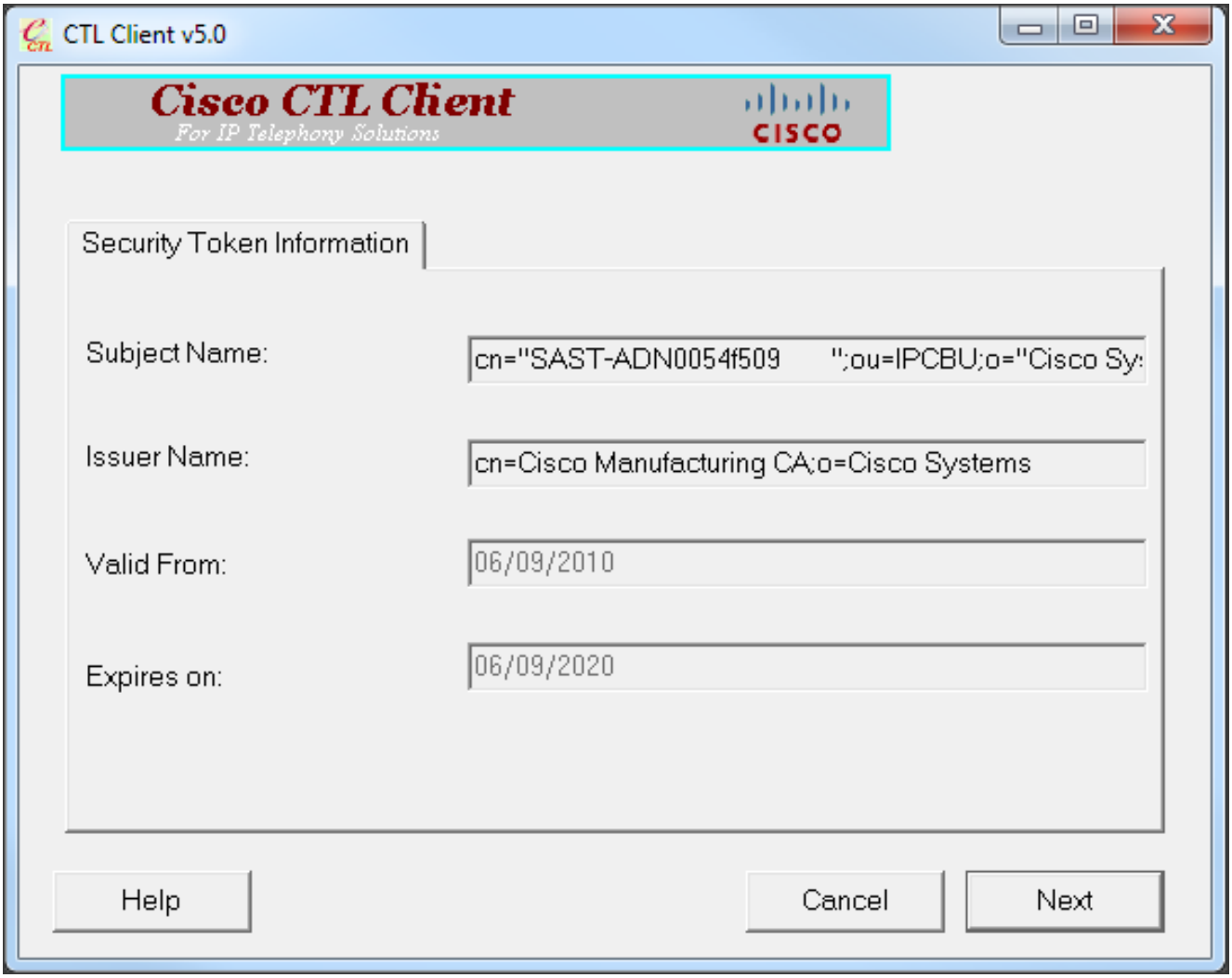
3. Cliquez sur la case d'option Non-**sécurisée de mode de batterie de Cisco Unified CallManager de positionnement**. Cliquez sur **Next** (Suivant).



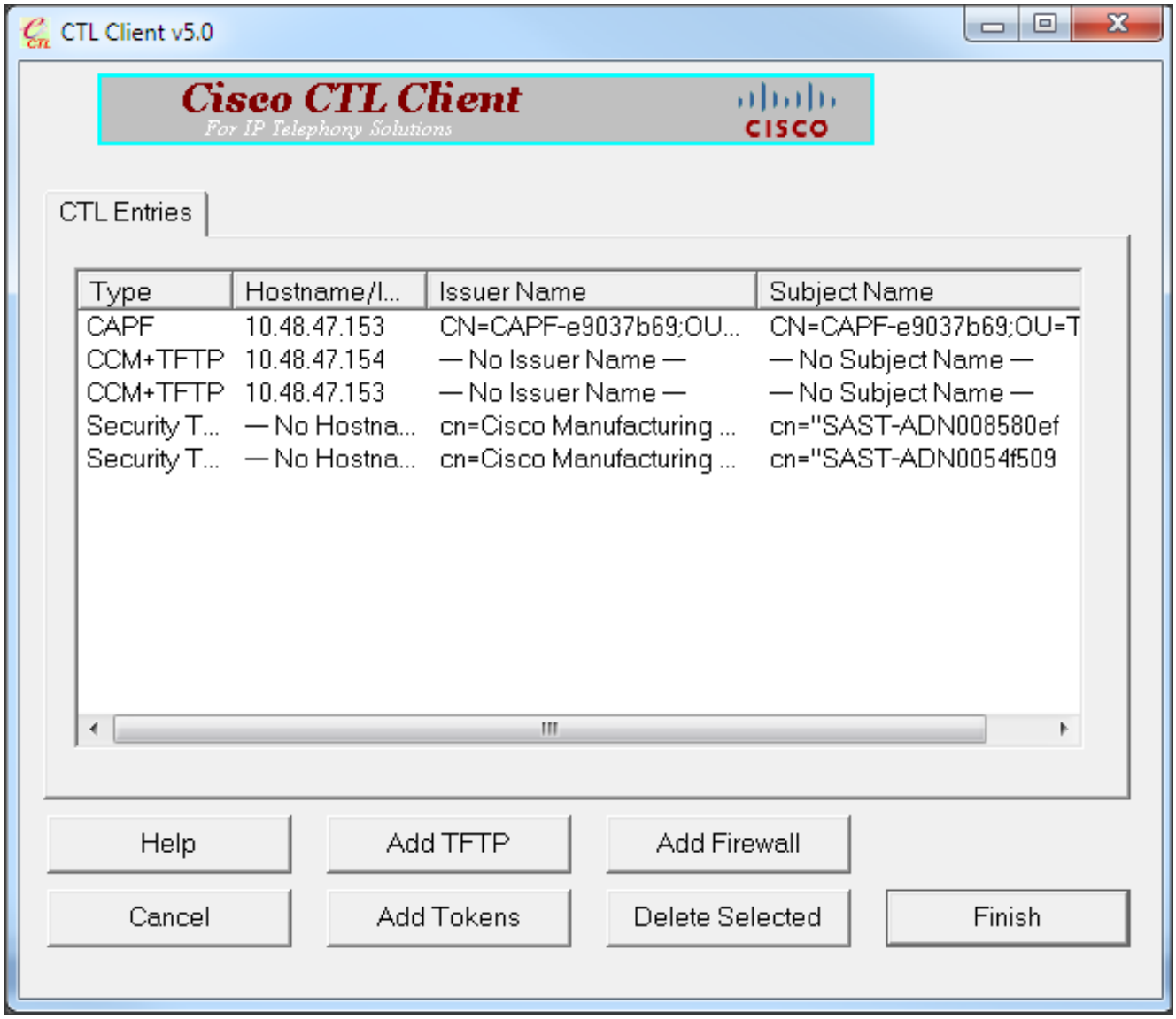
4. Insérez un jeton de Sécurité qui a été inséré pour configurer le plus défunt fichier CTL et pour cliquer sur OK. C'est l'un des jetons qui a été utilisé pour remplir liste de certificat dans CTLFile.tlv.



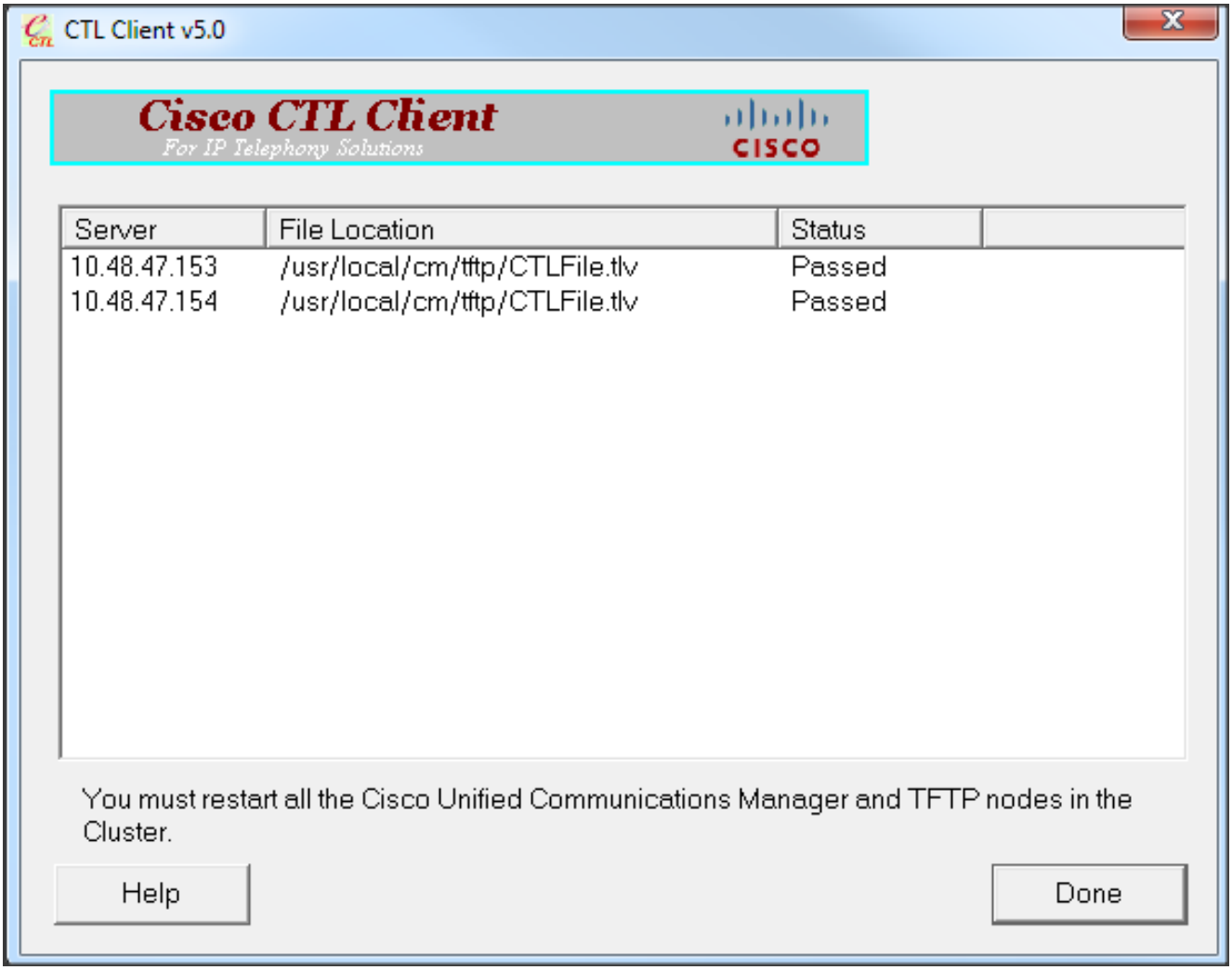
5. Les détails symboliques de Sécurité sont affichés. Cliquez sur **Next** (Suivant).



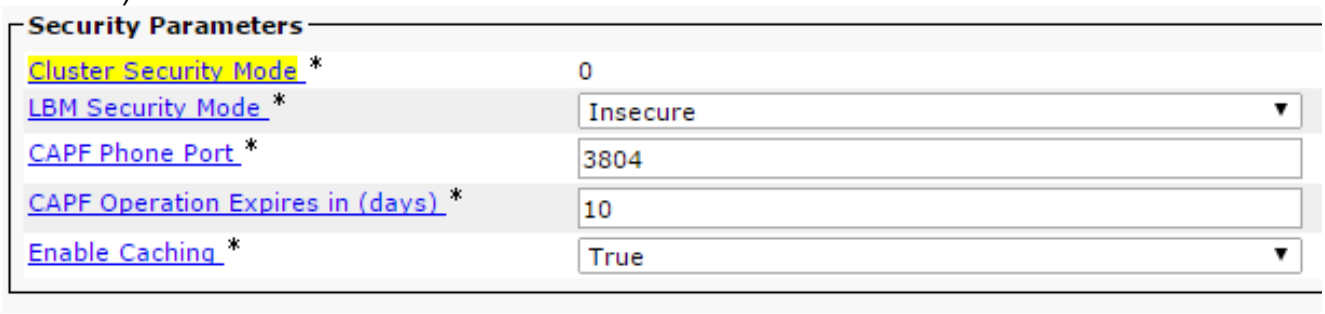
6. Le contenu du fichier CTL est affiché. Cliquez sur **Finish** (Terminer). Une fois incité pour le mot de passe, écrivez
Cisco123.



7. La liste de serveurs CUCM sur lesquels le fichier CTL existe est affichée. Cliquez sur **Done**.



8. Choisissez la **page > le System > Enterprise Parameters d'admin CUCM** et les vérifiez que la batterie était mode Non-sécurisé réglé ("0" indique Non-sécurisé).



9. Redémarrez le TFTP et les services de Cisco CallManager sur tous les Noeuds dans la batterie qui dirigent ces services.
10. Redémarrez tous les Téléphones IP de sorte qu'ils puissent obtenir la nouvelle version du fichier CTL de CUCM TFTP.

Changez la Sécurité de batterie CUCM du mode Non-sécurisé de mode mixte avec le CLI

Cette configuration est seulement pour la version 10.X et ultérieures CUCM. Afin de placer la security mode de batterie CUCM Non-sécurisée, sélectionnez la commande de non-sécurisé-

mode de positionnement-batterie de ctl d'utils sur Publisher CLI. Après que ce soit complet, redémarrez le TFTP et les services de Cisco CallManager sur tous les Noeuds dans la batterie qui dirigent ces services.

Voici l'échantillon CLI sorti qui affiche l'utilisation de la commande.

```
admin:utils ctl set-cluster non-secure-mode
This operation will set the cluster to non secure mode. Do you want to continue? (y/n):

Moving Cluster to Non Secure Mode
Cluster set to Non Secure Mode
Please Restart the TFTP and Cisco CallManager services on all nodes in the cluster that
run these services
admin:
```

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Afin de vérifier le CTLFIle.tlv, vous pouvez utiliser une de deux méthodes :

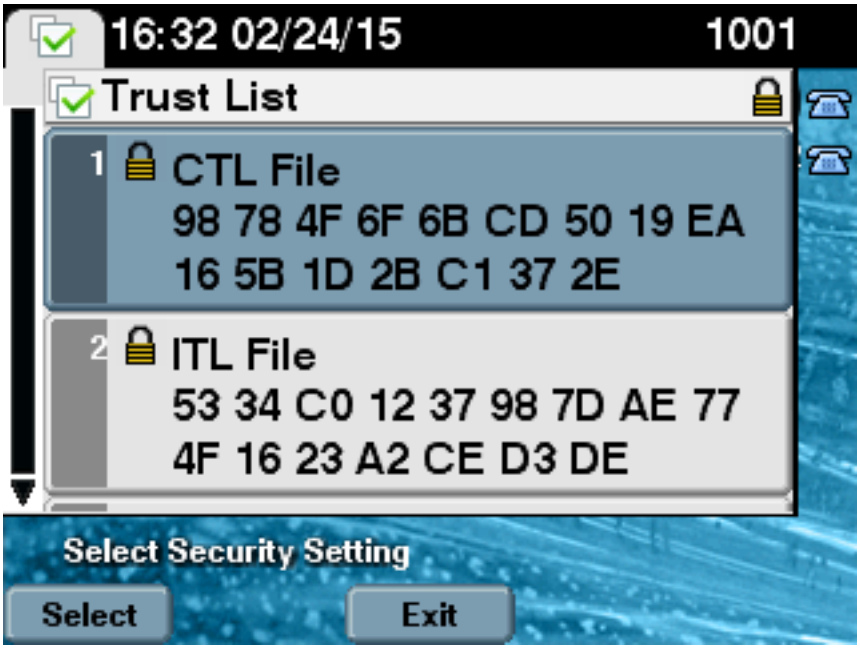
- Afin de vérifier le contenu et la somme de contrôle de MD5 du CTLFIle.tlv actuel du côté CUCM TFTP, sélectionnez la **commande de** showctl sur le CUCM CLI. Le fichier CTLFIle.tlv devrait être identique sur tous les Noeuds CUCM.
- Afin de vérifier la somme de contrôle de MD5 sur les 7975 téléphones IP, sélectionnez Settings **> configuration de sécurité > liste > fichier CTL de confiance**.

  Remarque: Quand vous vérifiez la somme de contrôle au téléphone que vous verrez le MD5 ou le SHA1, dépendant sur le type de téléphone.

Batterie CUCM réglée à la security mode - Somme de contrôle de fichier CTL

```
admin:show ctl
The checksum value of the CTL file:
98784f6f6bcd5019ea165b1d2bc1372e(MD5)
9c0aa839e5a84b18a43caf9f9ff23d8ebce90419(SHA1)
[...]
```

Du côté de téléphone IP, vous pouvez voir qu'il fait installer le même fichier CTL (la somme de contrôle de MD5 s'assortit une fois comparée à la sortie de CUCM).



Mode Non-sécurisé réglé par batterie CUCM - Contenu de fichier CTL

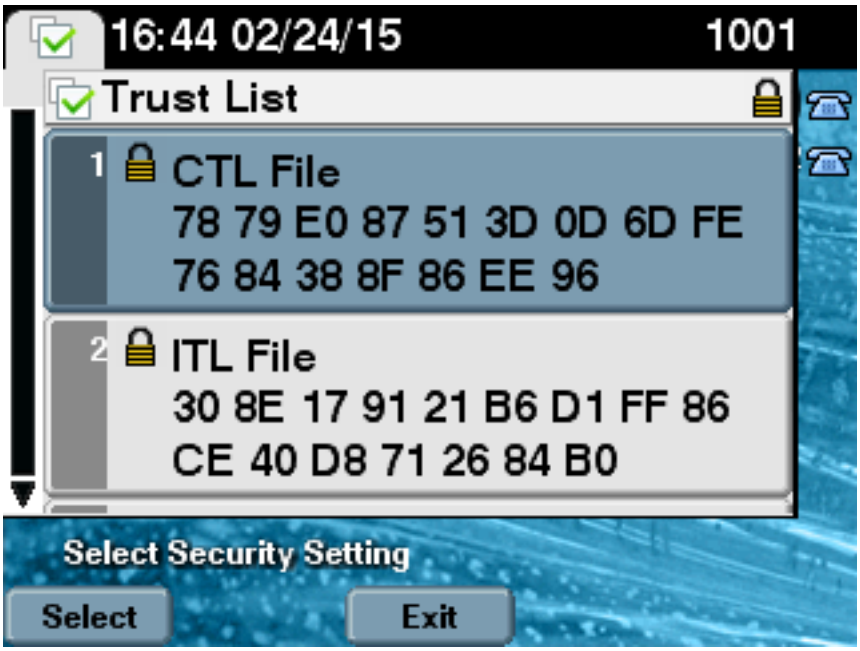
Voici un exemple d'un fichier CTL d'un mode Non-sécurisé réglé par batterie CUCM. Vous pouvez voir que les Certificats CCM+TFTP sont vides et ne contenez pas n'importe quel contenu. Le reste des Certificats dans les fichiers CTL ne sont pas changés et sont exactement identique que quand CUCM a été placé au mode mixte.

```
admin:show ctl
The checksum value of the CTL file:
7879e087513d0d6dfe7684388f86ee96(MD5)
be50e5f3e28e6a8f5b0a5fa90364c839fcc8a3a0(SHA1)


Length of CTL file: 3746
The CTL File was last modified on Tue Feb 24 16:37:45 CET 2015

Parse CTL File
----------------

Version: 1.2
HeaderLength: 304 (BYTES)

BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
3 SIGNERID 2 117
4 SIGNERNAME 56 cn="SAST-ADN0054f509 ";ou=IPCBU;o="Cisco Systems
5 SERIALNUMBER 10 3C:F9:27:00:00:00:AF:A2:DA:45
6 CANAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
7 SIGNATUREINFO 2 15
8 DIGESTALGORTITHM 1
9 SIGNATUREALGOINFO 2 8
10 SIGNATUREALGORTITHM 1
11 SIGNATUREMODULUS 1
12 SIGNATURE 128
45 ec 5 c 9e 68 6d e6
5d 4b d3 91 c2 26 cf c1
ee 8c b9 6 95 46 67 9e
19 aa b1 e9 65 af b4 67
36 7e e5 ee 60 10 b 1b
58 c1 6 64 40 cf e2 57
```

```
aa 86 73 14 ec 11 b a
3b 98 91 e2 e4 6e 4 50
ba ac 3e 53 33 1 3e a6
b7 30 0 18 ae 68 3 39
d1 41 d6 e3 af 97 55 e0
5b 90 f6 a5 79 3e 23 97
fb b8 b4 ad a8 b8 29 7c
1b 4f 61 6a 67 4d 56 d2
5f 7f 32 66 5c b2 d7 55
d9 ab 7a ba 6d b2 20 6
14 FILENAME 12
15 TIMESTAMP 4

CTL Record #:1
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN0054f509 ";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 3C:F9:27:00:00:00:AF:A2:DA:45
7 PUBLICKEY 140
9 CERTIFICATE 902 19 8F 07 C4 99 20 13 51 C5 AE BF 95 03 93 9F F2 CC 6D 93 90 (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.

CTL Record #:2
----
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 not used to sign the CTL file.

CTL Record #:3
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 33
2 DNSNAME 13 10.48.47.153
4 FUNCTION 2 CCM+TFTP
10 IPADDRESS 4

CTL Record #:4
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1004
2 DNSNAME 13 10.48.47.153
3 SUBJECTNAME 60 CN=CAPF-e9037b69;OU=TAC;O=Cisco;L=Krakow;ST=Malopolska;C=PL
4 FUNCTION 2 CAPF
5 ISSUERNAME 60 CN=CAPF-e9037b69;OU=TAC;O=Cisco;L=Krakow;ST=Malopolska;C=PL
6 SERIALNUMBER 16 79:59:16:C1:54:AF:31:0C:0F:AE:EA:97:2E:08:1B:31
7 PUBLICKEY 140
9 CERTIFICATE 680 A0 A6 FC F5 FE 86 16 C1 DD D5 B7 57 38 9A 03 1C F7 7E FC 07 (SHA1 Hash HEX)
```

```
10 IPADDRESS 4

CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 33
2 DNSNAME 13 10.48.47.154
4 FUNCTION 2 CCM+TFTP
10 IPADDRESS 4

The CTL file was verified successfully.

admin:
```

Du côté de téléphone IP, après qu'il ait été redémarré et ait téléchargé la version mise à jour de fichier CTL, vous pouvez voir que la somme de contrôle de MD5 s'assortit une fois comparée à la sortie de CUCM.



Mettez la Sécurité de batterie CUCM du mode Non-sécurisé de mode mixte quand des jetons USB sont perdus

Des jetons de Sécurité pour les batteries sécurisées ont pu être perdus. Dans cette situation, vous devez considérer ces deux scénarios :

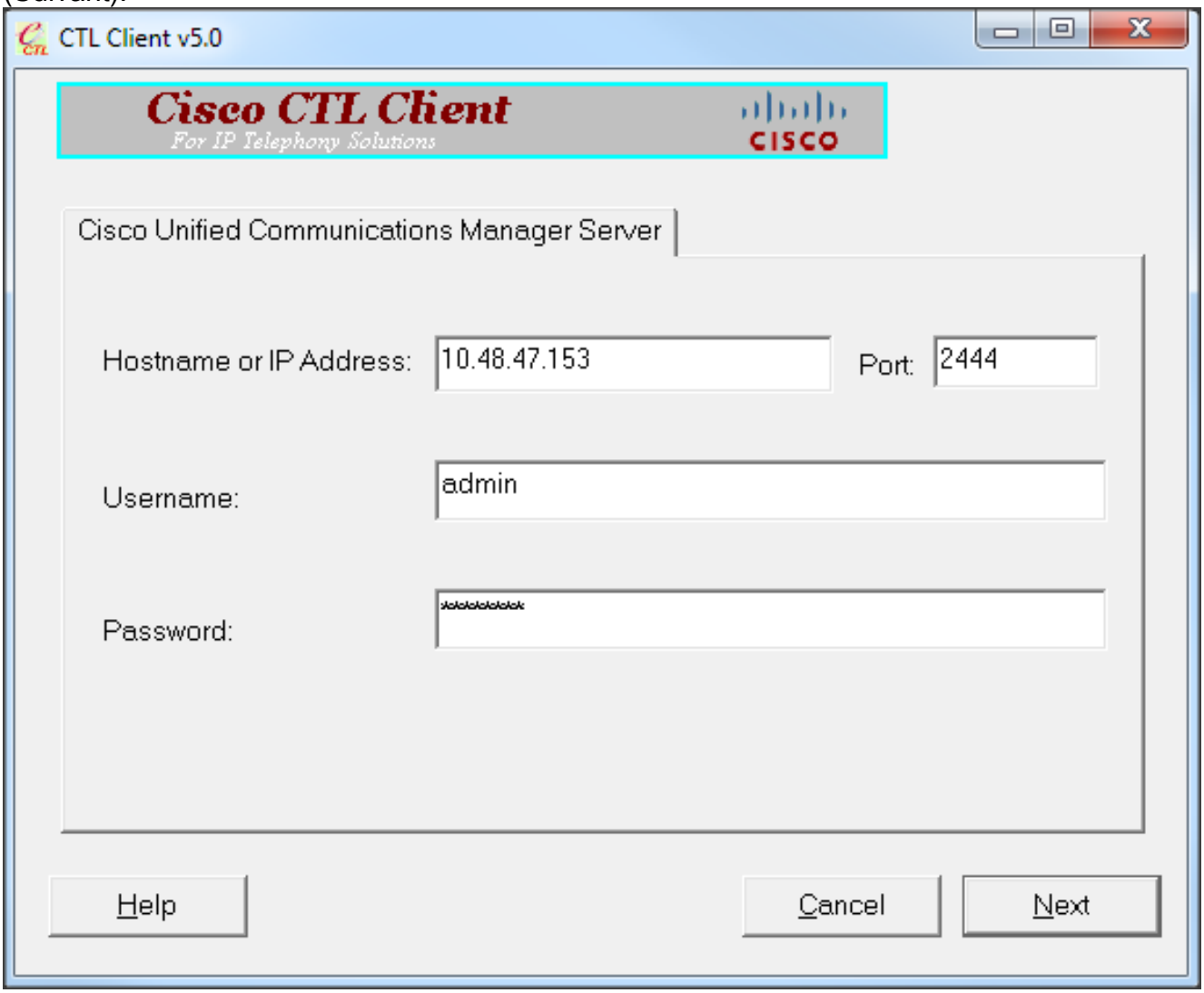
- La version 10.0.1 ou ultérieures de cluster run
- Les cluster run une version plus tôt que 10.x

Dans le premier scénario, remplissez la procédure décrite dans la modification la Sécurité de batterie CUCM du mode Non-sécurisé de mode mixte avec la section CLI afin de récupérer de la question. Puisque cette commande CLI n'exige pas un jeton CTL, elle pourrait être utilisée même si la batterie a été mise dans le mode mixte avec le client CTL.

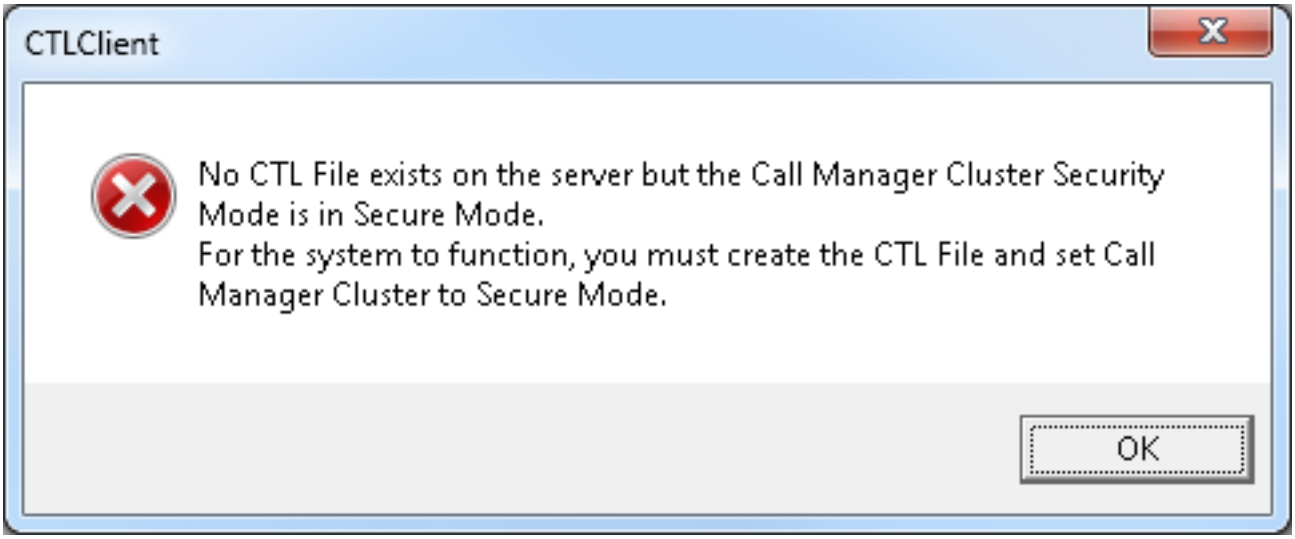
La situation obtient plus complexe quand une version plus tôt que 10.x de CUCM est en service. Si vous perdez ou oubliez le mot de passe d'un des jetons, vous pouvez encore employer l'autre pour exécuter le client CTL avec les fichiers CTL en cours. Il est fortement recommandé pour obtenir des autres eToken et l'ajoutent au fichier CTL dès que possible dans l'intérêt de la

Redondance. Si vous perdez ou oubliez les mots de passe pour tous les eTokens répertoriés dans votre fichier CTL, vous devez obtenir une nouvelle paire d'eTokens et exécuter une procédure manuelle comme expliqué ici.

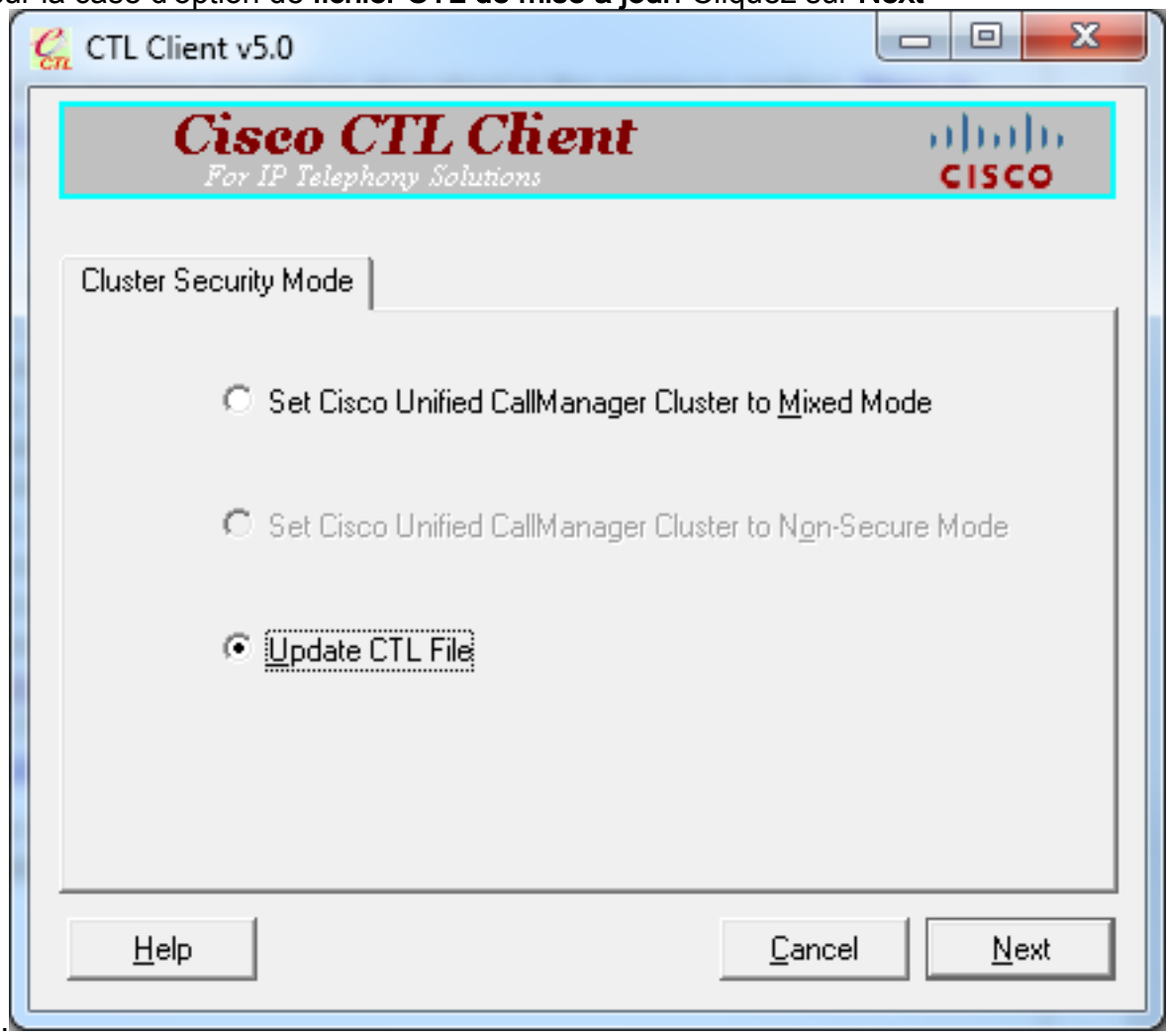
1. Sélectionnez la **commande du tftp CTLFile.tlv d'effacement de fichier** afin de supprimer le fichier CTL de tous les serveurs TFTP.`admin:file delete tftp CTLFile.tlv`
```
Delete the File CTLFile.tlv?
Enter "y" followed by return to continue: y
files: found = 1, deleted = 1

admin:show ctl
Length of CTL file: 0
CTL File not found. Please run CTLClient plugin or run the CLI - utils ctl..
to generate the CTL file.
Error parsing the CTL File.
```
2. Exécutez le client CTL. Introduisez l'adresse Internet IP/adresse du bar CUCM et des qualifications de l'administrateur CCM. Cliquez sur **Next** (Suivant).



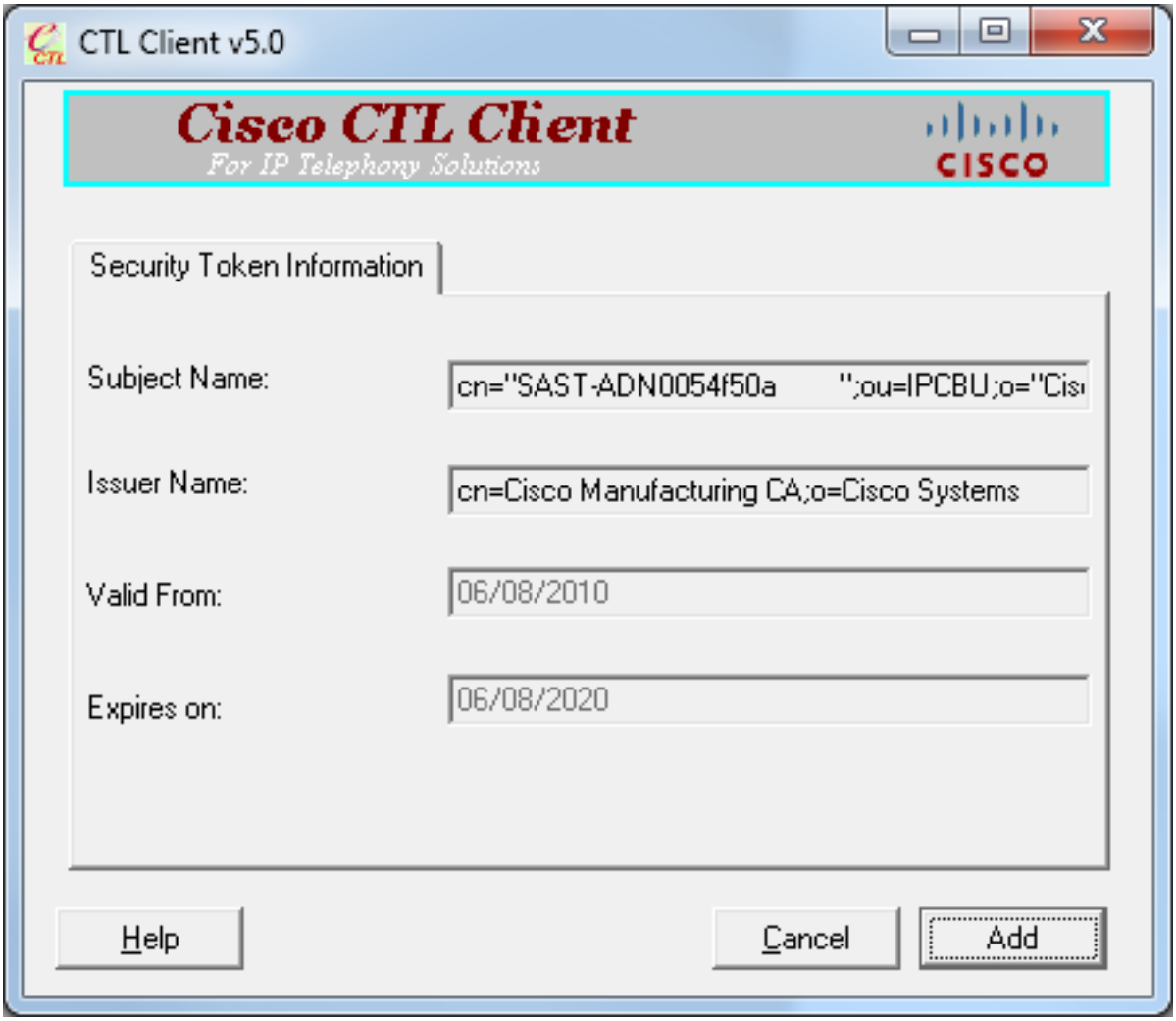
3. Puisque la batterie est dans le mode mixte, toutefois aucun fichier CTL n'existe sur Publisher, cet avertissement est affiché. Cliquez sur OK afin de l'ignorer et poursuivre en avant.



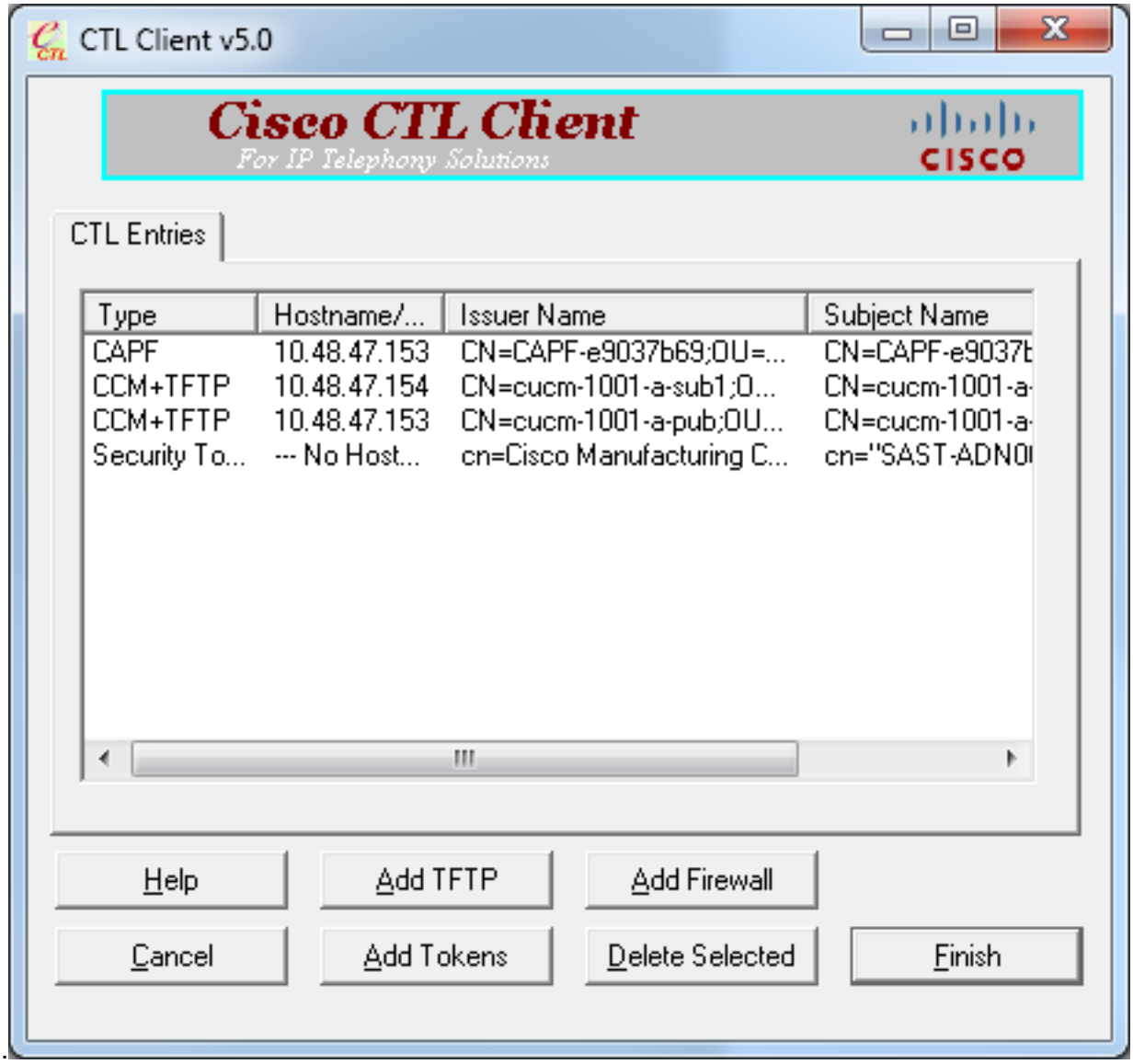
4. Cliquez sur la case d'option de **fichier CTL de mise à jour**. Cliquez sur **Next** (Suivant).



5. Le client CTL demande à ajouter un jeton de Sécurité. Cliquez sur Add afin de poursuivre.

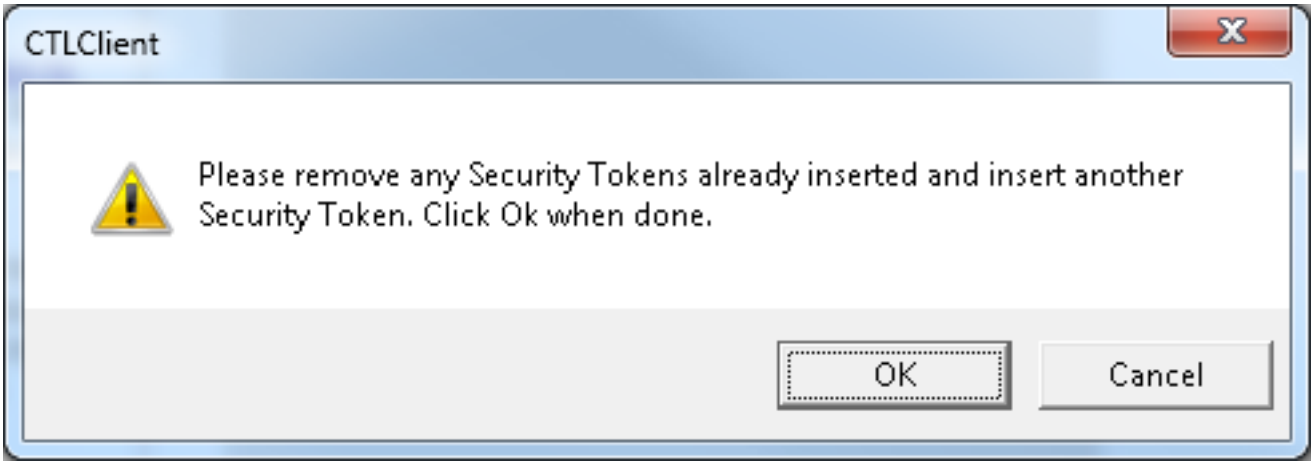


6. Les affichages de l'écran toutes les entrées dans nouveau CTL. Cliquez sur Add les **jetons** afin d'ajouter le deuxième jeton des nouvelles

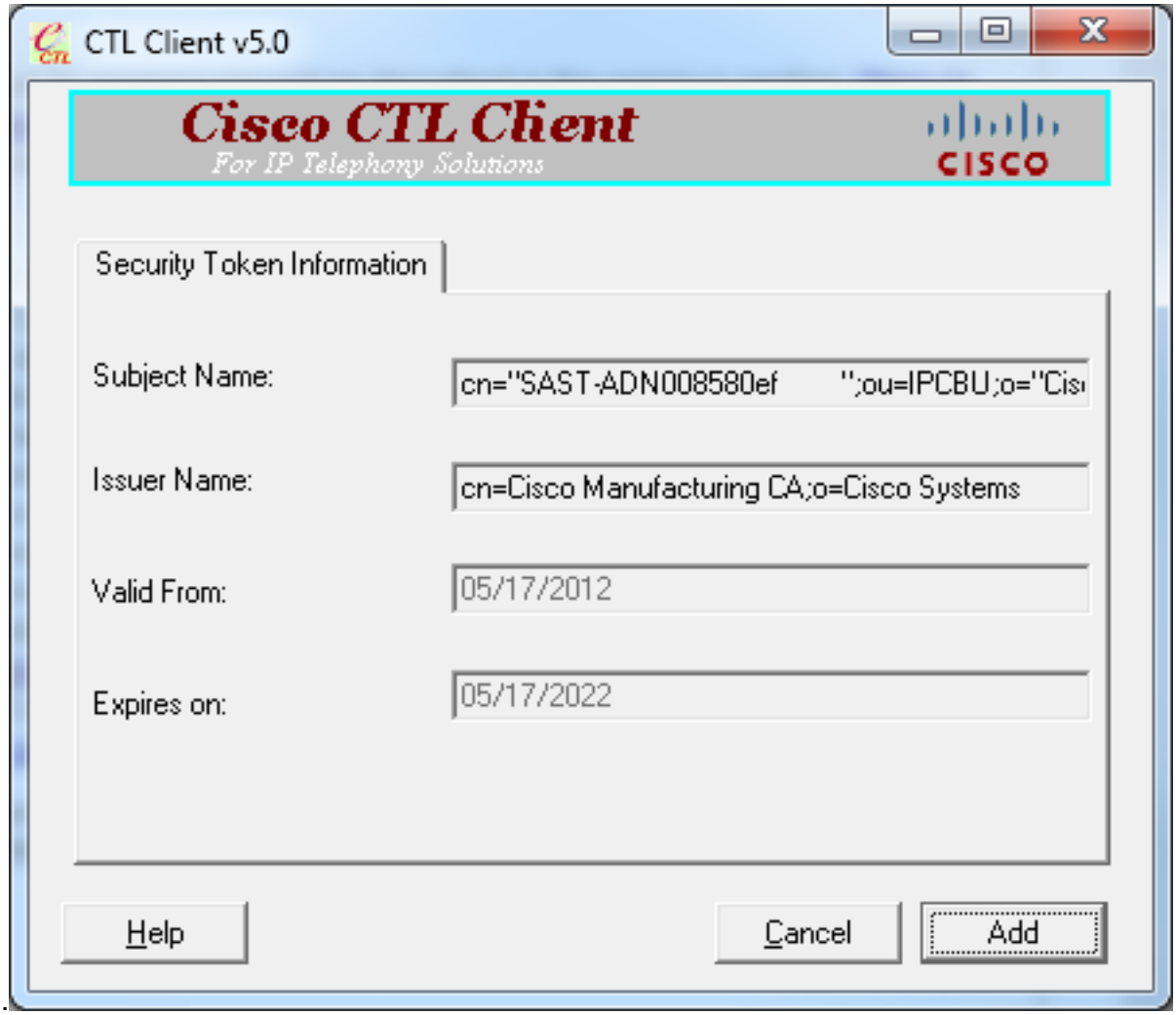


paires.

7. Vous serez incité à retirer le jeton en cours et à insérer un neuf. Cliquez sur OK une fois fait.

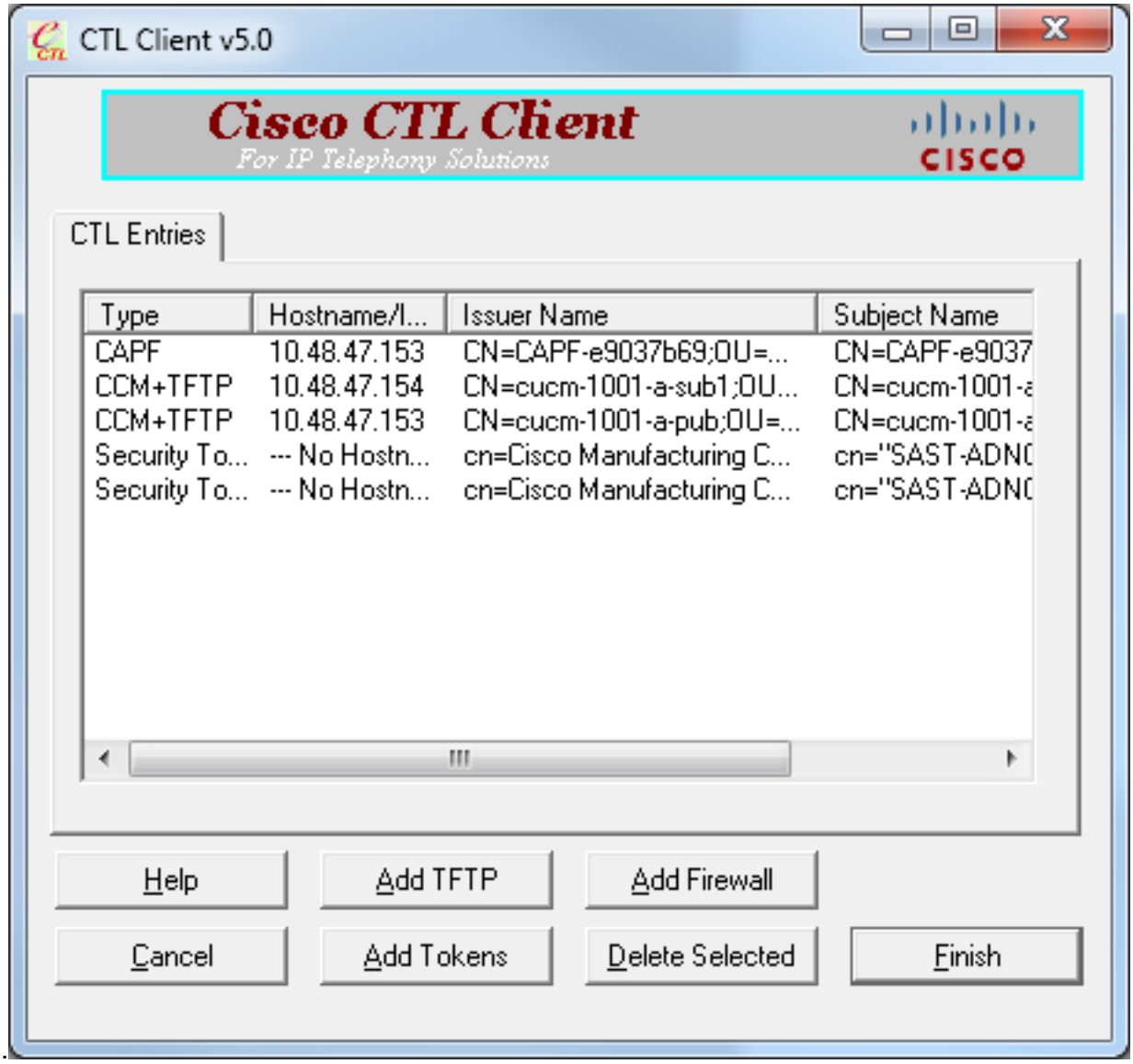


8. Un écran qui affiche des détails du nouveau jeton est affiché. Cliquez sur Add afin de les confirmer et ajouter ce



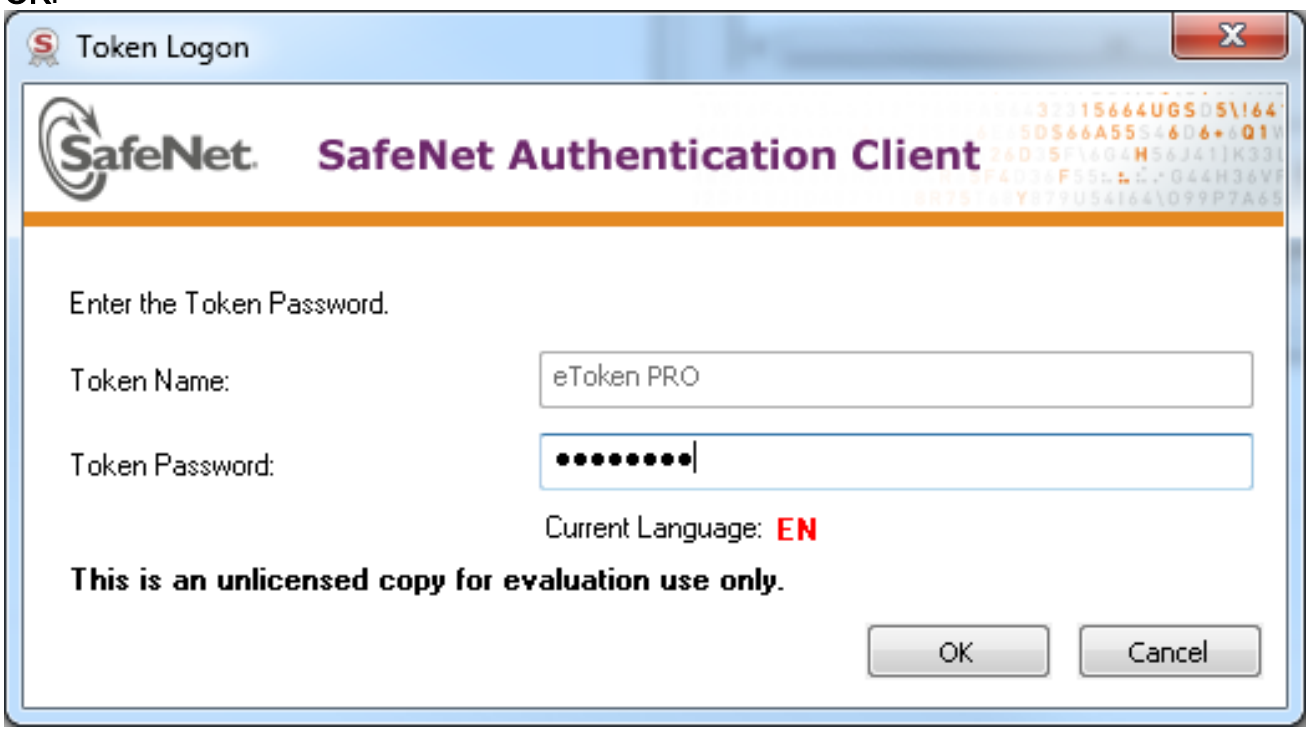
jeton.

9. Vous serez présenté avec la nouvelle liste d'entrées CTL qui affichent les deux jetons ajoutés. Cliquez sur Finish afin de générer de nouveaux fichiers

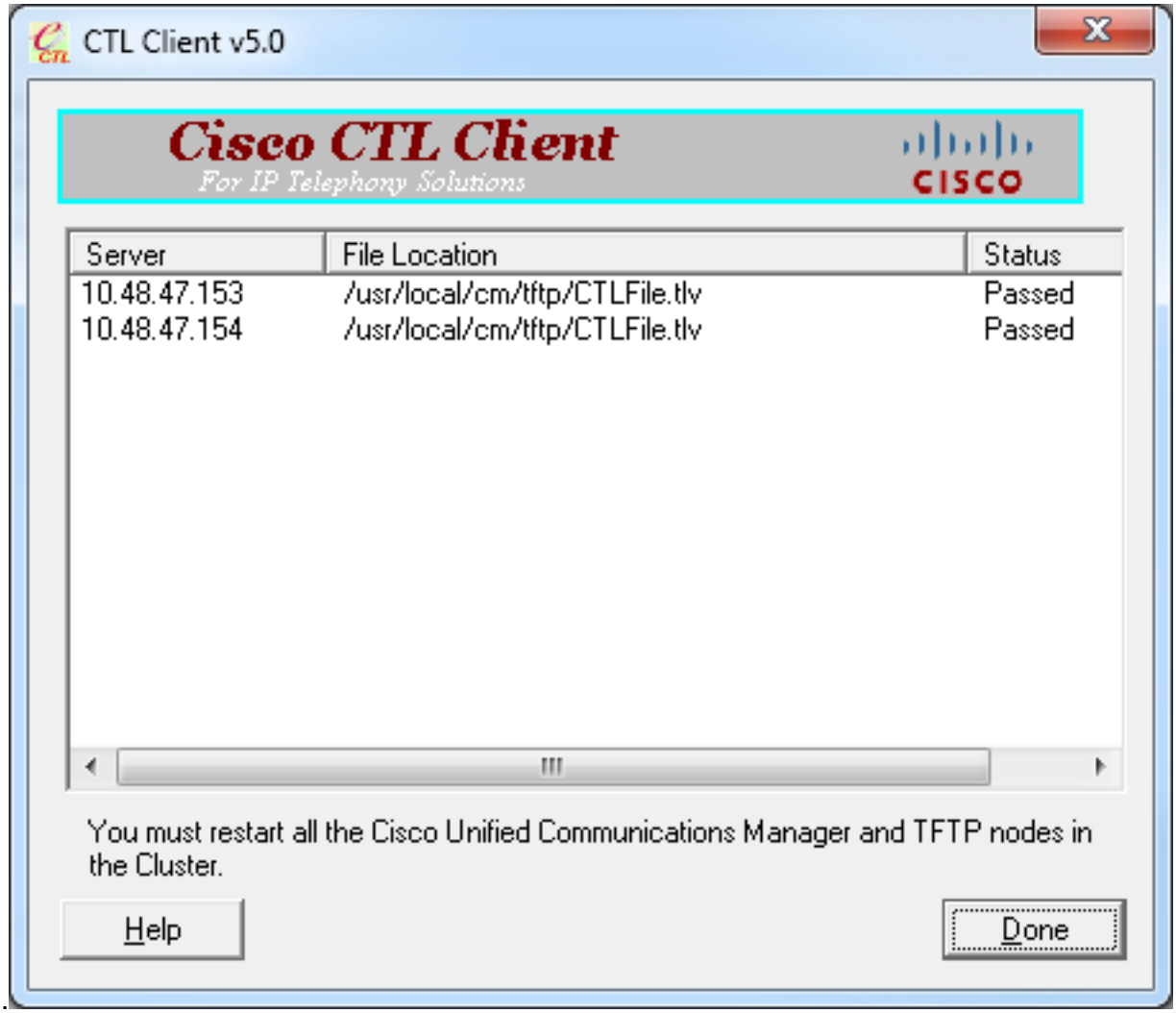


CTL.

10. Dans le domaine de mot de passe symbolique, écrivez **Cisco123**. Cliquez sur **OK**.



11. Vous verrez la confirmation que le processus était réussi. Cliquez sur **fait** afin de confirmer et quitter le client



CTL.

12. Redémarrez Cisco TFTP suivi du service de CallManager (utilité > Tools > Control Center de Cisco Unified - comportez les services). Le nouveau fichier CTL devrait être généré. Sélectionnez la commande de **ctl d'exposition** pour la vérification.`admin:show ctl`

```
The checksum value of the CTL file:
68a954fba070bbcc3ff036e18716e351(MD5)
4f7a02b60bb5083baac46110f0c61eac2dceb0f7(SHA1)


Length of CTL file: 5728
The CTL File was last modified on Mon Mar 09 11:38:50 CET 2015
```

13. Supprimez le fichier CTL de chaque téléphone dans la batterie (cette procédure pourrait varier basé sur le type de téléphone - consultez s'il vous plaît la documentation pour des détails, tels que le Téléphone IP Cisco Unified 8961, le guide d'administration 9951, et 9971).Remarque: Les téléphones pourraient encore pouvoir s'enregistrer (dépendant sur les paramètres de sécurité au téléphone) et fonctionner sans procéder à l'étape 13. Cependant, ils auront le vieux fichier CTL installé. Il pourrait entraîner des questions si des Certificats sont régénérés, un autre serveur est ajouté à la batterie ou le matériel serveur est remplacé. Il n'est pas recommandé pour partir de la batterie dans cet état.
14. Déplacez la batterie Non-sécurisée. Voyez la modification la Sécurité de batterie CUCM du mode Non-sécurisé de mode mixte avec la section de client CTL pour des détails.

Dépannez

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