# Konfigurationsbeispiel für CUCM-Cluster vom gemischten Modus in den nicht sicheren Modus geändert

## Inhalt



## Einleitung

In diesem Dokument werden die erforderlichen Schritte beschrieben, um den Sicherheitsmodus von Cisco Unified Communications Manager (CUCM) vom gemischten Modus in den nicht sicheren Modus zu ändern. Außerdem wird gezeigt, wie der Inhalt einer CTL-Datei (Certificate Trust List) geändert wird, wenn diese Verschiebung abgeschlossen ist.

Die Änderung des CUCM-Sicherheitsmodus umfasst drei Hauptkomponenten:

1a) Führen Sie den CTL-Client aus, und wählen Sie die gewünschte Variante des Sicherheitsmodus aus.
1b) Geben Sie den CLI-Befehl ein, um die gewünschte Variante des Sicherheitsmodus auszuwählen.
2. Starten Sie die Cisco CallManager- und Cisco TFTP-Dienste auf allen CUCM-Servern, auf denen diese Dienste ausgeführt werden, neu.
3. Starten Sie alle IP-Telefone neu, sodass sie die aktualisierte Version der CTL-Datei herunterladen können.

**Anmerkung:** Wenn der Sicherheitsmodus des Clusters von Gemischter Modus in Nicht

sicherer Modus geändert wird, ist die CTL-Datei auf dem/den Server(n) und den Telefonen weiterhin vorhanden, die CTL-Datei enthält jedoch keine CCM+TFTP (Server)-Zertifikate. Da CCM- und TFTP-Zertifikate (Server) nicht in der CTL-Datei vorhanden sind, muss das Telefon als nicht sicher beim CUCM registriert werden.

# Voraussetzungen

## Anforderungen

Cisco empfiehlt, Kenntnisse der CUCM-Version 10.0(1) oder höher zu erwerben. Stellen Sie darüber hinaus Folgendes sicher:

- Der CTL Provider-Dienst ist aktiviert und wird auf allen aktiven TFTP-Servern im Cluster ausgeführt. Standardmäßig wird der Service auf dem TCP-Port 2444 ausgeführt. Dies kann jedoch in der Konfiguration der CUCM-Serviceparameter geändert werden.
- Die CAPF-Dienste (Certificate Authority Proxy Function) sind aktiviert und werden auf dem Publisher-Knoten ausgeführt.
- Die Datenbankreplikation (DB) im Cluster funktioniert ordnungsgemäß, und die Server replizieren Daten in Echtzeit.

## Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- CUCM-Version 10.0.1.11900-2 Cluster mit zwei Knoten
- Cisco 7975 IP-Telefon (registriert mit Skinny Call Control Protocol (SCCP), Firmware-Version SCCP75.9-3-1SR3-1S)
- Zwei Cisco Security Tokens sind erforderlich, um den Cluster auf den gemischten Modus zu setzen.
- Eines der zuvor aufgeführten Sicherheitstoken ist erforderlich, um den Cluster in den ungesicherten Modus zu versetzen.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

# Hintergrundinformationen

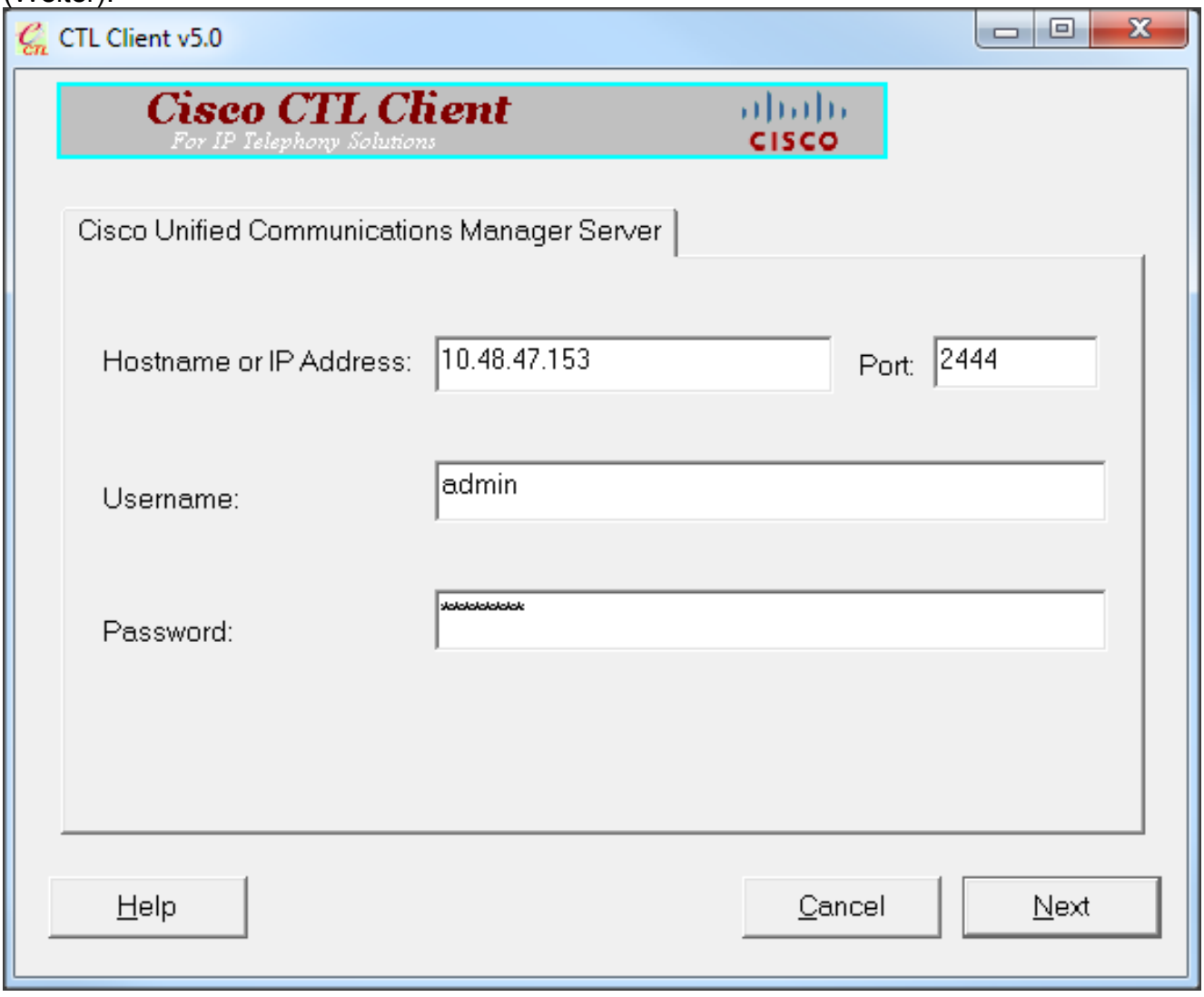
Um das CTL-Client-Plug-In auszuführen, muss auf mindestens ein Sicherheitstoken zugegriffen werden können, das eingefügt wurde, um die neueste CTL-Datei auf dem CUCM Publisher-Server zu erstellen oder zu aktualisieren. Mit anderen Worten: Mindestens eines der eToken-Zertifikate, die in der aktuellen CTL-Datei auf dem CUCM vorhanden sind, muss sich auf dem Sicherheitstoken befinden, das zum Ändern des Sicherheitsmodus verwendet wird.

# Konfigurieren

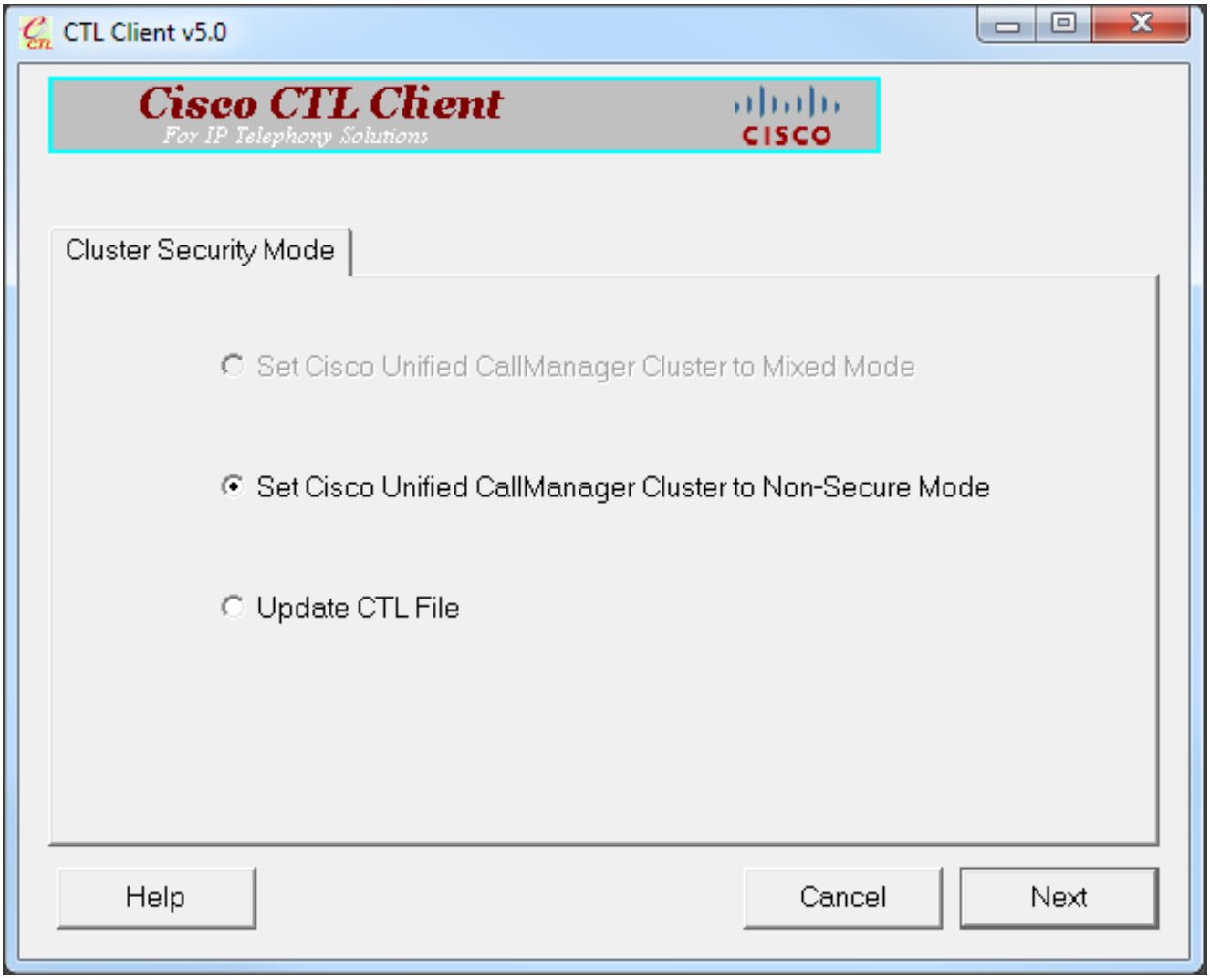
## Ändern der CUCM-Cluster-Sicherheit vom gemischten Modus in den ungesicherten Modus mit dem CTL-Client

Gehen Sie wie folgt vor, um die CUCM-Cluster-Sicherheit mit dem CTL-Client vom gemischten Modus in den nicht sicheren Modus zu ändern:

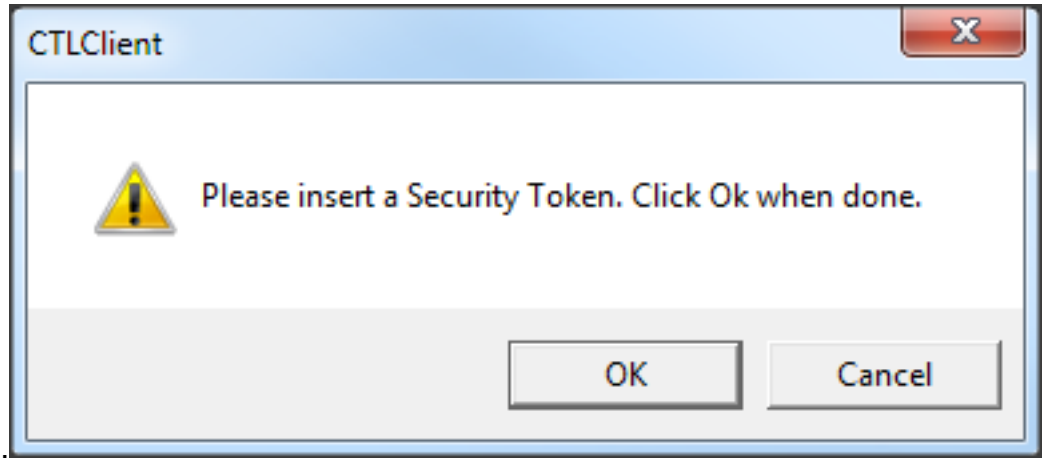
1. Rufen Sie ein Sicherheitstoken ab, das Sie zum Konfigurieren der neuesten CTL-Datei eingefügt haben.
2. Führen Sie den CTL-Client aus. Geben Sie den IP-Hostnamen/die IP-Adresse von CUCM Pub und die CCM-Administratoranmeldeinformationen an. Klicken Sie auf **Next** (Weiter).



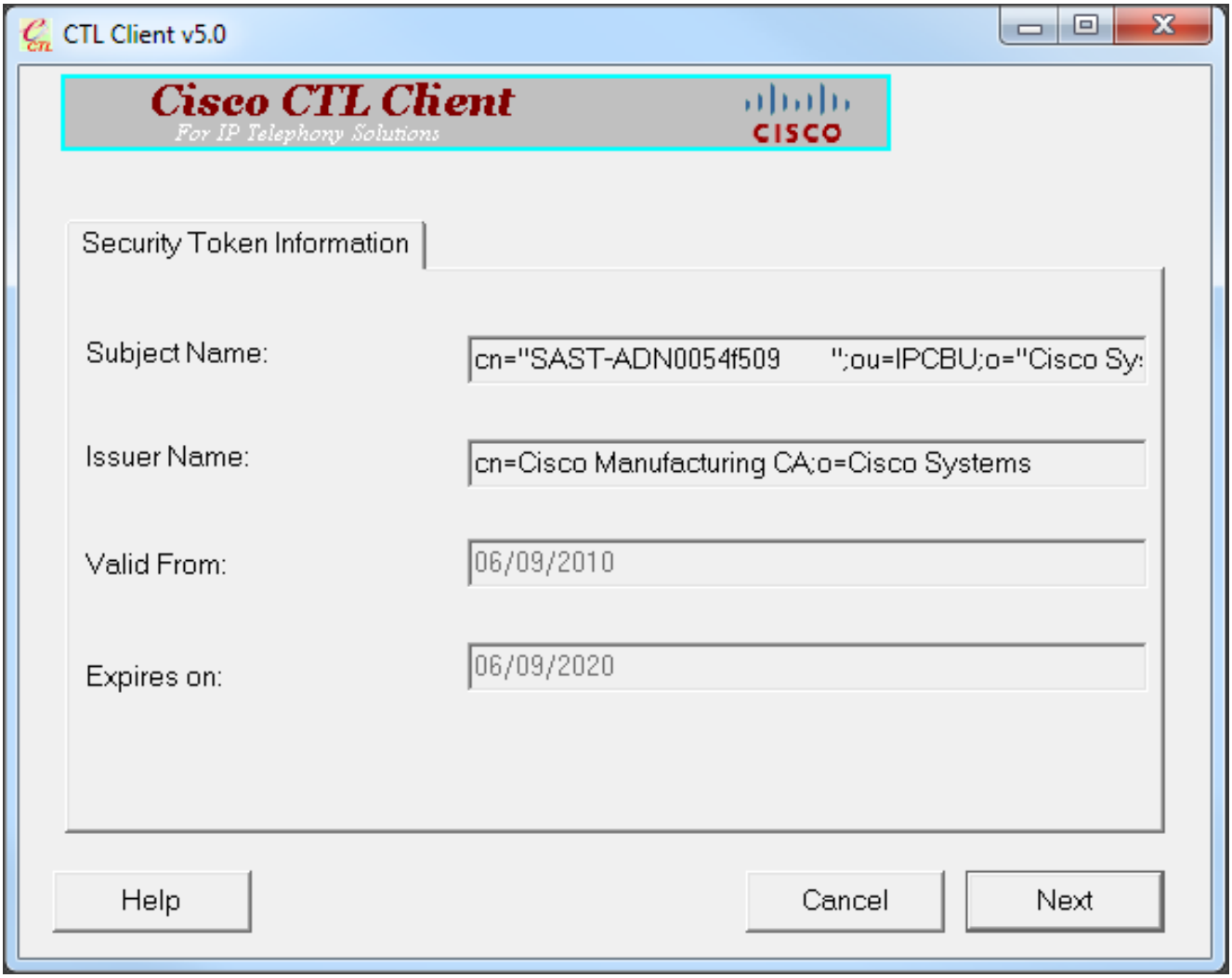

3. Klicken Sie auf das Optionsfeld **Cisco Unified CallManager-Cluster auf ungesicherten Modus setzen**. Klicken Sie auf **Next** (Weiter).



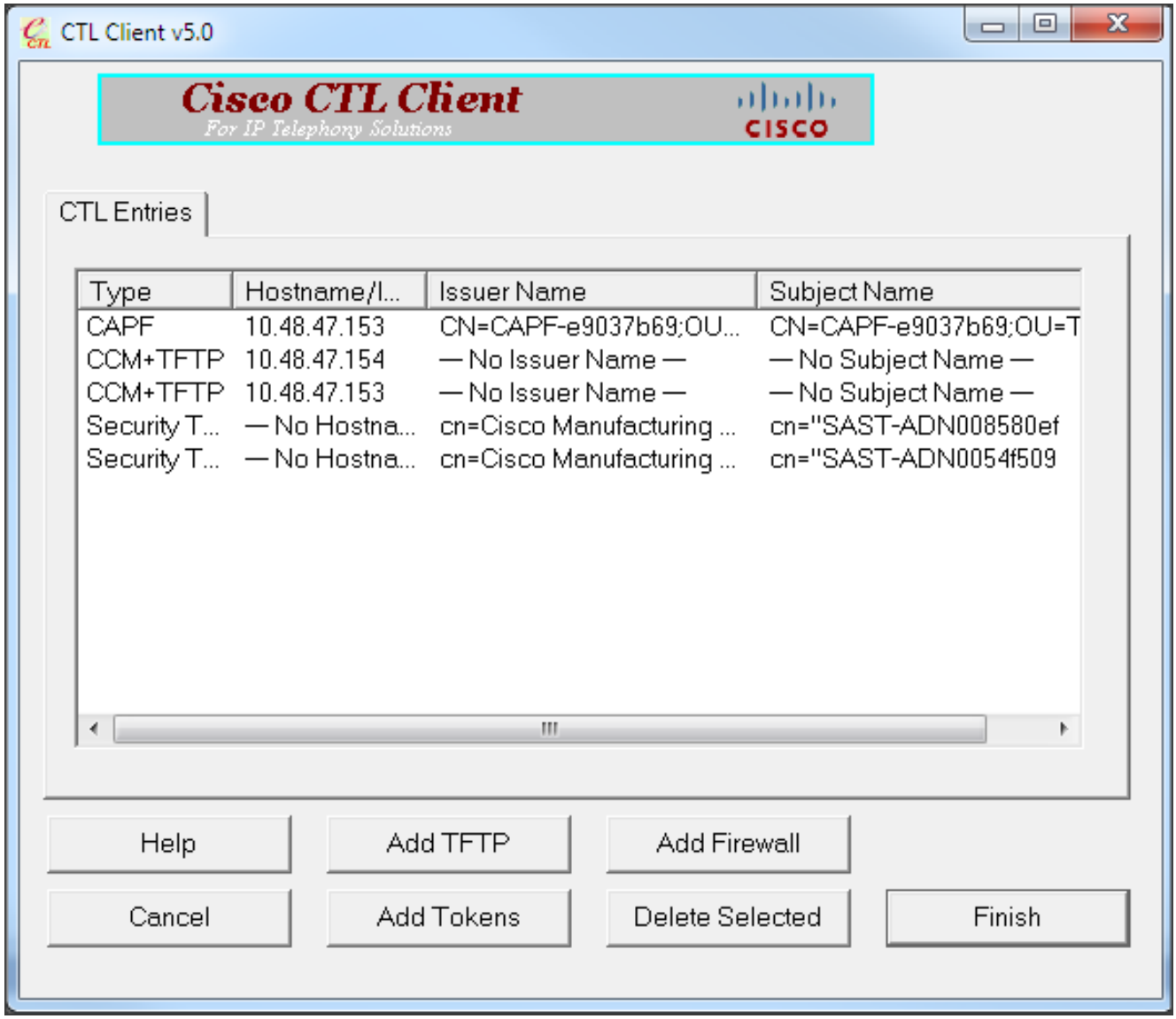

4. Fügen Sie ein Sicherheitstoken ein, das eingefügt wurde, um die neueste CTL-Datei zu konfigurieren, und klicken Sie auf **OK**. Dies ist eines der Token, die zum Füllen der Zertifikatsliste in CTLFile.tlv verwendet wurden.



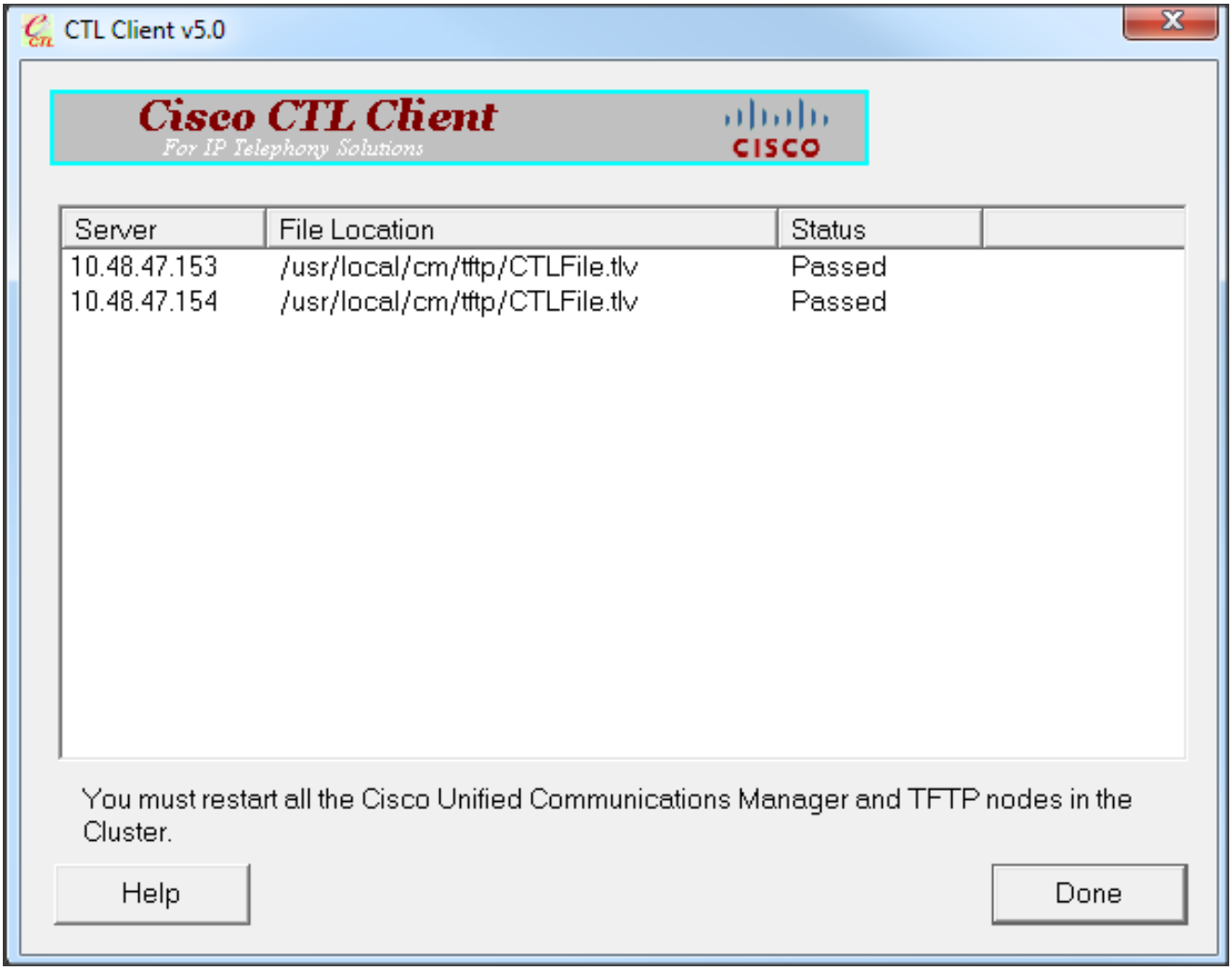

5. Die Details des Sicherheitstokens werden angezeigt. Klicken Sie auf **Next** (Weiter).



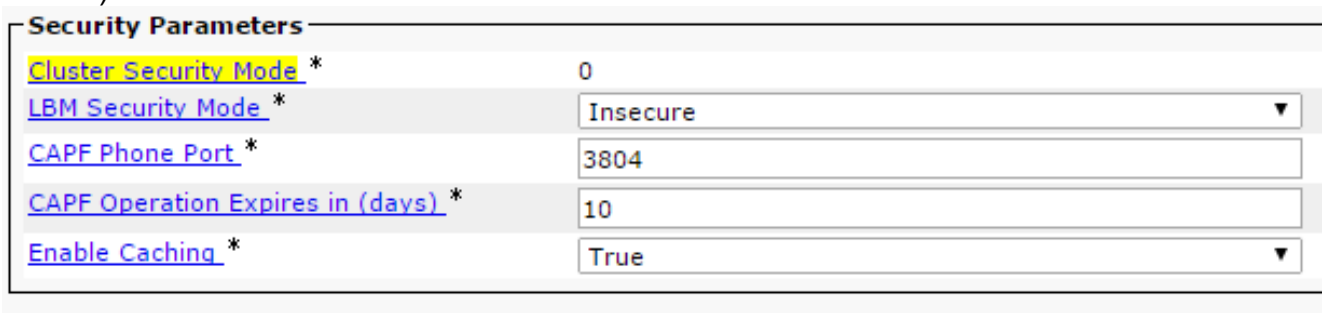

6. Der Inhalt der CTL-Datei wird angezeigt. Klicken Sie auf **Beenden**. Wenn Sie zur Eingabe des Kennworts aufgefordert werden, geben Sie **Cisco123**
**ein**.




7. Die Liste der CUCM-Server, auf denen die CTL-Datei vorhanden ist, wird angezeigt. Klicken Sie auf
**Fertig**.




8. Wählen Sie **CUCM-Admin-Seite > System > Enterprise Parameters aus,** und stellen Sie sicher, dass der Cluster auf den ungesicherten Modus gesetzt wurde ("0" bedeutet "nicht sicher").




9. Starten Sie die TFTP- und Cisco CallManager-Dienste auf allen Knoten im Cluster neu, auf denen diese Dienste ausgeführt werden.
10. Starten Sie alle IP-Telefone neu, damit sie die neue Version der CTL-Datei vom CUCM-TFTP erhalten.

## Ändern der CUCM-Cluster-Sicherheit vom gemischten Modus in den ungesicherten Modus mit der CLI

Diese Konfiguration gilt nur für CUCM Version 10.x und höher. Um den CUCM-Cluster-Sicherheitsmodus auf "Nicht sicher" festzulegen, geben Sie den Befehl **utils ctl set-cluster non-**

**secure-mode** in der Publisher-CLI ein. Starten Sie nach Abschluss dieses Vorgangs die TFTP- und Cisco CallManager-Dienste auf allen Knoten im Cluster neu, auf denen diese Dienste ausgeführt werden.

In der CLI-Beispielausgabe wird die Verwendung des Befehls veranschaulicht.

```
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:
```

# Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Um die Datei CTLFIle.tlv zu überprüfen, können Sie eine von zwei Methoden verwenden:

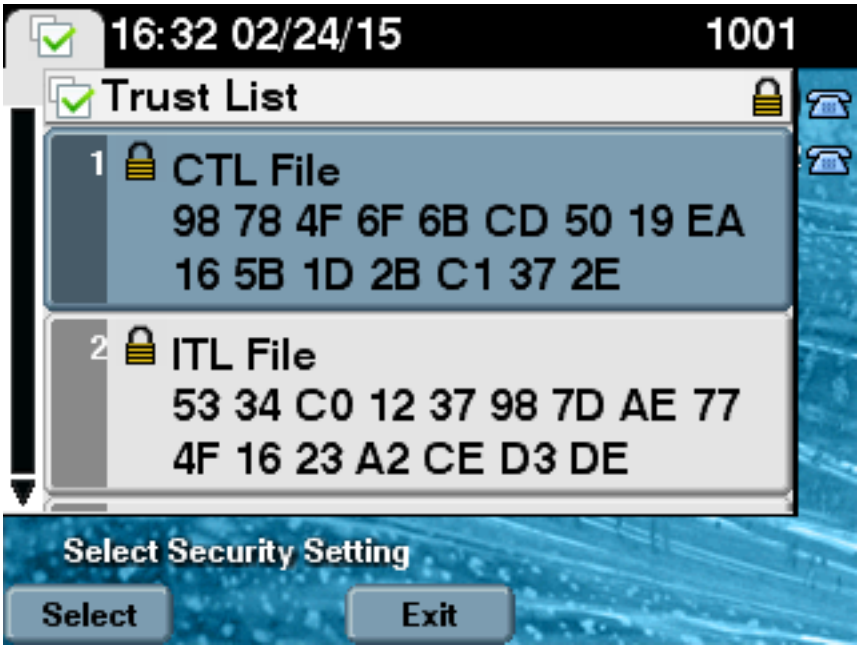
- Um den Inhalt und die MD5-Prüfsumme der CTLFIle.tlv auf der CUCM-TFTP-Seite zu überprüfen, geben Sie den Befehl **show ctl** in der CUCM-CLI ein. Die Datei "CTLFIle.tlv" sollte auf allen CUCM-Knoten identisch sein.
- Um die MD5-Prüfsumme auf dem IP-Telefon 7975 zu überprüfen, wählen Sie **Einstellungen > Sicherheitskonfiguration > Vertrauensliste > CTL-Datei aus**.

  **Anmerkung:** Wenn Sie die Prüfsumme am Telefon überprüfen, wird je nach Telefontyp entweder MD5 oder SHA1 angezeigt.

## Sicherheitsmodus für CUCM-Cluster festgelegt - CTL-Datei-Prüfsumme

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

Auf der Seite des IP-Telefons können Sie sehen, dass dieselbe CTL-Datei installiert ist (MD5-Prüfsumme stimmt im Vergleich zur Ausgabe von CUCM überein).




## CUCM-Cluster auf ungesicherten Modus gesetzt - CTL-Dateiinhalt

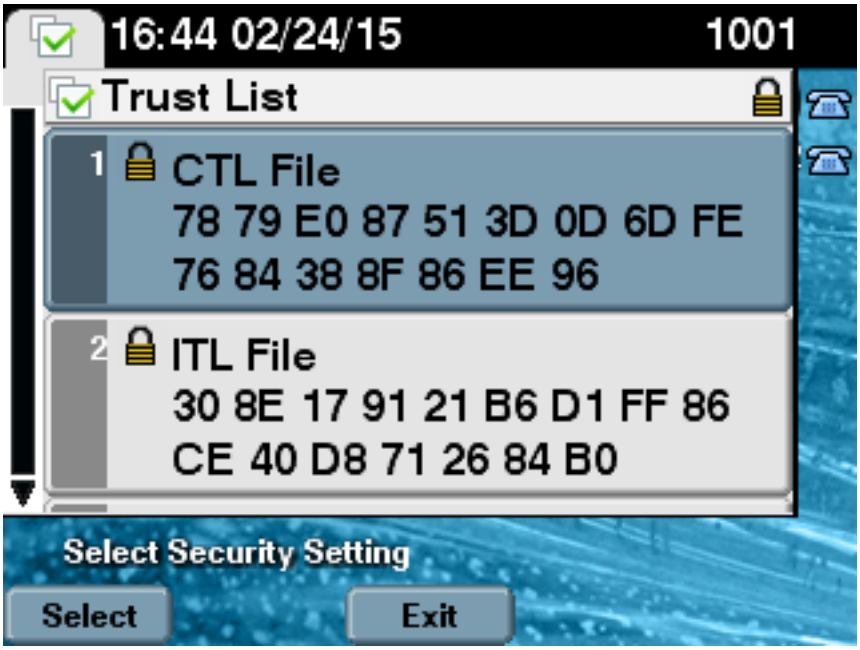
Das folgende Beispiel zeigt eine CTL-Datei von einem CUCM-Cluster, der auf den ungesicherten Modus gesetzt ist. Sie sehen, dass die CCM+TFTP-Zertifikate leer sind und keinen Inhalt enthalten. Die restlichen Zertifikate in den CTL-Dateien werden nicht geändert und entsprechen genau dem Zeitpunkt, als CUCM auf den gemischten Modus gesetzt wurde.

```
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:
```

Auf der Seite des IP-Telefons können Sie nach dem Neustart und dem Herunterladen der aktualisierten CTL-Datei sehen, dass die MD5-Prüfsumme im Vergleich zur Ausgabe von CUCM übereinstimmt.




## Setzen Sie die CUCM-Cluster-Sicherheit aus dem gemischten Modus in den ungesicherten Modus, wenn USB-Token verloren gehen.

Sicherheitstoken für gesicherte Cluster können verloren gehen. In dieser Situation müssen Sie die folgenden beiden Szenarien berücksichtigen:

- Auf dem Cluster wird Version 10.0.1 oder höher ausgeführt.
- Auf dem Cluster wird eine ältere Version als 10.x ausgeführt.

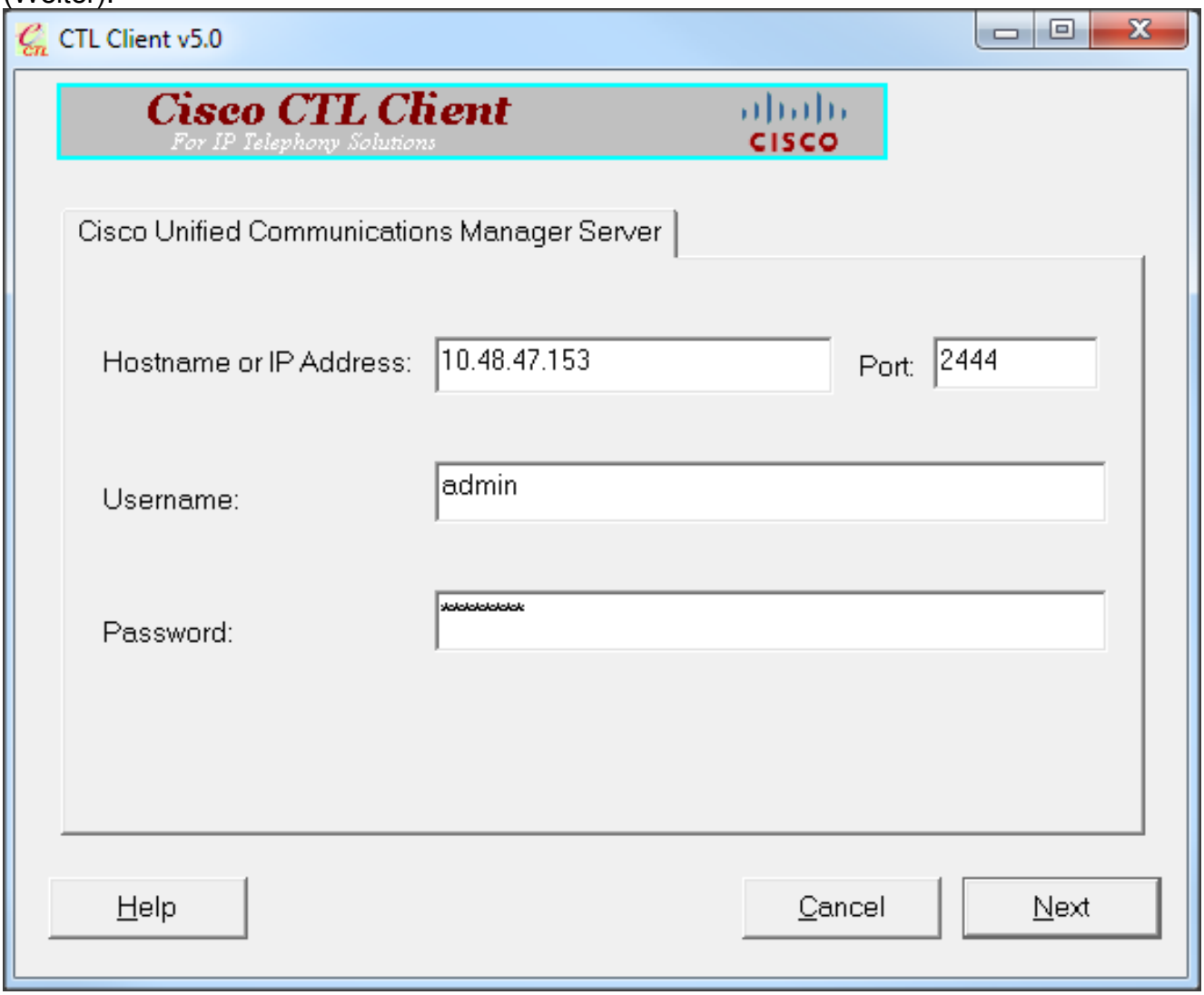
Führen Sie im ersten Szenario das im Abschnitt Ändern der CUCM-Clustersicherheit aus dem gemischten Modus in den ungesicherten Modus mit dem CLI beschriebene Verfahren aus, um das Problem zu beheben. Da für diesen CLI-Befehl kein CTL-Token erforderlich ist, kann er auch verwendet werden, wenn der Cluster mit dem CTL-Client in den gemischten Modus versetzt wurde.

Die Situation wird komplexer, wenn eine frühere Version als 10.x von CUCM verwendet wird. Wenn Sie das Passwort eines Tokens verlieren oder vergessen, können Sie das andere trotzdem verwenden, um den CTL-Client mit aktuellen CTL-Dateien auszuführen. Es wird dringend empfohlen, aus Redundanzgründen so schnell wie möglich ein weiteres eToken zu erhalten und der CTL-Datei hinzuzufügen. Wenn Sie die Kennwörter für alle in Ihrer CTL-Datei aufgelisteten eTokens verlieren oder vergessen, müssen Sie ein neues eToken-Paar abrufen und ein manuelles Verfahren ausführen, wie hier erläutert.

1. Geben Sie den Befehl **file delete tftp CTLFile.tlv** ein, um die CTL-Datei von allen TFTP-Servern zu löschen.

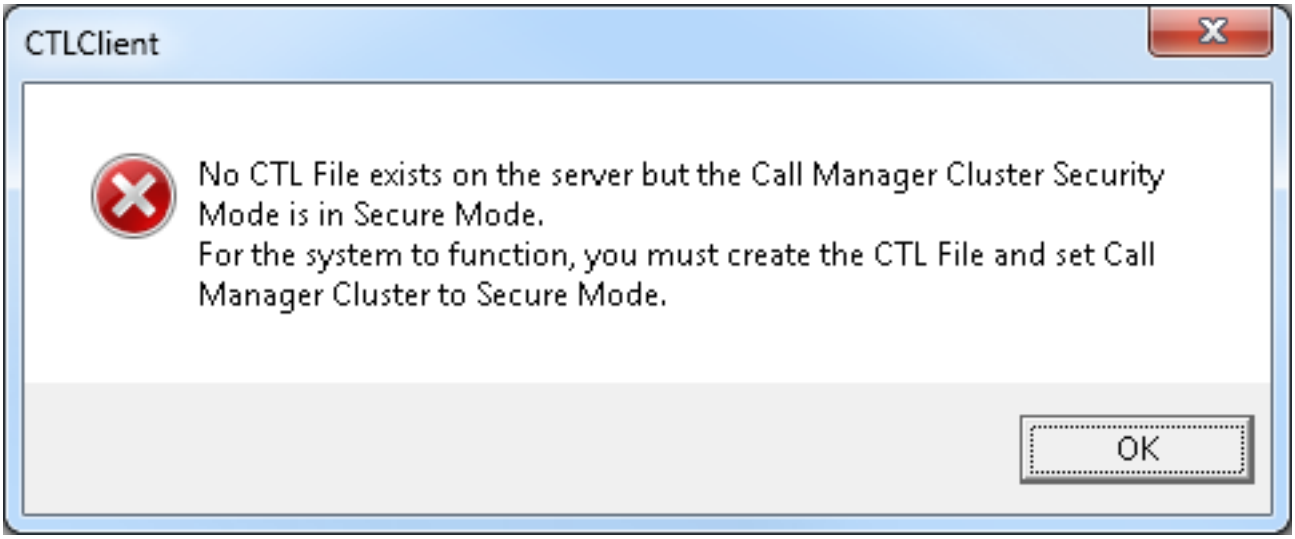
```
admin:file delete tftp CTLFile.tlv
Delete the File CTLFile.tlv?
Enter "y" followed by return to continue: y
files: found = 1, deleted = 1

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. Führen Sie den CTL-Client aus. Geben Sie den IP-Hostnamen/die IP-Adresse von CUCM Pub und die CCM-Administratoranmeldeinformationen ein. Klicken Sie auf **Next** (Weiter).

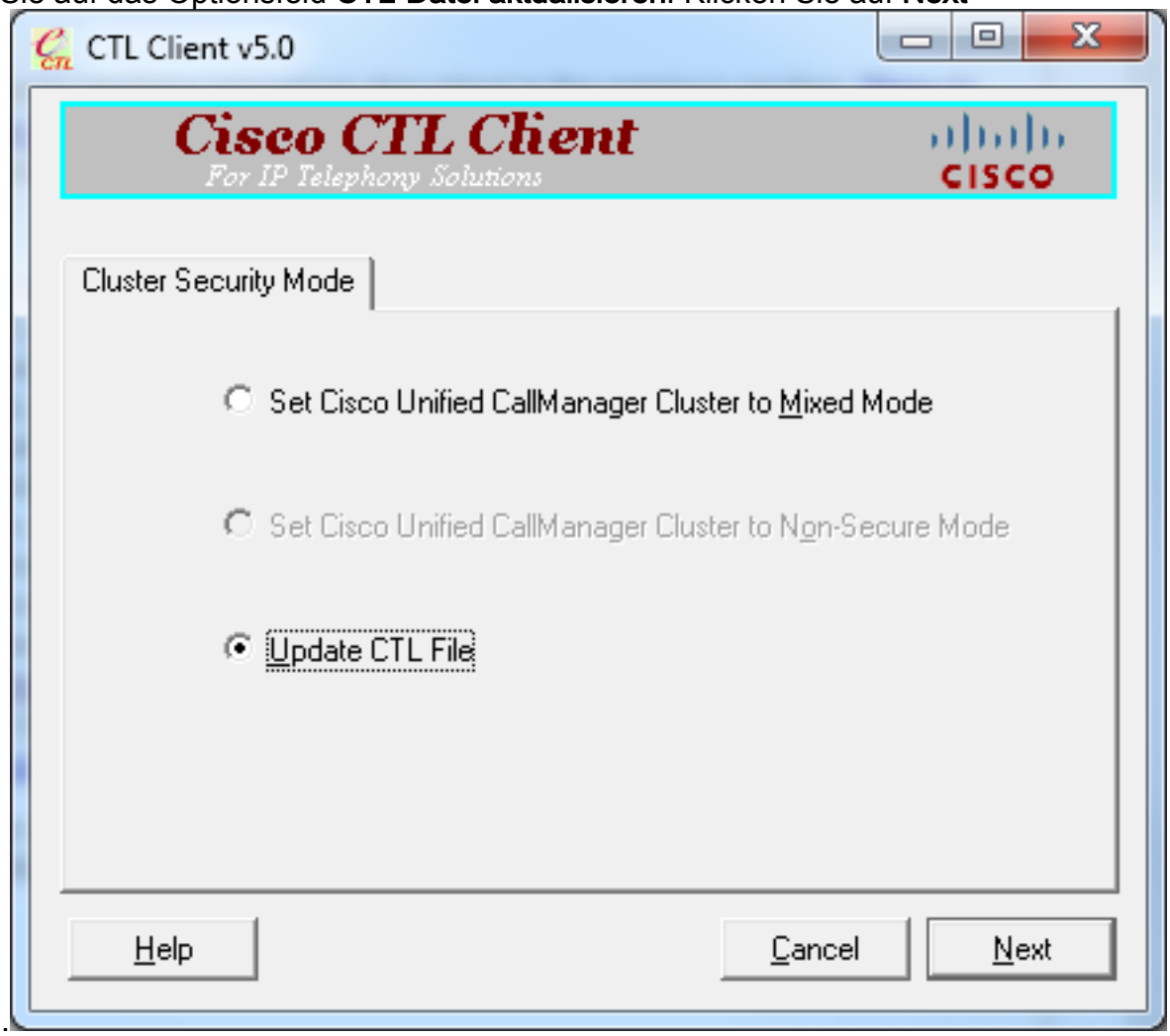



3. Da sich der Cluster im gemischten Modus befindet, jedoch keine CTL-Datei auf Publisher vorhanden ist, wird diese Warnung angezeigt. Klicken Sie auf **OK**, um das Fenster zu

ignorieren und
fortzufahren.

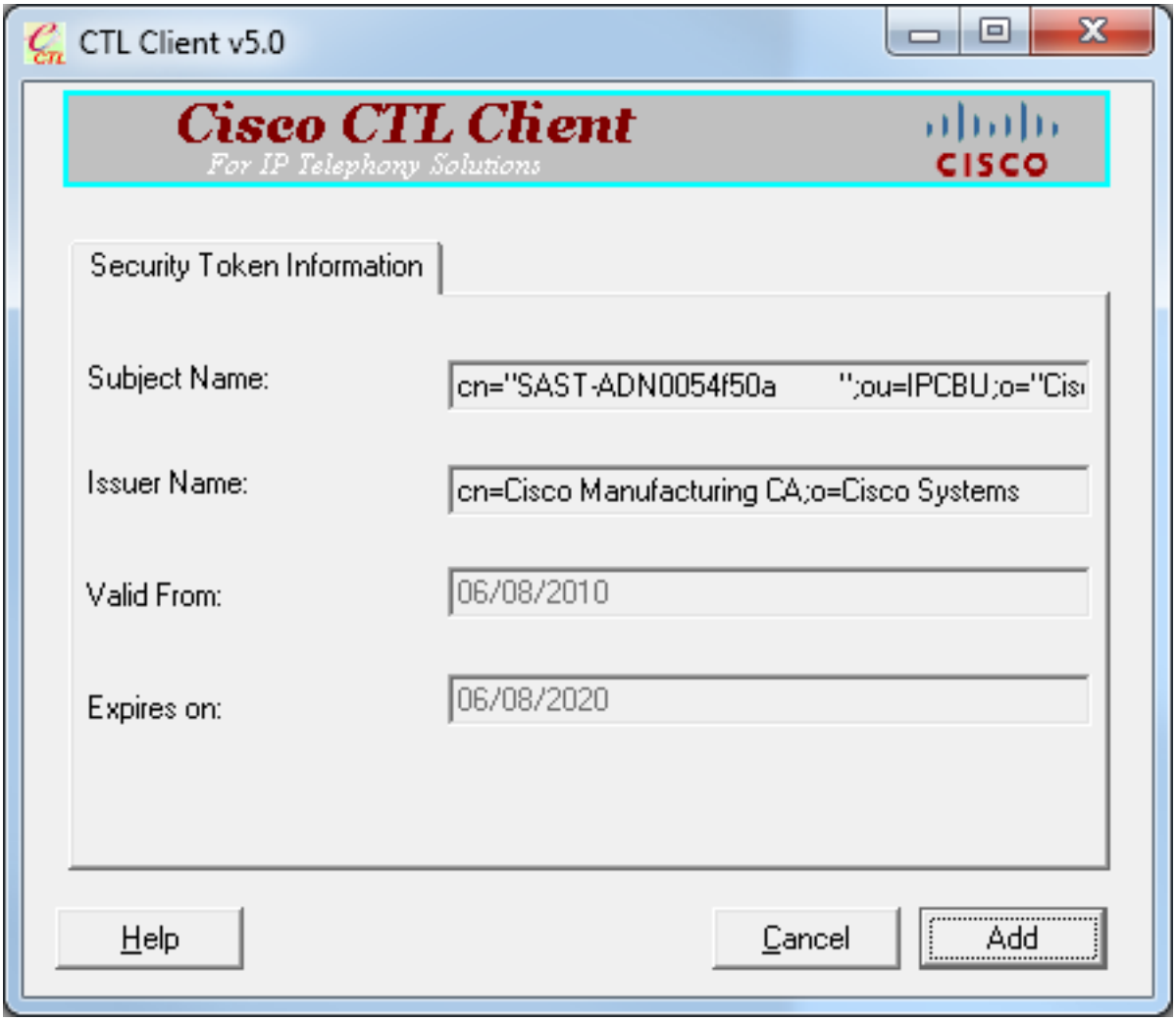



4. Klicken Sie auf das Optionsfeld **CTL-Datei aktualisieren**. Klicken Sie auf **Next**

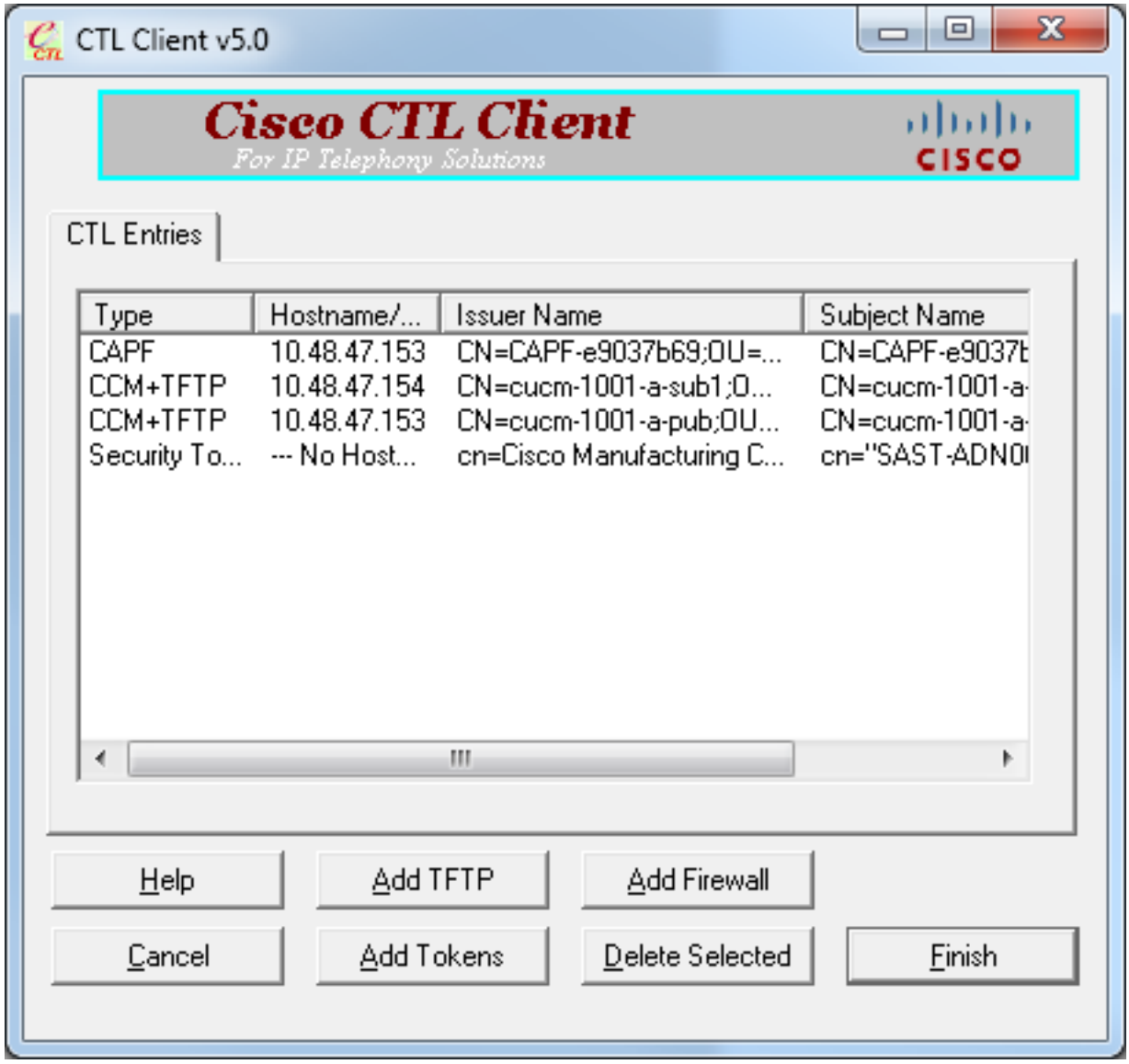



(Weiter).

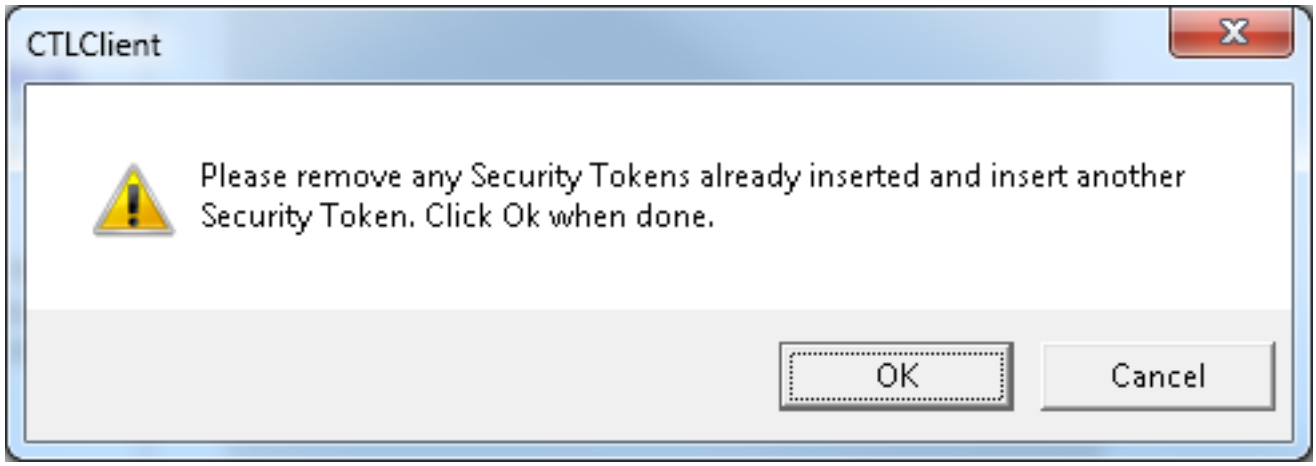
5. Der CTL-Client fordert auf, ein Sicherheitstoken hinzuzufügen. Klicken Sie auf **Hinzufügen**, um
fortzufahren.



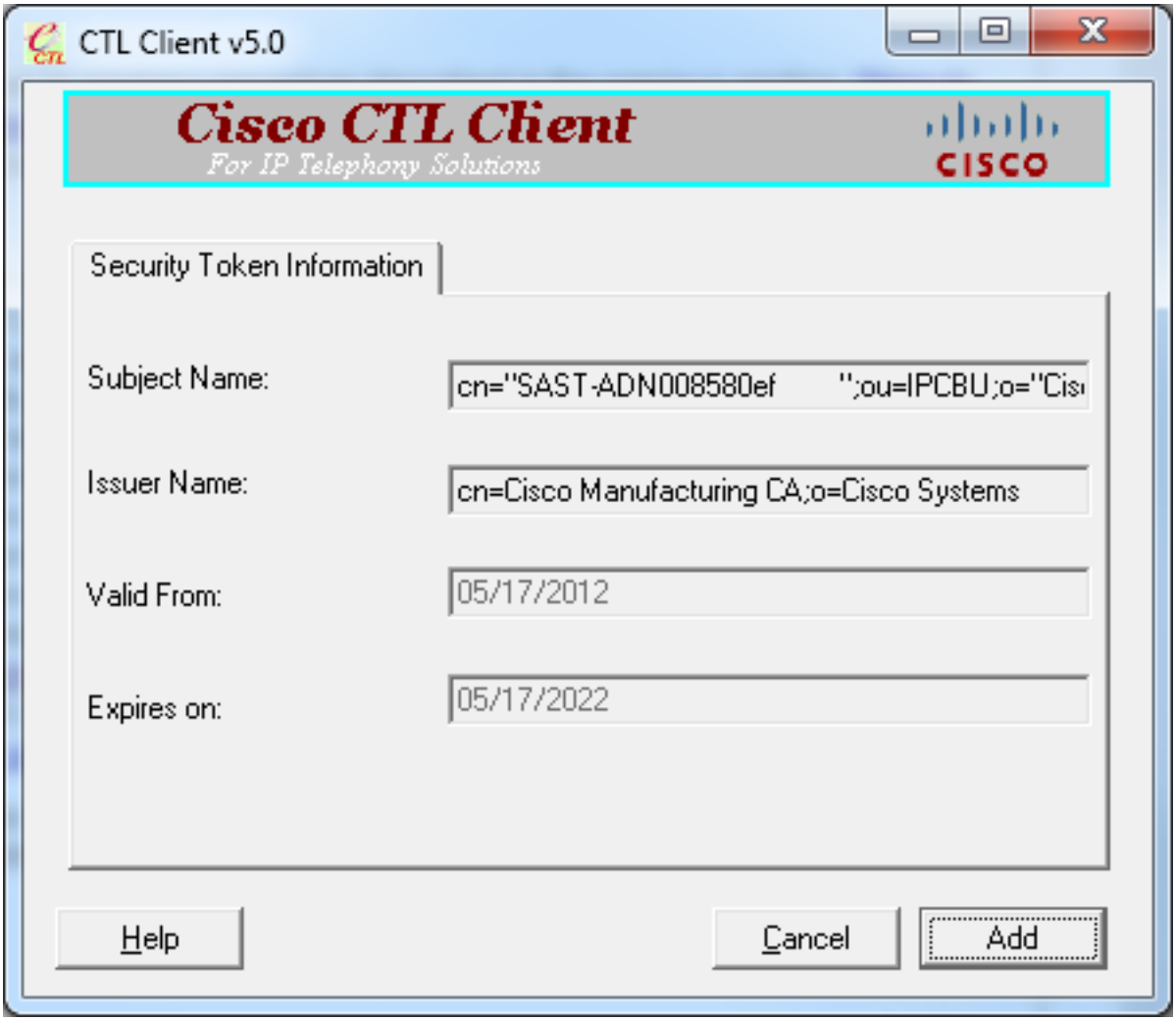

6. Auf dem Bildschirm werden alle Einträge in der neuen CTL angezeigt. Klicken Sie auf **Add Tokens (Token hinzufügen)**, um das zweite Token aus dem neuen Paar hinzuzufügen.



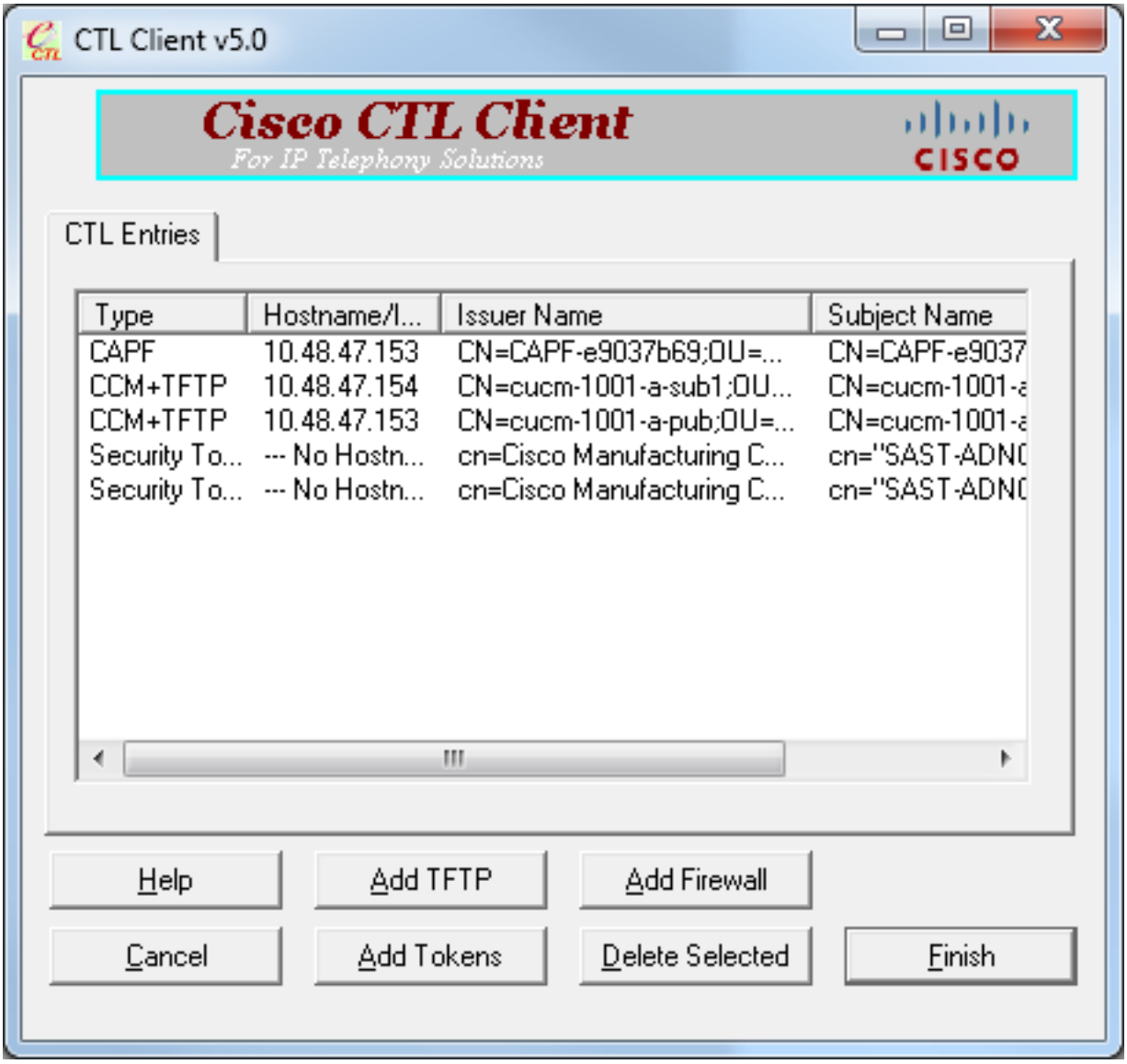

7. Sie werden aufgefordert, das aktuelle Token zu entfernen und ein neues Token einzufügen. Klicken Sie abschließend auf
OK.



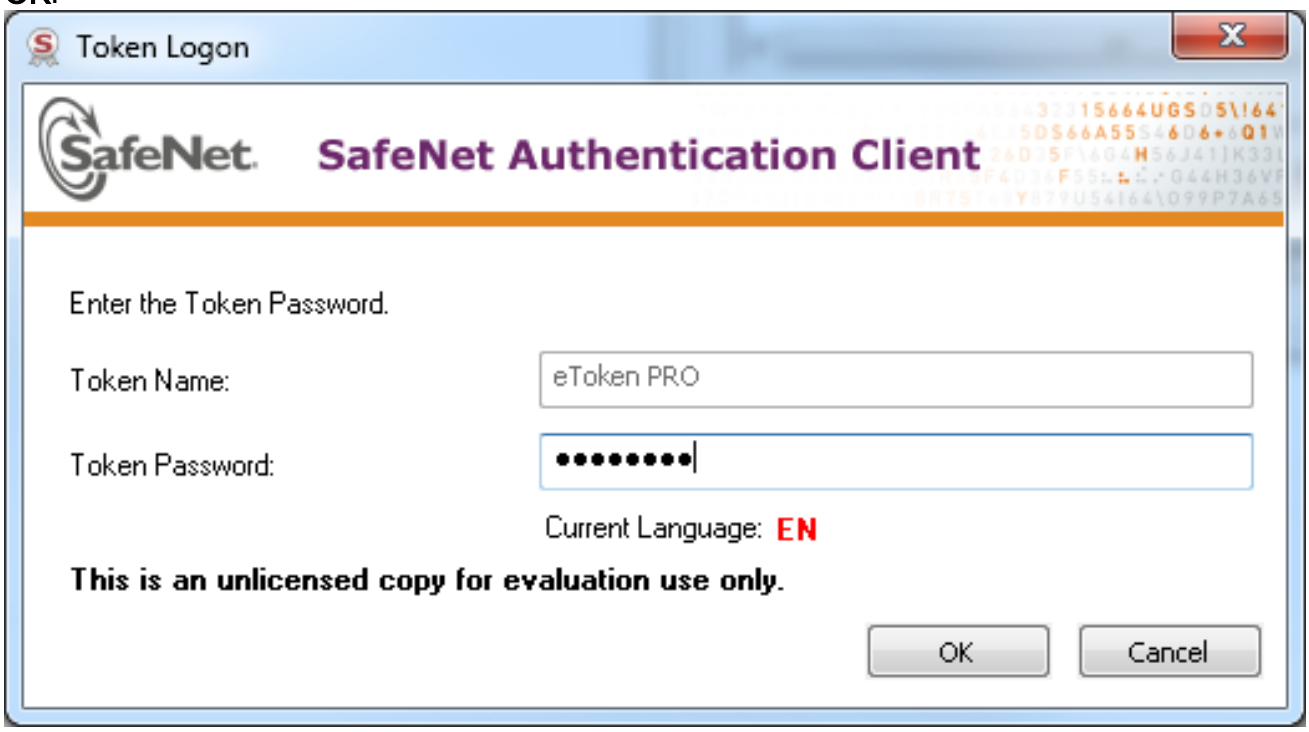

8. Es wird ein Bildschirm mit Details des neuen Tokens angezeigt. Klicken Sie auf **Hinzufügen**, um sie zu bestätigen und dieses Token
hinzuzufügen.




9. Es wird eine neue Liste von CTL-Einträgen angezeigt, die beide hinzugefügten Token enthalten. Klicken Sie auf **Fertig stellen**, um neue CTL-Dateien zu generieren.

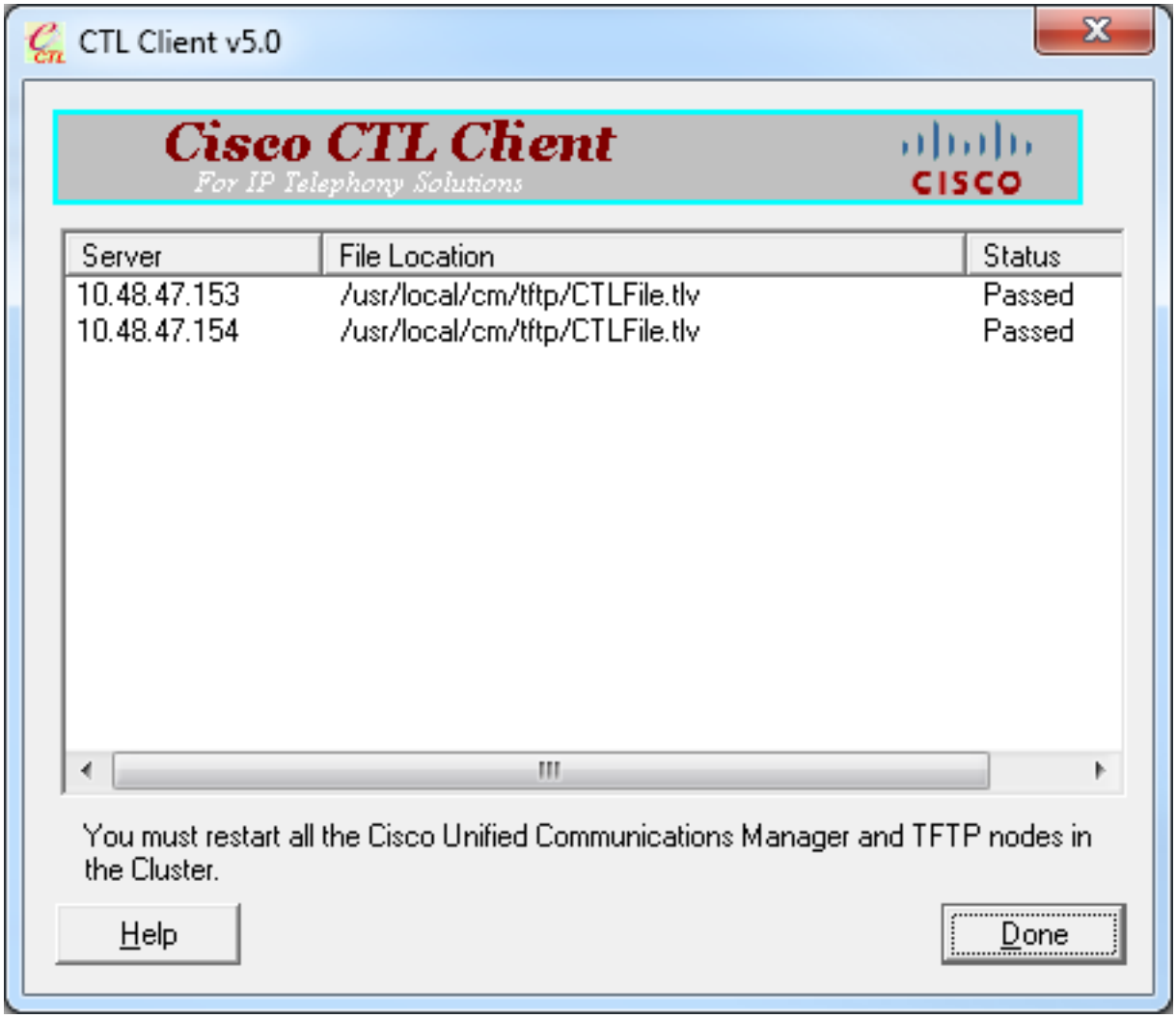



10. Geben Sie im Feld Token Password (Token-Kennwort) **Cisco123 ein**. Klicken Sie auf **OK**.




11. Sie sehen eine Bestätigung, dass der Prozess erfolgreich war. Klicken Sie auf **Fertig**, um den CTL-Client zu bestätigen und zu

beenden.




12. Starten Sie Cisco TFTP neu, gefolgt vom CallManager-Service (Cisco Unified Serviceability > Tools > Control Center - Feature Services). Die neue CTL-Datei sollte generiert werden. Geben Sie den Befehl **show ctl** zur Überprüfung ein.

```
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. Löschen Sie die CTL-Datei von jedem Telefon im Cluster (dieses Verfahren kann je nach Telefontyp variieren - weitere Informationen finden Sie in der Dokumentation, z. B. im Cisco Unified IP-Telefon 8961, 9951 und 9971 Administration Guide).**Anmerkung:** Die Telefone können sich möglicherweise noch registrieren (abhängig von den Sicherheitseinstellungen auf dem Telefon) und arbeiten, ohne mit Schritt 13 fortzufahren. Auf ihnen wird jedoch die alte CTL-Datei installiert. Dies kann zu Problemen führen, wenn Zertifikate neu generiert werden, ein anderer Server zum Cluster hinzugefügt wird oder die Serverhardware ersetzt wird. Es wird nicht empfohlen, den Cluster in diesem Status zu belassen.
14. Verschieben Sie den Cluster auf "Nicht sicher". Weitere Informationen finden Sie im Abschnitt Ändern der CUCM-Clustersicherheit von Gemischter Modus in Nicht-Sicherheitsmodus mit dem CTL-Client.

# Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.