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

目次

概要

資料がミックス モードから非セキュア モードに Cisco Unified Communications Manager （CUCM）セキュリティモードを変更するために必要なステップを記述したものです。 この移動が完了するとき Certificate trust list （CTL） ファイルのコンテンツがどのように変更されるかまた示します。

CUCM セキュリティモードを変更する 3 人のメジャー部分があります:

1a. CTL クライアントを実行し、セキュリティモードの望ましいバリアントを選択して下さい。
1b. セキュリティモードの望ましいバリアントを選択するために CLI コマンドを入力して下さい。
2. これらのサービスを動作するすべての CUCM サーバの Cisco Unified CallManager および Cisco TFTP サービスを再開して下さい。
3. 彼らが 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すべての IP 電話を再起動して下さい。

> **注:** クラスタ セキュリティモードがミックス モードから非セキュア モードにそれでもサーバと電話で存在 する CTL ファイル変更されるが CTL ファイル CCM+TFTP （サーバ）認証を含まれていません。 CCM+TFTP （サーバ）認証が CTL ファイルにないので、これは CUCM と非セキュアように登録するために電話を強制します。

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 サービスはアップ、クラスタの TFTP すべてのアクティブなサーバで動作します。 デフォルトでサービスは TCPポート 2444 で動作します、これは CUCM サービスパラメータ 設定で修正することができます。
- 認証局（CA）プロキシ 機能（CAPF）サービスはアップ、パブリッシャ ノードで動作します。
- クラスタのデータベース（DB）複製はリアルタイムのサーバ反復実験データ正しくはたらき。

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くものです。

- 2 つのノードの CUCM リリース 10.0.1.11900-2 クラスタ
- Cisco 7975 IP Phone （Skinny Client Control Protocol（SCCP）、ファームウェアのバージョン SCCP75.9-3-1SR3-1S に登録されている）
- 2 つの Ciscoセキュリティ トークンはミックス モードにクラスタを設定 して必要です
- 以前にリストされているセキュリティ トークンの 1 つは非セキュア モードにクラスタを設定して必要です

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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分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 プラグインを実行するために CUCM パブリッシャ サーバで存在 する最新の CTL ファイルを作成するか、またはアップデートするために挿入された少なくとも 1 つのセキュリティ トークンにアクセスできることを必要とします。 すなわち、CUCM の電流 CTL ファイルの存在がセキュリティモードを変更するのに使用するセキュリティ トークンである必要があること eToken 認証の少なくとも 1 つ。

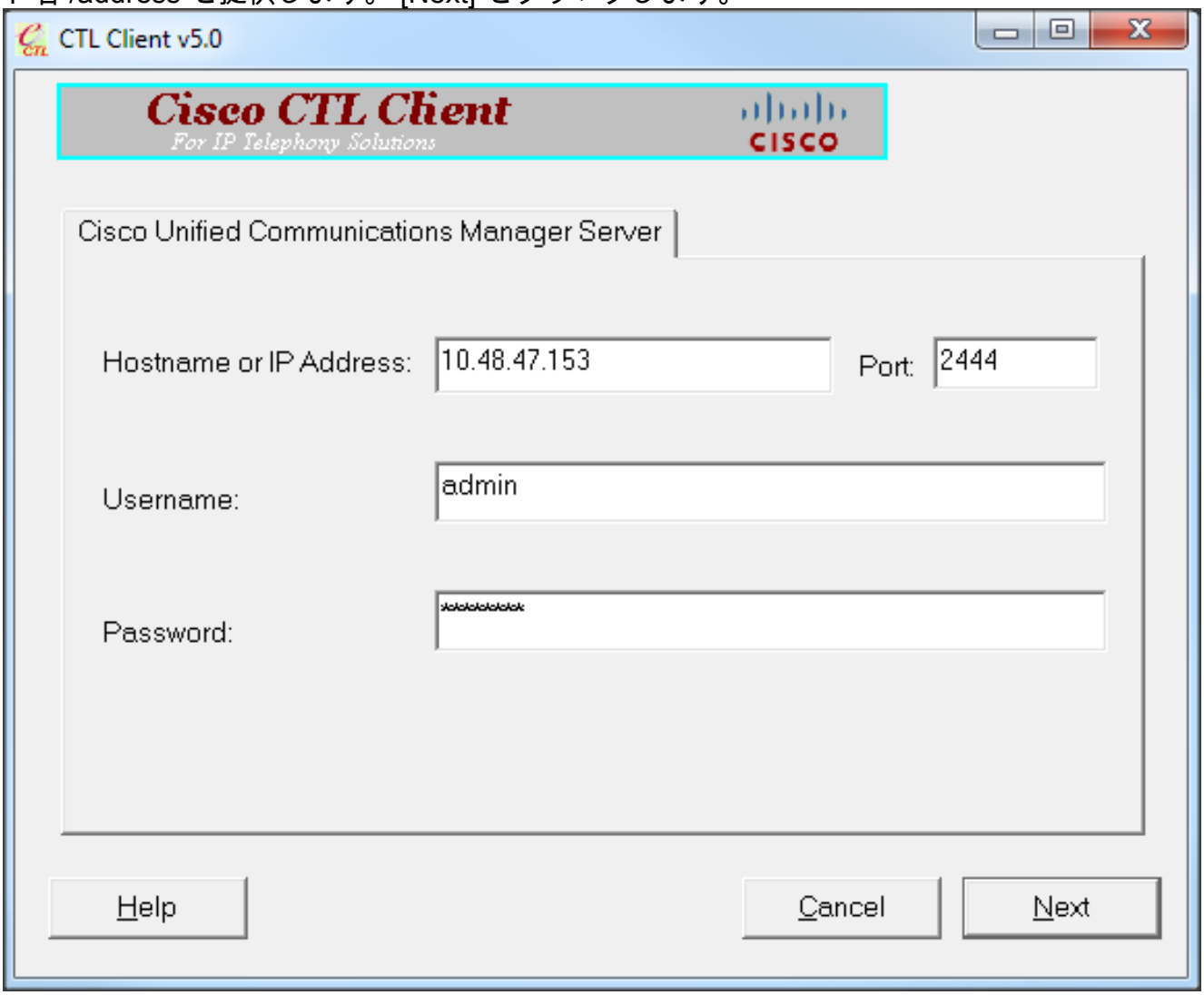
設定

ミックス モードから CTL クライアントとの非セキュア モードに CUCM クラスタ セキュリティを変更して下さい

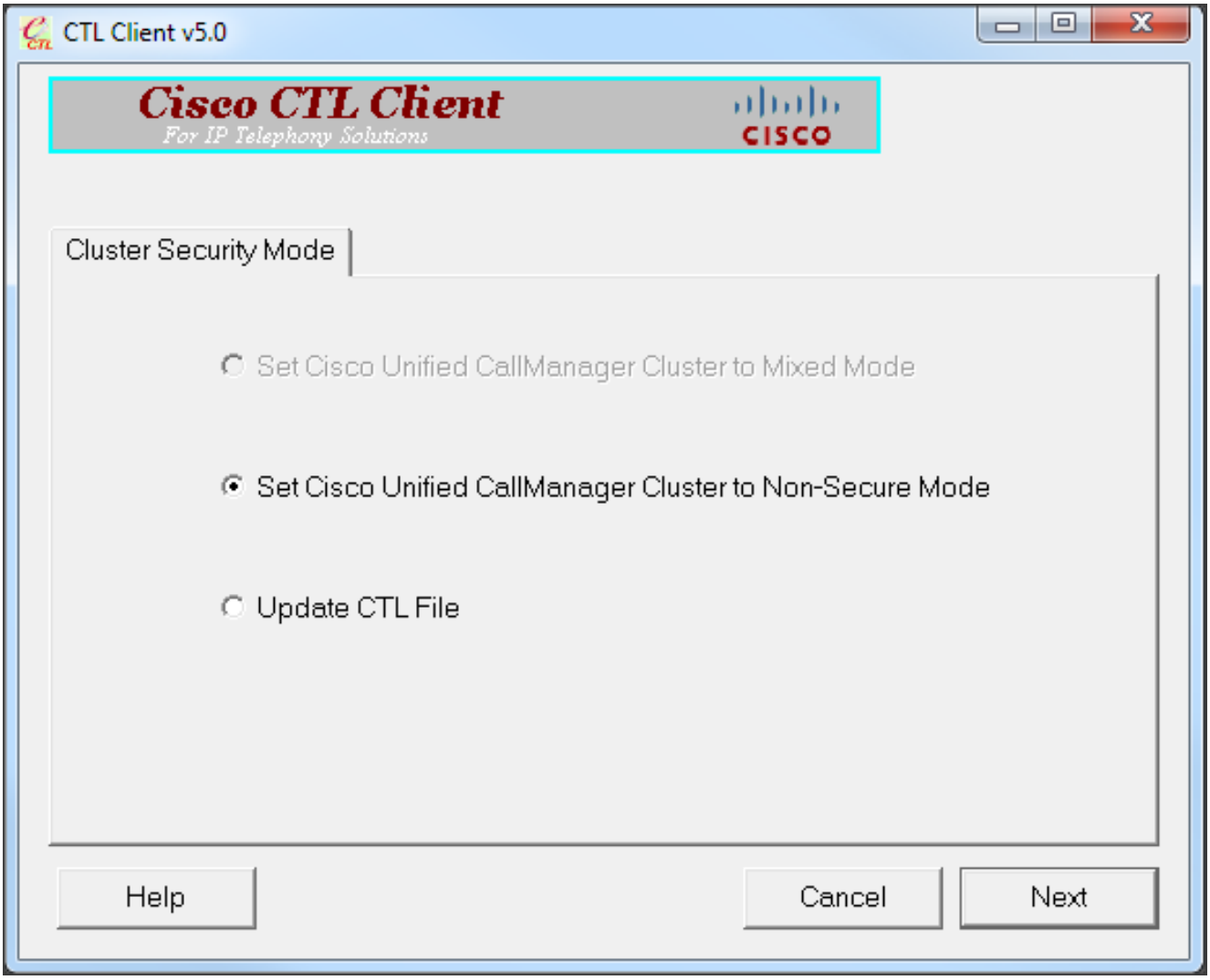
ミックス モードから CTL クライアントとの非セキュア モードに CUCM クラスタ セキュリティ

を変更するためにこれらのステップを完了して下さい:

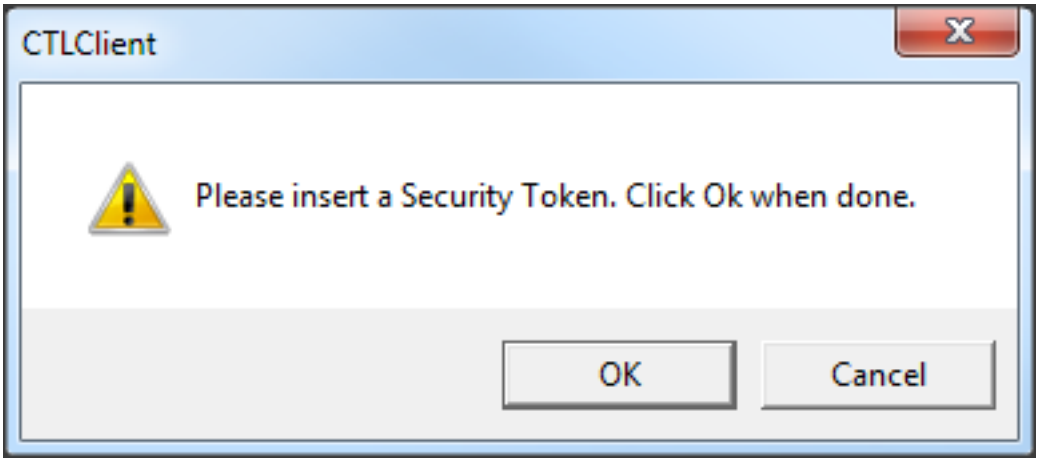
1. 最新の CTL ファイルを設定するために挿入した 1 つのセキュリティ トークンを得て下さい。
2. CTL クライアントを実行して下さい。 CUCM パブおよび CCM 管理者の資格情報の IP ホスト名 /address を提供します。 [Next] をクリックします。



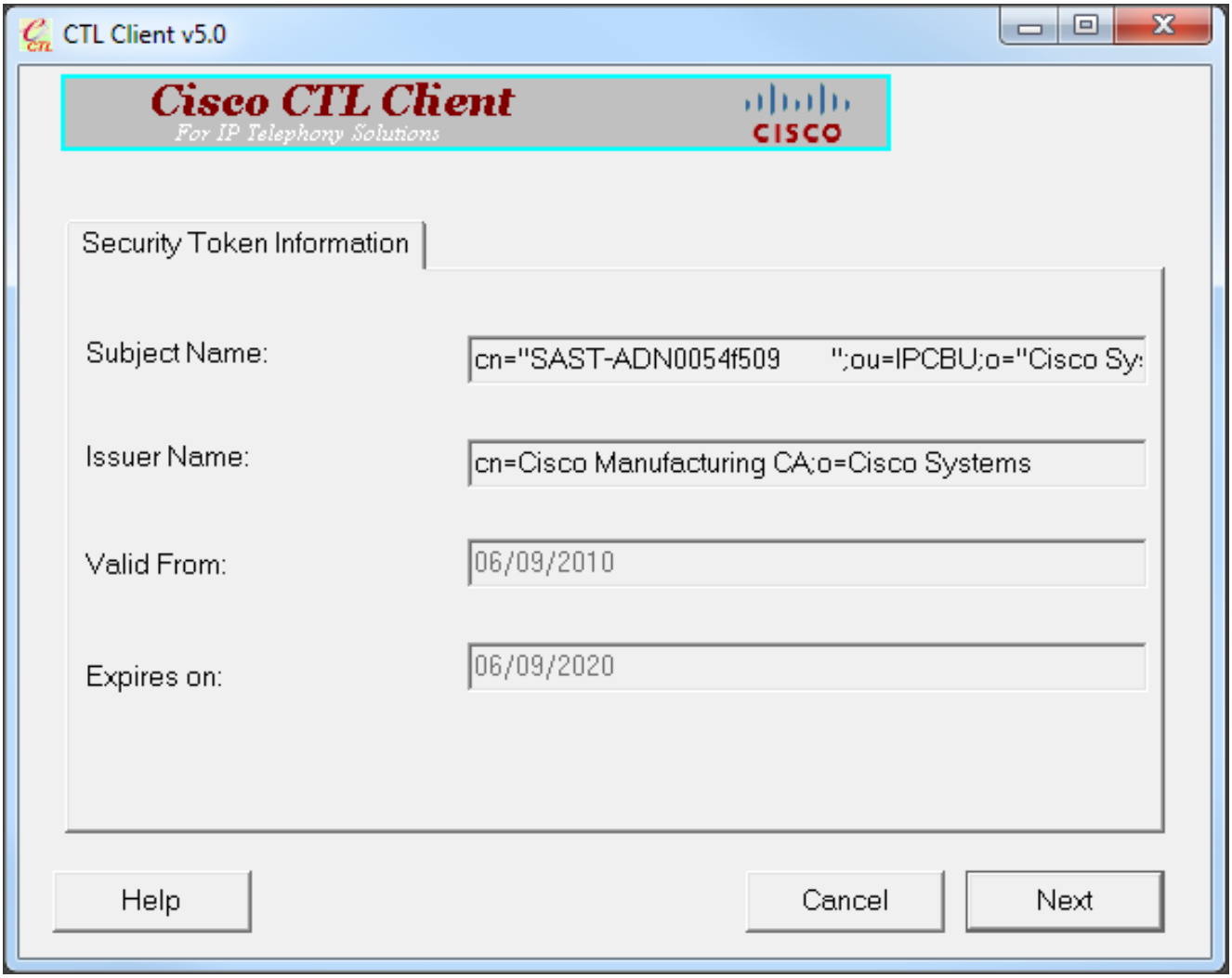
3. **非セキュア Modeオプション・ ボタンに一定 Cisco Unified コールマネージャクラスタを**クリックして下さい。 [Next] をクリックします。



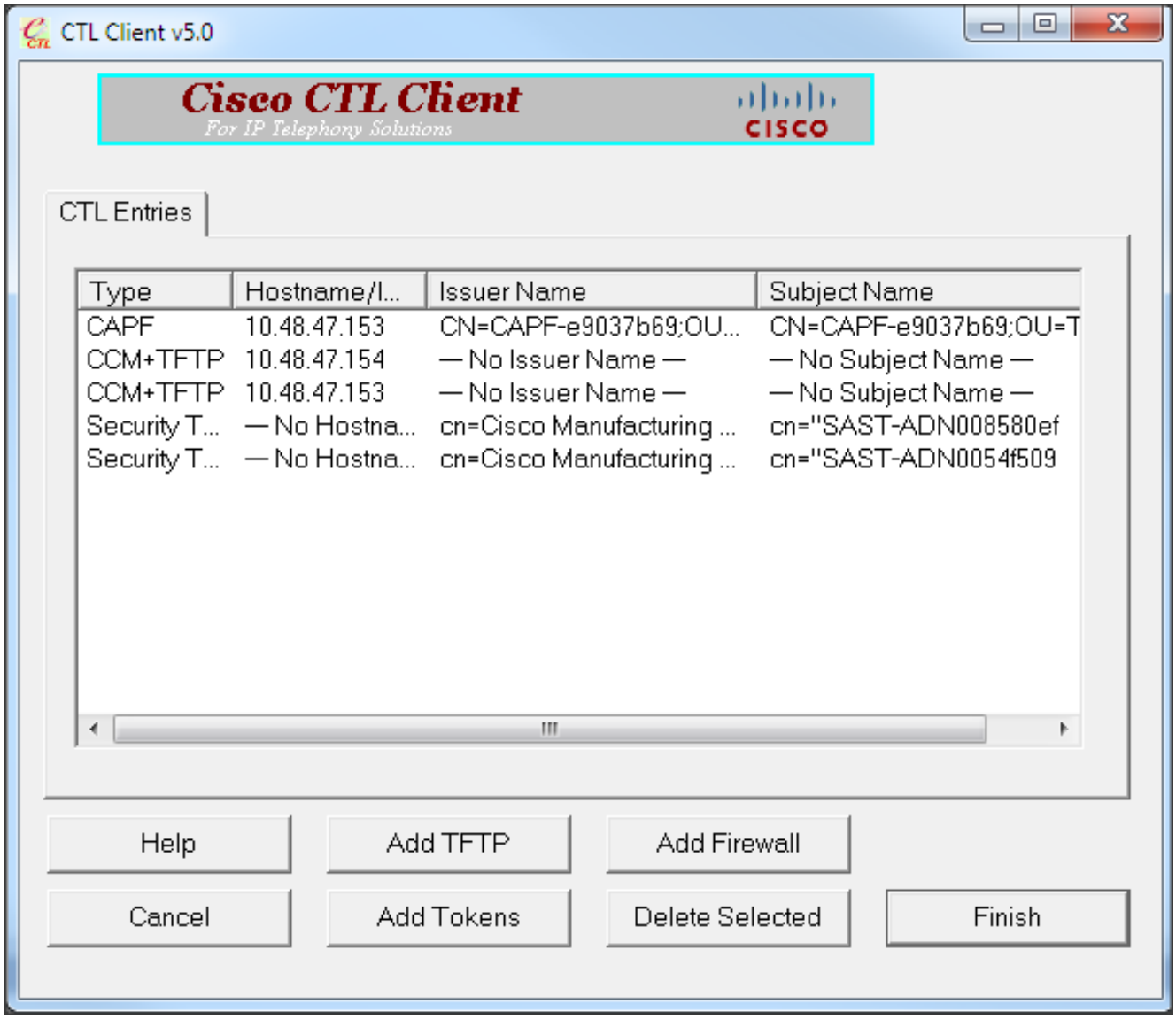
4. 最新の CTL ファイルを設定し、『OK』 をクリック するために挿入された 1 つのセキュリティ トークンを挿入して下さい。 これは CTLFile.tlv の認証リストを読み込むのに使用されたトークンの 1 つです。



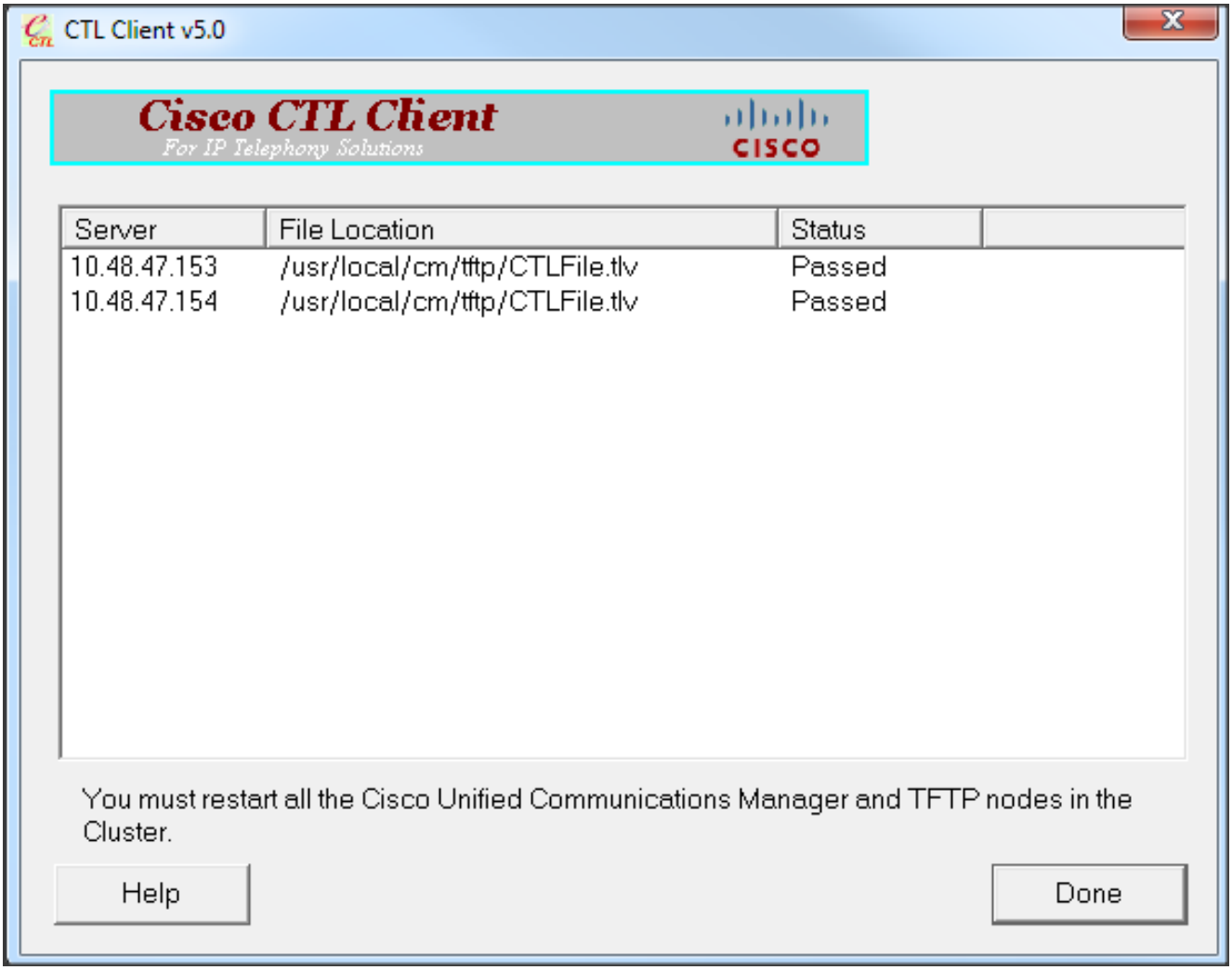
5. セキュリティ トークン詳細は表示する。 [Next] をクリックします。



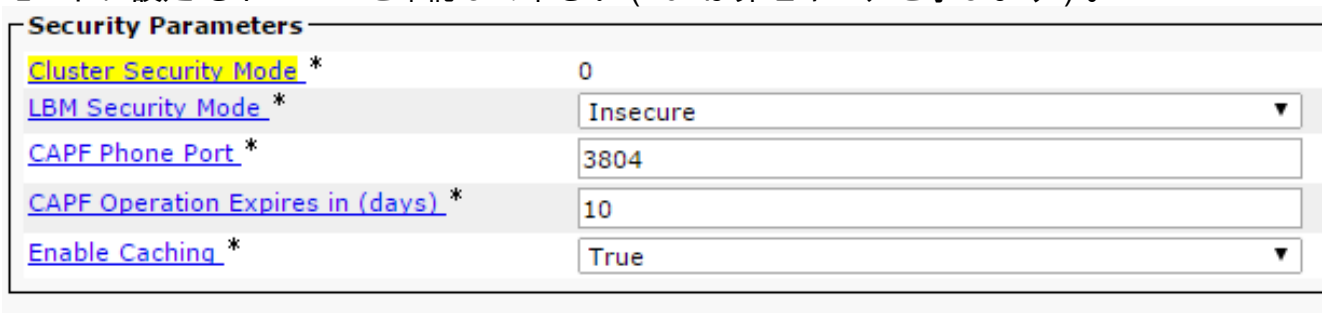
6. CTL ファイルのコンテンツは表示する。 **[Finish] をクリックします。** パスワードのためにプロンプト表示された場合、**Cisco123 を**入力して下さい。



7. CTL ファイル 存在が表示する CUCM サーバのリスト。 [Done] をクリックします。



8. **CUCM 管理者ページ > System > Enterprise Parameters** を選択し、クラスタが非セキュアモードに設定 されたことを確認して下さい（"0" は非セキュアを示します）。



9. これらのサービスを経営するクラスタのすべてのノードの TFTP および Cisco CallManagerサービスを再開して下さい。
10. 彼らが CUCM TFTP からの CTL ファイルの新しい バージョンを得ることができるようにすべての IP 電話を再起動して下さい。

ミックス モードから CLI の非セキュア モードに CUCM クラスタ セキュリティを変更して下さい

この設定は CUCM リリース 10.X およびそれ以降のためだけです。 CUCM クラスタ セキュリティモードを非セキュアに設定 するために、パブリッシャ CLI の **utils ctl 設定クラスタ非セキュアモード** コマンドを入力して下さい。 これが完了する後、これらのサービスを経営するクラスタの

すべてのノードの TFTP および Cisco CallManagerサービスを再開して下さい。

出力されるコマンドの使用を示すサンプル CLI はここにあります。

```
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、設定が正常に動作していることを確認します。

CTLFIle.tlv を確認するために、2 つのメソッドの 1 つを使用できます:

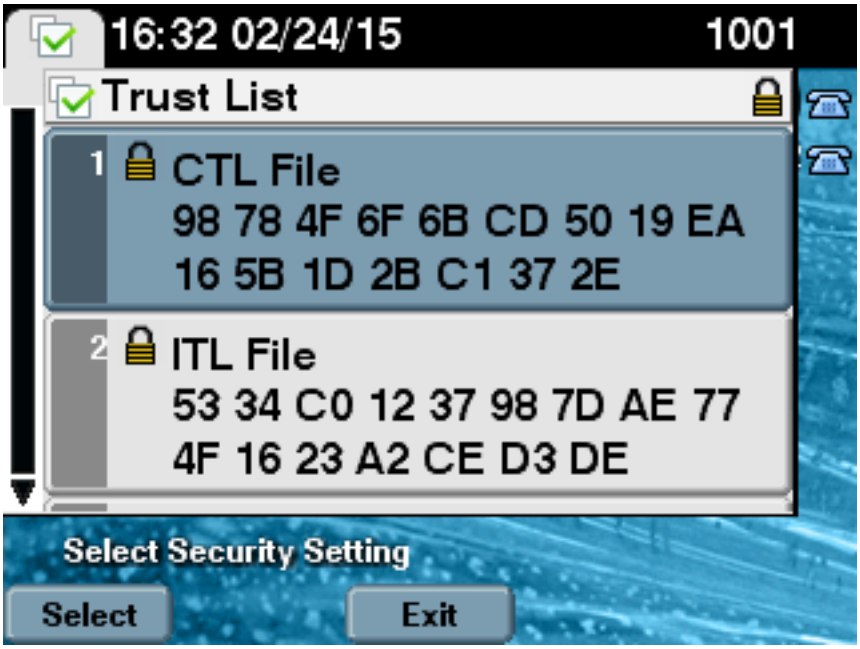
- CUCM TFTP 側の CTLFIle.tlv のコンテンツおよび MD5 チェックサムを確認するために CUCM CLI の showctl **コマンドを**入力して下さい。 CTLFIle.tlv ファイルはすべての CUCM ノードに同じであるはずです。
- 7975 IP Phone の MD5 チェックサムを確認するために、**> Security 設定 > 信頼リスト > CTL ファイルを**『Settings』 を選択 して下さい。

  注: MD5 か SHA1 を見る電話のチェックサムをチェックする時、電話のタイプに依存。

セキュリティモードに設定 される 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 Phone 側で、CUCM からの出力と比較されてと) 同じ CTL ファイルをインストールしてもらうことがわかります (MD5 チェックサムは一致します。



CUCM は非セキュア モードにクラスタ化しますセットを- CTL ファイル内容

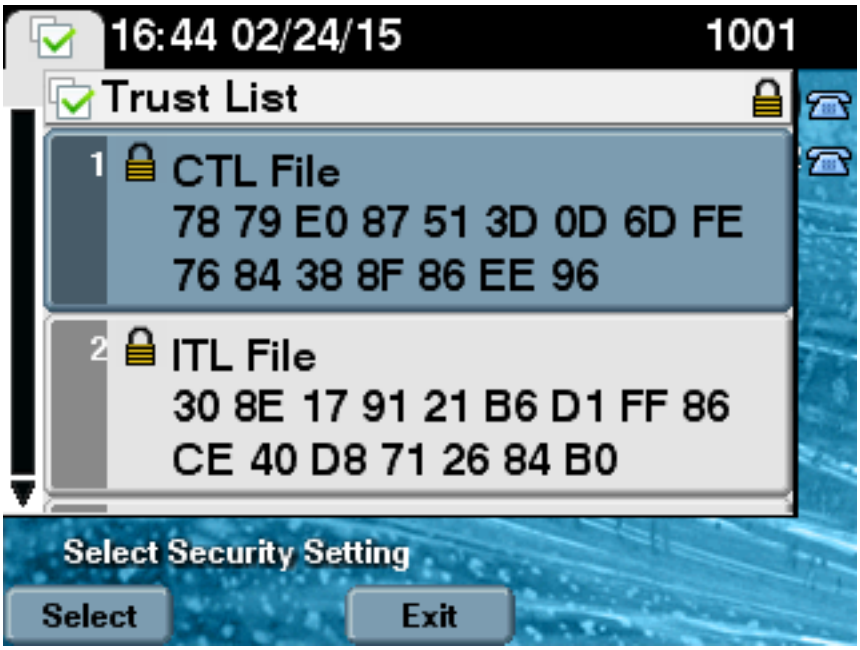
非セキュア モードに設定 される CUCM クラスタからの CTL ファイルの例はここにあります。 CCM+TFTP 認証が空であるわかり、コンテンツをことが含まれていません。 CTL ファイルの認証の他は CUCM がミックス モードに設定 されたときに同じと丁度変更されないし、です。

```
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 Phone 側で、再起動し、更新済 CTL ファイルのバージョンをダウンロードした後、CUCM からの出力と比較されてと MD5 チェックサムが一致することがわかります。



USB トークンが失われるときミックス モードから非セキュア モードに CUCM クラスタ セキュリティを置いて下さい

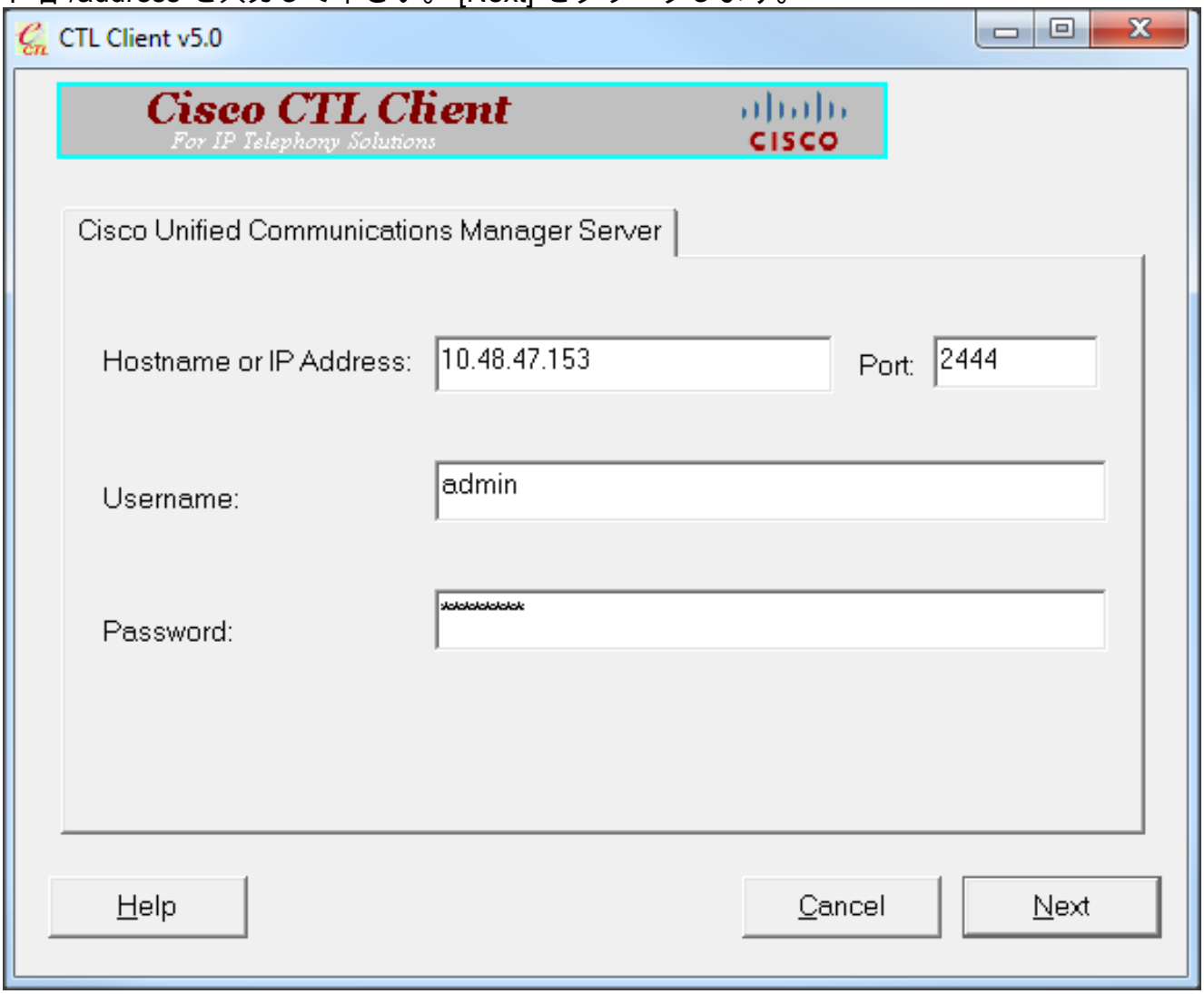
保護されたクラスタのためのセキュリティ トークンは失うことができます。 その状況では、これら二つのシナリオを考慮する必要があります:

- クラスタ実行バージョン 10.0.1 または それ 以降
- クラスタは 10.x 以前のバージョンを実行します

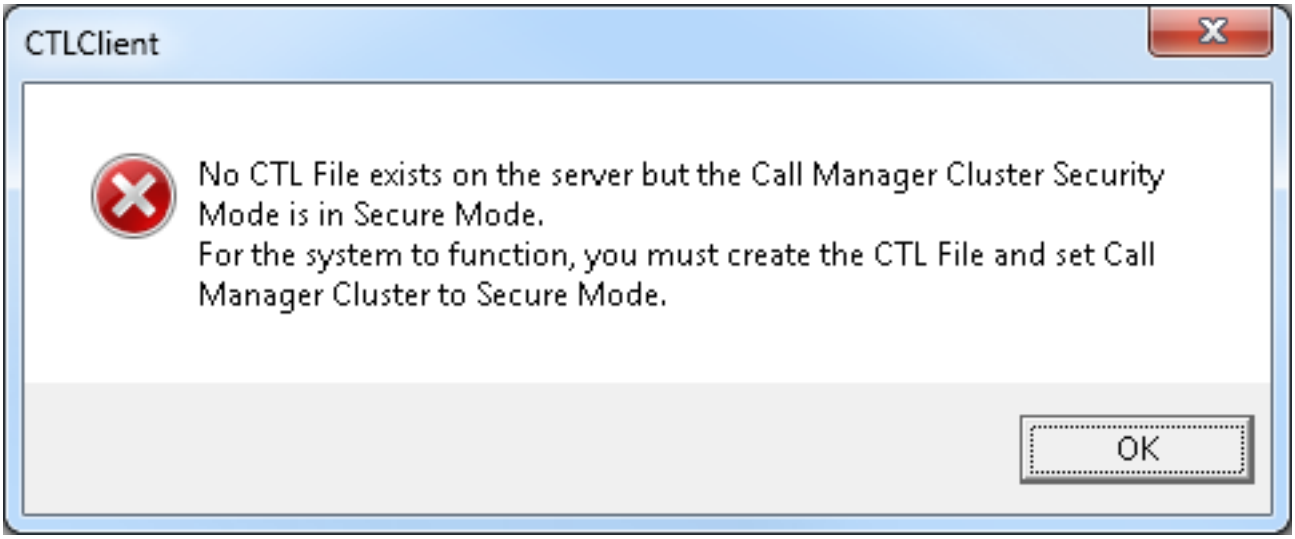
最初のシナリオでは、問題から回復 するためにミックス モードからの CLI セクションの非セキュア モードへの変更に CUCM クラスタ セキュリティ説明があるプロシージャを完了して下さい。 その CLI コマンドは CTL トークンを必要としないので、クラスタが CTL クライアントとのミックス モードに置かれても使用できます。

状況は CUCM の 10.x 以前のバージョンが使用中のとき複雑になります。 トークンの 1 つのパスワードを失うか、または忘れている場合、まだ他の現在の CTL ファイルと CTL クライアントを実行するのに 1 を使用できます。 それは冗長性のために CTL ファイルに強く推奨されています別のものを得るためにできるだけ早く eToken、追加しますそれを。 CTL ファイルにリストされているすべての eTokens のためのパスワードを失うか、または忘れている場合 eTokens の新しいペアを得、ここに説明されるように手動プロシージャを実行する必要があります。

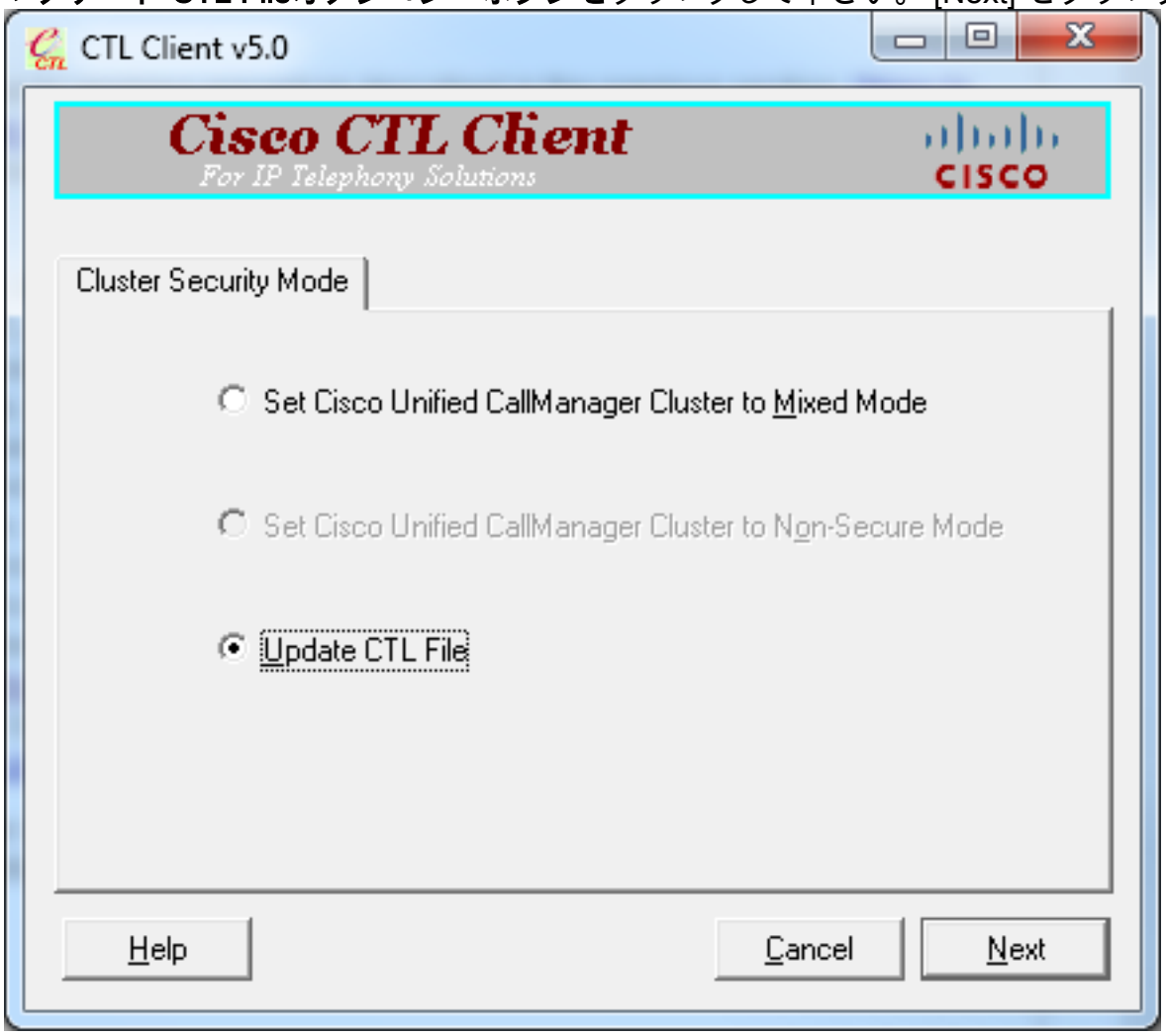
1. TFTP すべてのサーバから CTL ファイルを削除するために**ファイル削除 tftp CTLFile.tlv コマンドを**入力して下さい。admin:file delete tftp CTLFile.tlv
```
Delete the File CTLFile.tlv?
Enter "y" followed by return to continue: y
files: found = 1, deleted = 1

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て下さい。 CUCM パブおよび CCM 管理者の資格情報の IP ホスト名 /address を入力して下さい。 [Next] をクリックします。



3. クラスタがミックス モードにあるので、パブリッシャで存在 する CTL ファイルがこの警告表示するどんなに。 それを無視し、順方向に続行するために『OK』 をクリック して下さい。

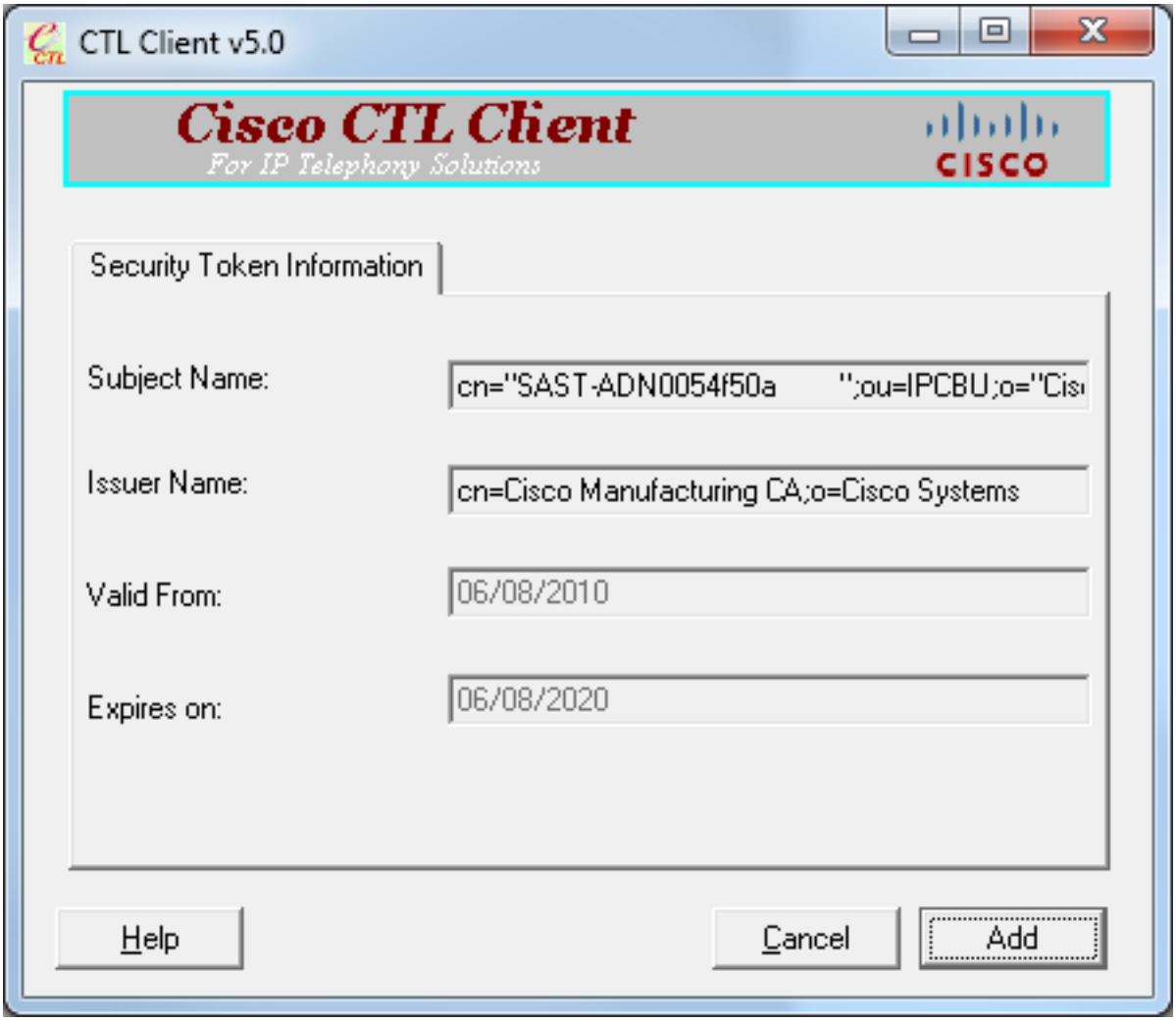


4. **アップデート CTL Fileオプション・ボタンを**クリックして下さい。 [Next] をクリックします

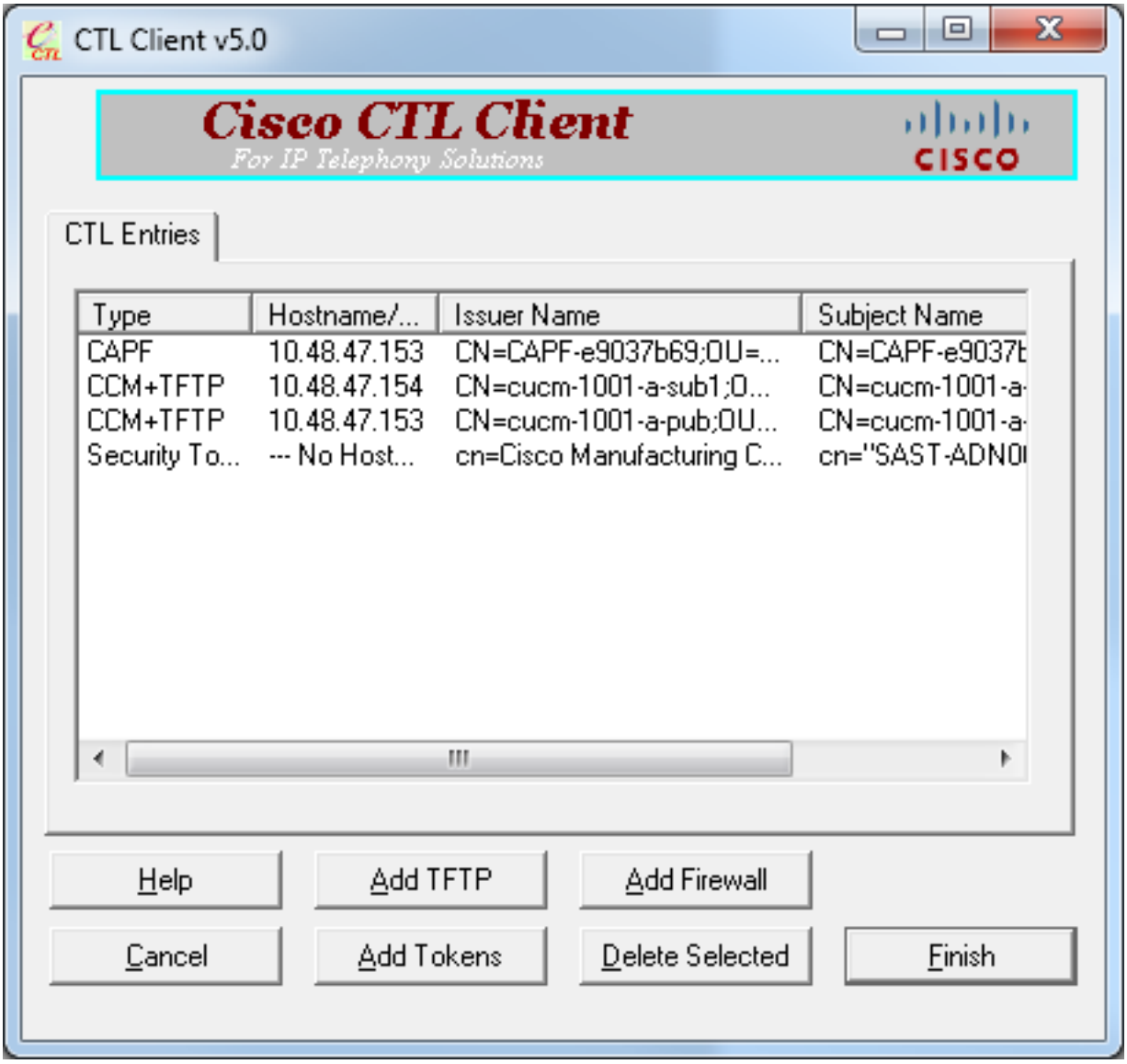


。

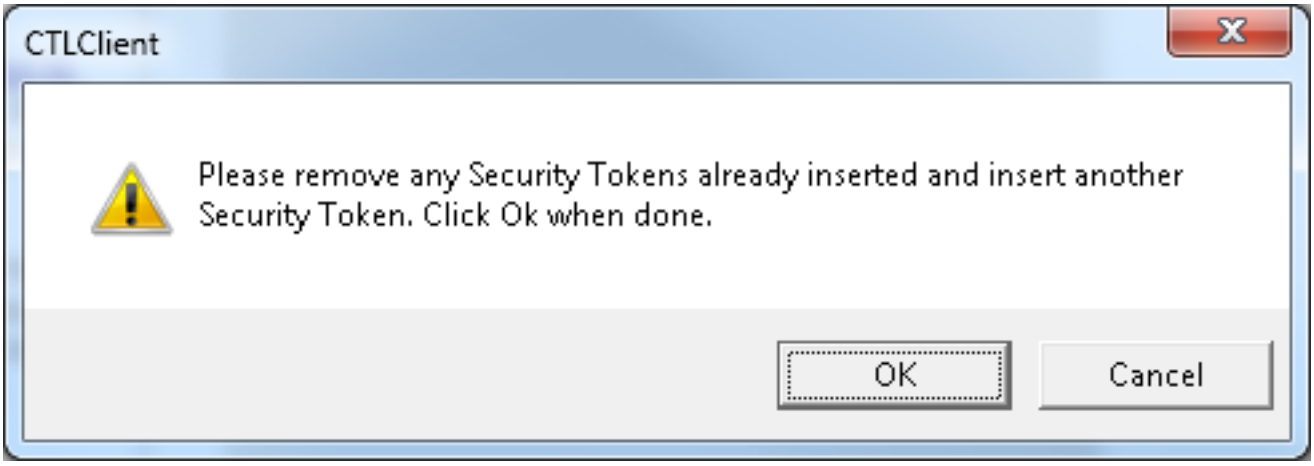
5. CTL クライアントはセキュリティ トークンを追加することを頼みます。 続行するために『 Add』 をクリック して下さい。



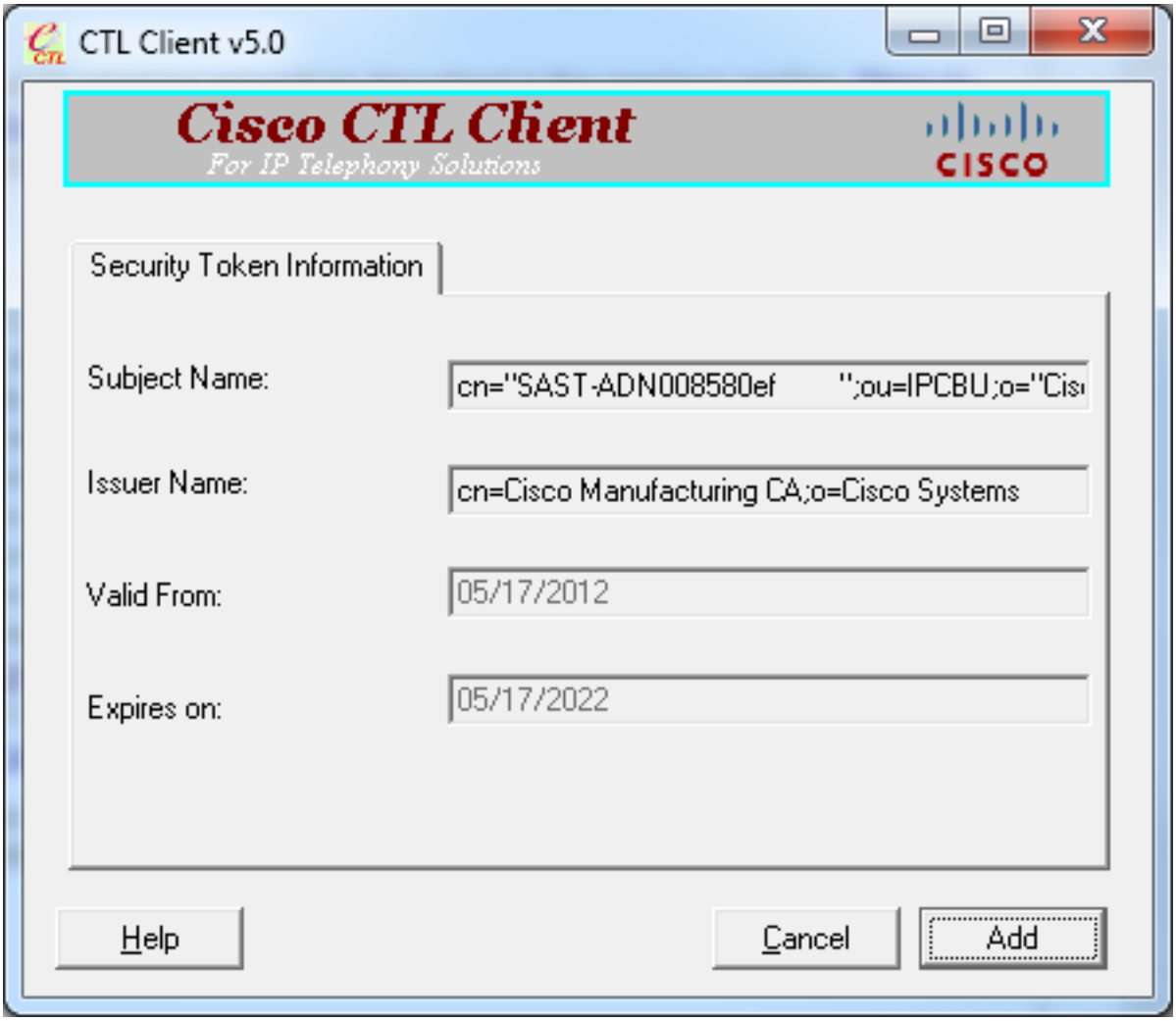
6. 画面 表示新しい CTL のすべてのエントリ。 新しいペアから第 2 トークンを追加するために**トークンを**『Add』 をクリック して下さい。



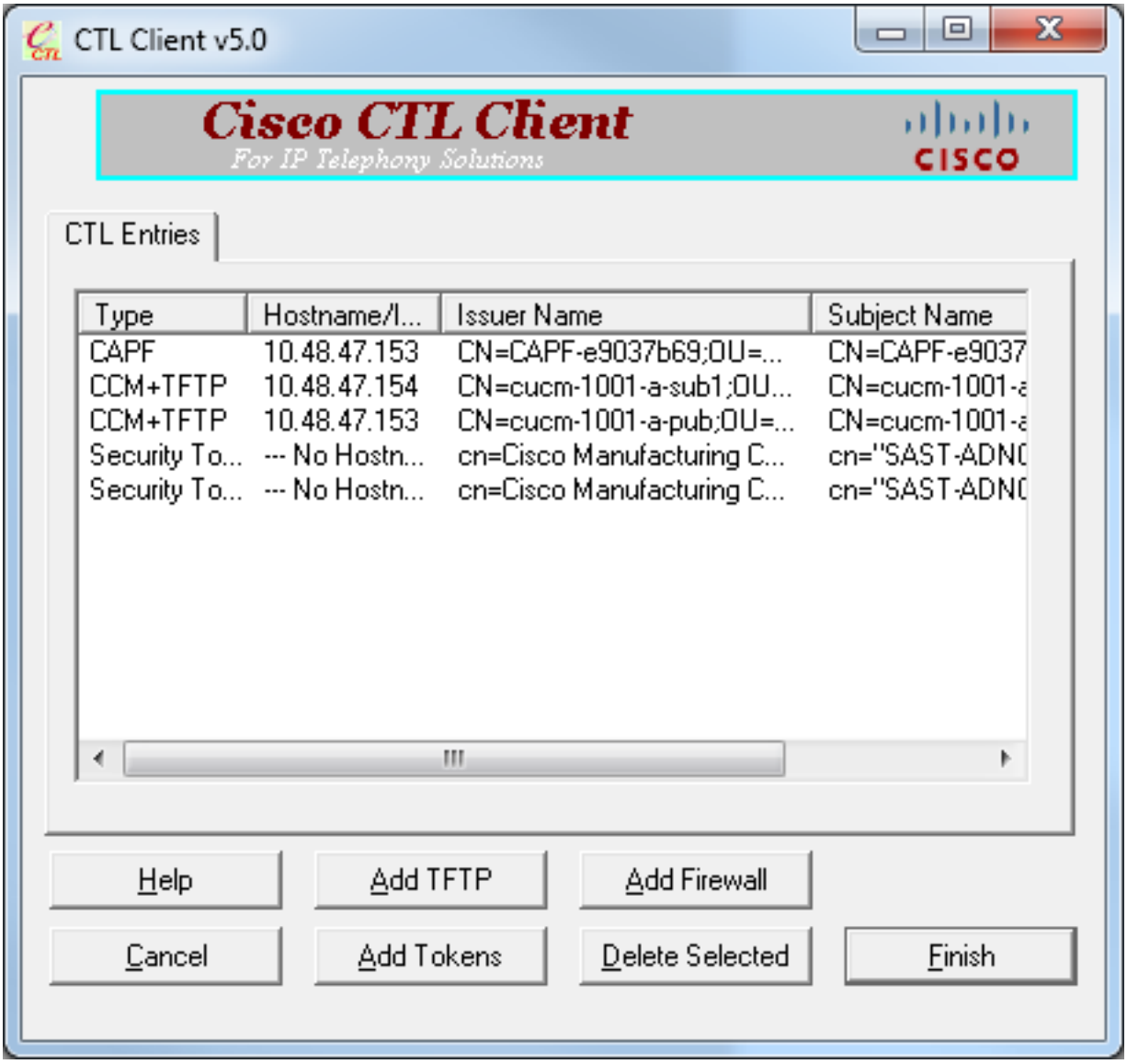
7. 現在のトークンを取除き、新しいものを挿入するためにプロンプト表示されます。 一度される『OK』 をクリック して下さい。



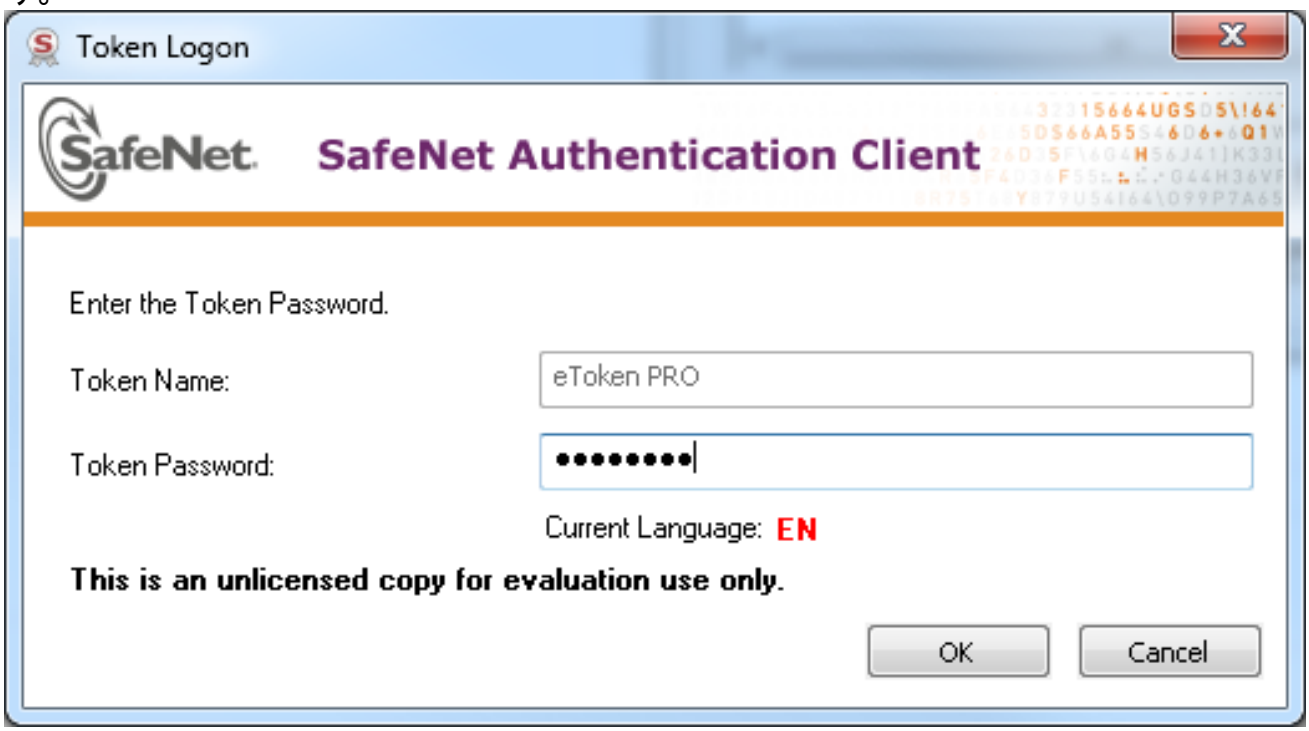
8. 画面は新しいトークンの詳細を示す表示する。 それらを確認し、このトークンを追加するために『Add』 をクリック して下さい。



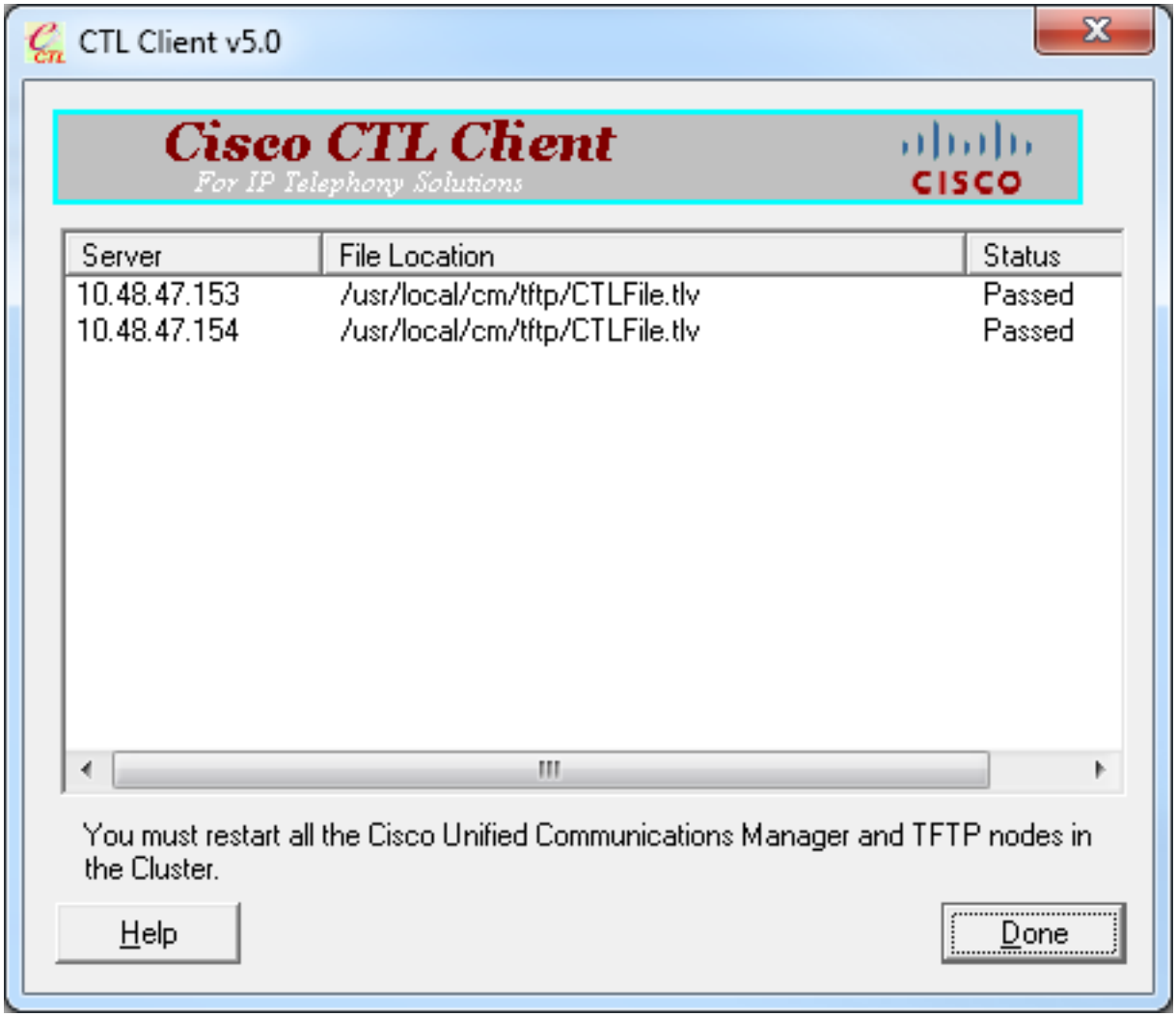
9. 両方の追加されたトークンを示す CTL エントリの新しいリストを記載します。 新しい CTL ファイルを生成するために『Finish』 をクリック して下さい。



10. トークン Password フィールドでは、**Cisco123 を**入力して下さい。 [OK] をクリックします。



11. プロセスが正常だったこと確認が表示されます。 CTL クライアントを確認し、終了するために『Done』 をクリック して下さい。



12. CallManagerサービス（Cisco Unified サービサビリティ > Tools > Control Center 先行させている Cisco TFTP を-機能 サービス）が再起動して下さい。 新しい CTL ファイルは生成する必要があります。 確認のための**提示 ctl** コマンドを入力して下さい。`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. クラスタの各電話から CTL ファイルを削除して下さい（このプロシージャは電話のタイプに基づいて異なる可能性があります- Cisco Unified IP Phone 8961、9951 および 9971 管理ガイドのような詳細についてはドキュメントを、参考にして下さい）。**注:** 電話はまだ（電話のセキュリティ設定に依存）登録され、ステップ 13 を続行しないではたらけますかもしれません。 ただし、インストールされたそれらに古い CTL ファイルがあります。 それはクラスタに認証が再生すれば、別のサーバ追加されます問題を引き起こす可能性がありますまたはサーバハードウェアは交換されます。 このステータスにクラスタを残すことを推奨しません。
14. 非セキュアにクラスタを移動して下さい。 詳細についてはミックス モードからの CTL クライアント セクションの非セキュア モードへの変更を CUCM クラスタ セキュリティ参照して下さい。

トラブルシューティング

現在のところ、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。