混合モードから非セキュア モードに変更された CUCM クラスタの設定例

内容

概要

このドキュメントでは Cisco Unified Communications Manager（CUCM）のセキュリティモードを混合モードから非セキュア モードへ切り替えるために必要な手順を説明します。また、切り替えと完了時に証明書信頼リスト（CTL）ファイルの内容がどのように変更されるかも示します。

CUCM セキュリティ モードの変更は主に 3 つの部分に分けることができます。

1a.CTL クライアントを実行し、必要な種類のセキュリティ モードを選択します。
1b.必要な種類のセキュリティ モードを選択するための CLI コマンドを入力します。
2.これらのサービスを実行するすべてのCUCMサーバでCisco CallManagerおよびCisco TFTPサービスを再起動します。
3.すべてのIP Phoneを再起動して、CTLファイルの更新バージョンをダウンロードできるようにします。

> **注**：クラスタのセキュリティ モードが混合モードから非セキュア モードに変更されても CTL ファイルは各サーバと電話機に残存しますが、この CTL ファイルには CCM+TFTP（サーバ）証明書は一切含まれません。CTL ファイルに CCM+TFTP（サーバ）証明書は含まれないため、電話機は CUCM に強制的に非セキュアに登録されます。

前提条件

要件

CUCM バージョン 10.0(1) 以降の知識があることが推奨されます。また、次のことを確認してください。

- CTL プロバイダー サービスは、クラスタのすべてのアクティブな TFTP サーバ上で実行され、アップ状態になっていること。このサービスはデフォルトで TCP ポート 2444 で実行され、これは CUCM サービス パラメータ設定で変更できます。
- 認証局プロキシ機能（CAPF）サービスがパブリッシャ ノードで実行され、アップ状態になっていること。
- クラスタ内のデータベース（DB）の複製が正常に動作しており、サーバがデータをリアルタイムに複製していること。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CUCM リリース 10.0.1.11900-2（2 ノードのクラスタ）
- Cisco 7975 IP フォン（Skinny Client Control Protocol（SCCP）、ファームウェア バージョン SCCP75.9-3-1SR3-1S を使用して登録されたもの）
- クラスタを混合モードに設定するには、2 つのシスコ セキュリティ トークンが必要です。
- クラスタを非セキュア モードに設定するには、上記のセキュリティ トークンのうち 1 つが必要です。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

CTL クライアントのプラグインを実行するには、CUCM パブリッシャ サーバに存在する最新の CTL ファイルを作成または更新するために挿入される、少なくとも 1 つのセキュリティ トークンへのアクセスが必要です。つまり、CUCM の現在の CTL ファイルに存在する eToken 証明書のうちの少なくとも 1 つが、セキュリティ モードの変更で使用するセキュリティ トークンにも含まれている必要があります。

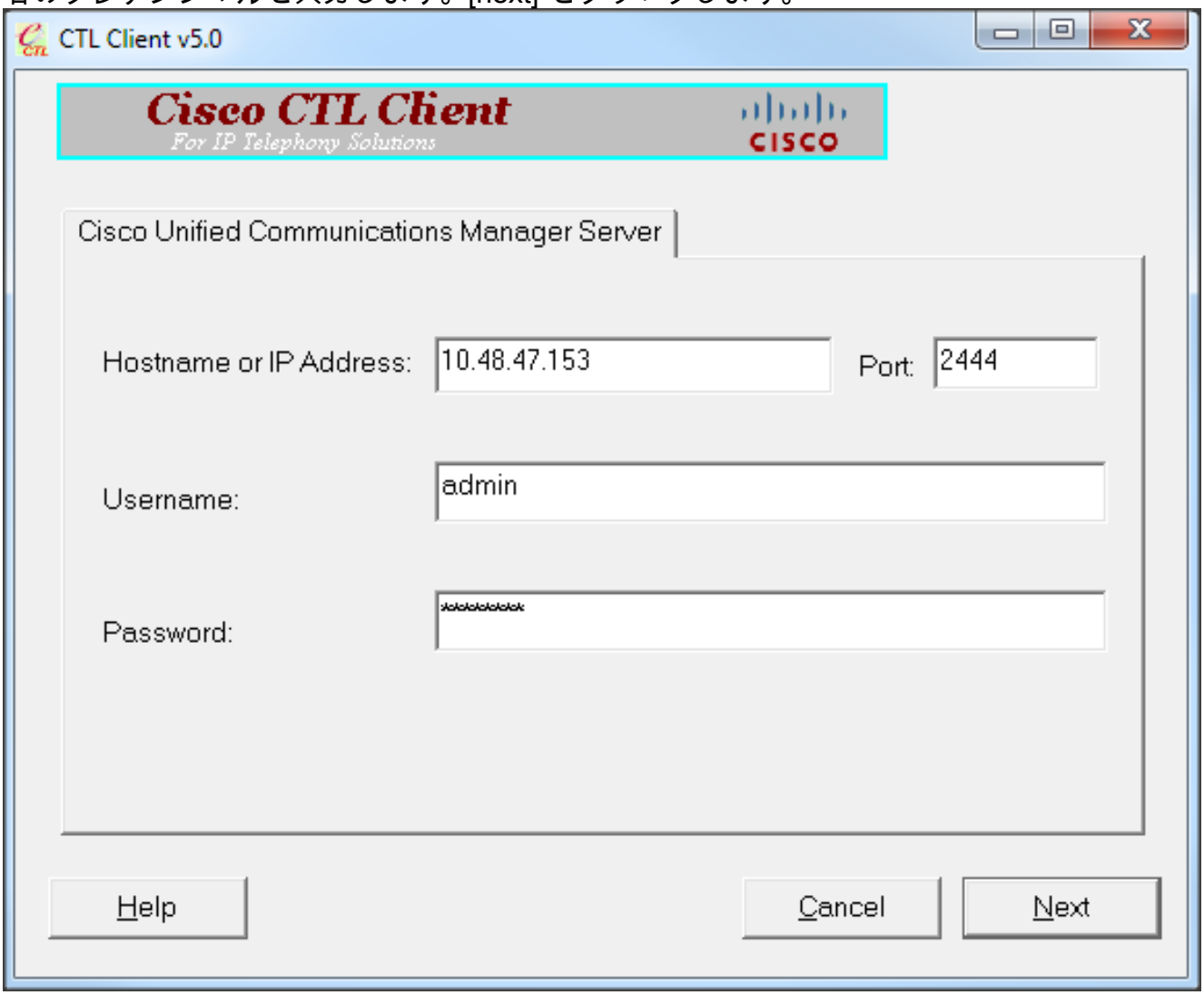
設定

CTL クライアントで CUCM クラスタセキュリティを混合モードから非セキュアモードに変更する

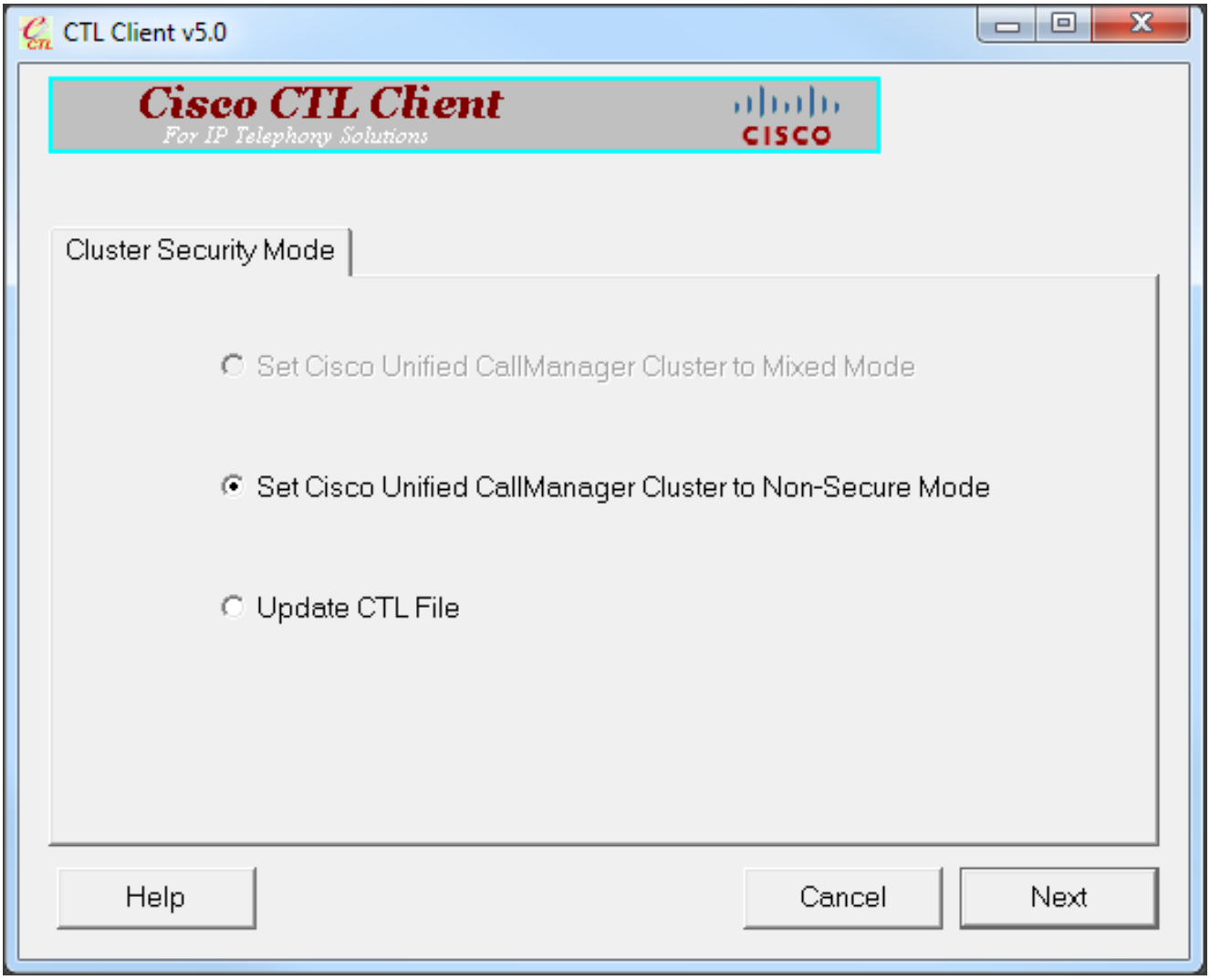
CTL クライアントで CUCM クラスタセキュリティを混合モードから非セキュアモードに変更す

るには、次の手順を実行します。

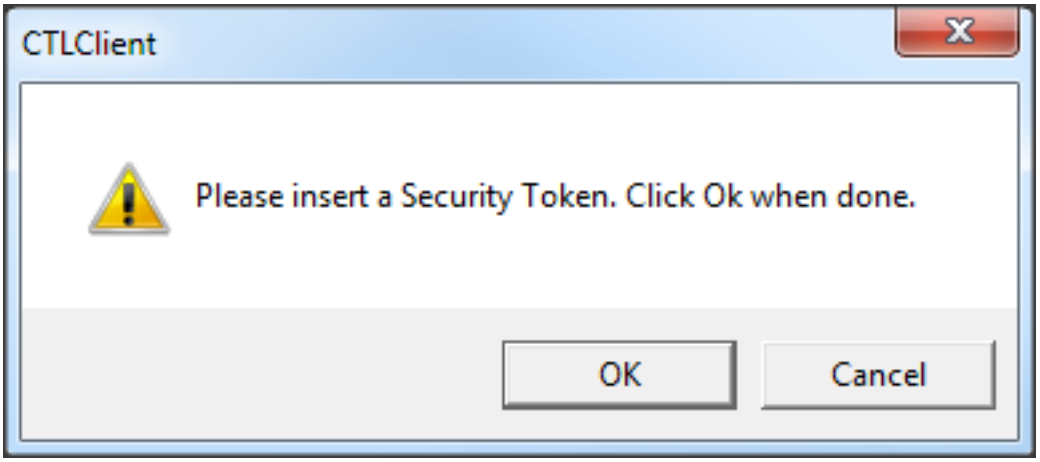
1. 最新の CTL ファイルを設定するために挿入したセキュリティ トークンのうちの 1 つを取得します。
2. CTL クライアントを実行します。CUCM パブリッシャの IP ホスト名/アドレスと CCM 管理者のクレデンシャルを入力します。[next] をクリックします。



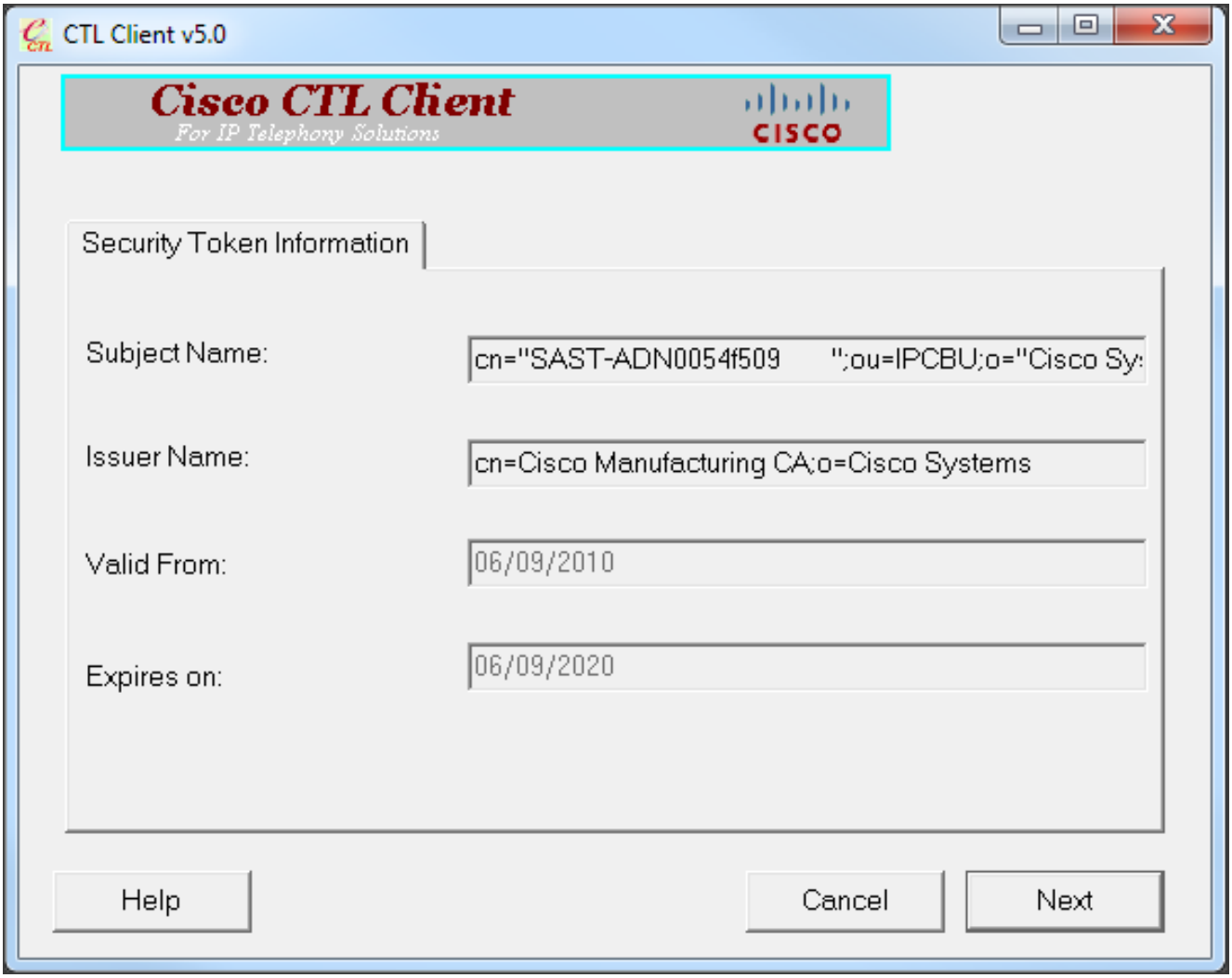
3. [Set Cisco Unified CallManager Cluster to Non-Secure Mode] オプション ボタンをクリックします。[next] をクリックします。



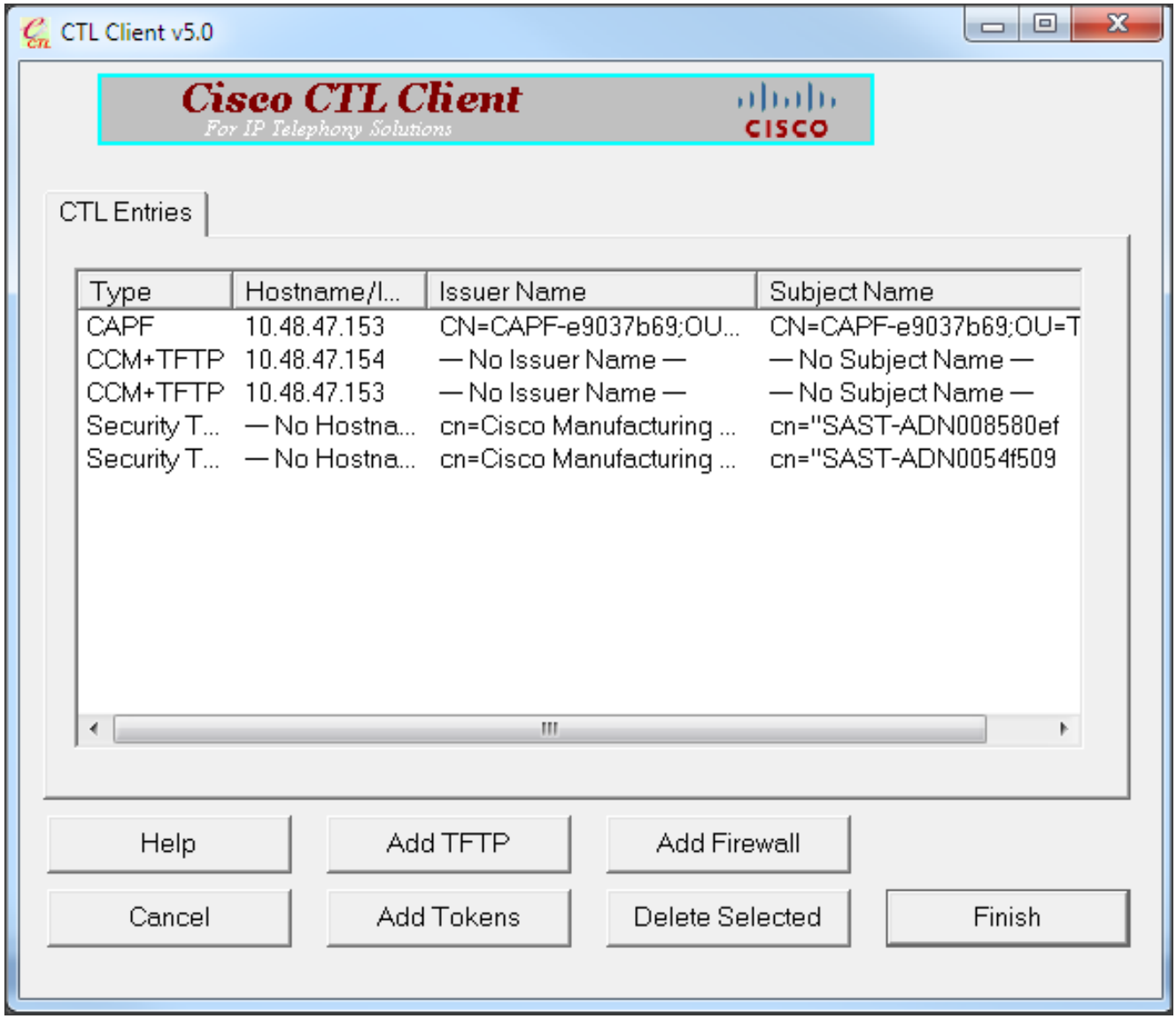
4. 最新の CTL ファイルの設定で挿入したセキュリティ トークンのうち 1 つを挿入し、[OK] をクリックします。これは CTLFile.tlv 内の証明書のリストを入力するために使用されたトークンのうちの 1 つです。



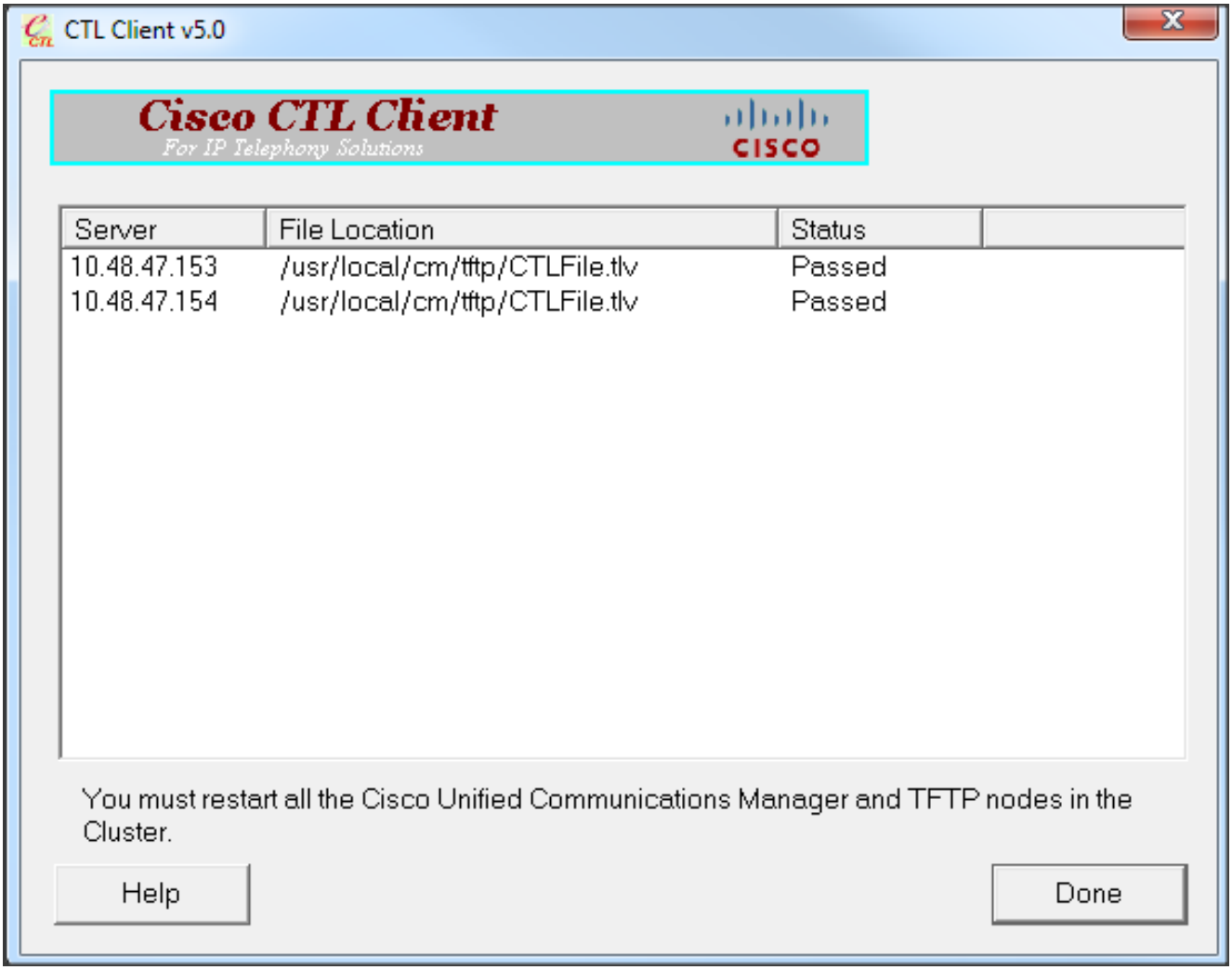
5. セキュリティ トークンの詳細が表示されます。[next] をクリックします。



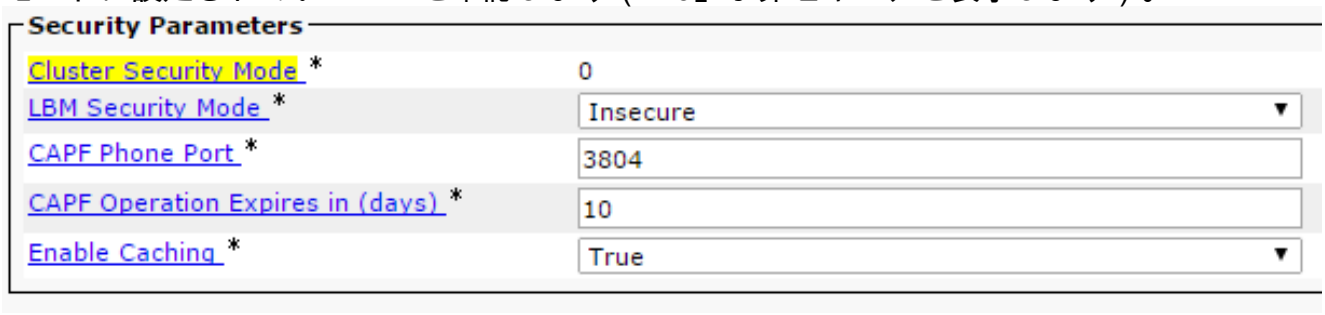
6. CTL ファイルの内容が表示されます。[Finish] をクリックします。パスワードの入力を求められたら、「Cisco123」 と入力します。



7. CTL ファイルが存在する CUCM サーバのリストが表示されます。[Done] をクリックします。



8. [CUCM Admin Page] > [System] > [Enterprise Parameters]を選択し、クラスタが非セキュアモードに設定されていることを確認します（「0」が非セキュアを表示します）。



9. TFTP サービスおよび Cisco CallManager サービスを実行しているクラスタ内のすべてのノードで、これらのサービスを再起動します。
10. IP 電話が CUCM TFTP から新しいバージョンの CTL ファイルを取得できるように、すべての IP 電話を再起動します。

CLI で CUCM クラスタセキュリティを混合モードから非セキュアモードに変更する

これは、CUCM リリース 10.X 以降のみの設定です。CUCM クラスタ セキュリティ モードを非セキュアに設定するには、パブリッシャの CLI で **utils ctl set-cluster non-secure-mode コマンドを入力します。**完了したら、TFTP サービスおよび Cisco CallManager サービスを実行している

クラスタ内のすべてのノードで、これらのサービスを再起動します。

コマンドを使った場合の CLI の出力のサンプルを以下に示します。

```
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:
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

CTLFIle.tlv を確認するには、次の 2 つの方法があります。

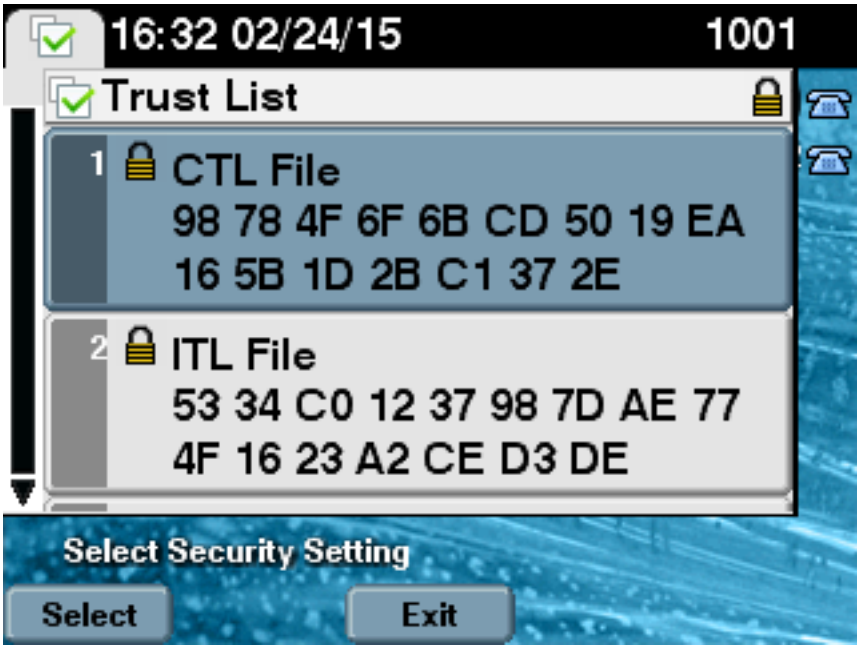
- CUCM TFTP側にあるCTLFIle.tlvの内容とMD5チェックサムを確認するには、CUCM CLIで **show ctl**コマンドを入力します。CTLFIle.tlv ファイルは、すべての CUCM ノードで同一のものでなければなりません。
- 7975 IP Phone で MD5 チェックサムを確認するには、[Settings] > [Security Configuration] > [Trust List] > [CTL File] を選択します。

  注：電話のチェックサムを確認すると、電話のタイプに応じて、MD5 または SHA1 が表示されます。

セキュリティ モードに設定された CUCM クラスタ - CTL ファイル チェックサム

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

IP フォン側で同一の CTL ファイルがインストールされているか確認できます (同一なら MD5 チェックサムは CUCM が出力したものと一致します) 。



非セキュア モードに設定された CUCM クラスタ - CTL ファイルの内容

非セキュア モードに設定されている CUCM クラスタからの CTL ファイルの例を示します。CCM+TFTP 証明書が空で、一切内容が含まれないことが確認できます。CTL ファイルの残りの証明書は変更されず、CUCM が混合モードに設定されていたときとまったく同じです。

```
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)
```

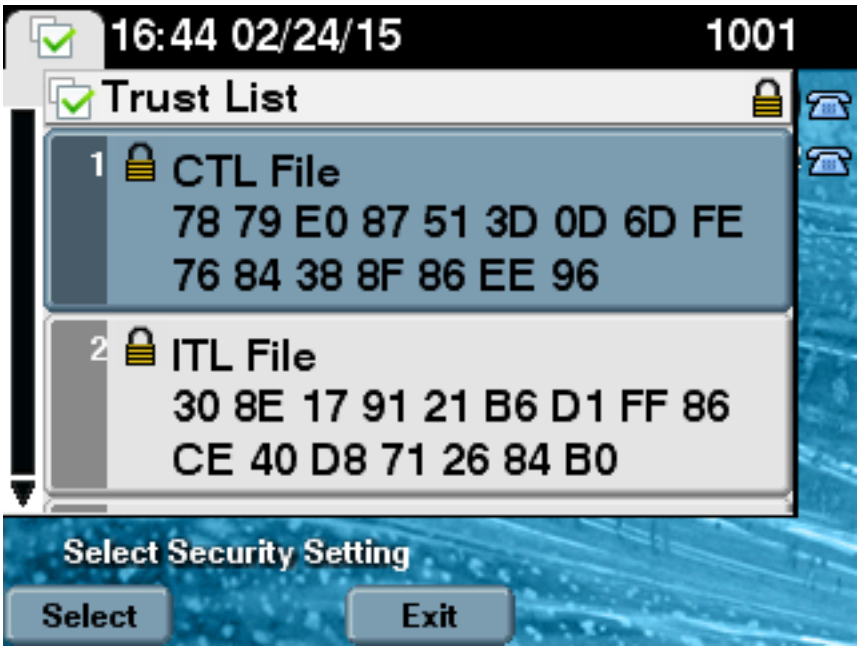
```
10 IPADDRESS 4

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:
```

IP フォンが再起動し、新しいバージョンの CTL ファイルをダウンロードした後には、IP フォン側で MD5 チェックサムが CUCM の出力と一致することが確認できます。



USB トークン喪失時に CUCM クラスタ セキュリティを混合モードから非セキュア モードへ切り替える

セキュア クラスタのセキュリティ トークンが失われることがあります。この状況では、次の 2 つのシナリオを考慮する必要があります。

- クラスタがバージョン 10.0.1 以降を実行している場合
- クラスタがバージョン 10.x 以前を実行している場合

最初のシナリオでは、問題を解決するため、CLI で CUCM クラスタセキュリティを混合モードから非セキュアモードに変更するセクションの手順を実行してください。CLI コマンドは CTL トークンを必要としないため、このコマンドは CTL クライアントでクラスタを混合モードにしてあっても使用できます。

バージョン 10.x 以前の CUCM が使用されている場合は、状況はより複雑です。いずれかのトークンのパスワードを紛失または失念した場合でも、他のトークンを使い、現行の CTL ファイルと CTL クライアントを実行できます。冗長性を確保するため、可能な限り、他の eToken を取得し、CTL ファイルに含めておくことを強く推奨します。CTL ファイルに記載されているすべての eToken のパスワードを紛失または失念した場合は、新しい eToken のペアを取得し、ここで説明

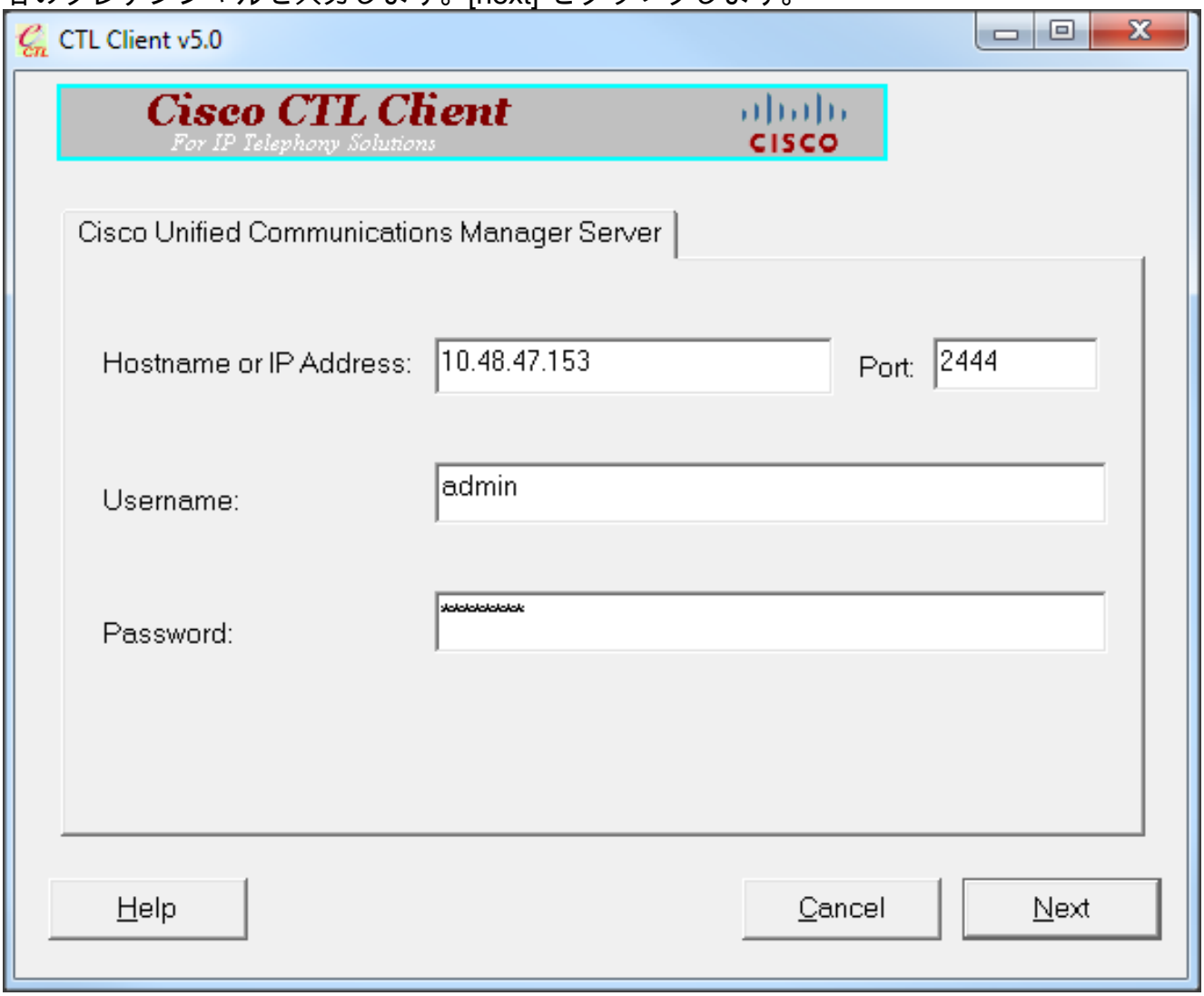
する手順を手作業で実行する必要があります。

1. **file delete tftp CTLFile.tlv コマンドを入力し、すべての TFTP サーバから CTL ファイルを削除します。**

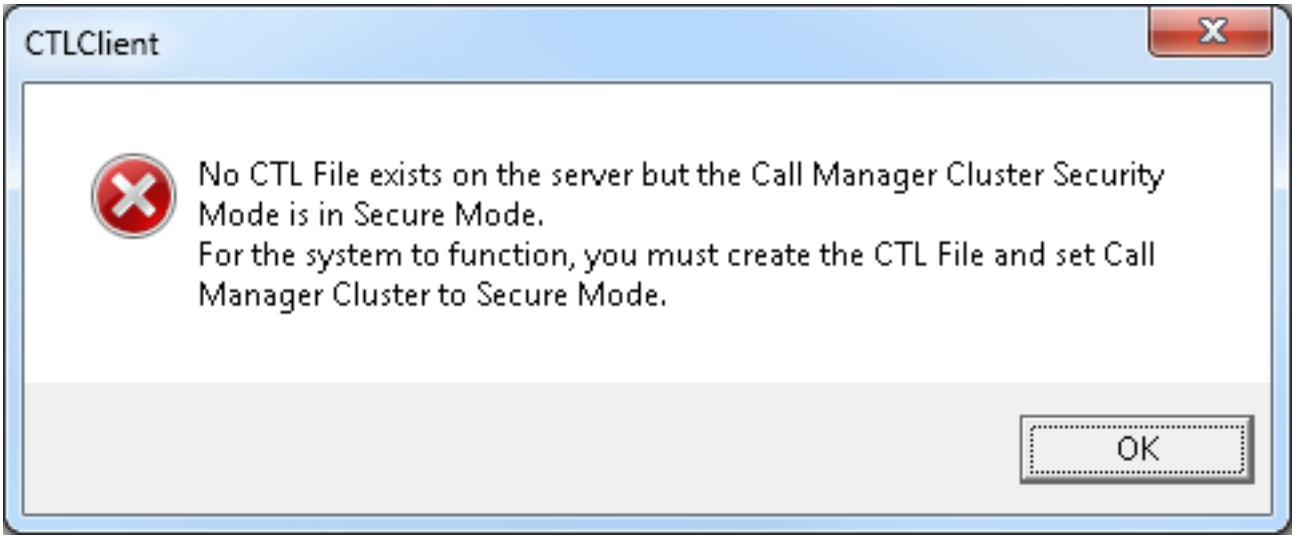
```
admin:file delete tftp CTLFile.tlv
Delete the File CTLFile.tlv?
Enter "y" followed by return to continue: y
files: found = 1, deleted = 1

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.
```

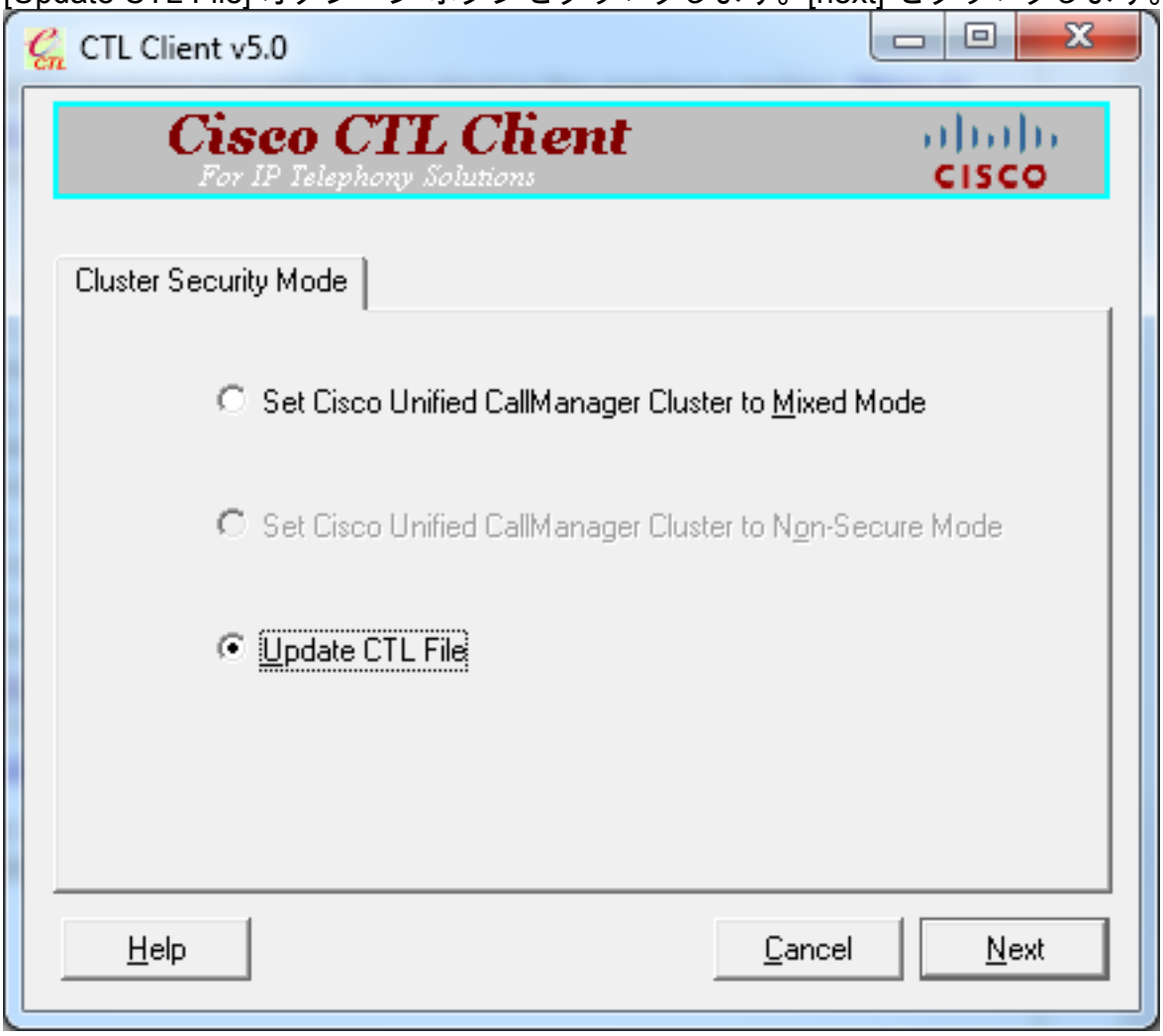
2. CTL クライアントを実行します。CUCM パブリッシャの IP ホスト名/アドレスと CCM 管理者のクレデンシャルを入力します。[next] をクリックします。



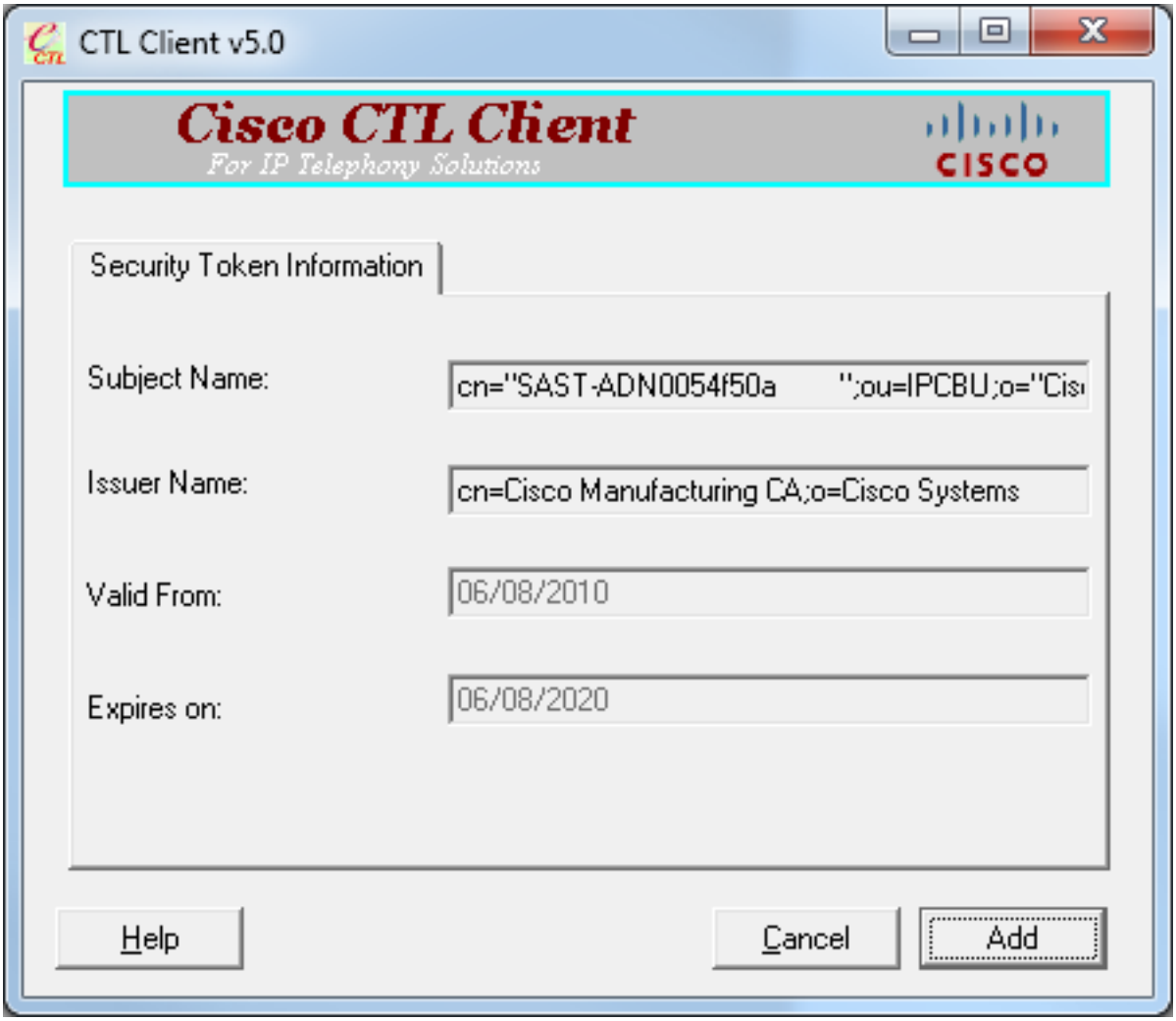
3. クラスタは混合モードになっており、CTL ファイルは存在しないため、このことを示す警告が表示されます。[OK] をクリックしてこれを無視し、[proceed forward] で次へ進みます。



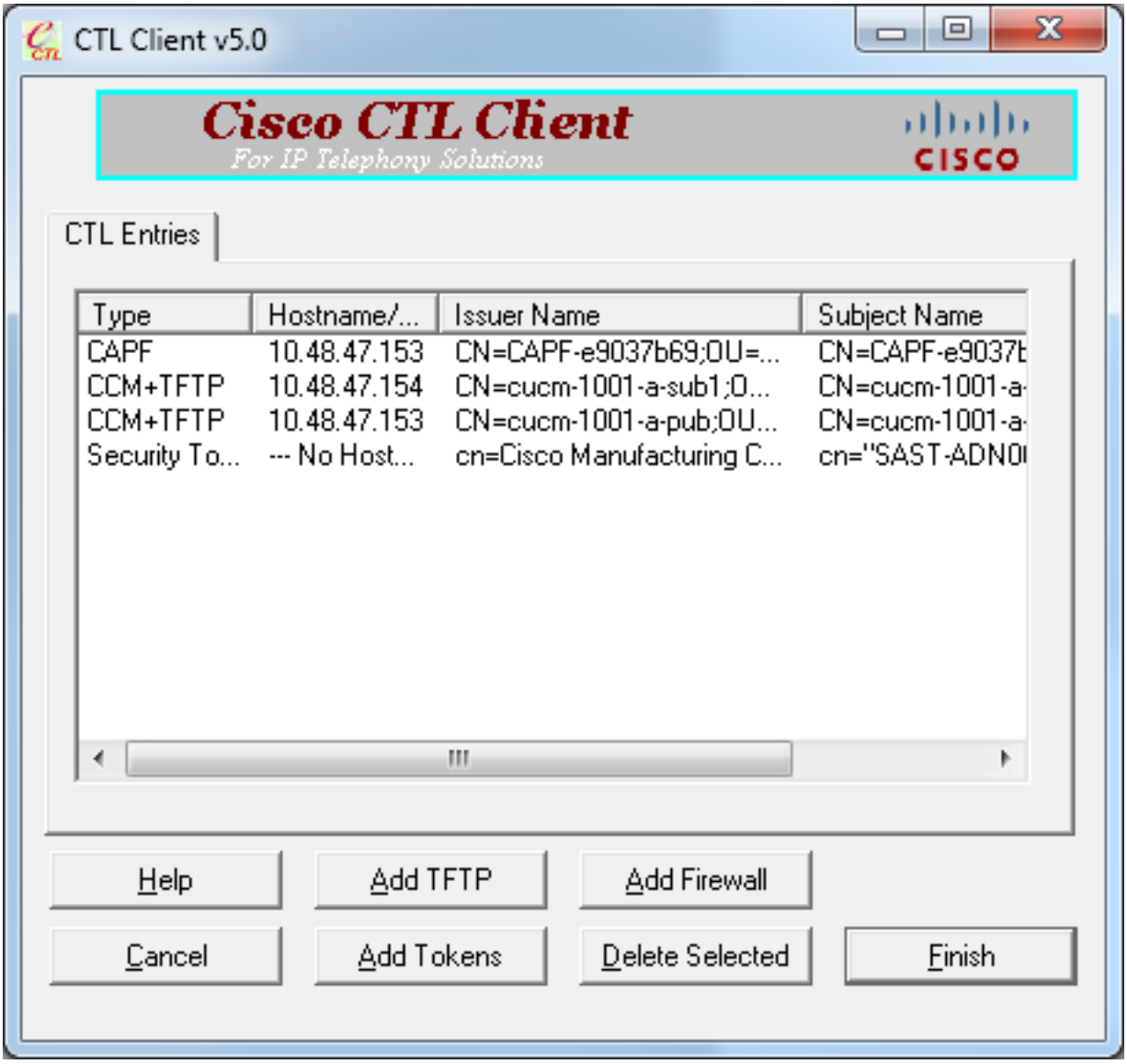
4. [Update CTL File] オプション ボタンをクリックします。[next] をクリックします。



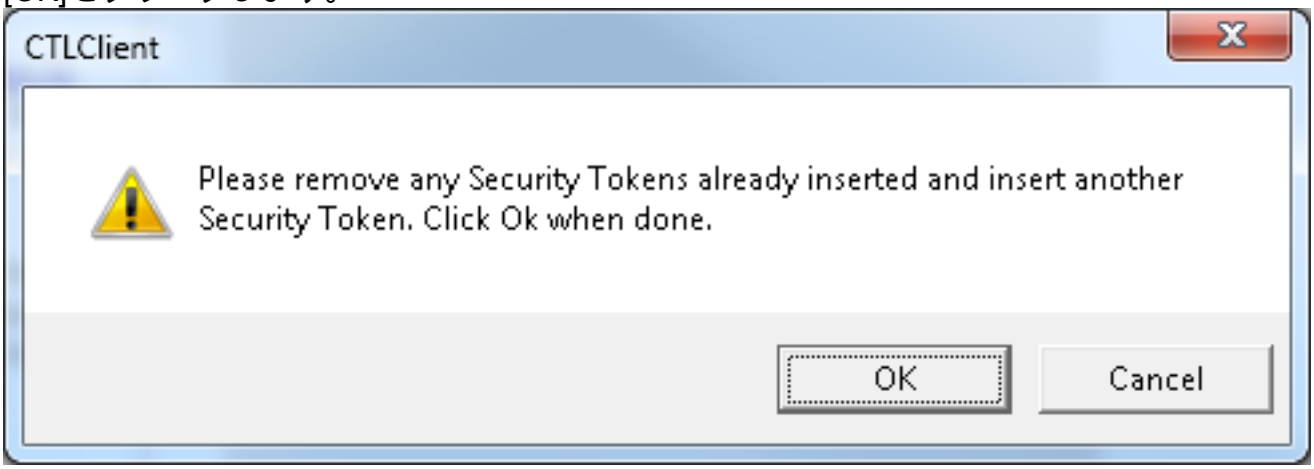
5. CTL クライアントは、セキュリティ トークンを追加のための表示を行います。[Add] をクリックして続行します。



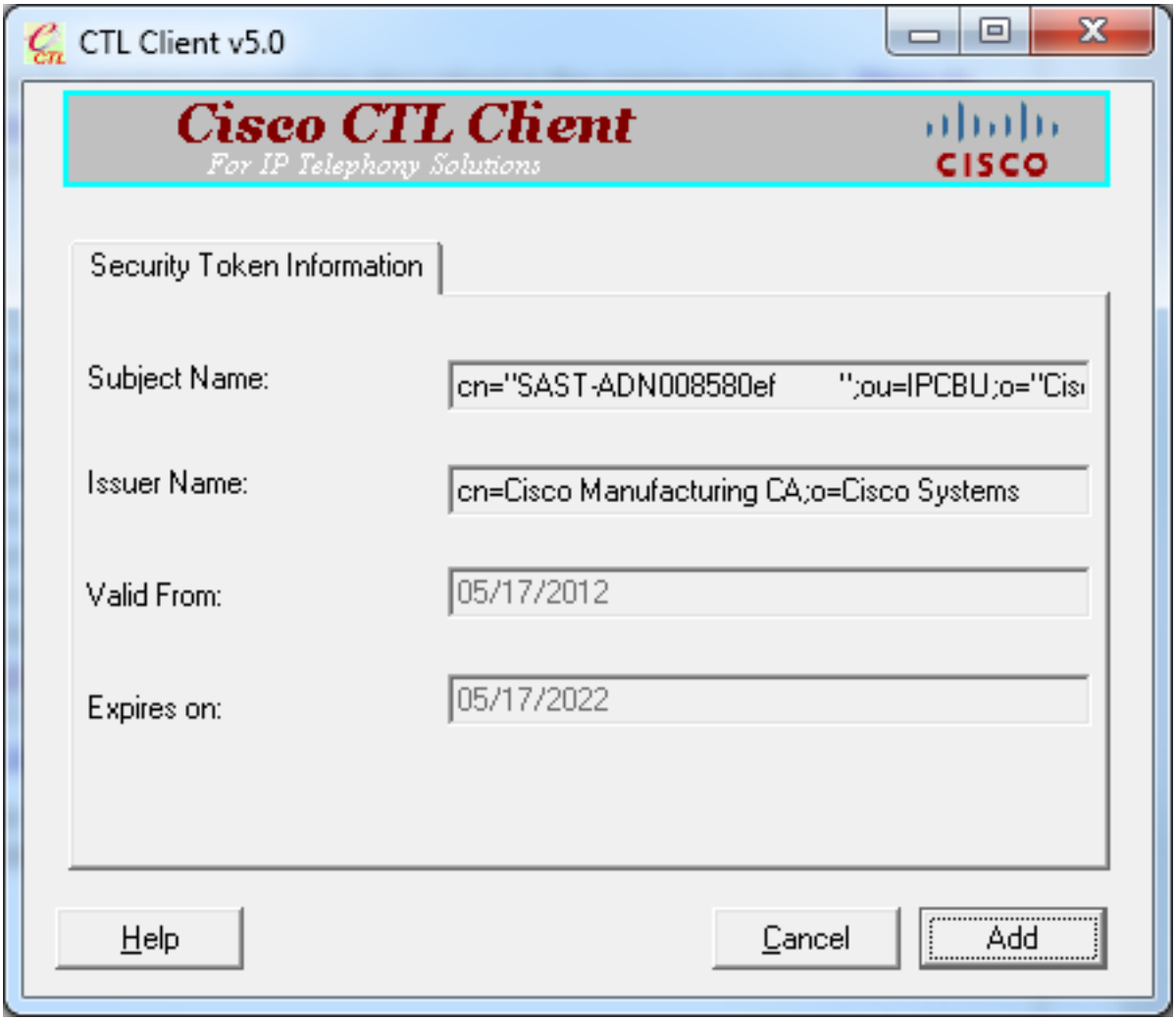
6. 新しい CTL のすべてエントリが表示されます。[Add Tokens] をクリックし、新しいペアの 2 つ目のトークンを追加します。



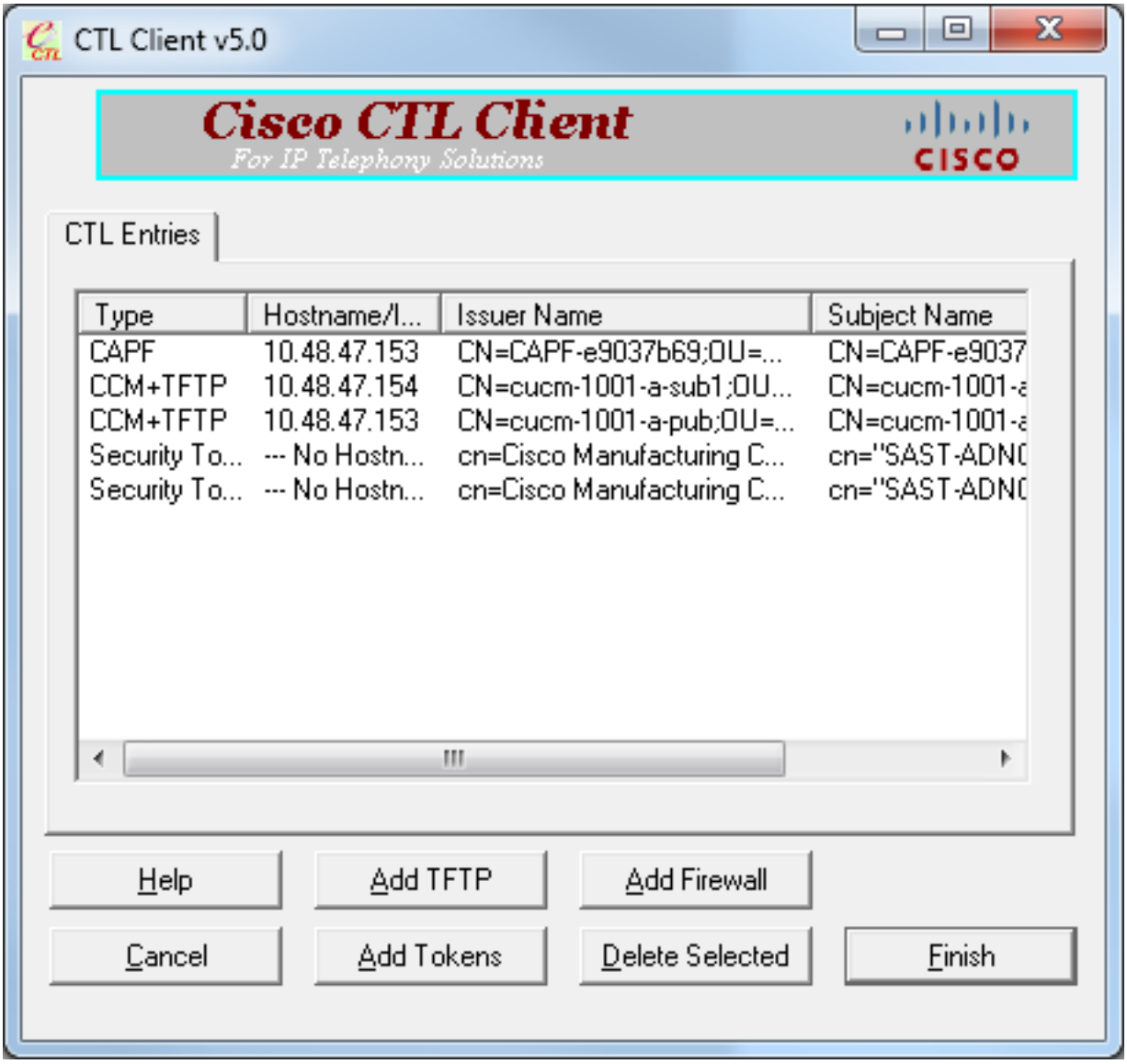
7. 現在のトークンを削除し、新しいユーザを挿入するか、確認が表示されます。完了したら[OK]をクリックします。



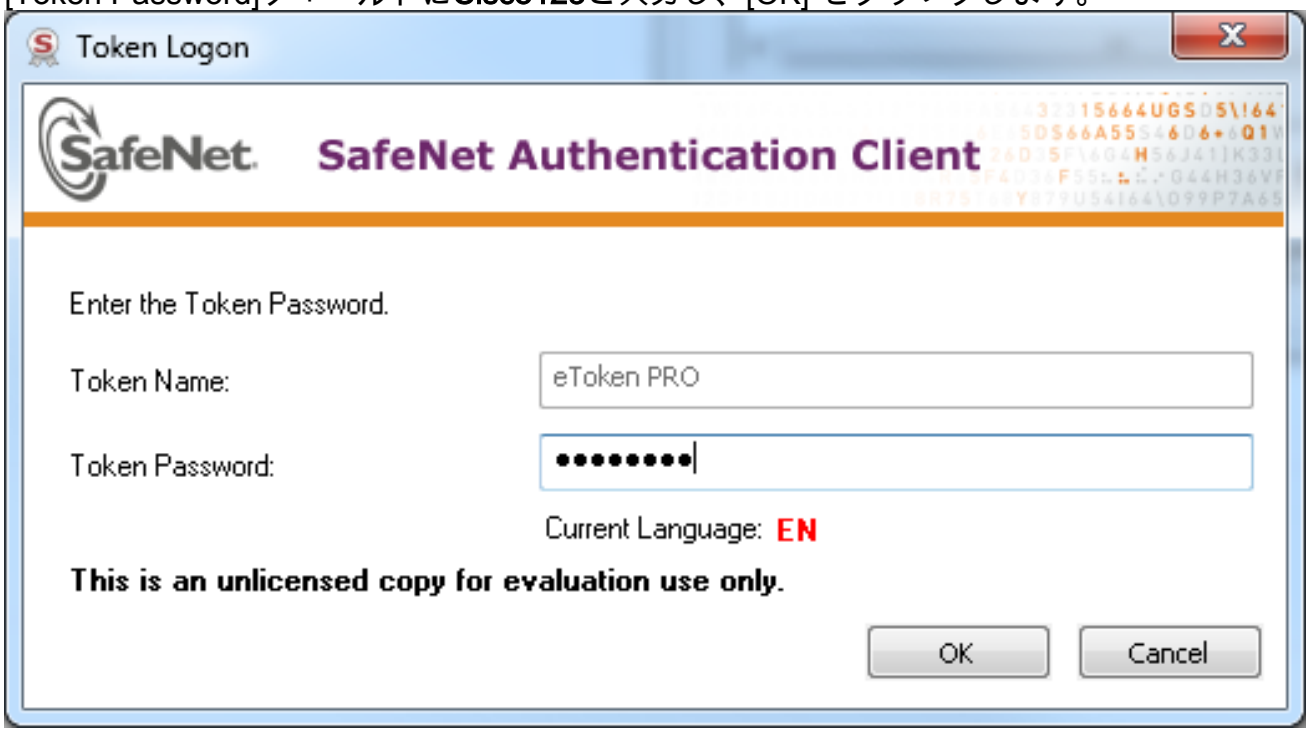
8. 新しいトークンの詳細を示す画面が表示されます。[Add] をクリックして、トークンの詳細を確認し、トークンを追加します。



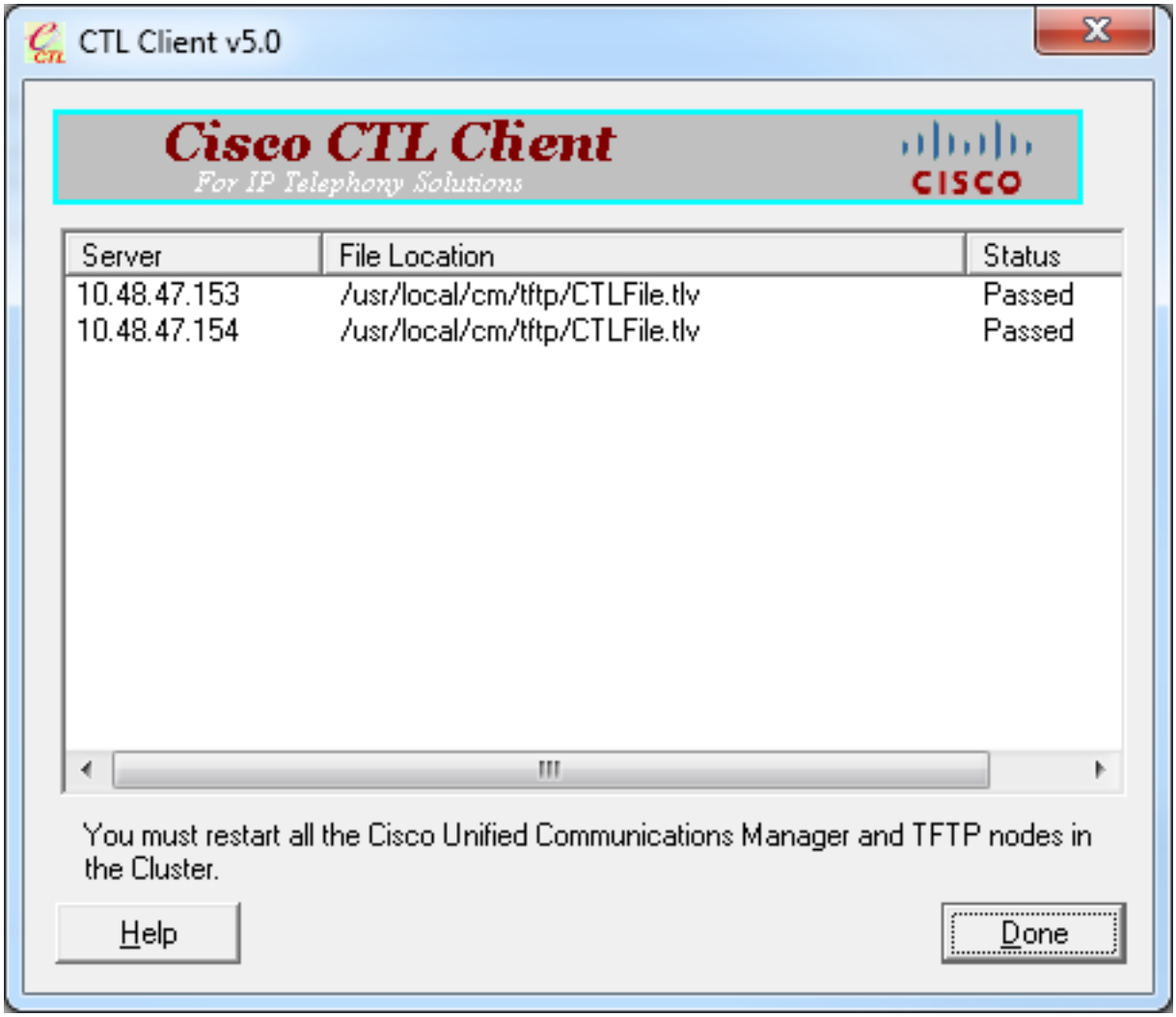
9. 両方のトークンが追加された新しい CTL エントリのリストが表示されます。[Finish] をクリックして、新しい CTL ファイルを生成します。



10. [Token Password]フィールドに**Cisco123**と入力し、[OK] をクリックします。



11. プロセスが成功したことを示す確認が表示されます。[Done] をクリックし、以上を確認して CTL クライアントを終了します。



12. CallManager サービスに続いて Cisco TFTP を再起動します（[Cisco Unified Serviceability] > [Tools] > [Control Center - Feature Services]）。 新しい CTL ファイルが生成されます。 確認のために **show ctl コマンドを入力します。**

```
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. クラスタの各電話機から CTL ファイルを削除します（この手順は電話の種類により異なることがあります - 詳細は Cisco Unified IP Phone 8961、9951、9971 アドミニストレーション ガイドなどのドキュメンテーションを参照してください）。**注：**電話機は（電話機のセキュリティ設定に応じて）引き続き登録でき、手順13に進まなくても動作する場合があります。ただし、古いCTLファイルがインストールされます。このことにより、証明書を再生成した場合、クラスタに他のサービスが追加された場合、サーバのハードウェアが交換された場合に問題が発生することがあります。クラスタをこの状態で放置することは推奨されません。
14. クラスタを非セキュアに変更してください。詳細は CTL クライアントで CUCM クラスタ セキュリティを混合モードから非セキュアモードに変更するセクションを参照してください。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。