

CUCM Cluster geconverteerd van gemengde modus naar niet-beveiligde modus

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Verander de CUCM Cluster Security van gemengde modus in niet-beveiligde modus met de CTL-client](#)

[Verander de CUCM Cluster Security van gemengde modus in niet-beveiligde modus met de CLI](#)

[Verifiëren](#)

[CUCM Cluster ingesteld op Security Mode - CTL-checksum voor bestanden](#)

[CUCM Cluster ingesteld op niet-beveiligde modus - CTL-inhoud](#)

[Plaats de CUCM Cluster Security van gemengde mode in niet-beveiligde modus wanneer USB-penningen verloren zijn](#)

[Problemen oplossen](#)

Inleiding

Het document beschrijft de stappen die vereist zijn om de beveiligingsmodus van Cisco Unified Communications Manager (CUCM) te wijzigen van gemengde modus in niet-beveiligde modus. Het toont ook hoe de inhoud van een dossier van de Vertrouwen van het Certificaat (CTL) wordt veranderd wanneer deze beweging wordt voltooid.

Er zijn drie belangrijke onderdelen om de CUCM security modus te wijzigen:

- 1 bis. Start de CTL-client en selecteer de gewenste variant van Security Mode.
- 1 ter. Typ de CLI-opdracht om de gewenste variant van de beveiligingsmodus te selecteren.
2. Start Cisco CallManager en Cisco TFTP-services opnieuw op alle CUCM-servers die deze services uitvoeren.
3. Start alle IP-telefoons opnieuw, zodat ze de bijgewerkte versie van het CTL-bestand kunnen downloaden.

Opmerking: Als de clusterbeveiligingsmodus wordt gewijzigd van gemengde modus in niet-beveiligde modus, bestaat het CTL-bestand nog steeds op de server(s) en op de telefoons, maar het CTL-bestand bevat geen CCM+TFTP (server)-certificaten. Aangezien de CCM+TFTP (server) certificaten niet in het CTL bestand bestaan, dwingt dit de telefoon om als niet-veilig met CUCM te registreren.

Voorwaarden

Vereisten

Cisco raadt u aan om kennis te hebben van CUCM versie 10.0(1) of hoger. Zorg er bovendien voor dat:

- De CTL Provider service is opgezet en loopt op alle actieve TFTP-servers in de cluster. Standaard wordt de service uitgevoerd op TCP poort 2444, maar dit kan worden gewijzigd in de configuratie van CUCM Service Parameter.
- De Service Proxy-functie (CAPF) van de certificaatinstantie is ingeschakeld en werkt op het knooppunt van de uitgeverij.
- De (DB)-replicatie van de databank in de cluster werkt correct en de servers reproduceren gegevens in real-time.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- CUCM release 10.0.1.1900-2 cluster van twee knooppunten
- Cisco 7975 IP-telefoon (geregistreerd met Sony Call Control Protocol (SCCP), firmware versie SCCP75.9-3-1SR3-1S)
- Er zijn twee Cisco Security Tokens nodig om het cluster in de gemengde modus te zetten
- Een van de eerder genoemde Security Tokens is nodig om het cluster op niet-beveiligde modus in te stellen

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Om de CTL-clientstekker uit te voeren moet u toegang hebben tot ten minste één beveiligingstoken die is ingevoegd om het laatste CTL-bestand te maken of bij te werken, bestaat op de CUCM-server. Met andere woorden: ten minste één van de Token-certificaten die in het huidige CTL-bestand op CUCM bestaan, moet op het beveiligingstoken zijn dat wordt gebruikt om de beveiligingsmodus te wijzigen.

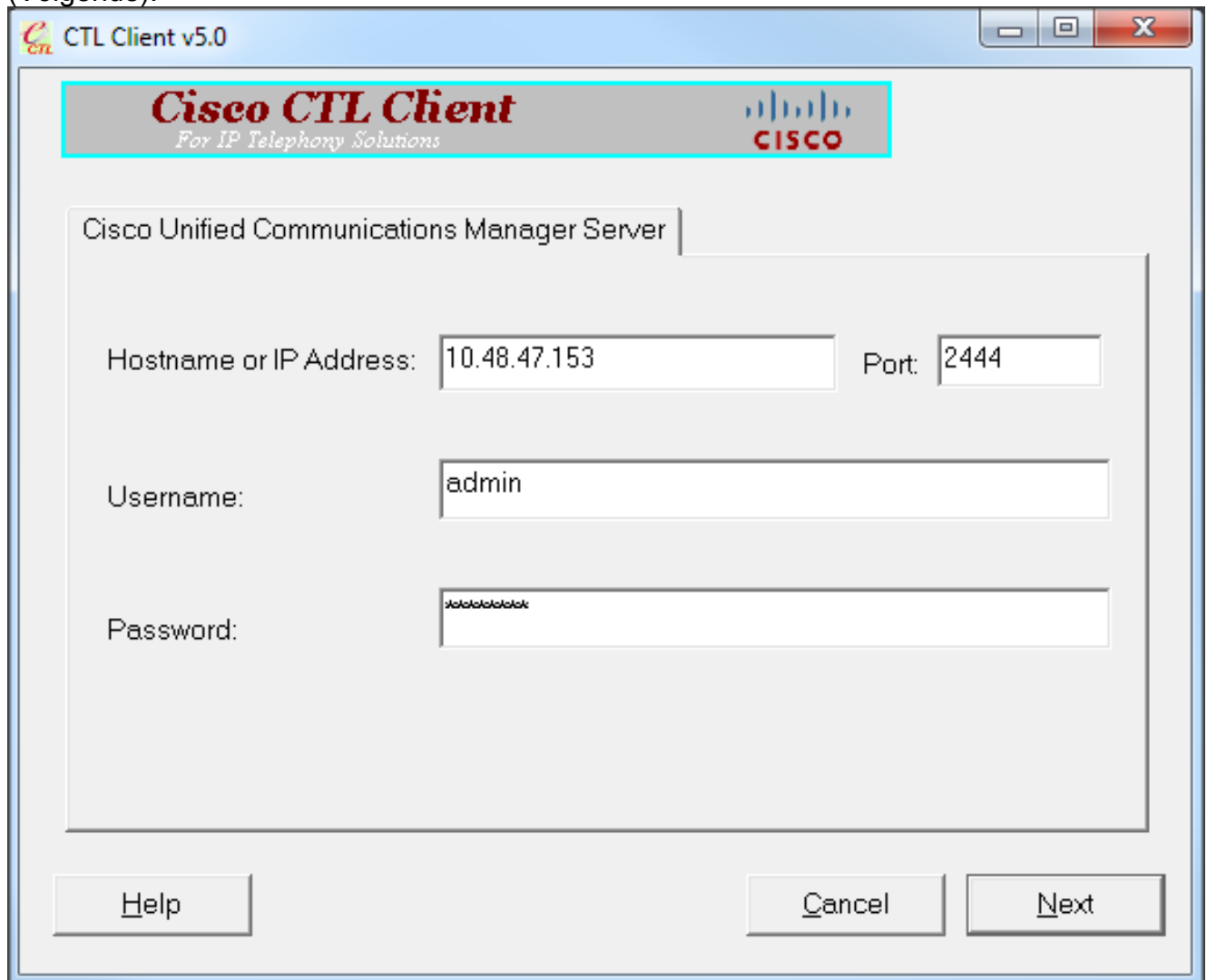
Configureren

Verander de CUCM Cluster Security van gemengde modus in niet-beveiligde modus met de CTL-client

Voltooi deze stappen om de CUCM-clusterbeveiliging van gemengde modus naar niet-beveiligde

modus met de CTL-client te wijzigen:

1. Verkrijg één veiligheidstoken die u hebt ingevoegd om het laatste CTL-bestand te configureren.
2. Start de CTL client. Geef de IP-hostnaam/het adres van de CUCM-functie en de CCM-Administrator-referenties op. Klik op **Next** (Volgende).



CTL Client v5.0

Cisco CTL Client
For IP Telephony Solutions

CISCO

Cisco Unified Communications Manager Server

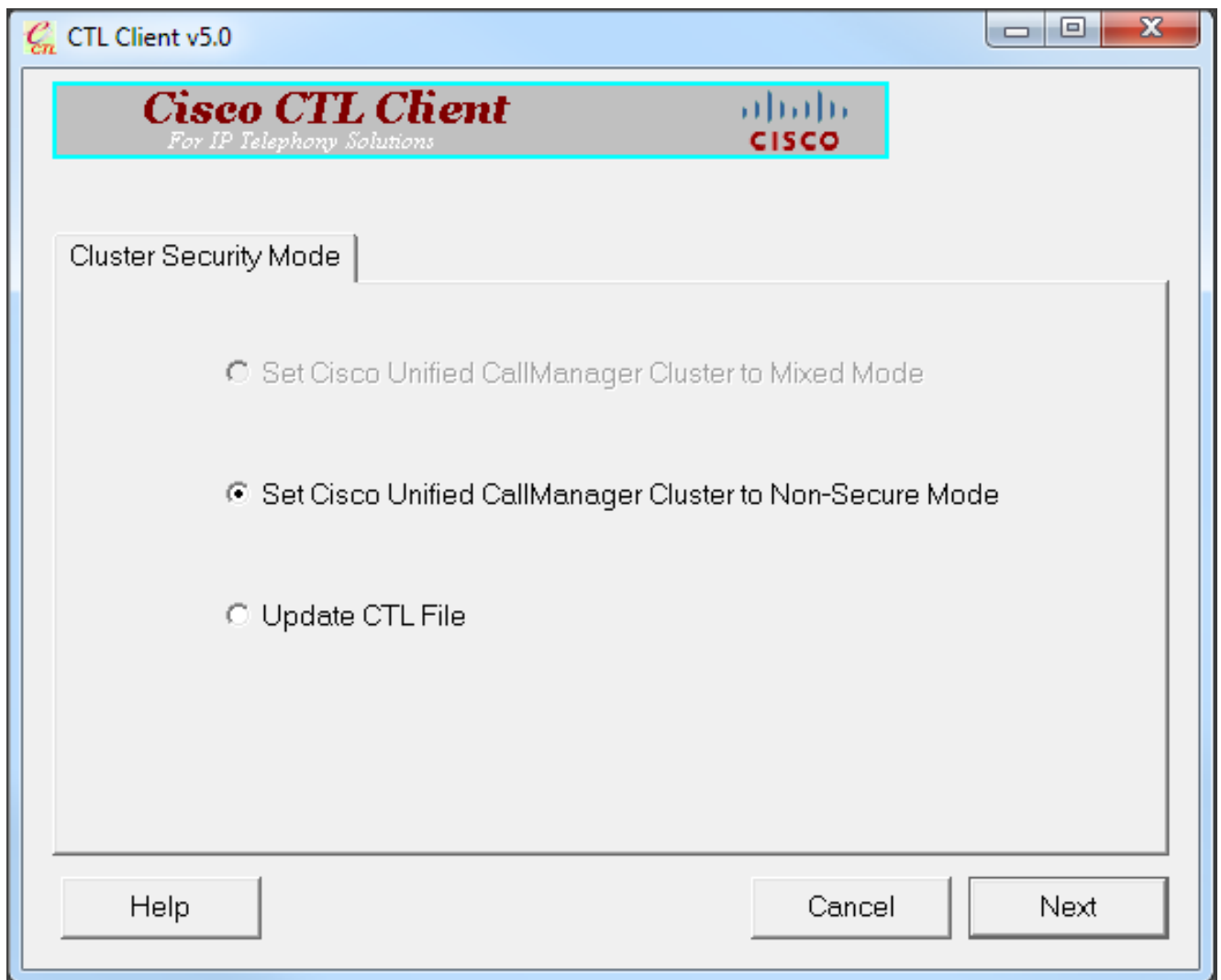
Hostname or IP Address: 10.48.47.153 Port: 2444

Username: admin

Password: *

Help Cancel Next

3. Klik op de radioknop **Instellen Cisco Unified CallManager Cluster op niet-beveiligde modus**. Klik op **Next** (Volgende).

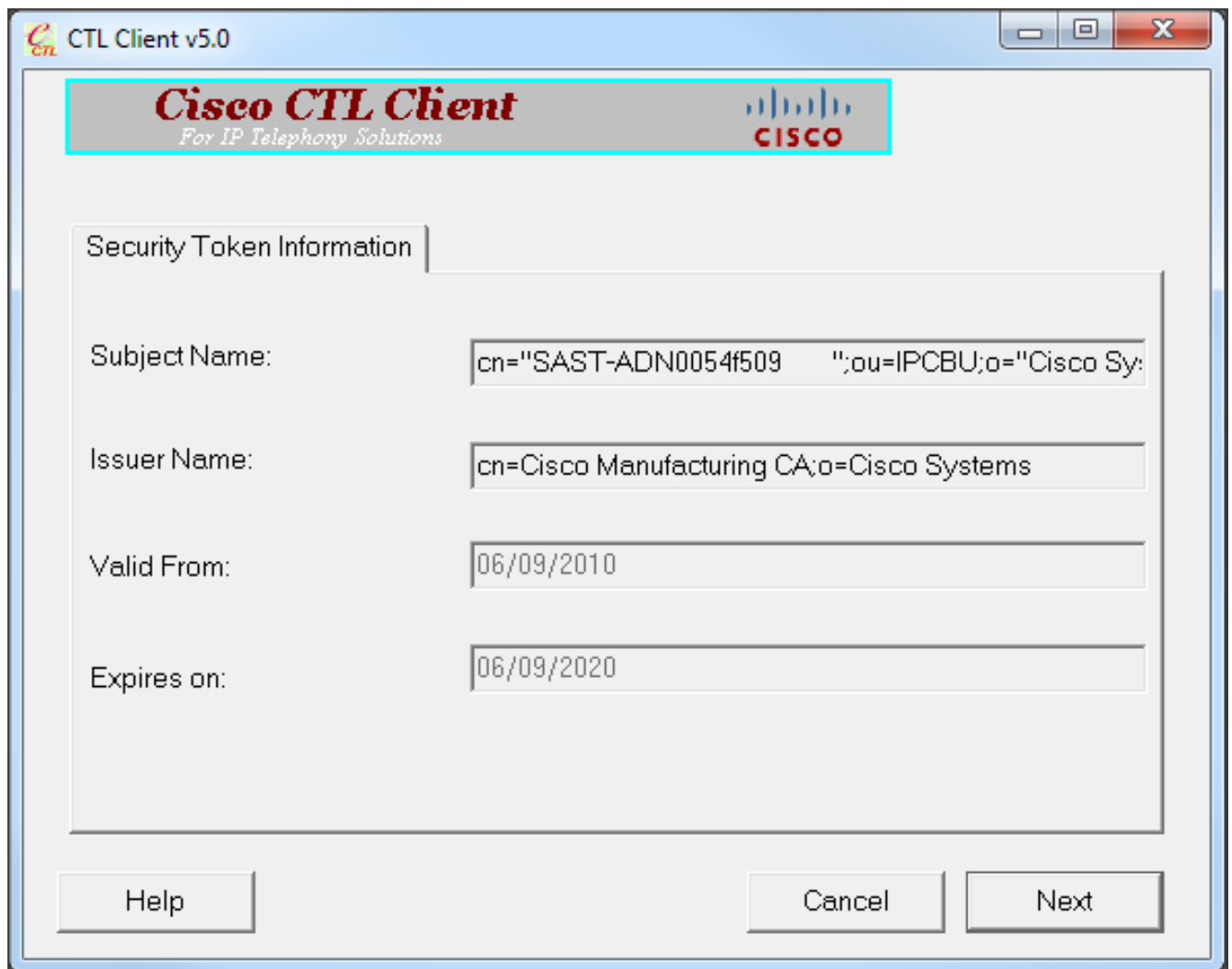


4. Steek één beveiligingstoken op die is ingevoegd om het laatste CTL-bestand te configureren en klik op **OK**. Dit is een van de penningen die werden gebruikt om de certificaatlijst in CTLFile.tlv op te

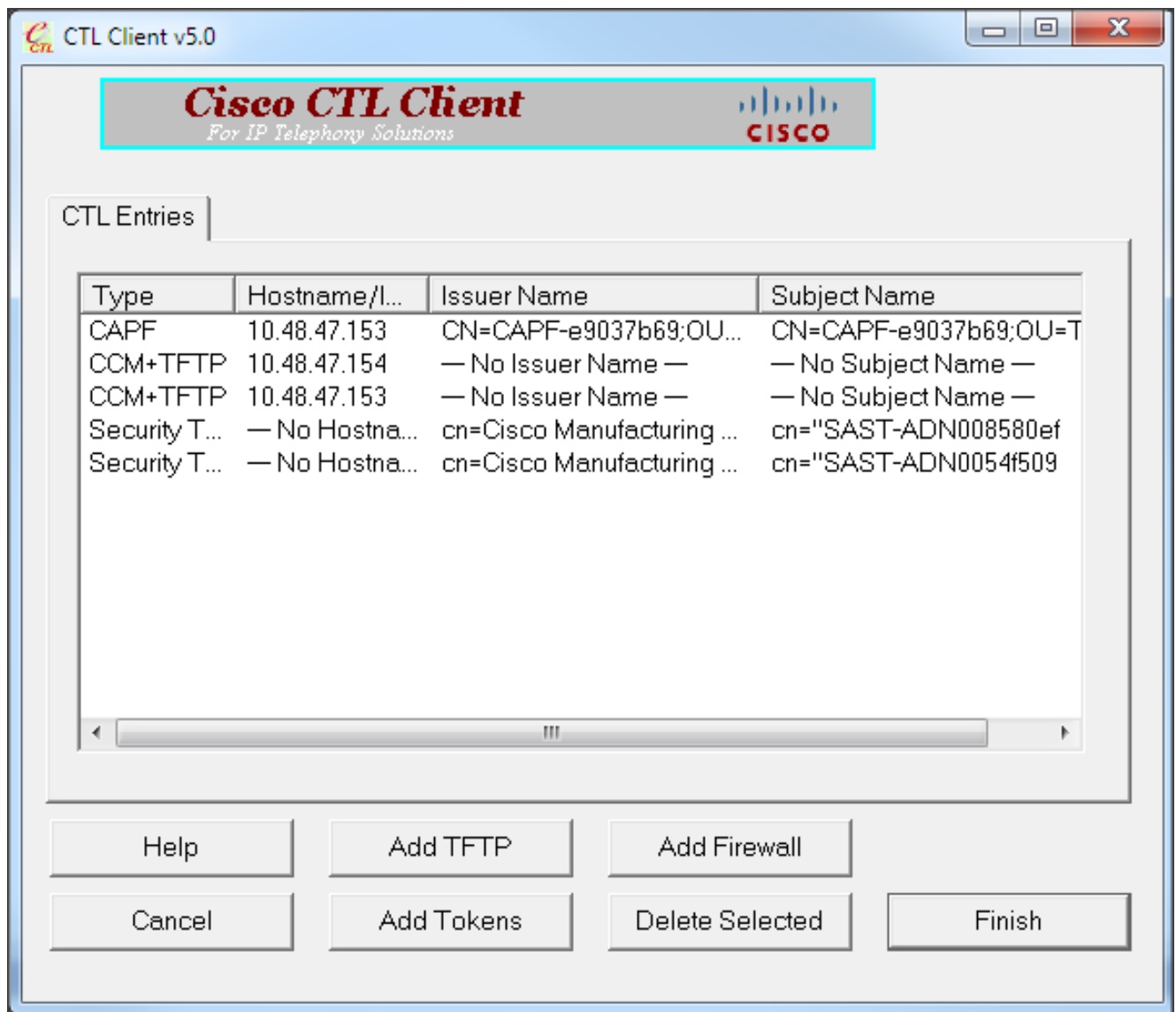


geven.

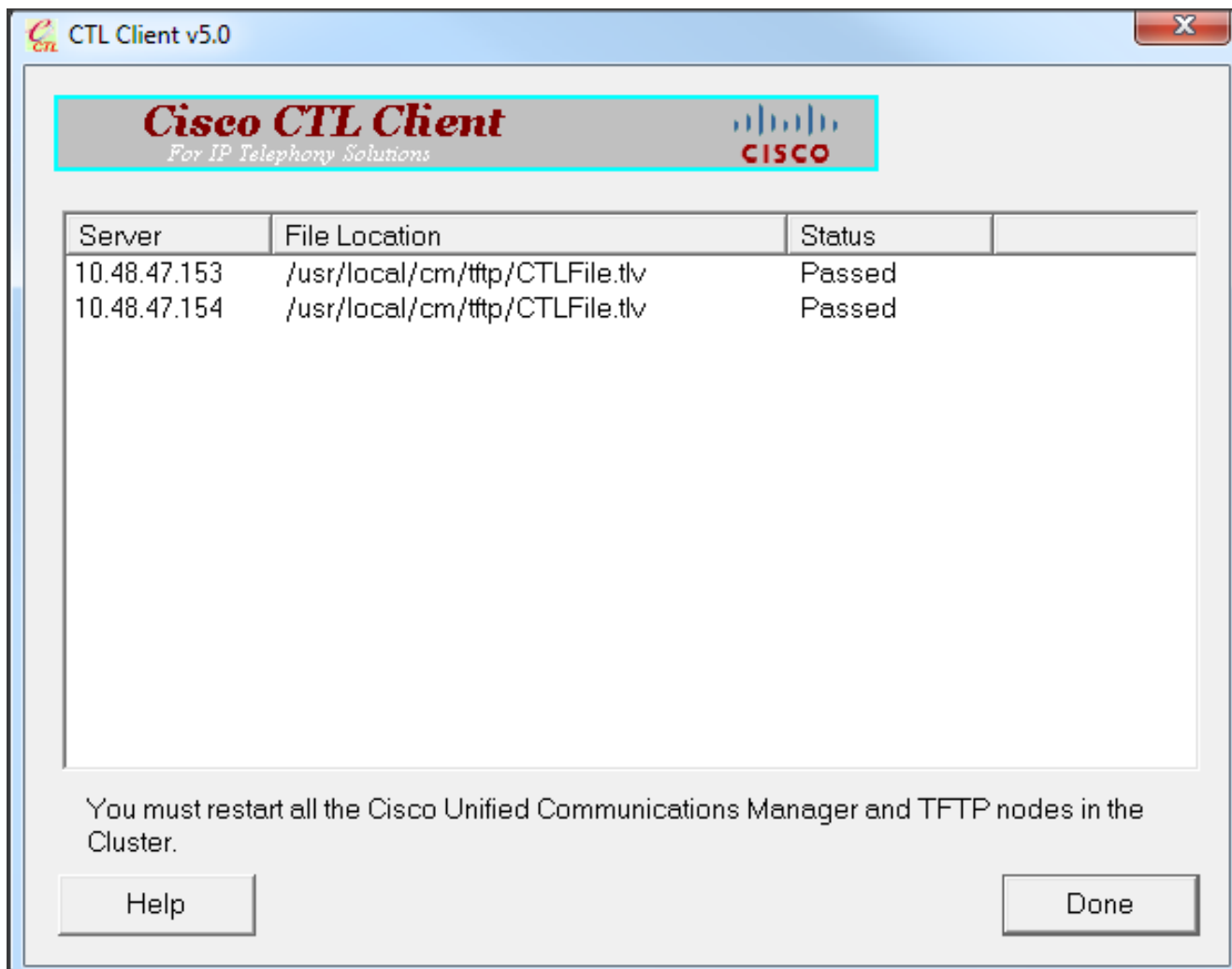
5. De Security Token-gegevens worden weergegeven. Klik op **Next** (Volgende).



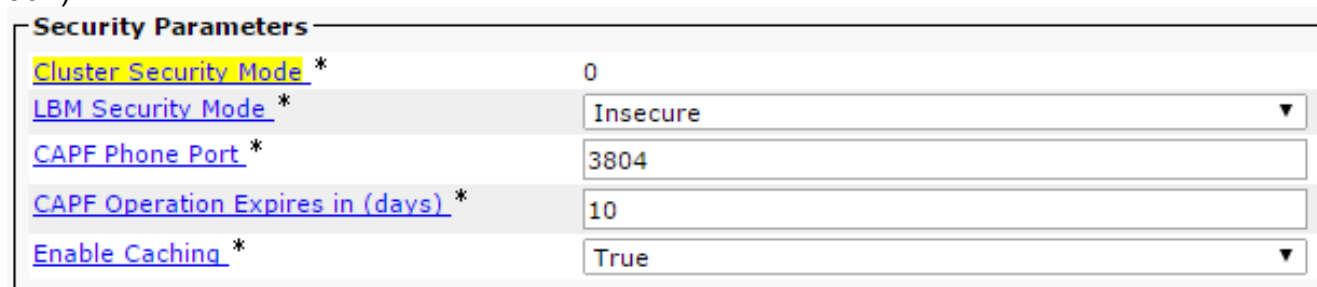
6. De inhoud van het CTL bestand wordt weergegeven. Klik op **Finish** (Voltooien). Voer wanneer dit om het wachtwoord wordt gevraagd **Cisco123** in.



7. De lijst van CUCM-servers waarop het CTL-bestand bestaat, wordt weergegeven. Klik op **Klaar**.



8. Kies CUCM Admin Pagina > **Systeem** > **Enterprise-parameters** en controleer of het cluster is ingesteld op Niet-beveiligde modus ("0" geeft niet-beveiligde modus aan).



9. Start de TFTP- en Cisco CallManager-services opnieuw op alle knooppunten in de cluster die deze services uitvoeren.
10. Start alle IP-telefoons opnieuw zodat ze de nieuwe versie van het CTL-bestand kunnen verkrijgen via CUCM TFTP.

Verander de CUCM Cluster Security van gemengde modus in niet-beveiligde modus met de CLI

Deze configuratie is alleen voor CUCM release 10.X en hoger. Om de CUCM Cluster Security modus in te stellen op niet-beveiligd, voert u de **utils ctl set-cluster niet-beveiligde-mode** opdracht

op uitgever CLI in. Nadat dit volledig is, herstart de TFTP en de diensten van Cisco CallManager op alle knooppunten in de cluster die deze services uitvoeren.

Hier wordt een voorbeeld gegeven van CLI uitvoer die het gebruik van de opdracht toont.

```
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:
```

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

U kunt CTLFile.tlv op een van de twee manieren controleren:

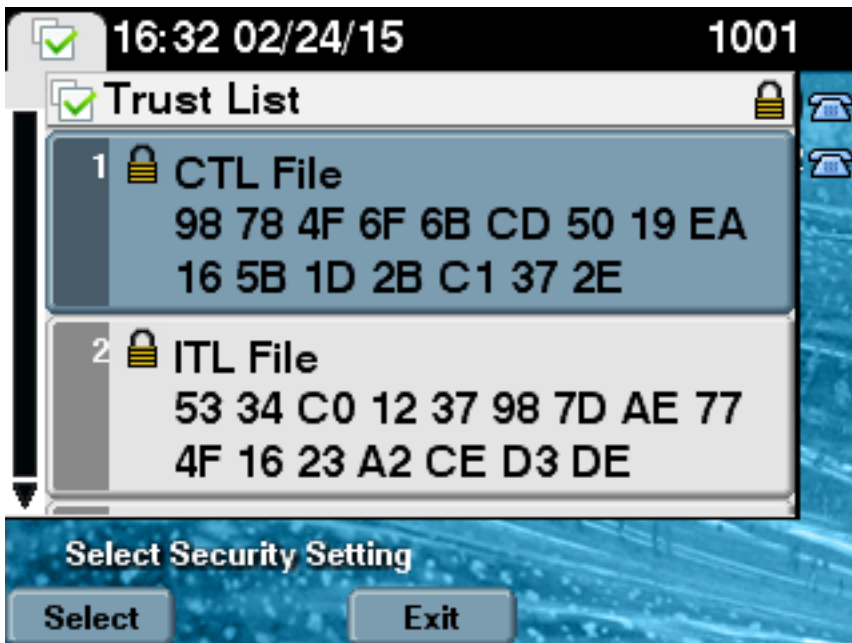
- Om de inhoud en MD5 checksum van de CTLFile.tlv aan de kant van CUCM TFTP te controleren, voert u de opdracht **Show ctl in** op de CUCM CLI. Het CTLFile.tlv-bestand moet op alle CUCM-knooppunten hetzelfde zijn.
- Om het checksum van de MD5 op de IP-telefoon 7975 te controleren, kiest u **Instellingen > Beveiligingsconfiguratie > Trustlijst > CTL-bestand**.

Opmerking: Wanneer u de checksum aan de telefoon controleert, ziet u MD5 of SHA1, afhankelijk van het telefoontype.

CUCM Cluster ingesteld op Security Mode - CTL-checksum voor bestanden

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

Aan de kant van de IP-telefoon kunt u zien dat het hetzelfde CTL-bestand is geïnstalleerd (MD5-checksum overeenkomsten in vergelijking met de uitvoer van CUCM).



CUCM Cluster ingesteld op niet-beveiligde modus - CTL-inhoud

Hier is een voorbeeld van een CTL-bestand van een CUCM-cluster ingesteld op Niet-beveiligde modus. U kunt zien dat de CCM+TFTP-certificaten leeg zijn en geen inhoud bevatten. De rest van de certificaten in de CTL bestanden wordt niet gewijzigd en is precies hetzelfde als toen CUCM op Gemengde modus werd ingesteld.

```
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
```

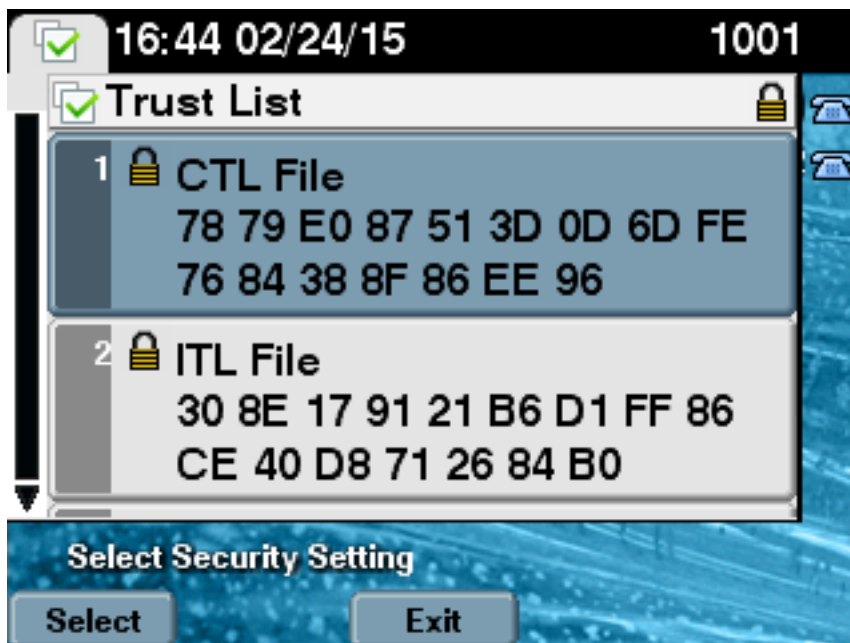
CTL Record #:5

```
-----
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:

Aan de kant van de IP-telefoon, nadat het opnieuw is opgestart en de bijgewerkte versie van het CTL-bestand is gedownload, kunt u zien dat de MD5-checksum overeenkomt met het resultaat van CUCM.



Plaats de CUCM Cluster Security van gemengde mode in niet-beveiligde modus wanneer USB-penningen verloren zijn

Security penningen voor beveiligde clusters kunnen verloren gaan. In die situatie moet je deze twee scenario's in overweging nemen:

- Het cluster werkt versie 10.0.1 of hoger
- Het cluster runt een versie eerder dan 10.x

In het eerste scenario, voltooi de procedure die in het [gedeelte CUCM Cluster Security van gemengde modus naar niet-beveiligde modus](#) is beschreven met de CLI-sectie om van het probleem te herstellen. Aangezien die CLI-opdracht geen CTL-token vereist, kan deze worden gebruikt zelfs als de cluster in Gemengde modus met de CTL-client is geplaatst.

De situatie wordt complexer wanneer een versie eerder dan 10.x van CUCM in gebruik is. Als je het wachtwoord van een van de penningen verliest of vergeet, kan je de andere nog steeds

gebruiken om de CTL client te besturen met de huidige CTL bestanden. Het wordt sterk aanbevolen om een ander Token te verkrijgen en het zo snel mogelijk aan het CTL bestand toe te voegen omwille van redundantie. Als u de wachtwoorden voor alle in uw CTL-bestand vermelde eTokens verliest of vergeet, moet u een nieuw paar eTokens kopen en een handprocedure uitvoeren zoals hier wordt uitgelegd.

1. Typ de opdracht voor het wissen van het bestand met CTLFile.tlv om het CTL-bestand van alle TFTP-servers te verwijderen.

```
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
```

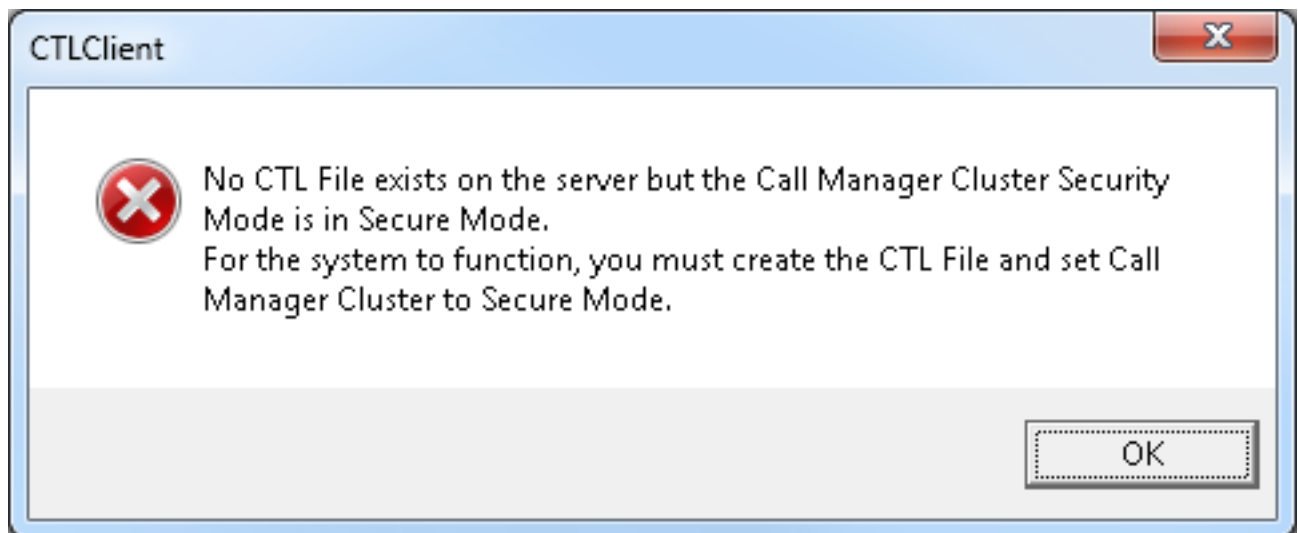
```
CTL File not found. Please run CTLClient plugin or run the CLI - utils ctl..  
to generate the CTL file.
```

```
Error parsing the CTL File.
```

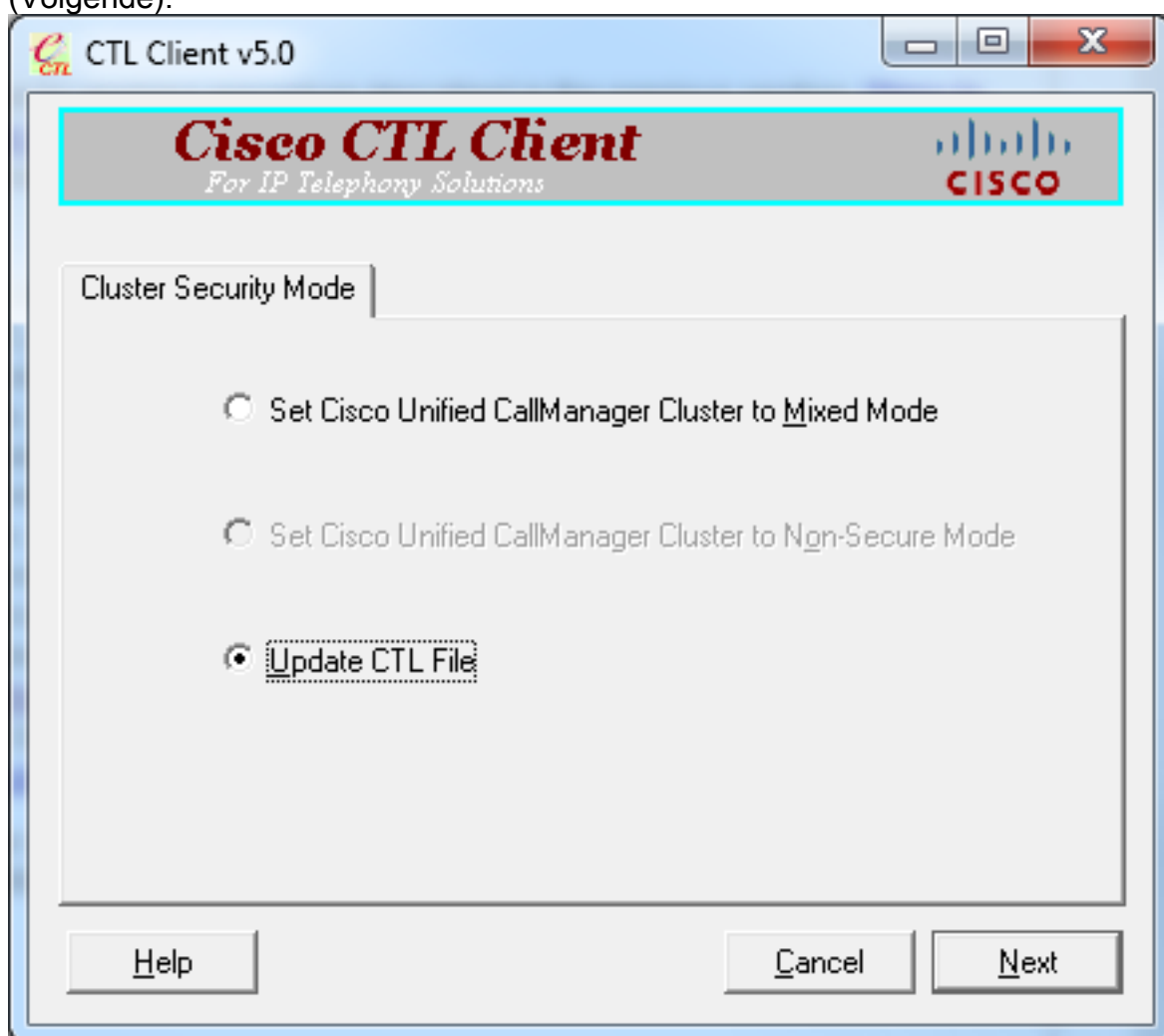
2. Start de CTL client. Voer de IP-hostnaam/het adres van de CUCM-functie in en de CCM-Administrator-referenties. Klik op **Next** (Volgende).

The screenshot shows the Cisco CTL Client v5.0 configuration window. The window title is "CTL Client v5.0". The main header area contains the Cisco CTL Client logo and the Cisco logo. Below the header, the text "Cisco Unified Communications Manager Server" is displayed. The configuration fields are: Hostname or IP Address: 10.48.47.153, Port: 2444, Username: admin, and Password: [masked]. At the bottom, there are three buttons: Help, Cancel, and Next.

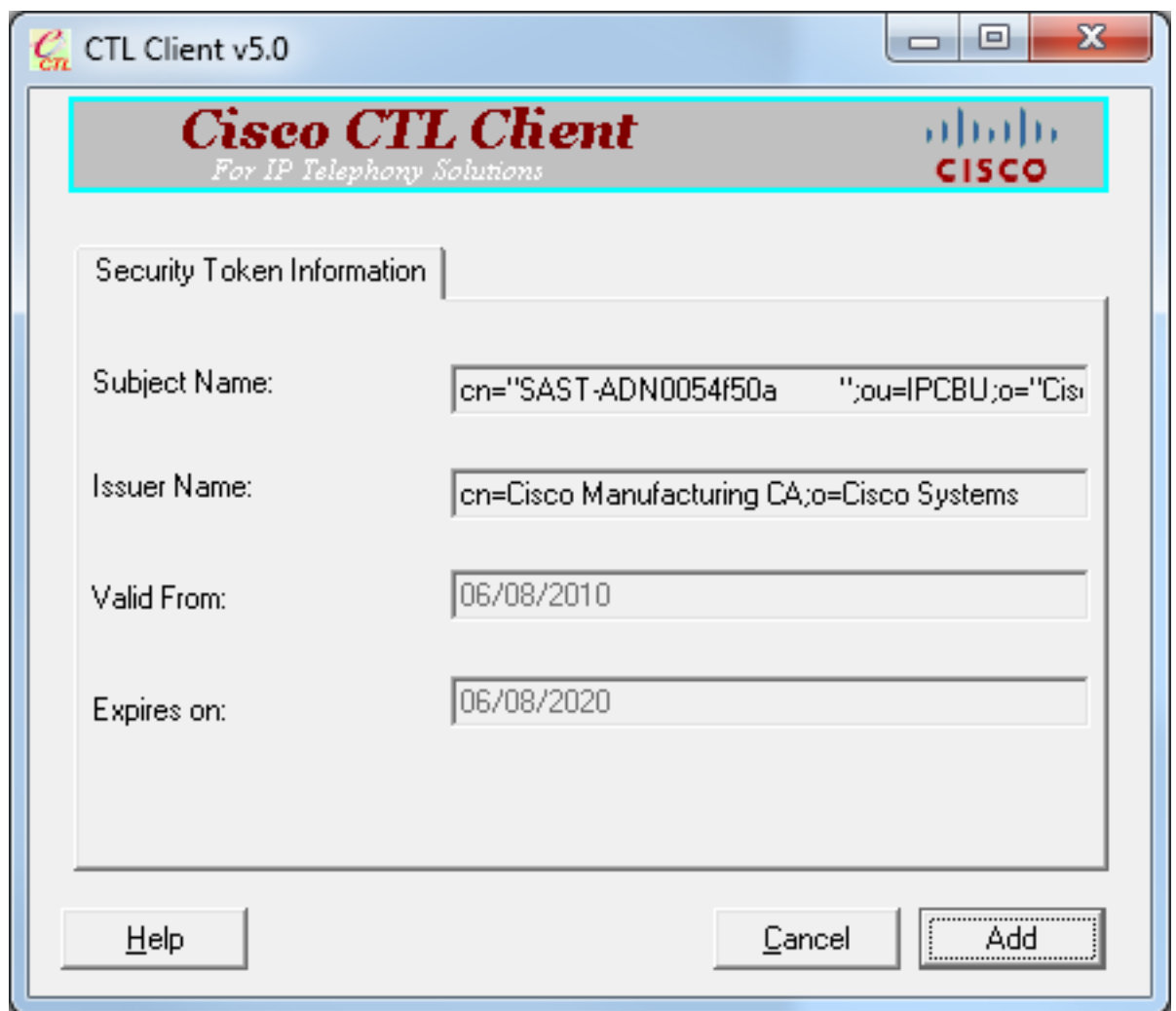
3. Aangezien het cluster in Gemengde modus is, maar er geen CTL-bestand op Publisher bestaat, wordt deze waarschuwing weergegeven. Klik op **OK** om deze te negeren en verder te gaan.



4. Klik op de radioknop **Update CTL File**. Klik op **Next** (Volgende).

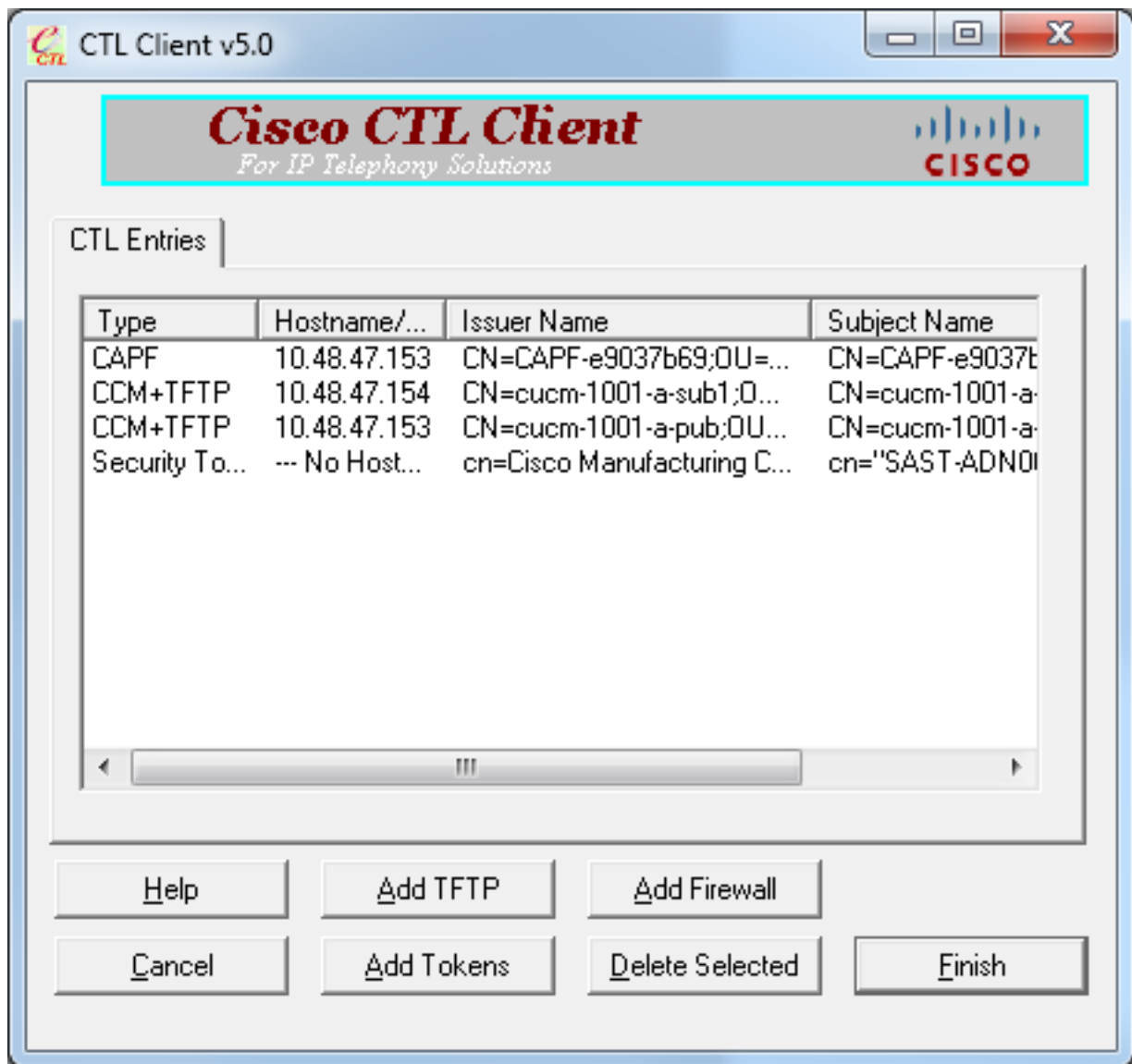


5. De CTL client vraagt om een beveiligingsToken toe te voegen. Klik op **Toevoegen** om verder

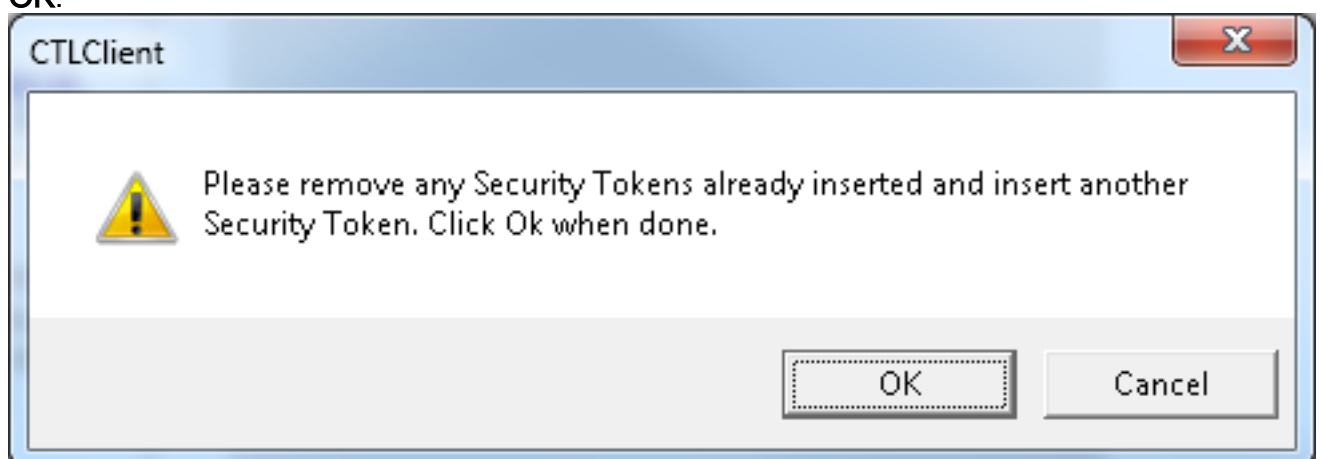


te gaan.

6. Het scherm toont alle ingangen in nieuw CTL. Klik op **Add Tokens** om het tweede token uit het nieuwe paar toe te voegen.



7. U wordt gevraagd de huidige token op te halen en een nieuw token op te nemen. Klik eenmaal op **OK**.



8. Er wordt een scherm weergegeven met informatie over het nieuwe token. Klik op **Toevoegen** om deze te bevestigen en dit token toe te voegen.

CTL Client v5.0

Cisco CTL Client
For IP Telephony Solutions

CISCO

Security Token Information

Subject Name:

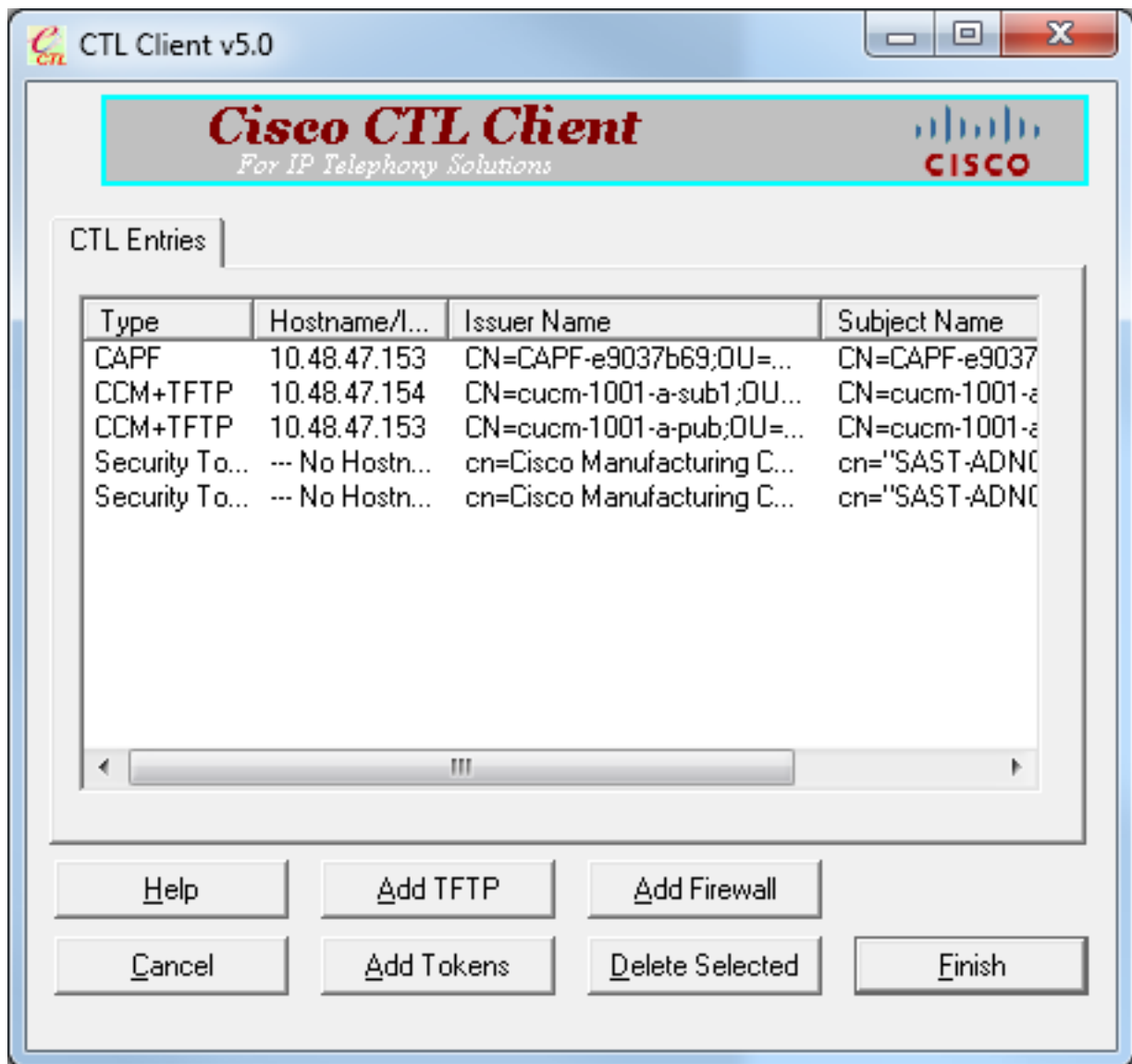
Issuer Name:

Valid From:

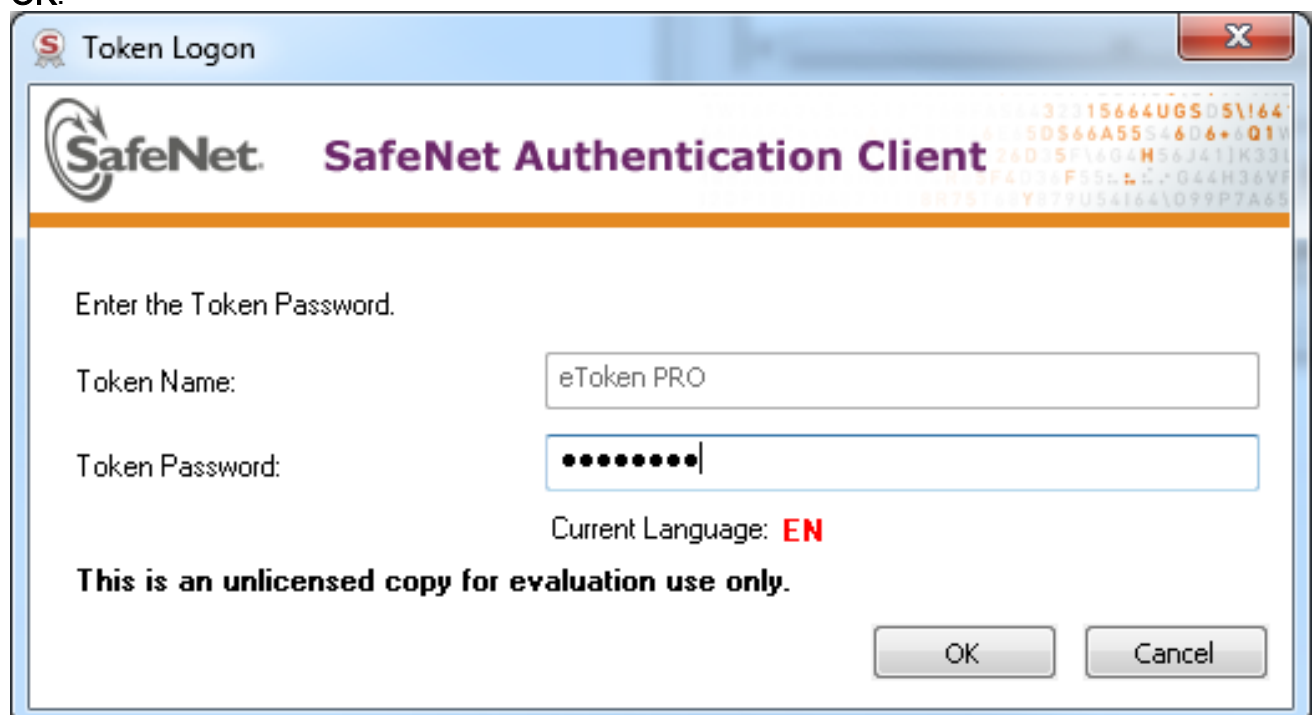
Expires on:

voegen.

9. Er wordt een nieuwe lijst met CTL-items gepresenteerd die beide Tokens toevoegen. Klik op **Voltooien** om nieuwe CTL-bestanden te genereren.

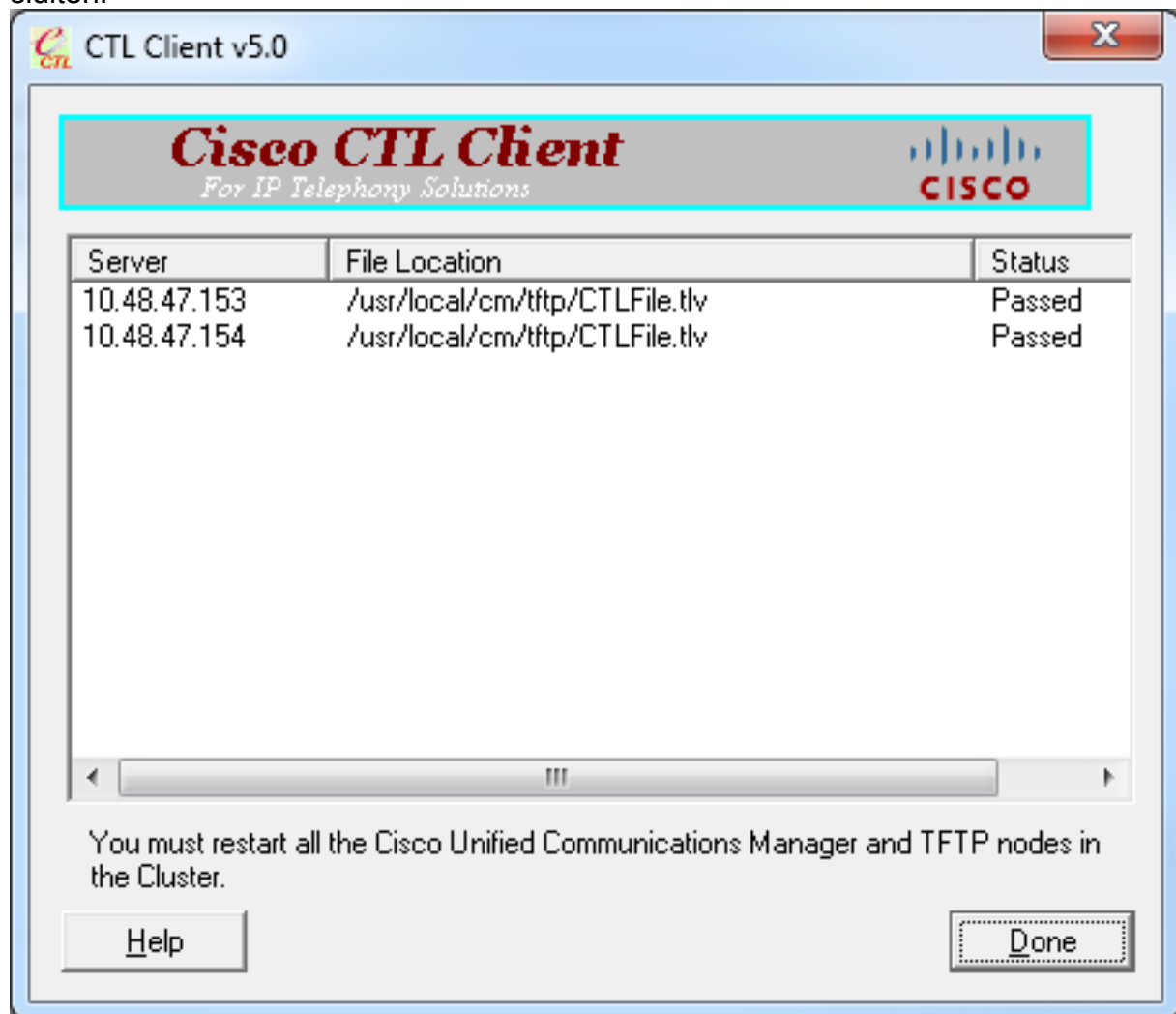


10. Typ in het veld Token Password **Cisco123**. Klik op **OK**.



11. U zult zien dat het proces succesvol was. Klik op **Gereed** om de CTL-client te bevestigen en af te

sluiten.



12. Start Cisco TFTP opnieuw, gevolgd door de CallManager-service (Cisco Unified Services > Tools > Control Center - functieservices). Het nieuwe CTL-bestand moet worden gegenereerd. Typ de opdracht **tonen ctl** voor verificatie.

```
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. Verwijder het CTL-bestand van elke telefoon in het cluster (deze procedure kan variëren afhankelijk van het type telefoon - raadpleeg dan documentatie voor details, zoals de [Cisco Unified IP-telefoon 8961, 9951 en 9971 beheergids](#)). **Opmerking:** De telefoons kunnen nog steeds in staat zijn om te registreren (afhankelijk van de beveiligingsinstellingen op de telefoon) en te werken zonder stap 13 uit te voeren. Niettemin wordt het oude CTL-bestand geïnstalleerd. Het kan problemen veroorzaken als certificaten worden geregenereerd, wordt een andere server toegevoegd aan de cluster of wordt de serverhardware vervangen. Het wordt niet aanbevolen het cluster in deze status te laten.
14. Verplaats de cluster naar niet-veilig. Zie de [sectie CUCM Cluster Security wijzigen van gemengde modus in niet-beveiligde modus met de](#) sectie [CTL-client](#) voor meer informatie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.