Exemple de configuration du cluster CUCM en mode mixte en mode non sécurisé

Contenu

Introduction

Le document décrit les étapes requises pour passer du mode de sécurité de Cisco Unified Communications Manager (CUCM) du mode mixte au mode non sécurisé. Elle montre également comment le contenu d'un fichier CTL (Certificate Trust List) est modifié une fois ce déplacement terminé.

Le changement du mode de sécurité CUCM se compose de trois parties principales :

1 bis. Exécutez le client CTL et sélectionnez la variante souhaitée du mode de sécurité.
1 ter. Entrez la commande CLI afin de sélectionner la variante souhaitée de Security Mode.
2. Redémarrez les services Cisco CallManager et Cisco TFTP sur tous les serveurs CUCM qui exécutent ces services.
3. Redémarrez tous les téléphones IP afin qu'ils puissent télécharger la version mise à jour du fichier CTL.

> **Note**: Si le mode de sécurité du cluster passe du mode mixte au mode non sécurisé, le fichier CTL existe toujours sur les serveurs et sur les téléphones, mais il ne contient aucun certificat CCM+TFTP (serveur). Étant donné que les certificats CCM+TFTP (serveur) n'existent pas dans le fichier CTL, cela oblige le téléphone à s'enregistrer comme non sécurisé avec CUCM.

Conditions préalables

Conditions requises

Cisco vous recommande d'avoir des connaissances au sujet de CUCM version 10.0 (1) ou version ultérieure. En outre, vérifiez que :

- Le service CTL Provider est actif et s'exécute sur tous les serveurs TFTP actifs du cluster. Par défaut, le service s'exécute sur le port TCP 2444, mais il peut être modifié dans la configuration du paramètre de service CUCM.
- Les services CAPF (Certificate Authority Proxy Function) sont actifs et s'exécutent sur le noeud Éditeur.
- La réplication de base de données dans le cluster fonctionne correctement et les serveurs répliquent les données en temps réel.

Components Used

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

- CUCM version 10.0.1.11900-2 cluster de deux noeuds
- Téléphone IP Cisco 7975 (enregistré avec le protocole SCCP (Skinny Call Control Protocol), version du microprogramme SCCP75.9-3-1SR3-1S)
- Deux jetons de sécurité Cisco sont nécessaires pour définir le cluster en mode mixte
- L'un des jetons de sécurité répertoriés précédemment est nécessaire pour définir le cluster en mode non sécurisé

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.

Informations générales

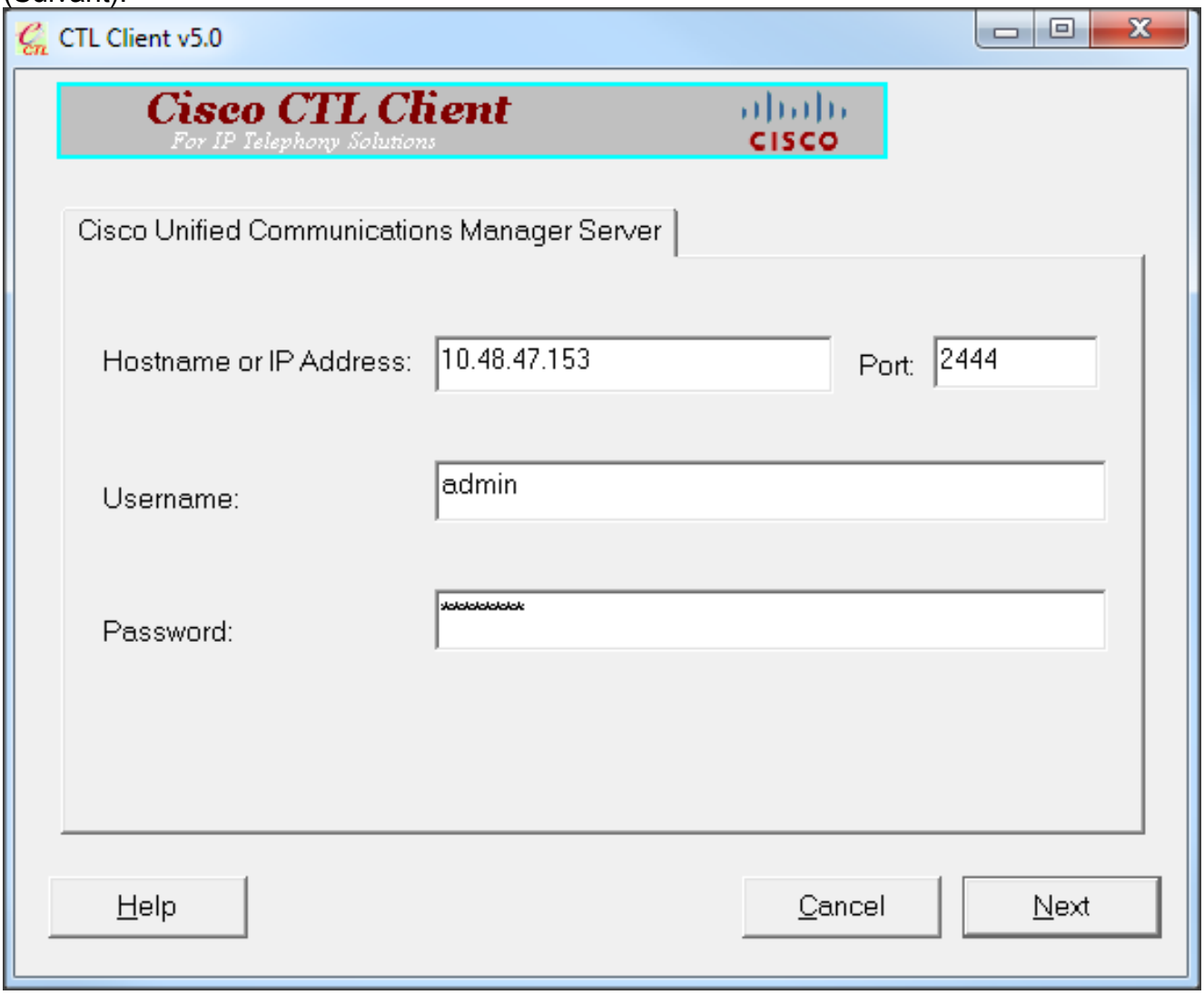
Pour exécuter le plug-in client CTL, vous devez avoir accès à au moins un jeton de sécurité inséré afin de créer ou de mettre à jour le dernier fichier CTL existant sur le serveur de publication CUCM. En d'autres termes, au moins un des certificats eToken qui existe dans le fichier CTL actuel sur CUCM doit se trouver sur le jeton de sécurité utilisé pour changer le mode de sécurité.

Configuration

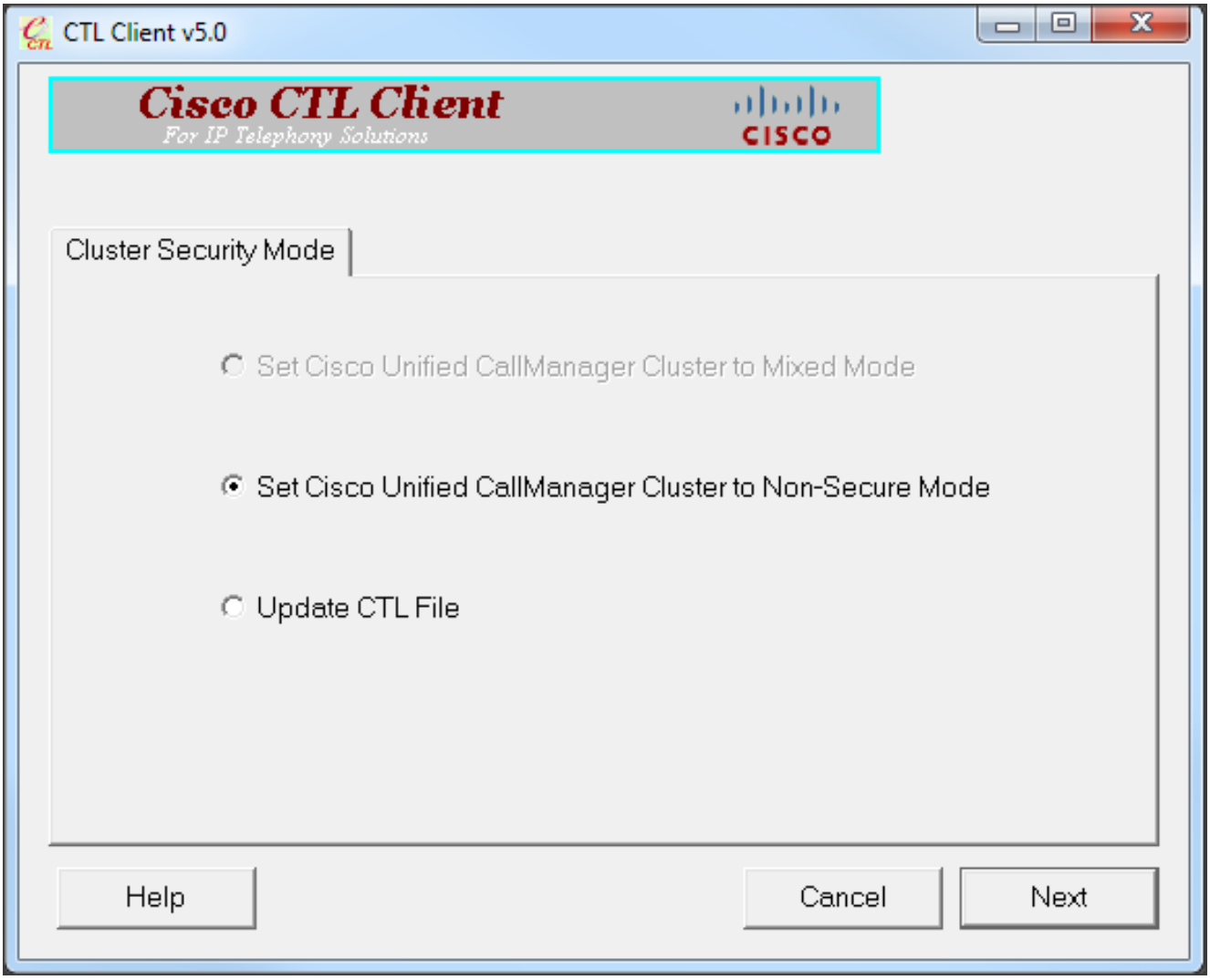
Modifier la sécurité du cluster CUCM du mode mixte au mode non sécurisé avec le client CTL

Complétez ces étapes afin de changer la sécurité du cluster CUCM du mode Mixed au mode Non-Secure avec le client CTL :

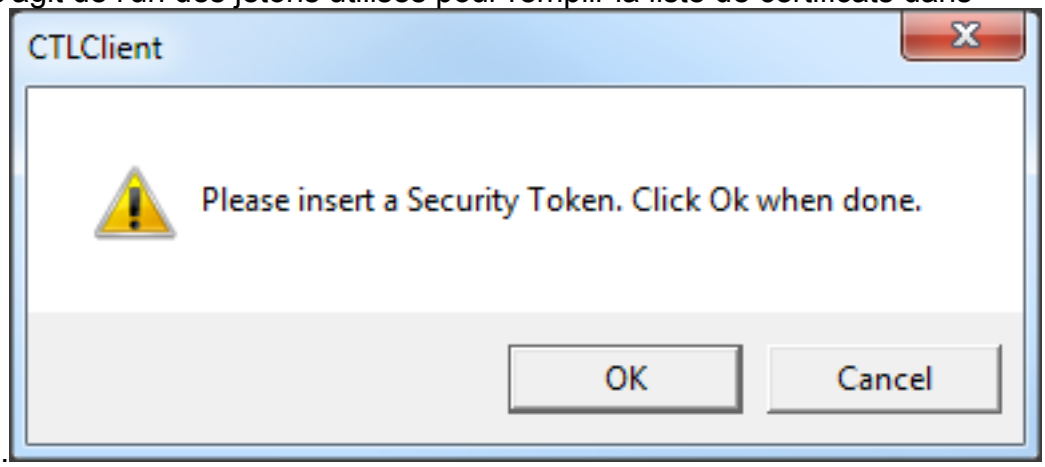
1. Obtenez un jeton de sécurité que vous avez inséré pour configurer le dernier fichier CTL.
2. Exécutez le client CTL. Indiquez le nom d'hôte/l'adresse IP du CUCM Pub et les informations d'identification de l'administrateur CCM. Cliquez sur **Next** (Suivant).



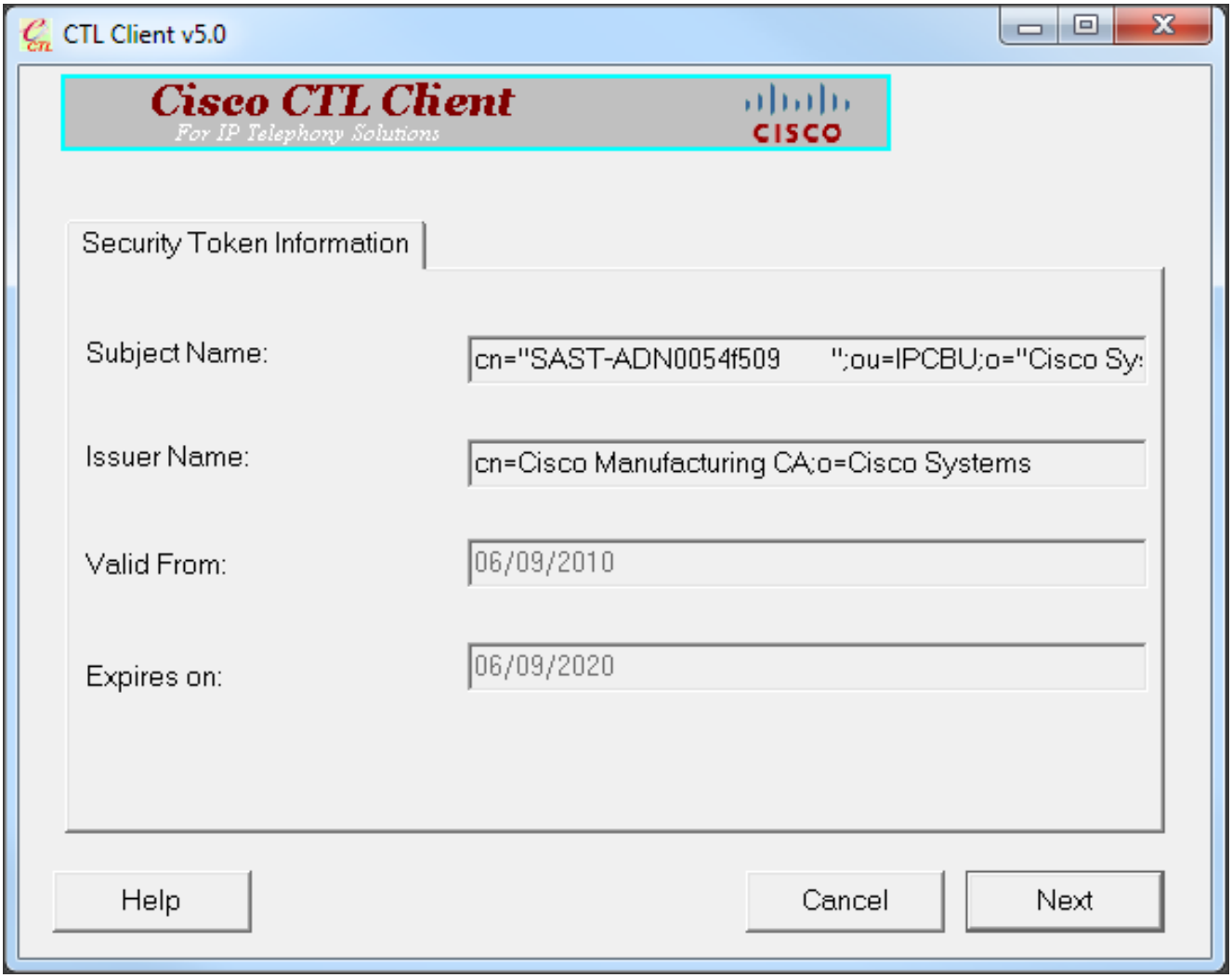
3. Activez la case d'option **Set Cisco Unified CallManager Cluster to Non-Secure Mode**. Cliquez sur **Next** (Suivant).



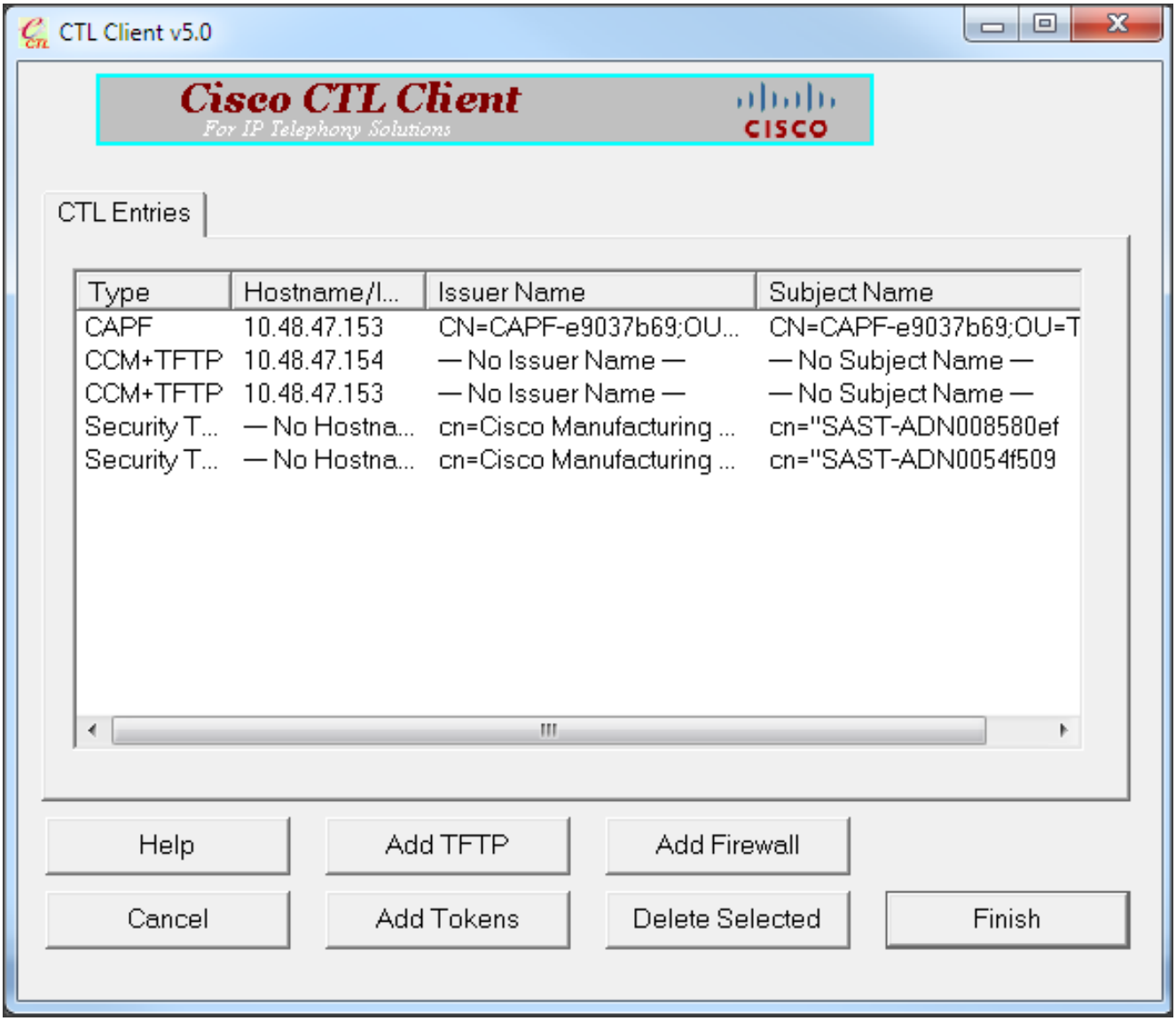
4. Insérez un jeton de sécurité qui a été inséré pour configurer le dernier fichier CTL et cliquez sur **OK**. Il s'agit de l'un des jetons utilisés pour remplir la liste de certificats dans CTLFile.tlv.



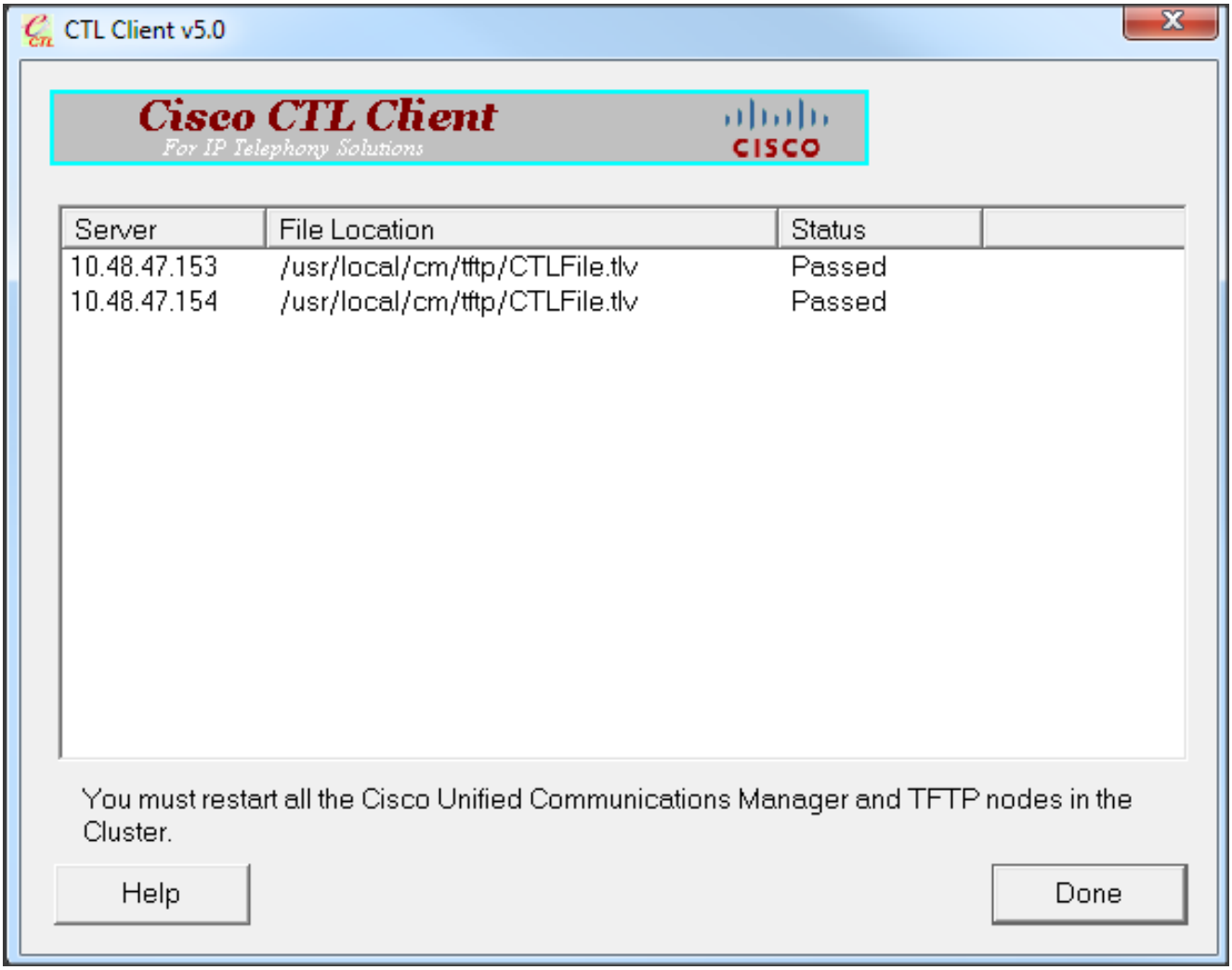
5. Les détails du jeton de sécurité s'affichent. Cliquez sur **Next** (Suivant).



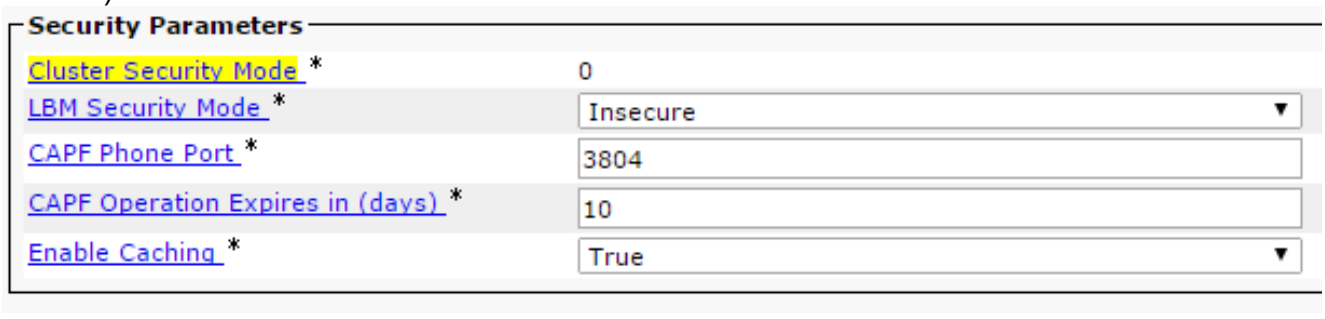
6. Le contenu du fichier CTL s'affiche. **Cliquez sur Finish.** Lorsque vous y êtes invité, saisissez **Cisco123**.



7. La liste des serveurs CUCM sur lesquels le fichier CTL existe s'affiche. Cliquez sur **Done**.



8. Choisissez **CUCM Admin Page > System > Enterprise Parameters** et vérifiez que le cluster a été défini sur Non-Secure Mode ("0" indique Non-Secure).



9. Redémarrez les services TFTP et Cisco CallManager sur tous les noeuds du cluster qui exécutent ces services.
10. Redémarrez tous les téléphones IP afin qu'ils puissent obtenir la nouvelle version du fichier CTL à partir du serveur TFTP CUCM.

Passer la sécurité du cluster CUCM du mode mixte au mode non sécurisé avec l'interface de ligne de commande

Cette configuration est uniquement disponible pour CUCM version 10.X et ultérieure. Afin de définir le mode CUCM Cluster Security sur Non-Secure, entrez la commande **utils ctl set-cluster**

non-secure-mode sur l'interface de ligne de commande du serveur de publication. Une fois cette opération terminée, redémarrez les services TFTP et Cisco CallManager sur tous les noeuds du cluster qui exécutent ces services.

Voici un exemple de sortie CLI qui montre 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:
```

Vérification

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

Pour vérifier le fichier CTLFIle.tlv, vous pouvez utiliser l'une des deux méthodes suivantes :

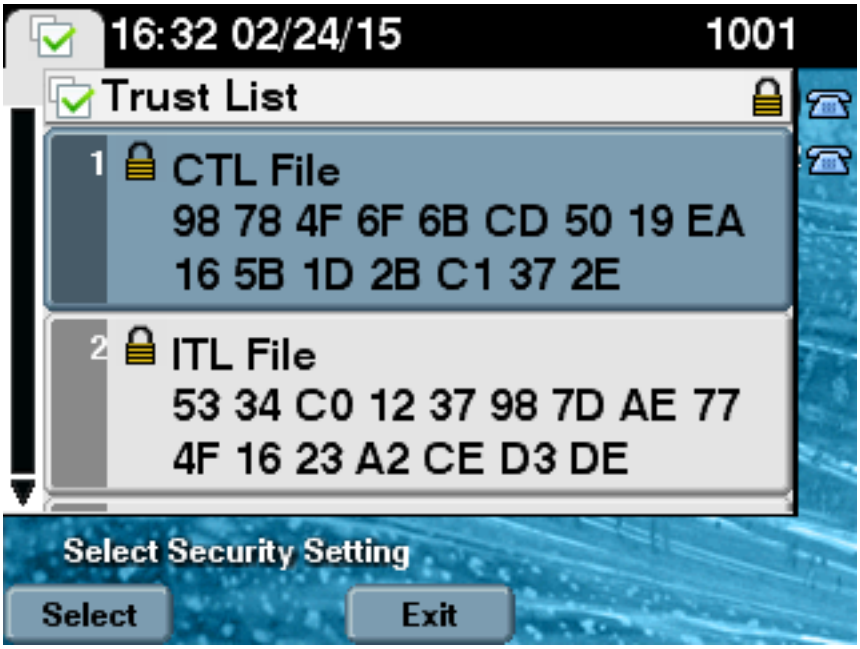
- Afin de vérifier le contenu et la somme de contrôle MD5 du fichier CTLFIle.tlv présent du côté TFTP de CUCM, entrez la commande **show ctl** sur l'interface de ligne de commande de CUCM. Le fichier CTLFIle.tlv doit être identique sur tous les noeuds CUCM.
- Afin de vérifier la somme de contrôle MD5 sur le téléphone IP 7975, choisissez **Settings > Security Configuration > Trust List > CTL File**.

  Note: Lorsque vous cochez la somme de contrôle sur le téléphone, vous voyez soit MD5 soit SHA1, selon le type de téléphone.

Cluster CUCM défini en mode de sécurité - Somme de contrôle du fichier CTL

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

Du côté du téléphone IP, vous pouvez voir que le même fichier CTL est installé (la somme de contrôle MD5 correspond à la sortie de CUCM).



Cluster CUCM défini en mode non sécurisé - Contenu du fichier CTL

Voici un exemple de fichier CTL d'un cluster CUCM défini en mode non sécurisé. Vous pouvez constater que les certificats CCM+TFTP sont vides et ne contiennent aucun contenu. Les autres certificats des fichiers CTL ne sont pas modifiés et sont exactement les mêmes que lorsque CUCM a été défini en 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
```

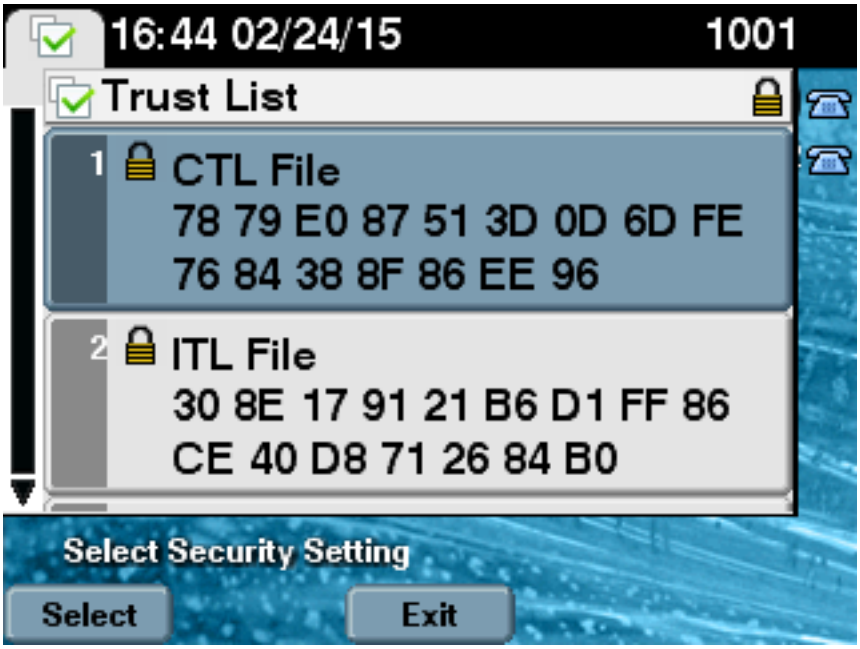
```
7 PUBLICKEY 140
9 CERTIFICATE 680 A0 A6 FC F5 FE 86 16 C1 DD D5 B7 57 38 9A 03 1C F7 7E FC 07 (SHA1 Hash HEX)
10 IPADDRESS 4

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 du téléphone IP, après avoir redémarré et téléchargé la version mise à jour du fichier CTL, vous pouvez voir que la somme de contrôle MD5 correspond à la sortie de CUCM.



Placez la sécurité du cluster CUCM du mode mixte au mode non sécurisé en cas de perte de jetons USB

Les jetons de sécurité des clusters sécurisés peuvent être perdus. Dans ce cas, vous devez envisager les deux scénarios suivants :

- Le cluster exécute la version 10.0.1 ou ultérieure
- Le cluster exécute une version antérieure à 10.x

Dans le premier scénario, complétez la procédure décrite dans la section Modifier la sécurité du cluster CUCM du mode mixte au mode non sécurisé avec l'interface de ligne de commande afin de récupérer du problème. Comme cette commande CLI ne nécessite pas de jeton CTL, elle peut être utilisée même si le cluster a été mis en mode mixte avec le client CTL.

La situation devient plus complexe lorsqu'une version antérieure à 10.x de CUCM est utilisée. Si vous perdez ou oubliez le mot de passe de l'un des jetons, vous pouvez toujours utiliser l'autre pour exécuter le client CTL avec les fichiers CTL actuels. Il est fortement recommandé d'obtenir

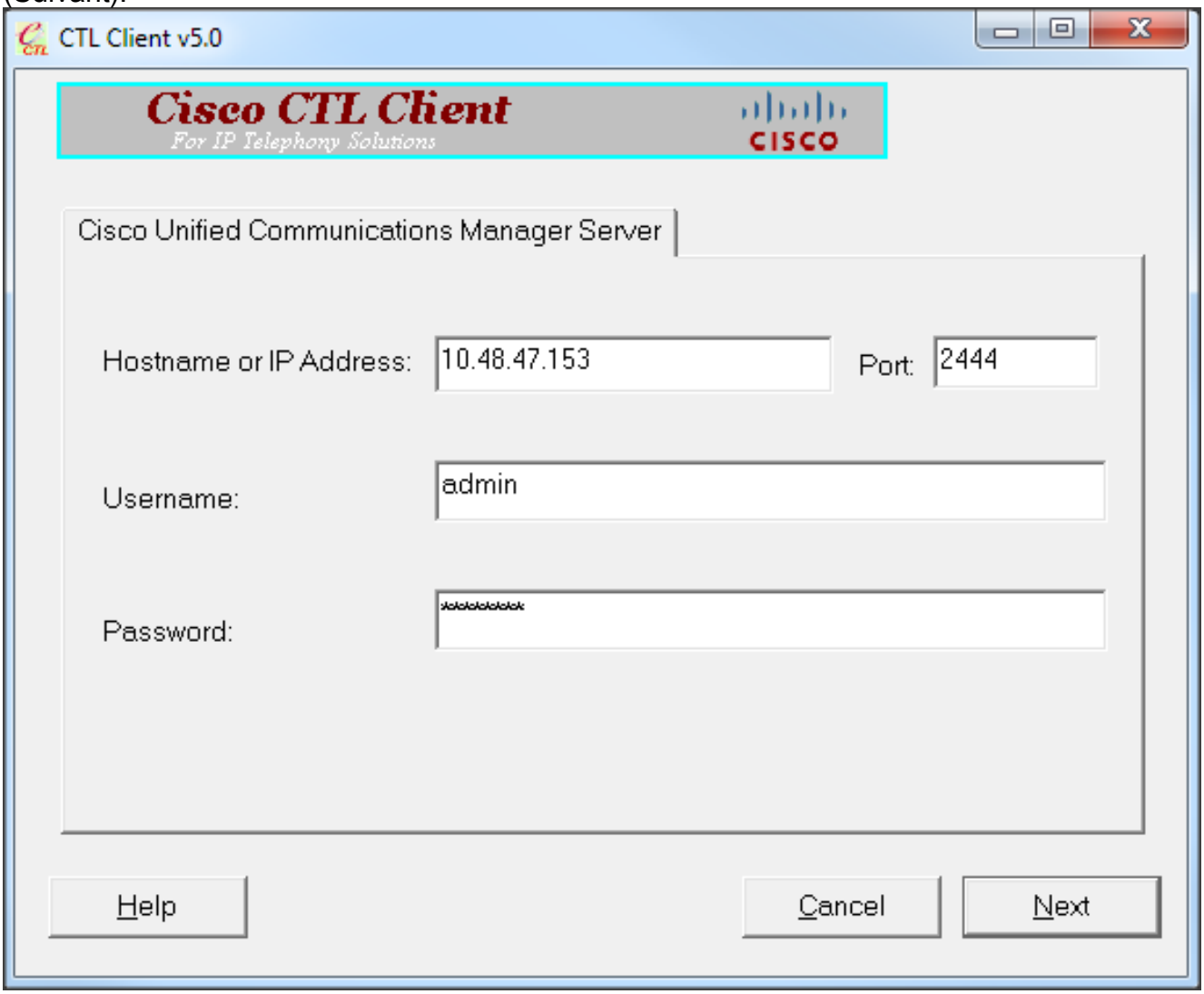
un autre eToken et de l'ajouter au fichier CTL dès que possible pour des raisons de redondance. Si vous perdez ou oubliez les mots de passe de tous les eTokens répertoriés dans votre fichier CTL, vous devez obtenir une nouvelle paire d'eTokens et exécuter une procédure manuelle comme expliqué ici.

1. Entrez la commande **file delete tftp CTLFile.tlv** afin de supprimer le fichier CTL de tous les serveurs TFTP.

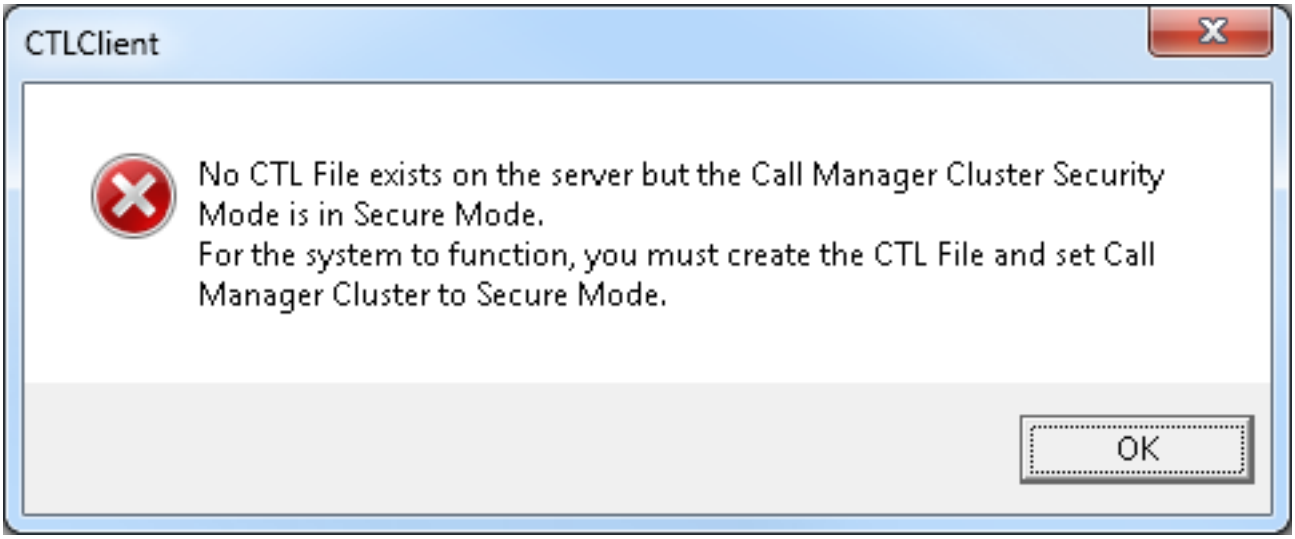
```
admin:file delete tftp CTLFile.tlv
Delete the File CTLFile.tlv?
Enter "y" followed by return to continue: y
files: found = 1, deleted = 1

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.
```

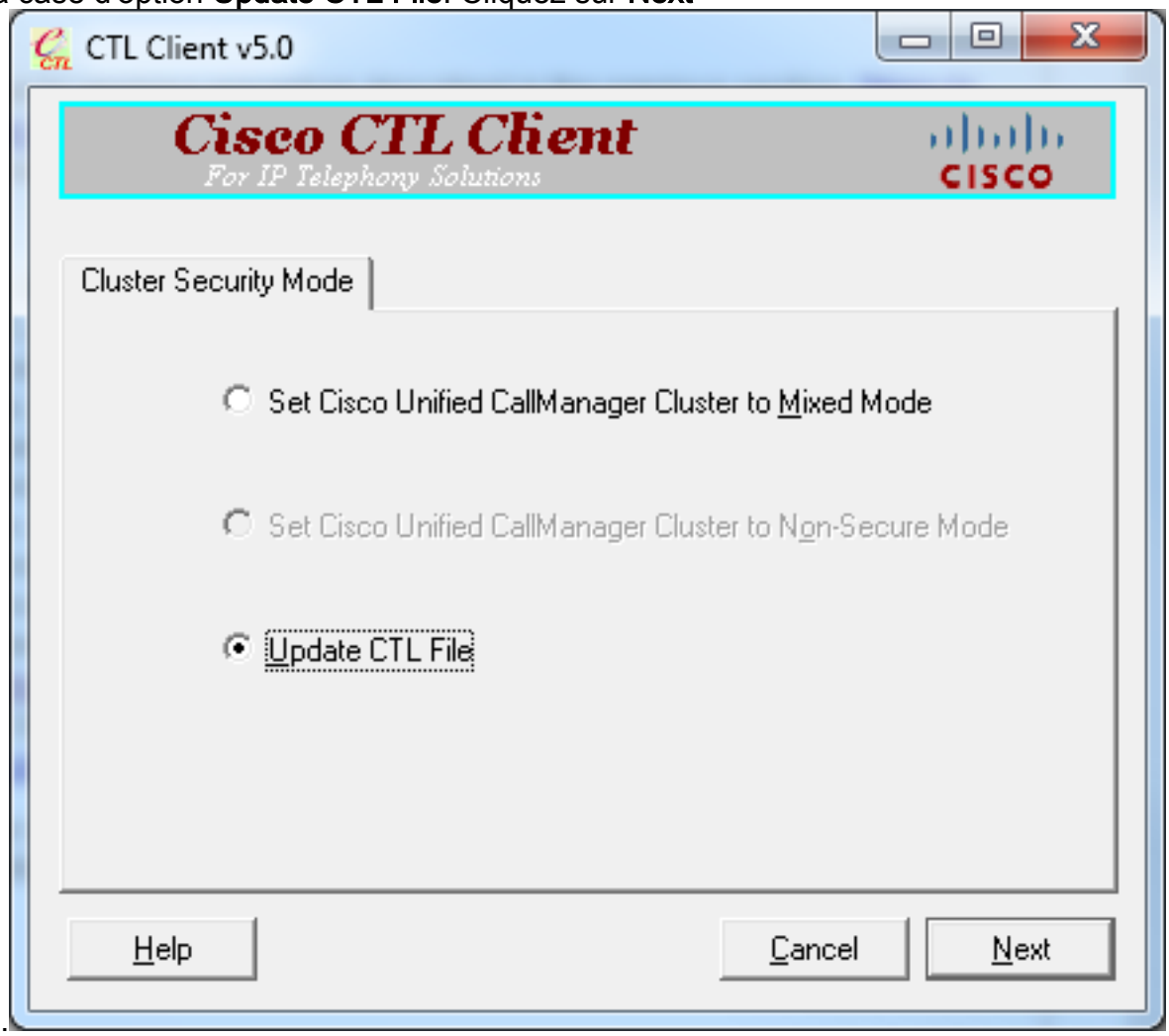
2. Exécutez le client CTL. Saisissez le nom d'hôte/l'adresse IP du CUCM Pub et les informations d'identification de l'administrateur CCM. Cliquez sur **Next** (Suivant).



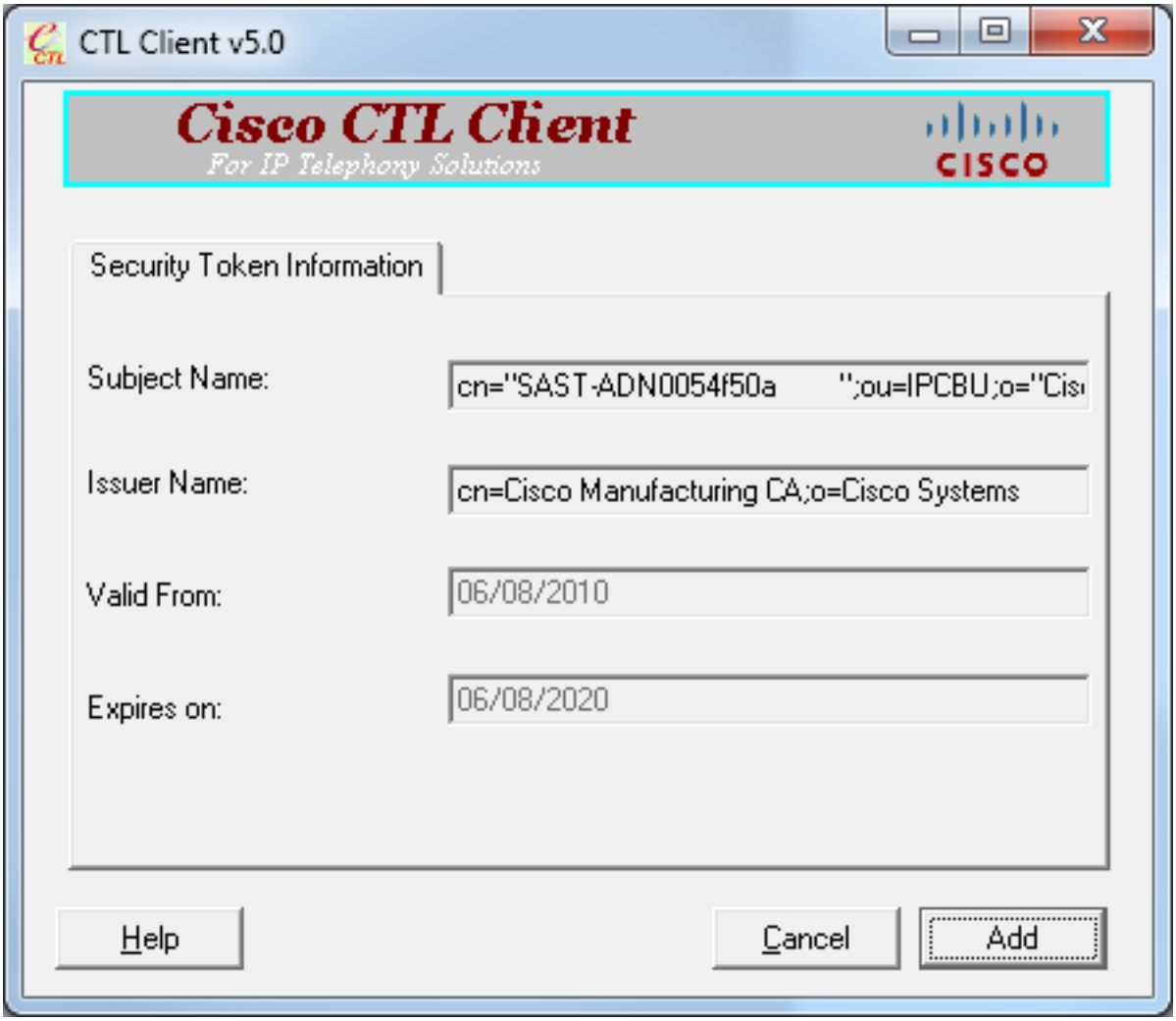
3. Étant donné que le cluster est en mode Mixed, mais qu'aucun fichier CTL n'existe sur Publisher, cet avertissement s'affiche. Cliquez sur **OK** afin de l'ignorer et continuer.



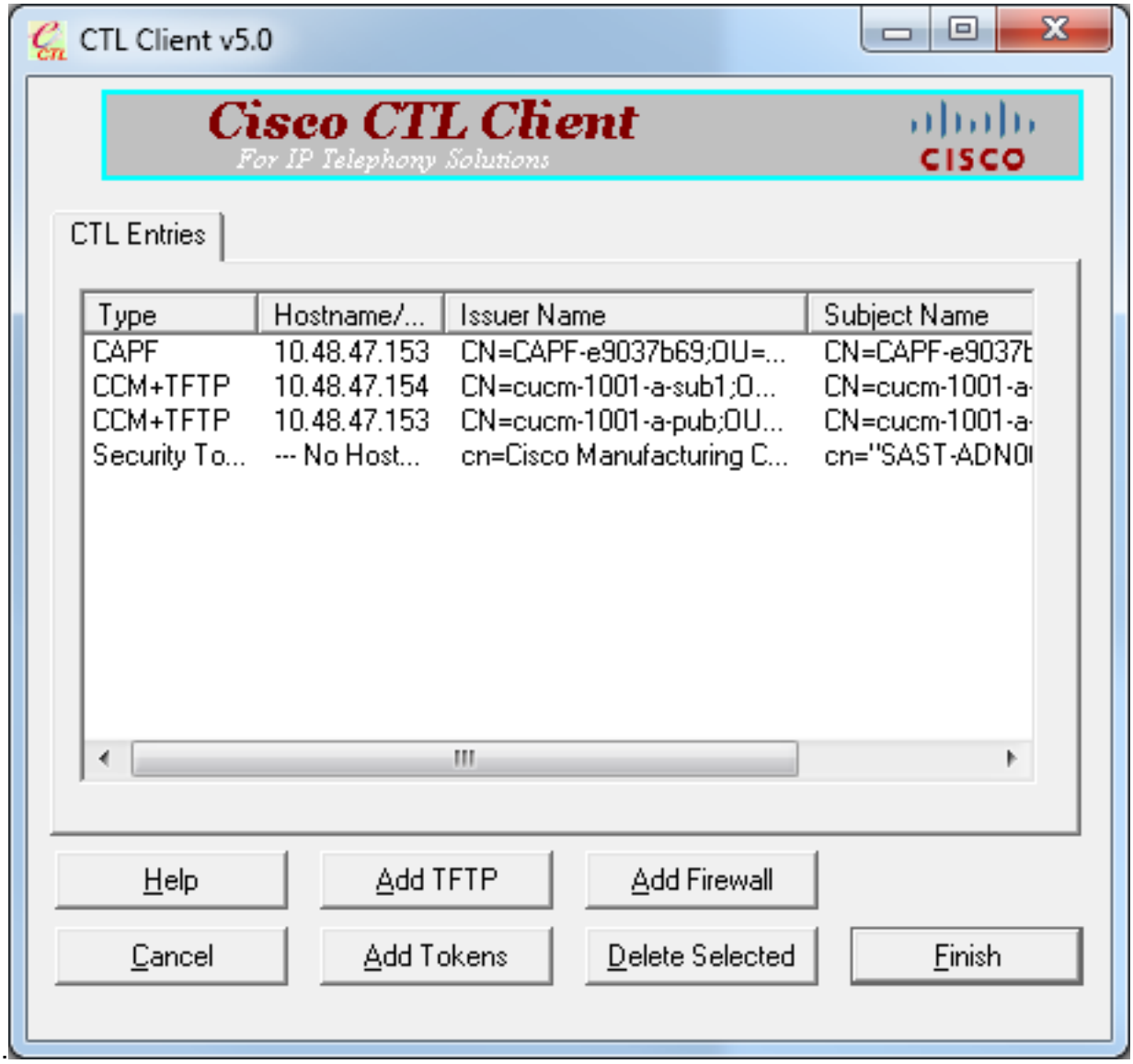
4. Activez la case d'option **Update CTL File**. Cliquez sur **Next** (Suivant).



5. Le client CTL demande à ajouter un jeton de sécurité. Cliquez sur **Add** afin de continuer.

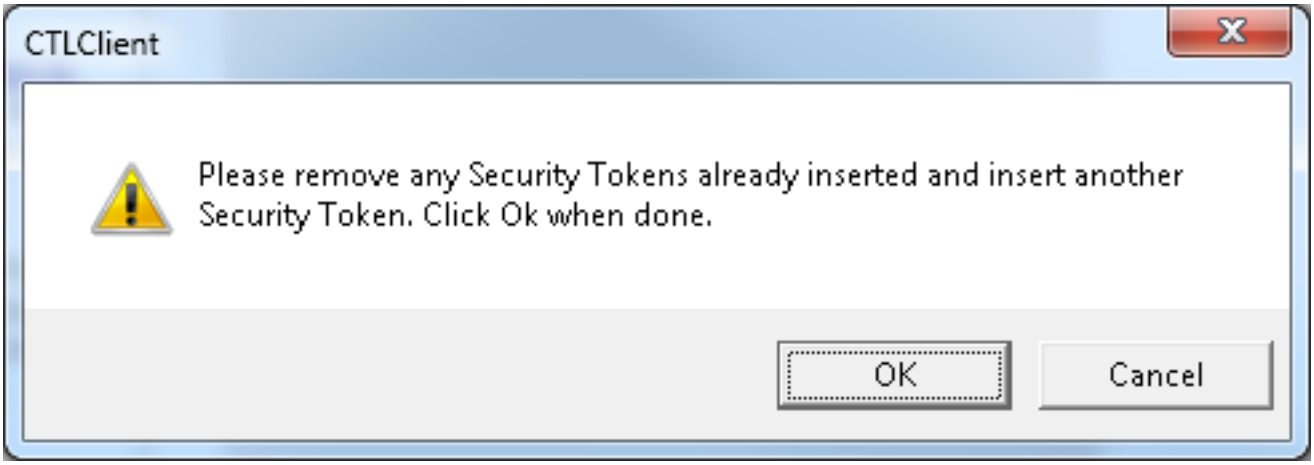


6. L'écran affiche toutes les entrées de la nouvelle CTL. Cliquez sur **Add Tokens** afin d'ajouter le deuxième jeton de la nouvelle

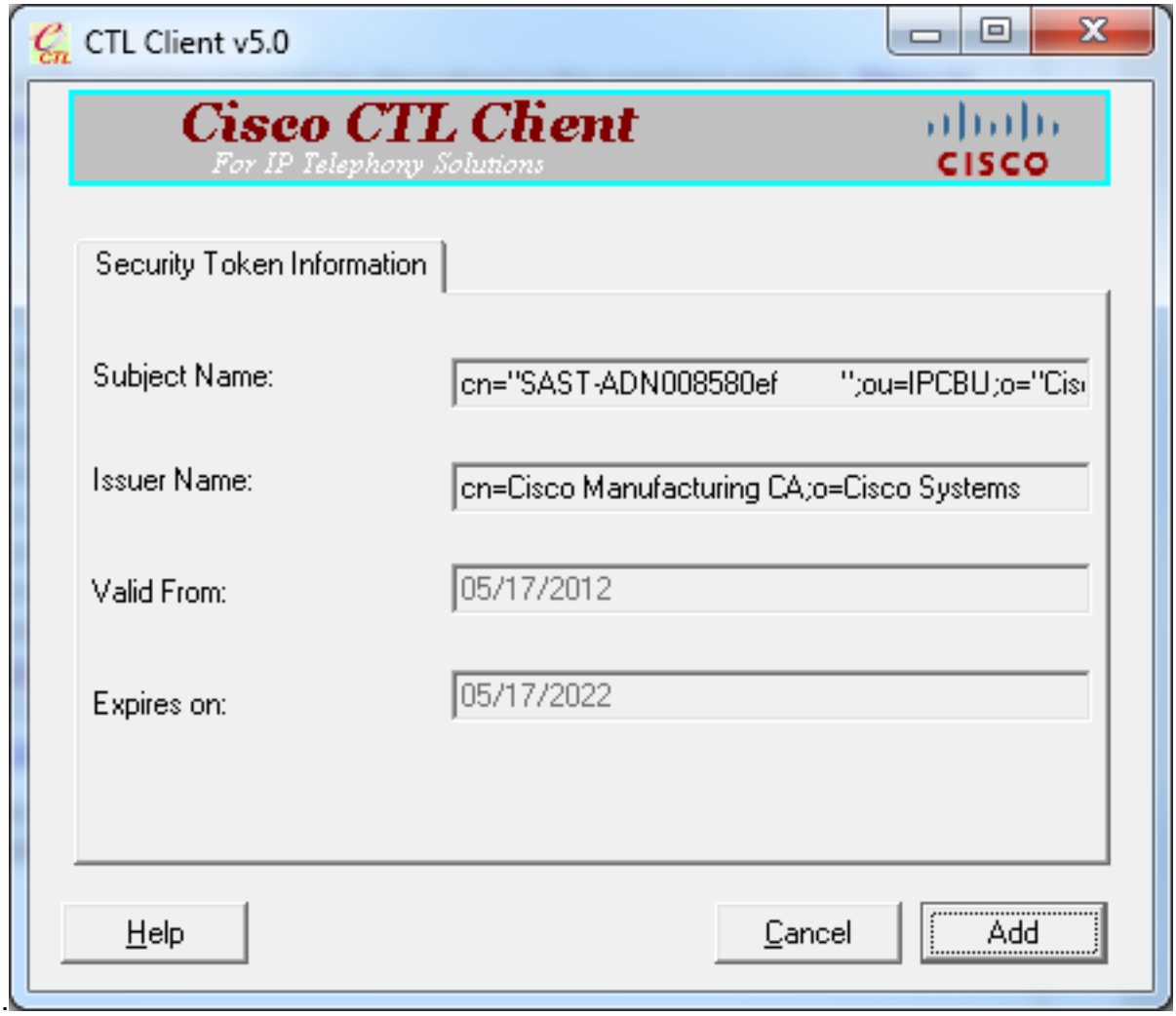


paire.

7. Vous serez invité à supprimer le jeton actuel et à en insérer un nouveau. Cliquez sur **OK** une fois
terminé.

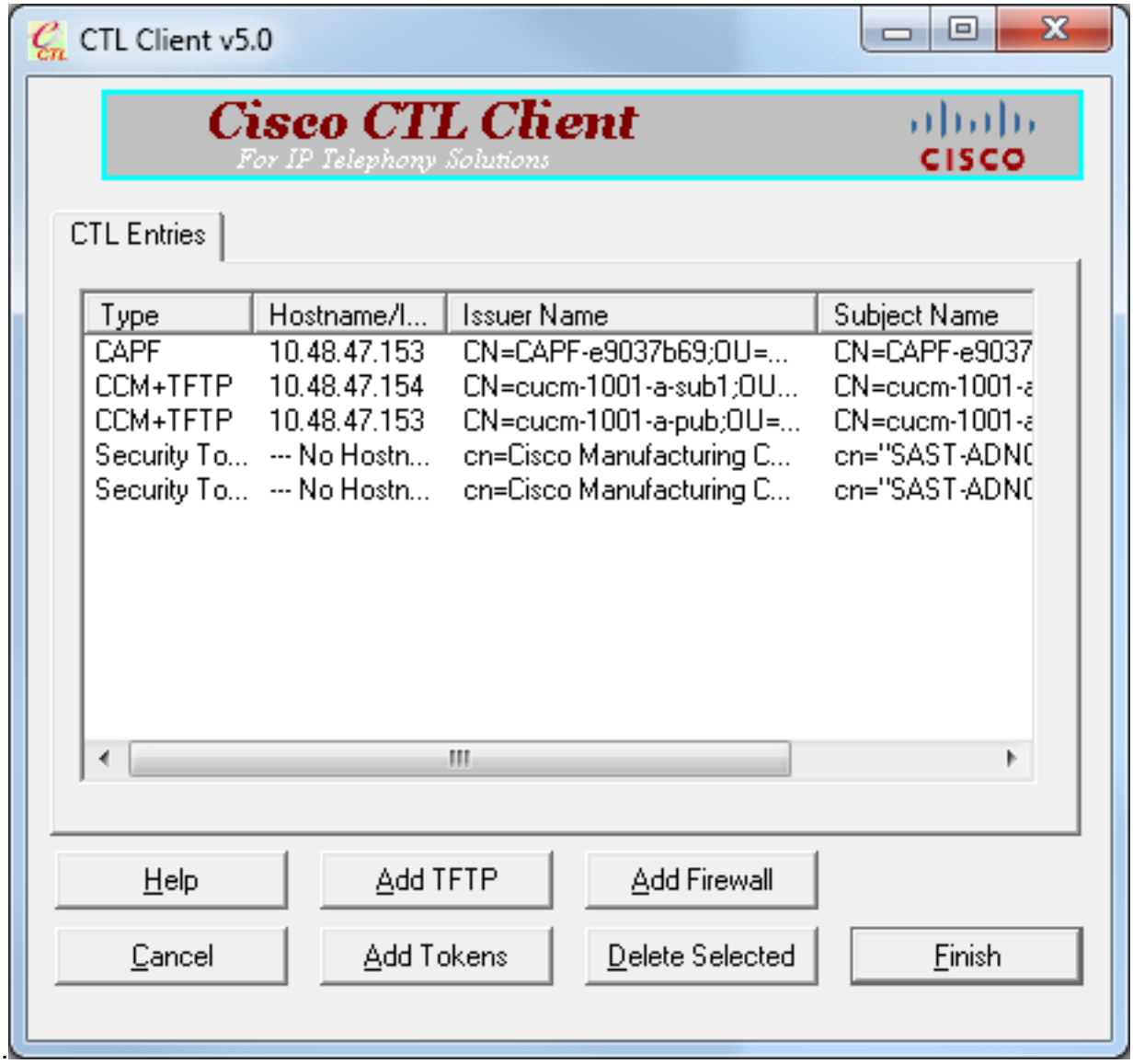


8. Un écran qui affiche les détails du nouveau jeton s'affiche. Cliquez sur **Add** afin de les confirmer et ajouter ce



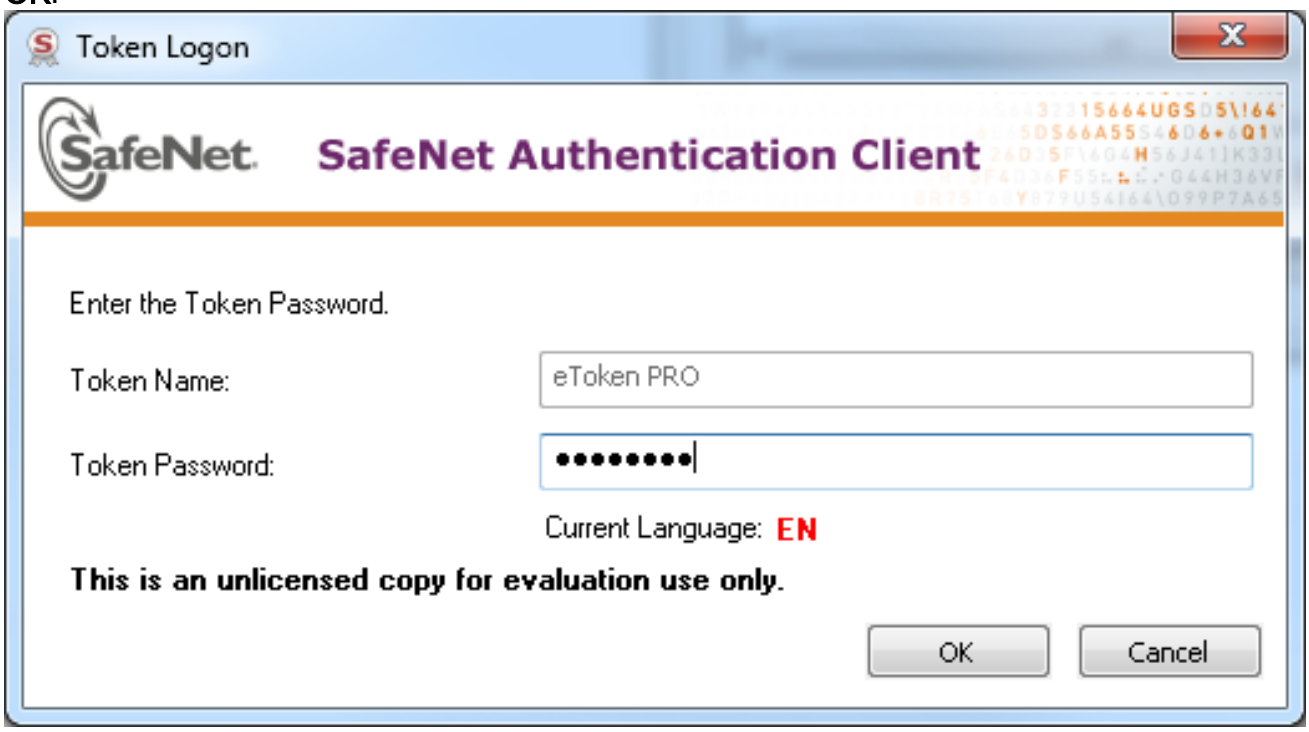
jeton.

9. Une nouvelle liste d'entrées CTL s'affiche et affiche les deux jetons ajoutés. Cliquez sur **Finish** afin de générer de nouveaux fichiers

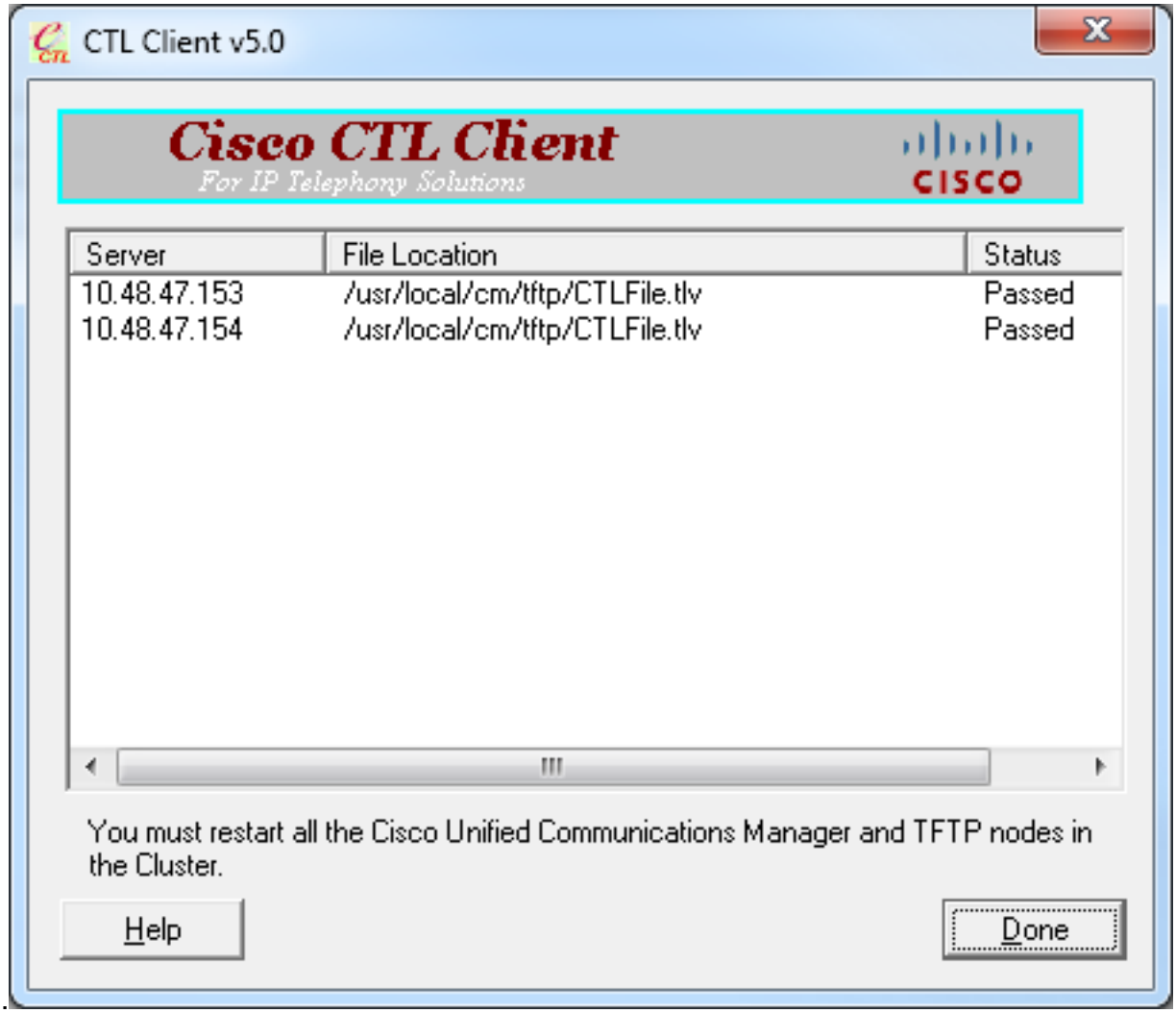


CTL.

10. Dans le champ Mot de passe de jeton, entrez **Cisco123**. Cliquez sur **OK**.



11. Vous verrez une confirmation que le processus a réussi. Cliquez sur **Done** afin de confirmer et quitter le client



CTL.

12. Redémarrez Cisco TFTP, puis le service CallManager (Cisco Unified Serviceability > Tools > Control Center - Feature Services). Le nouveau fichier CTL doit être généré. Entrez la commande **show ctl** 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 du cluster (cette procédure peut varier en fonction du type de téléphone. Pour plus d'informations, consultez la documentation, par exemple le Guide d'administration des téléphones IP Cisco Unified 8961, 9951 et 9971).**Note**: Les téléphones peuvent toujours être en mesure de s'enregistrer (en fonction des paramètres de sécurité du téléphone) et de fonctionner sans passer à l'étape 13. Toutefois, l'ancien fichier CTL sera installé. Cela peut entraîner des problèmes si les certificats sont régénérés, si un autre serveur est ajouté au cluster ou si le matériel du serveur est remplacé. Il n'est pas recommandé de laisser le cluster dans cet état.
14. Déplacez le cluster vers Non-Secure. Pour plus d'informations, consultez la section Modifier la sécurité du cluster CUCM du mode mixte au mode non sécurisé avec le client CTL.

Dépannage

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