CUCM群集從混合模式更改為非安全模式的配置示例

目錄

簡介

本文檔介紹將Cisco Unified Communications Manager(CUCM)安全模式從混合模式更改為非安全模式所需的步驟。它還顯示完成此移動時證書信任清單(CTL)檔案的內容如何更改。

更改CUCM安全模式需要三個主要部分：

1a。運行CTL客戶端並選擇所需的安全模式變體。
1b。輸入CLI命令以選擇所需的安全模式變體。
2.在運行這些服務的所有CUCM伺服器上重新啟動Cisco CallManager和Cisco TFTP服務。
3.重新啟動所有IP電話，以便它們可以下載更新版本的CTL檔案。

> **附註**：如果將群集安全模式從混合模式更改為非安全模式，則伺服器和電話上仍存在CTL檔案，但CTL檔案不包含任何CCM+TFTP（伺服器）證書。由於CTL檔案中不存在CCM+TFTP（伺服器）證書，因此會強制電話在CUCM中註冊為非安全。

必要條件

需求

思科建議您瞭解CUCM 10.0(1)版或更高版本。此外，請確保：

- CTL提供程式服務已啟動，並在群集中的所有活動TFTP伺服器上運行。預設情況下，該服務在TCP埠2444上運行，但可以在CUCM服務引數配置中修改該服務。
- 證書頒發機構代理功能(CAPF)服務已啟動並在發佈器節點上運行。
- 群集中的資料庫(DB)複製工作正常，伺服器即時複製資料。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- CUCM版本10.0.1.11900-2集群兩個節點
- Cisco 7975 IP電話(使用精簡型呼叫控制協定(SCCP)註冊，韌體版本SCCP75.9-3-1SR3-1S)
- 必須將群集設定為混合模式需要兩個思科安全令牌
- 要將群集設定為非安全模式，必須使用前面列出的安全令牌之一

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

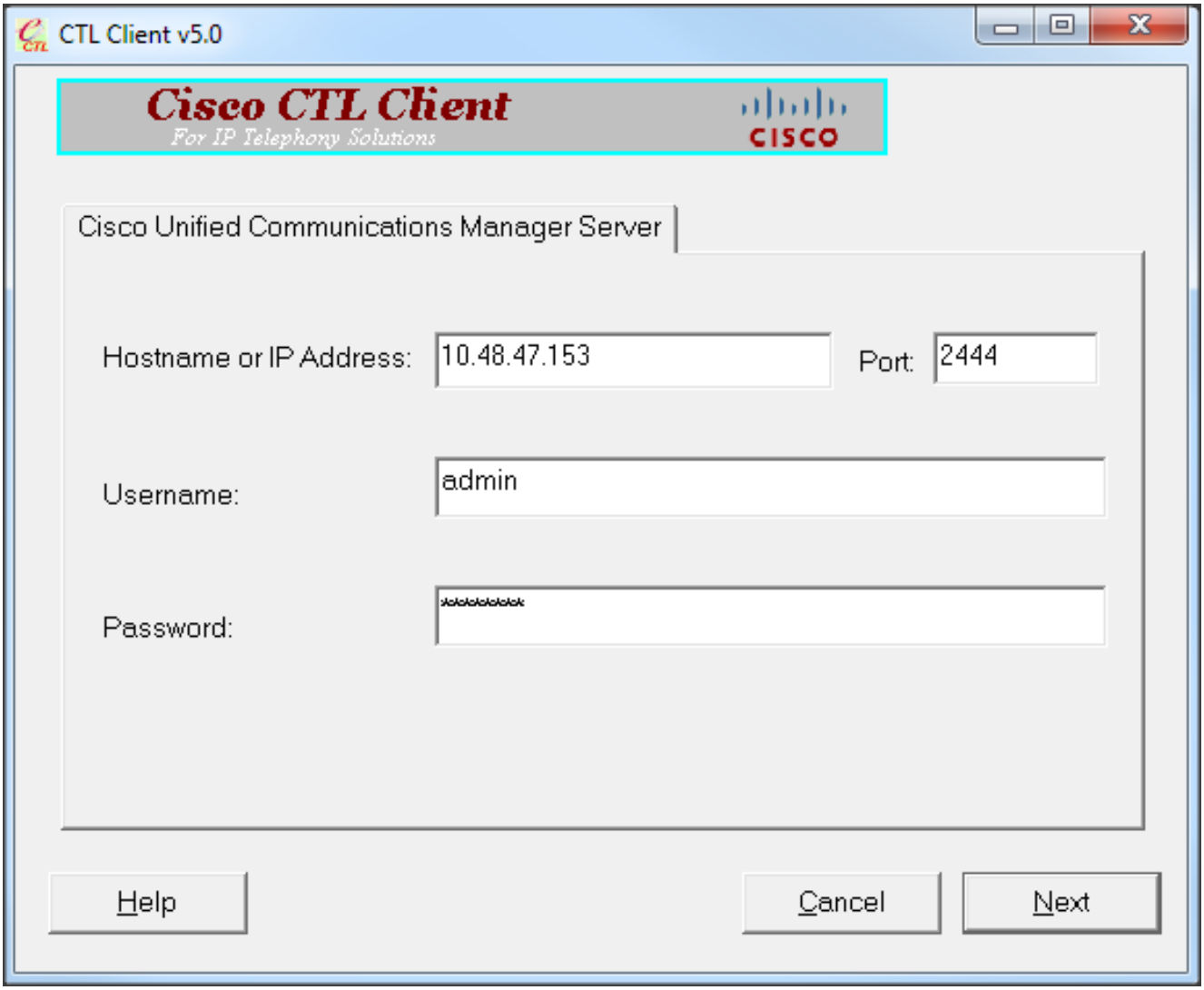
要運行CTL客戶端外掛，需要至少訪問一個插入的安全令牌，以便建立或更新CUCM發佈伺服器上存在的最新CTL檔案。換句話說，CUCM上當前CTL檔案中至少存在一個用於更改安全模式的安全令牌上的eToken證書。

設定

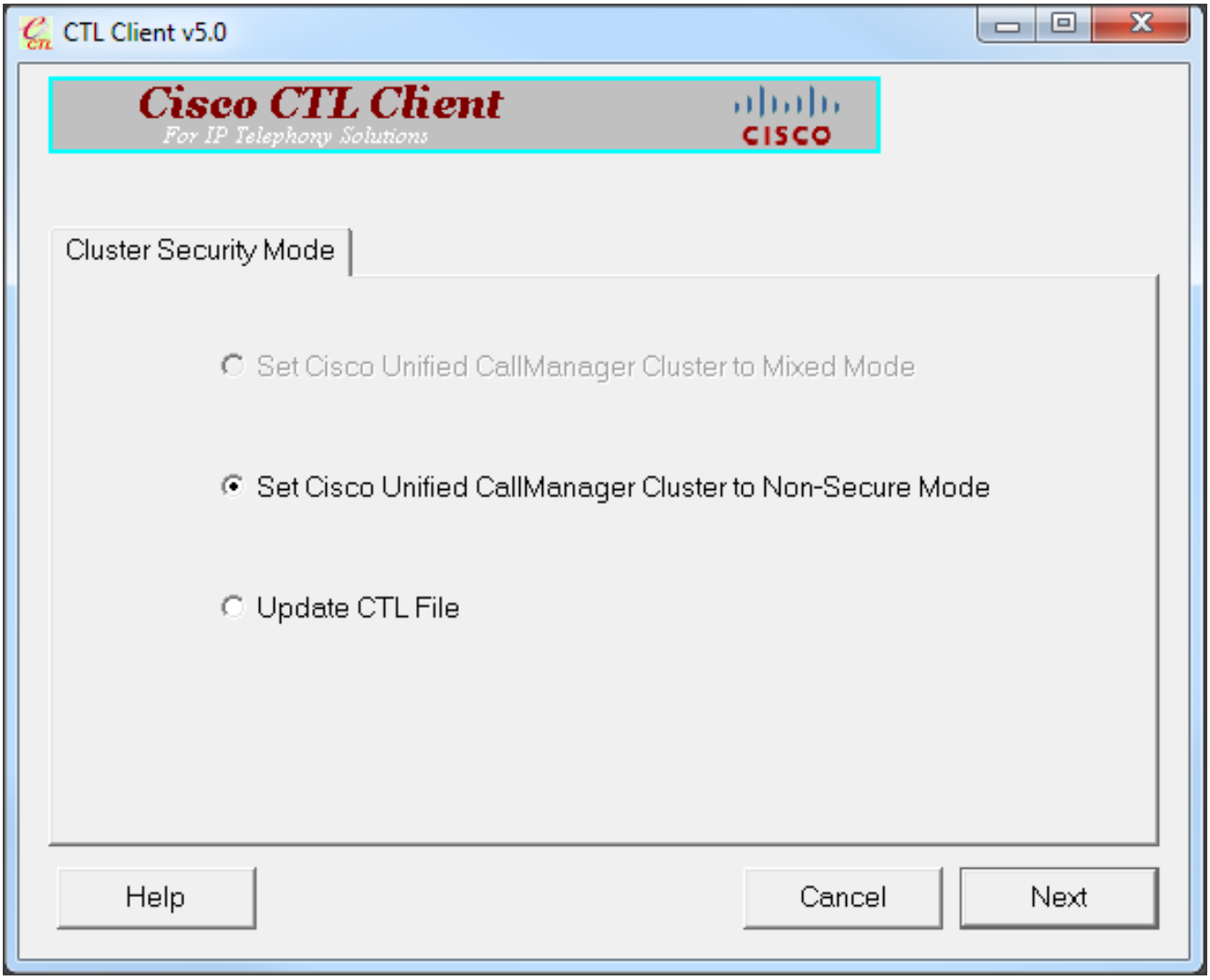
使用CTL客戶端將CUCM集群安全從混合模式更改為非安全模式

完成以下步驟，以便使用CTL客戶端將CUCM集群安全性從混合模式更改為非安全模式：

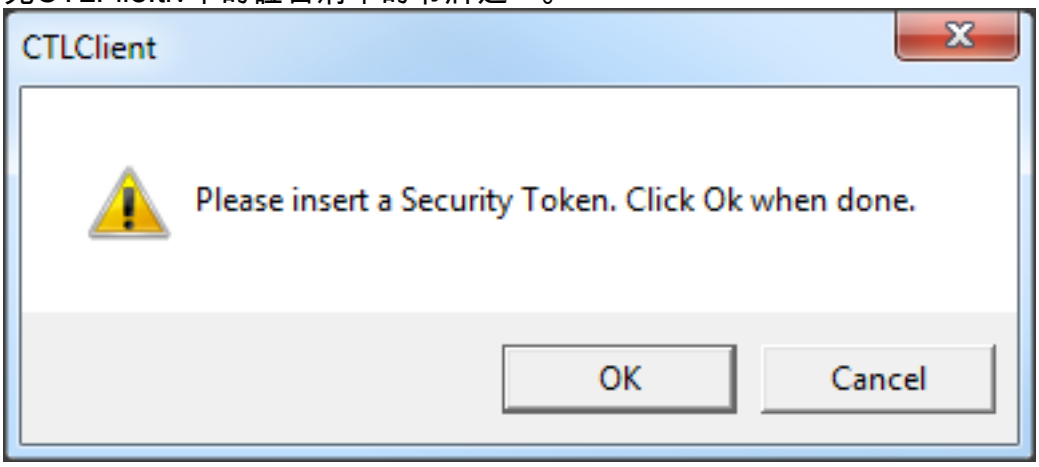
1. 獲取您插入的一個安全令牌以配置最新的CTL檔案。
2. 運行CTL客戶端。提供CUCM Pub的IP主機名/地址和CCM管理員憑據。按「**Next**」（下一步）。



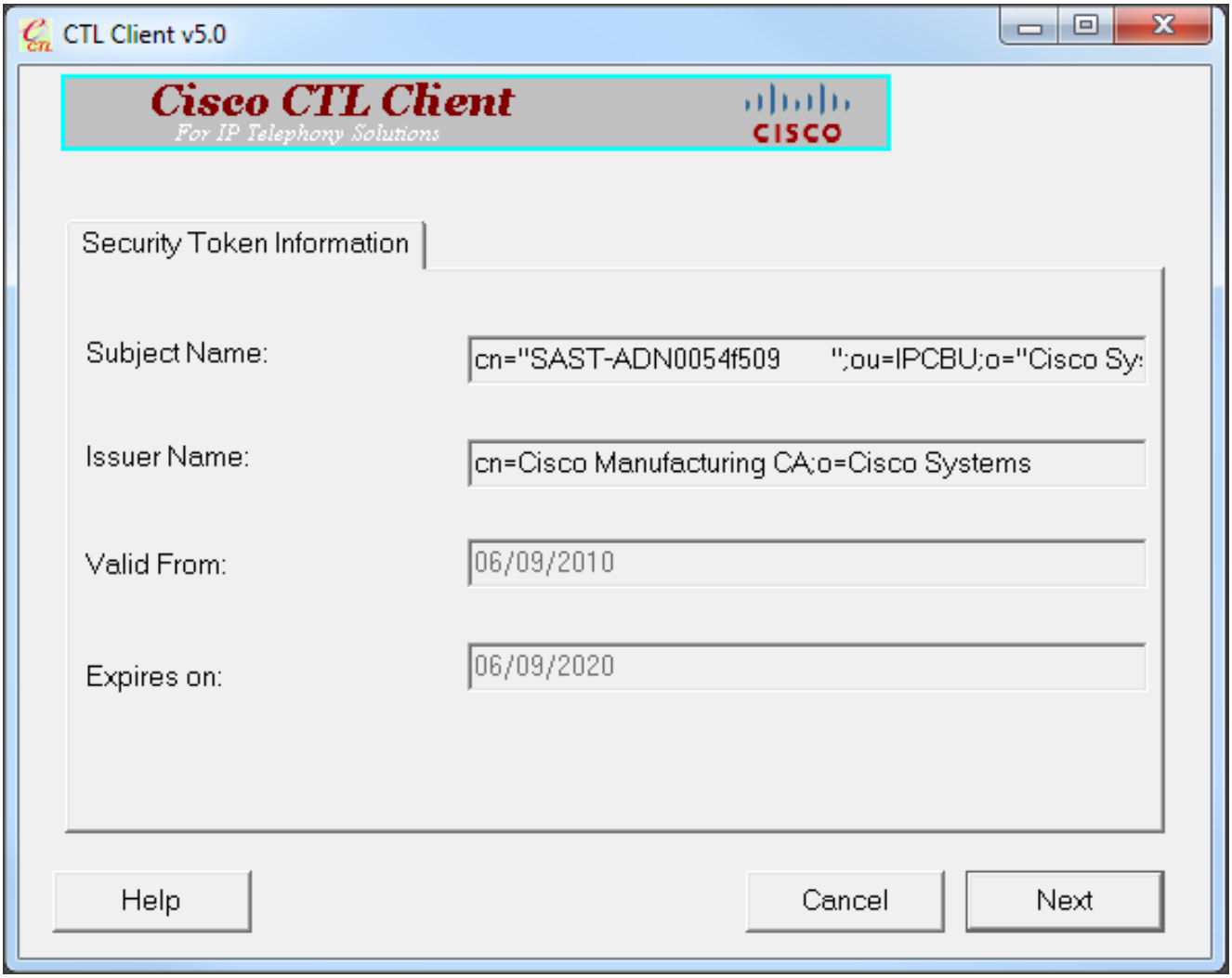
3. 按一下**Set Cisco Unified CallManager Cluster to Non-Secure Mode**單選按鈕。按「**Next**」（下一步）。



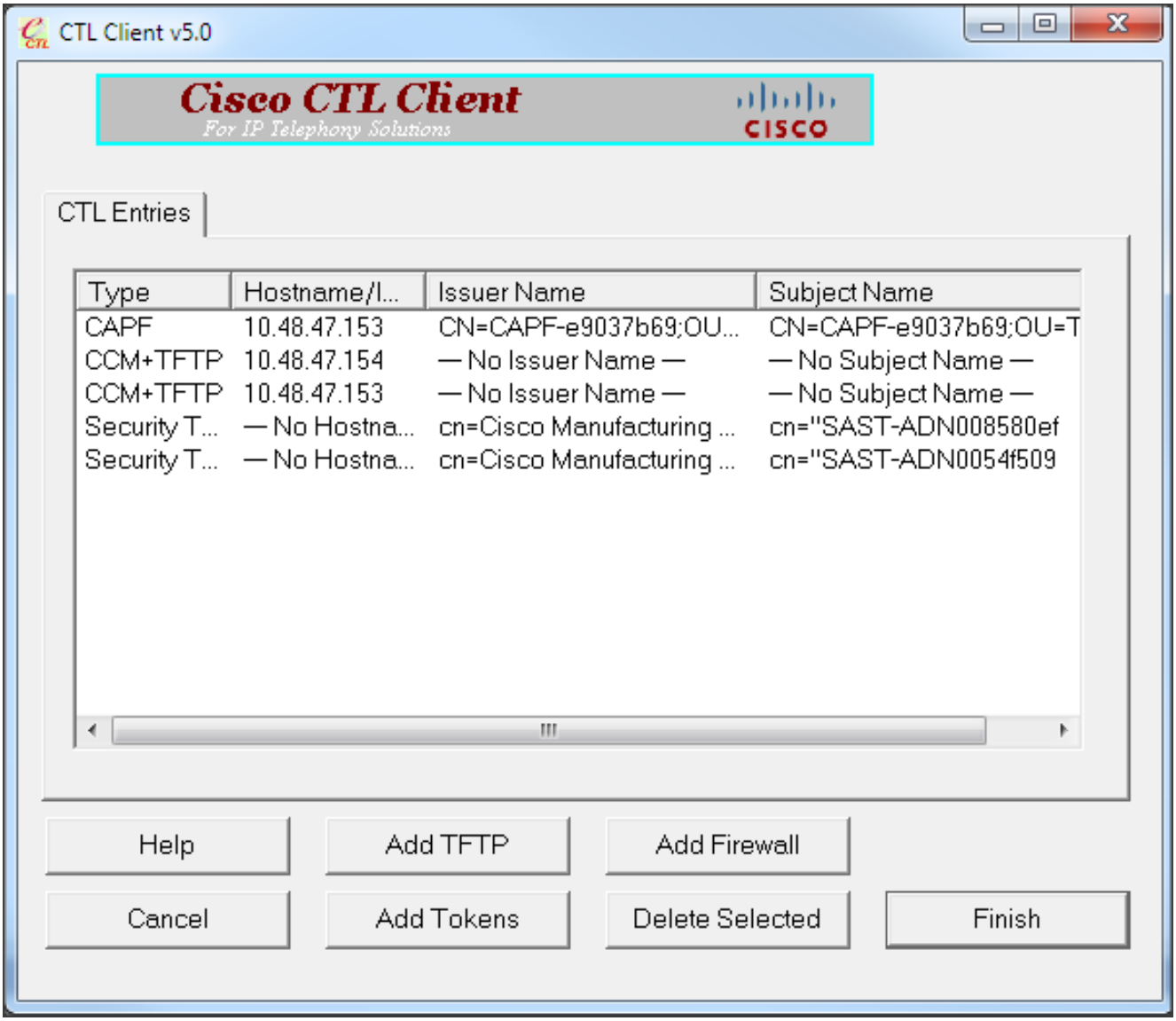
4. 插入一個安全標籤，該安全標籤被插入以配置最新的CTL檔案，然後按一下**OK**。這是用於填充CTLFile.tlv中的證書清單的令牌之一。



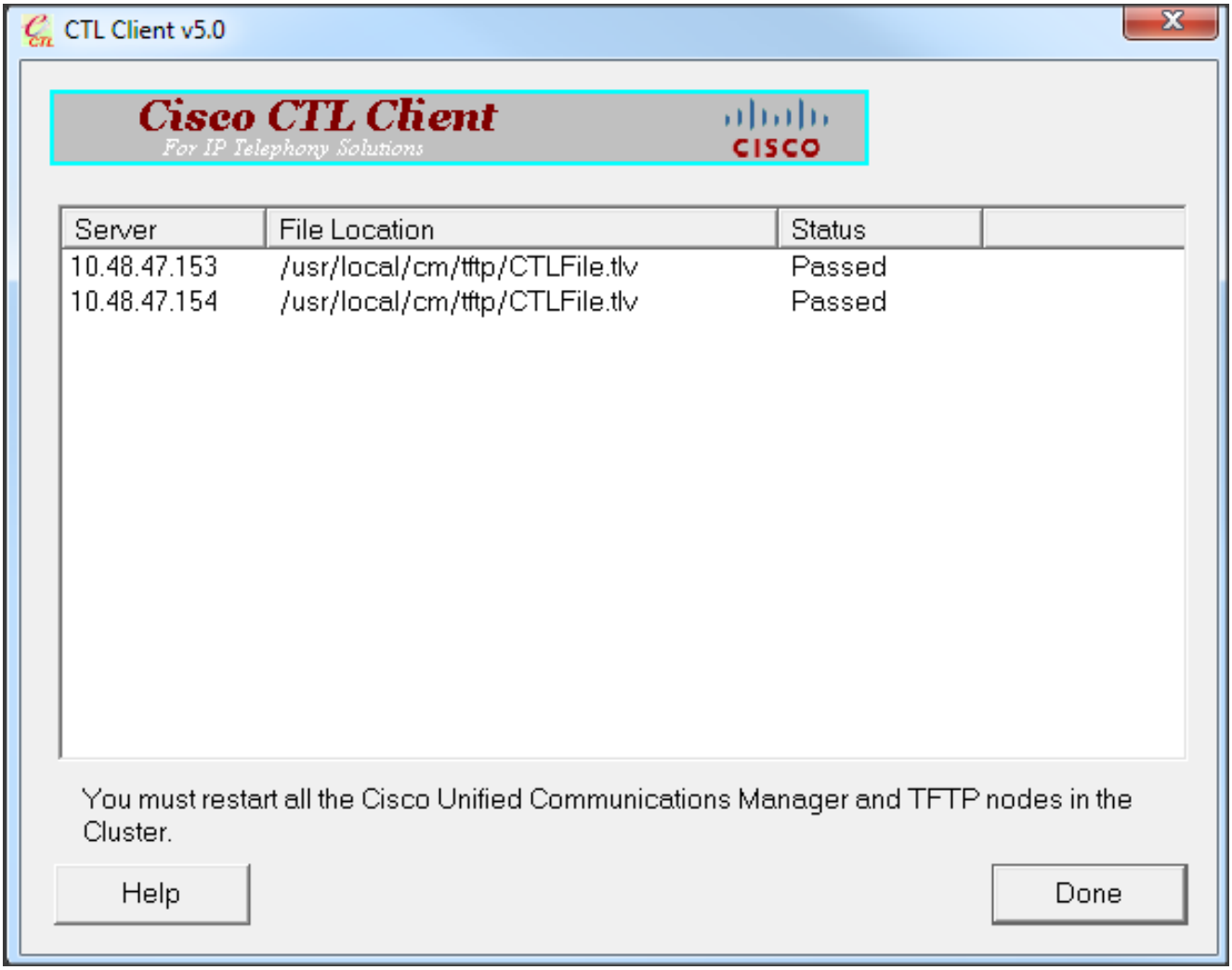
5. 系統將顯示安全令牌詳細資訊。按「**Next**」（下一步）。



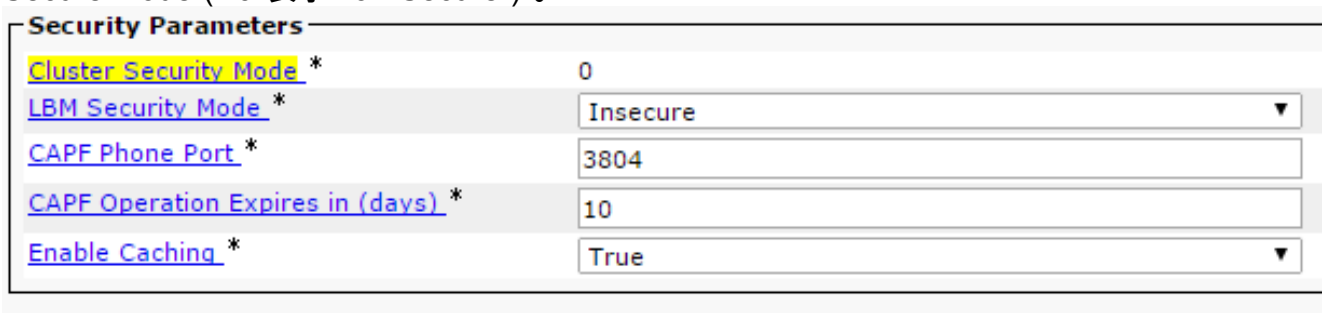
6. 顯示CTL檔案的內容。按一下「**Finish**」（結束）。系統提示輸入密碼時，輸入**Cisco123**。



7. 將顯示CTL檔案所在的CUCM伺服器清單。按一下「**完成**」。



8. 選擇**CUCM Admin Page > System > Enterprise Parameters**，並驗證群集是否已設定為Non-Secure Mode（"0"表示Non-Secure）。



9. 在運行這些服務的群集中的所有節點上重新啟動TFTP和Cisco CallManager服務。
10. 重新啟動所有IP電話，以便它們可以從CUCM TFTP獲取新版本的CTL檔案。

使用CLI將CUCM集群安全性從混合模式更改為非安全模式

此配置僅適用於CUCM 10.X版及更高版本。若要將CUCM群集安全模式設定為Non-Secure，請在Publisher CLI上輸入**utils ctl set-cluster non-secure-mode**命令。完成後，在運行這些服務的群集中的所有節點上重新啟動TFTP和Cisco CallManager服務。

以下是顯示命令使用的CLI輸出示例。

```
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:
```

驗證

使用本節內容，確認您的組態是否正常運作。

若要驗證CTLFIle.tlv，可以使用以下兩種方法之一：

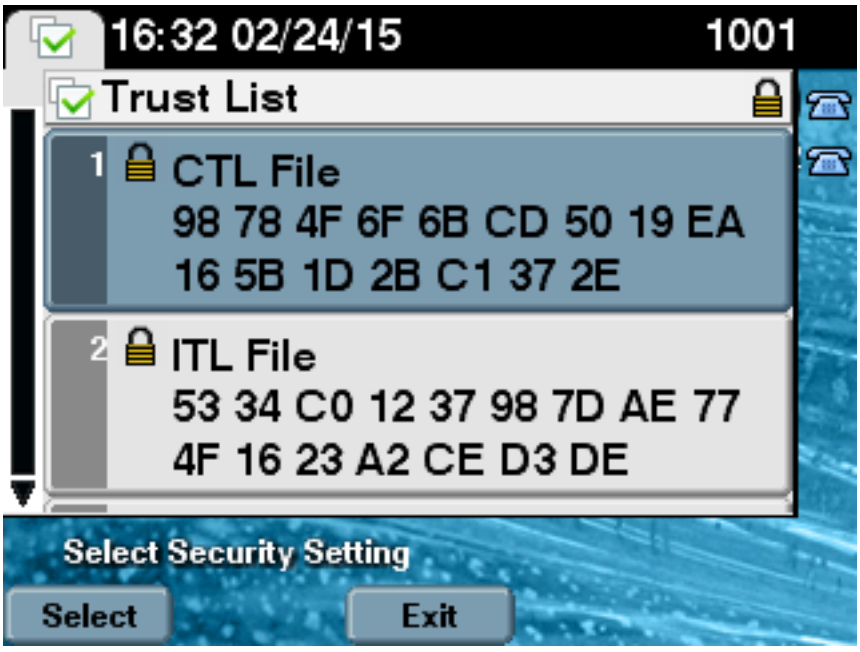
- 要驗證CUCM TFTP端存在的CTLFIle.tlv的內容和MD5校驗和，請在CUCM CLI上輸入**show ctl**命令。所有CUCM節點上的CTLFIle.tlv檔案應該相同。
- 若要驗證7975 IP電話上的MD5校驗和，請選擇**設定>安全配置>信任清單> CTL檔案**。

  附註：檢查電話上的校驗和時，您會看到MD5或SHA1，具體取決於電話型別。

CUCM群集設定為安全模式 — CTL檔案校驗和

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

在IP電話端，您可以看到安裝了相同的CTL檔案（與CUCM的輸出相比，MD5校驗和匹配）。



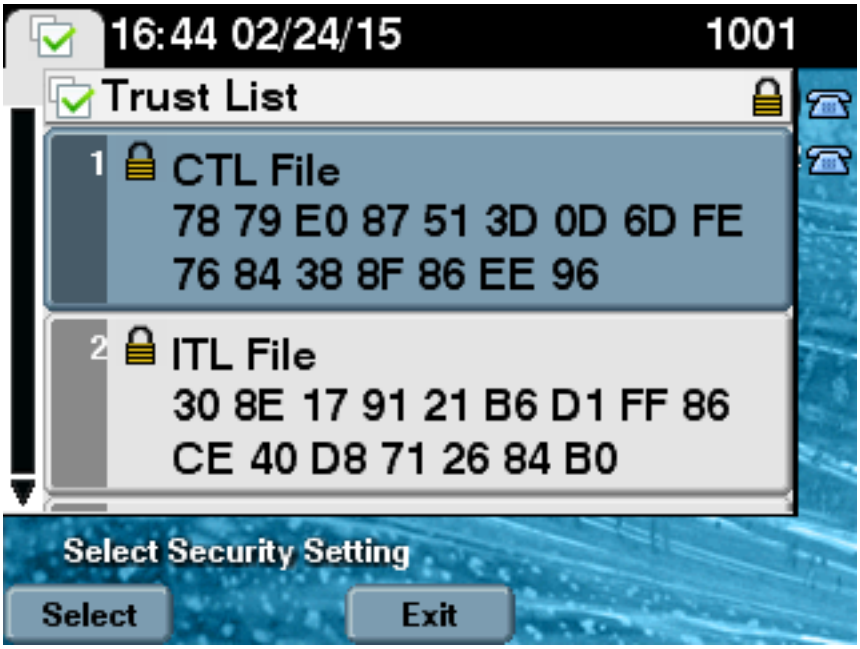
CUCM群集設定為非安全模式 — CTL檔案內容

以下是一個從CUCM群集設定為非安全模式的CTL檔案的示例。您可以看到CCM+TFTP證書是空的，不包含任何內容。CTL檔案中的其餘證書沒有更改，並且與CUCM設定為混合模式時完全相同。

```
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:
```

在IP電話端，重新啟動並下載更新的CTL檔案版本後，與CUCM的輸出相比，可以看到MD5校驗和匹配。



丟失USB令牌時，將CUCM群集安全從混合模式置於非安全模式

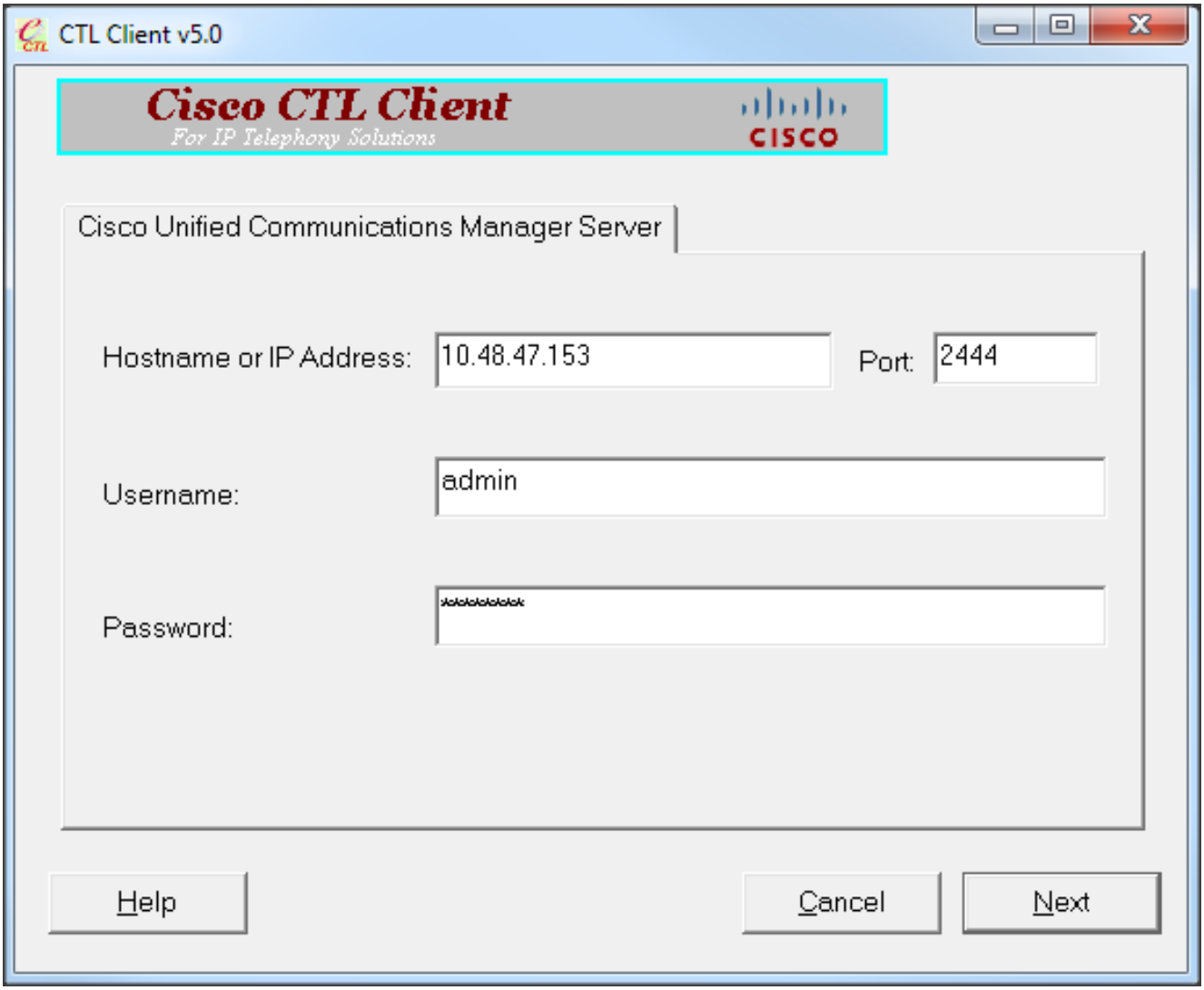
安全群集的安全令牌可能丟失。在這種情況下，您需要考慮以下兩種情況：

- 群集運行版本10.0.1或更高版本
- 群集運行早於10.x的版本

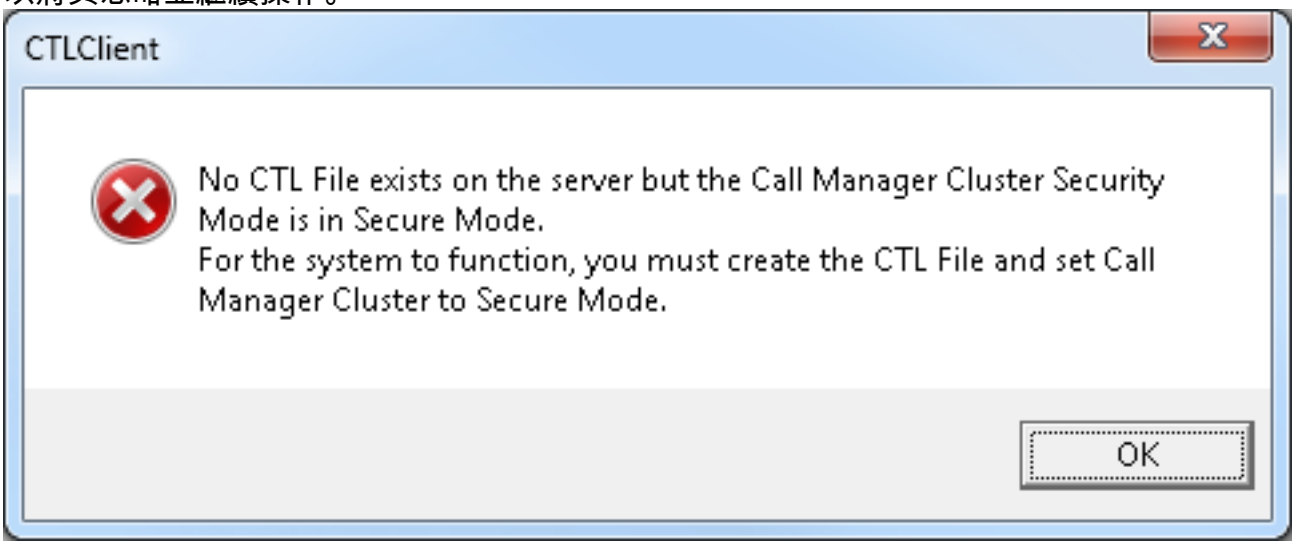
在第一個場景中，完成使用CLI將CUCM集群安全性從混合模式更改為非安全模式一節中介紹的過程以便從問題中恢復。因為CLI命令不需要CTL令牌，所以即使群集與CTL客戶端處於混合模式，也可以使用它。

當使用低於10.x的CUCM版本時，情況會變得更加複雜。如果您丟失或忘記其中一個令牌的密碼，您仍然可以使用另一個令牌運行具有當前CTL檔案的CTL客戶端。強烈建議獲取另一個eToken，並儘快將其新增到CTL檔案中以便進行冗餘。如果您丟失或忘記了CTL檔案中列出的所有eTokens的密碼，您需要獲得一對eTokens並運行一個手動過程，如下所述。

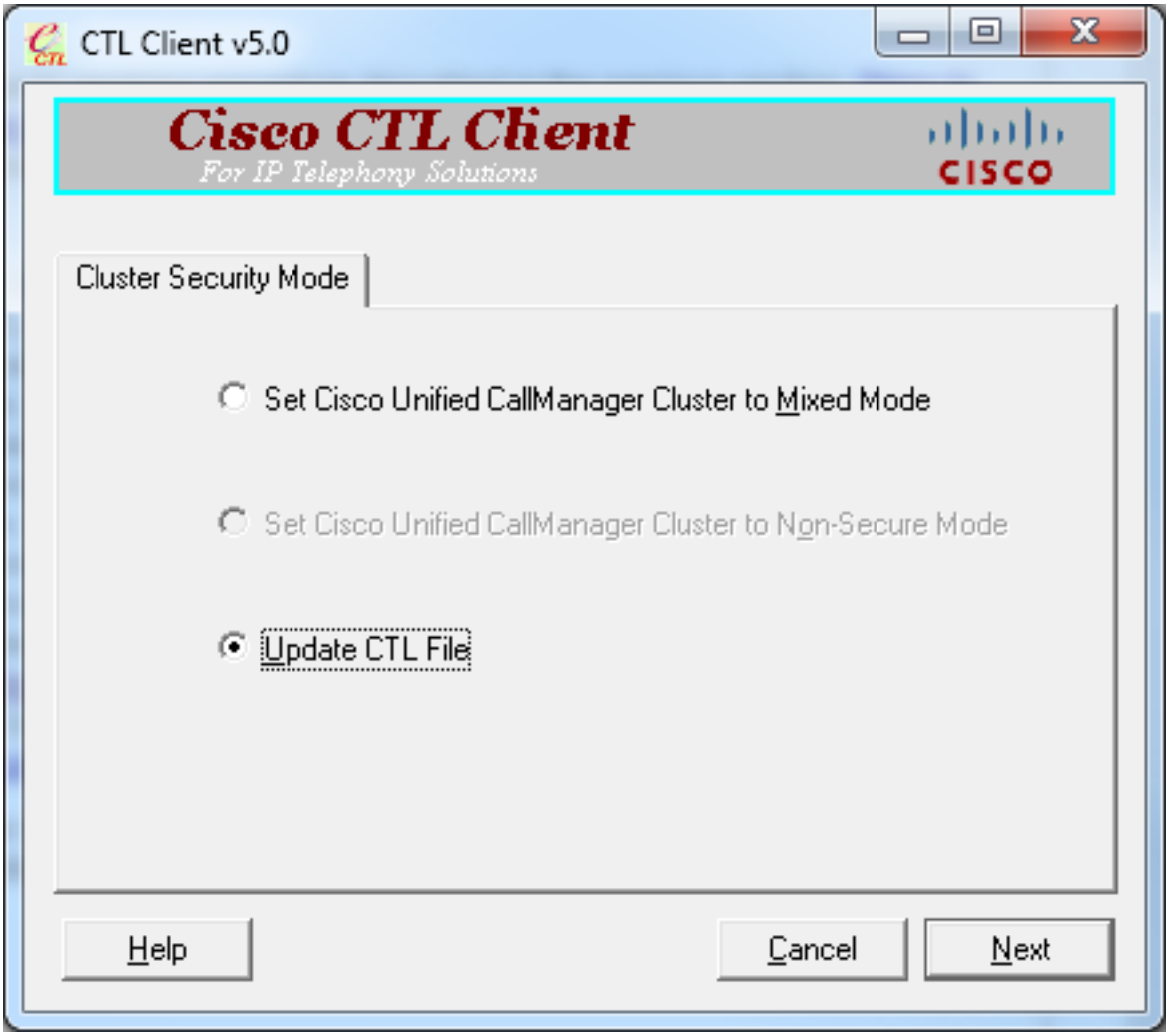
1. 輸入**file delete tftp CTLFile.tlv**命令以從所有TFTP伺服器中刪除CTL檔案。
```
admin:file delete tftp CTLFile.tlv
Delete the File CTLFile.tlv?
Enter "y" followed by return to continue: y
files: found = 1, deleted = 1

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. 運行CTL客戶端。輸入CUCM Pub的IP主機名/地址和CCM管理員憑據。按「**Next**」（下一步）。



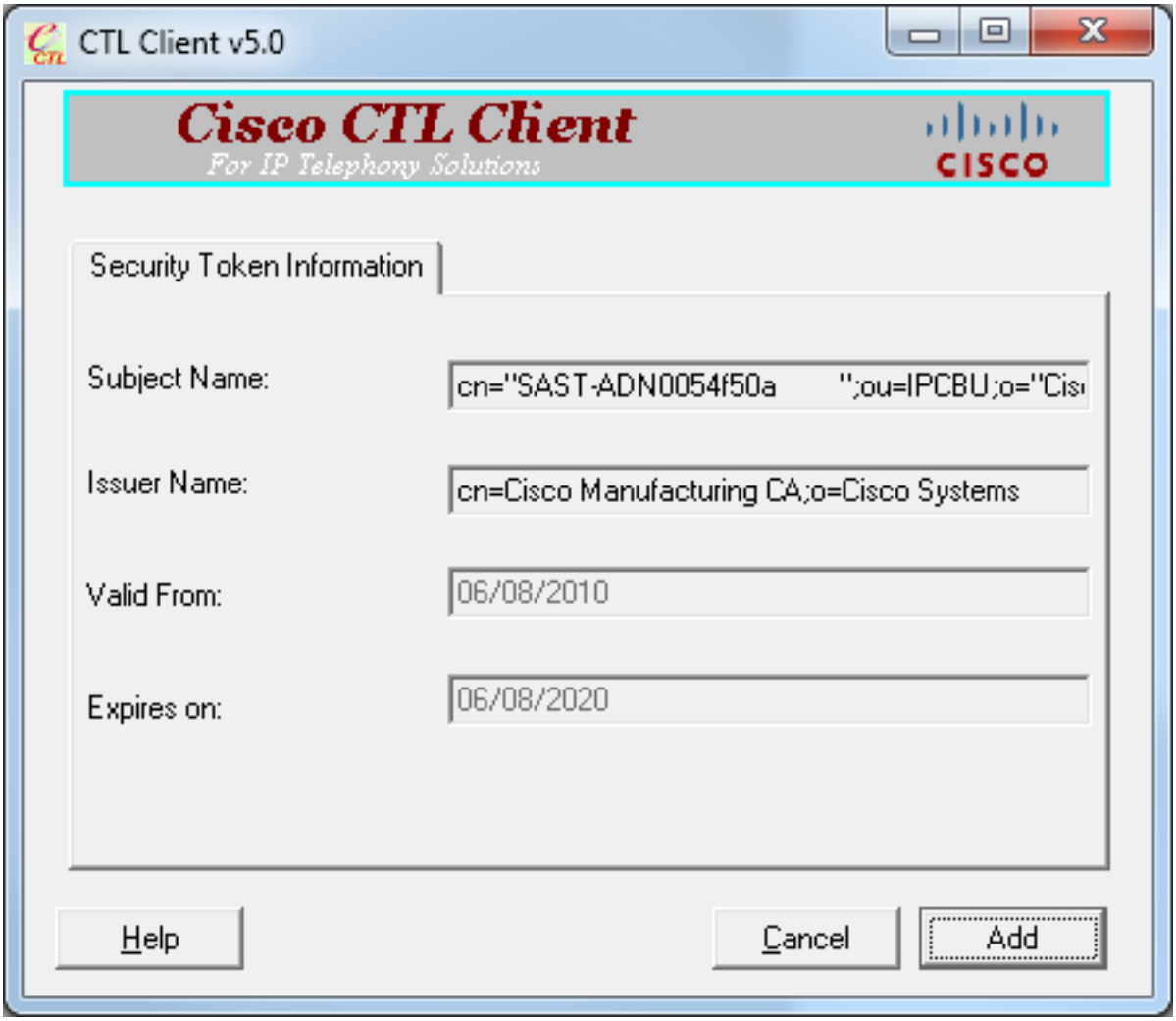
3. 由於群集處於混合模式，但Publisher上不存在CTL檔案，因此會顯示此警告。按一下「**OK**」以將其忽略並繼續操作。



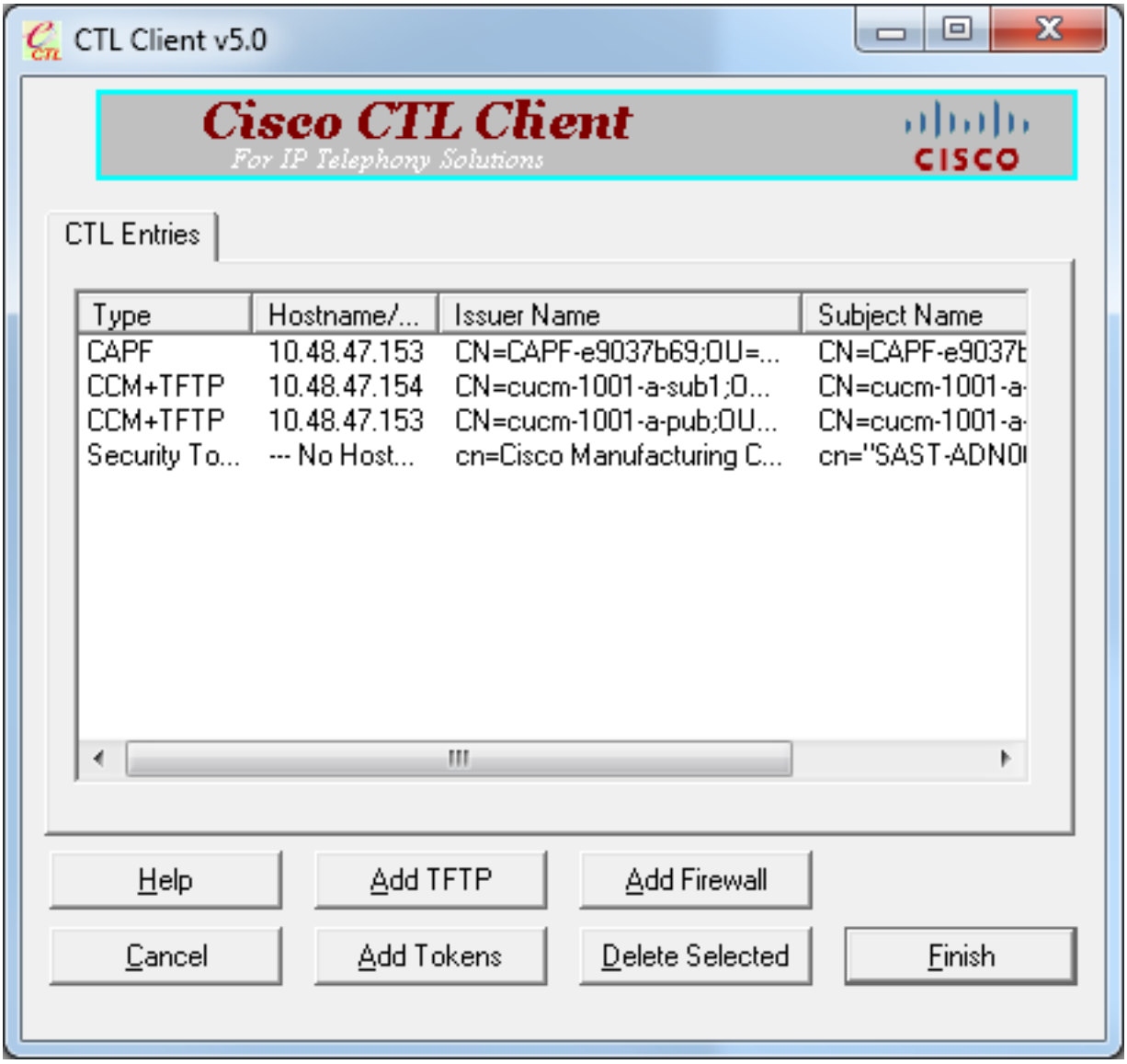
4. 按一下**Update CTL File**單選按鈕。按「**Next**」（下一步）。



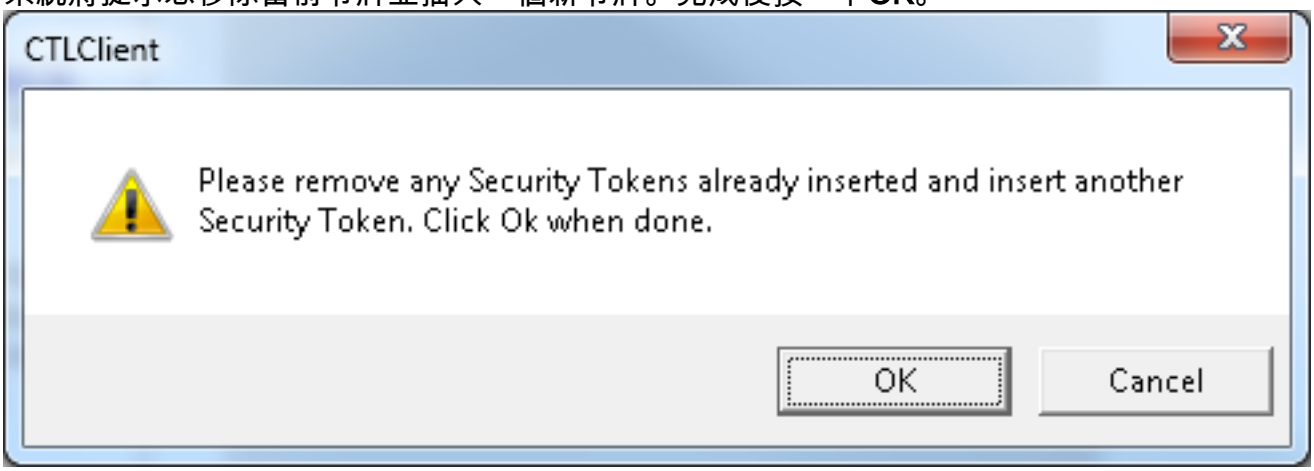
5. CTL客戶端請求新增安全令牌。按一下「Add」以繼續。



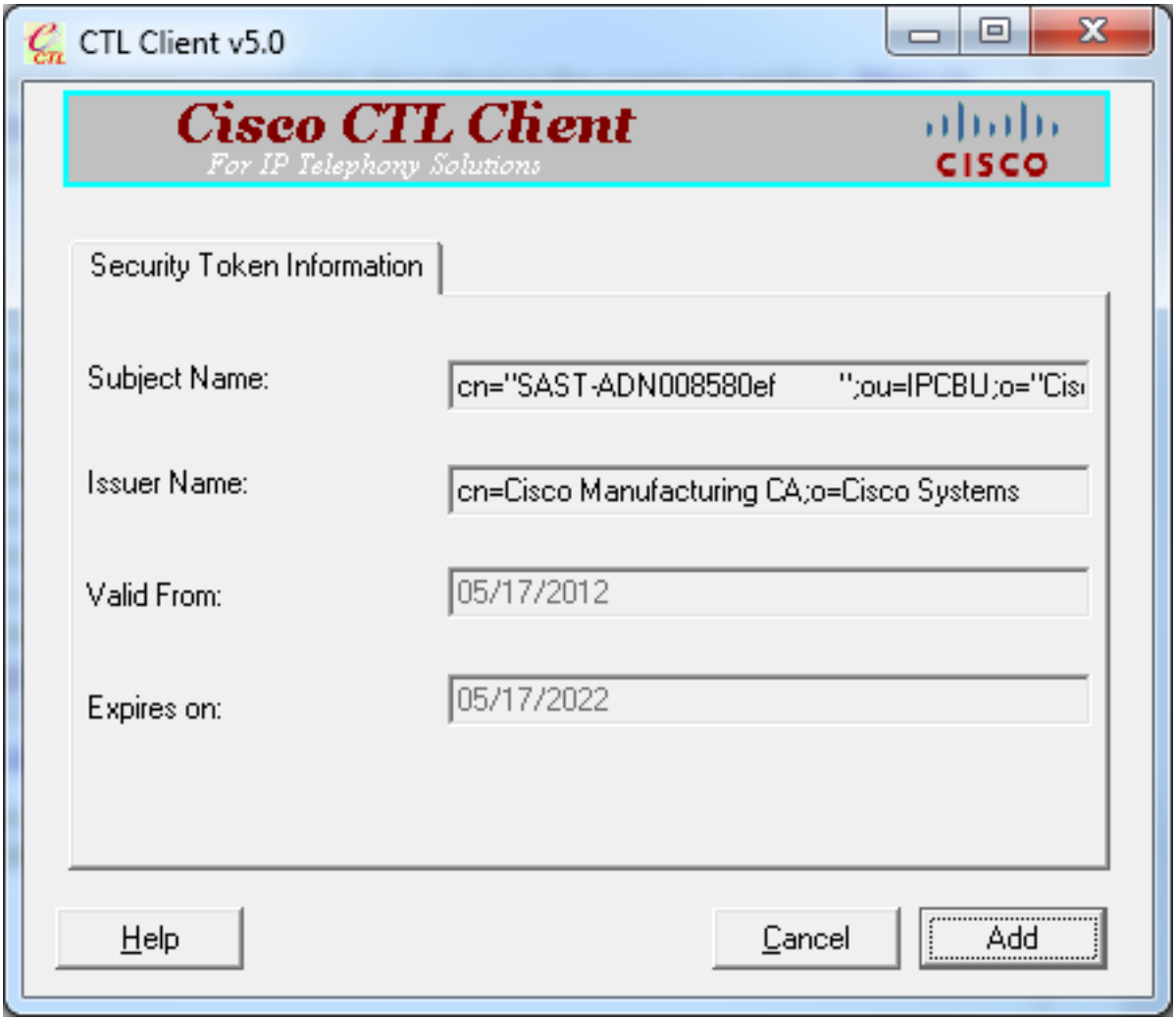
6. 螢幕將顯示新CTL中的所有條目。按一下**Add Tokens**以新增配對中的第二個權杖。



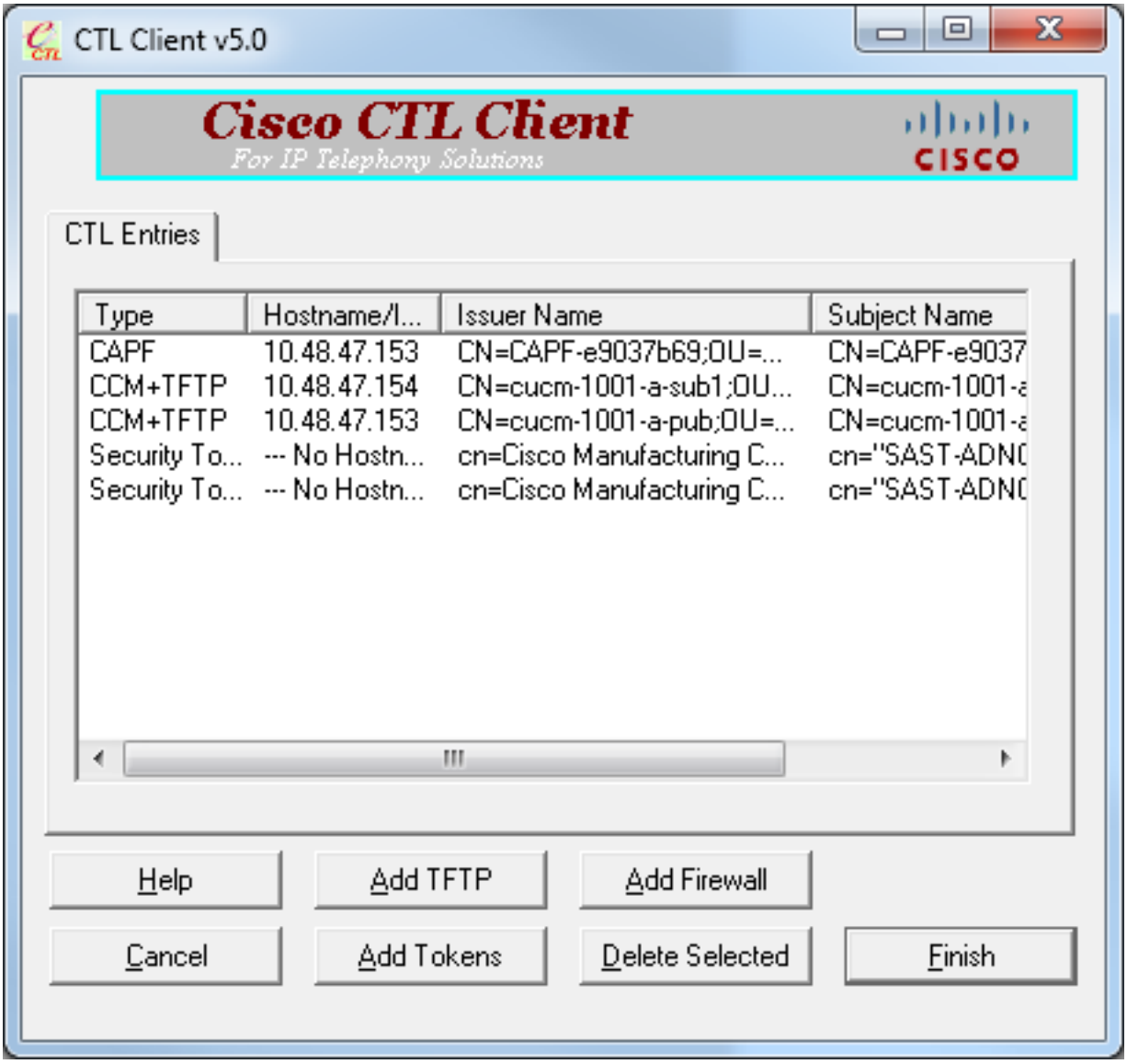
7. 系統將提示您移除當前令牌並插入一個新令牌。完成後按一下**OK**。



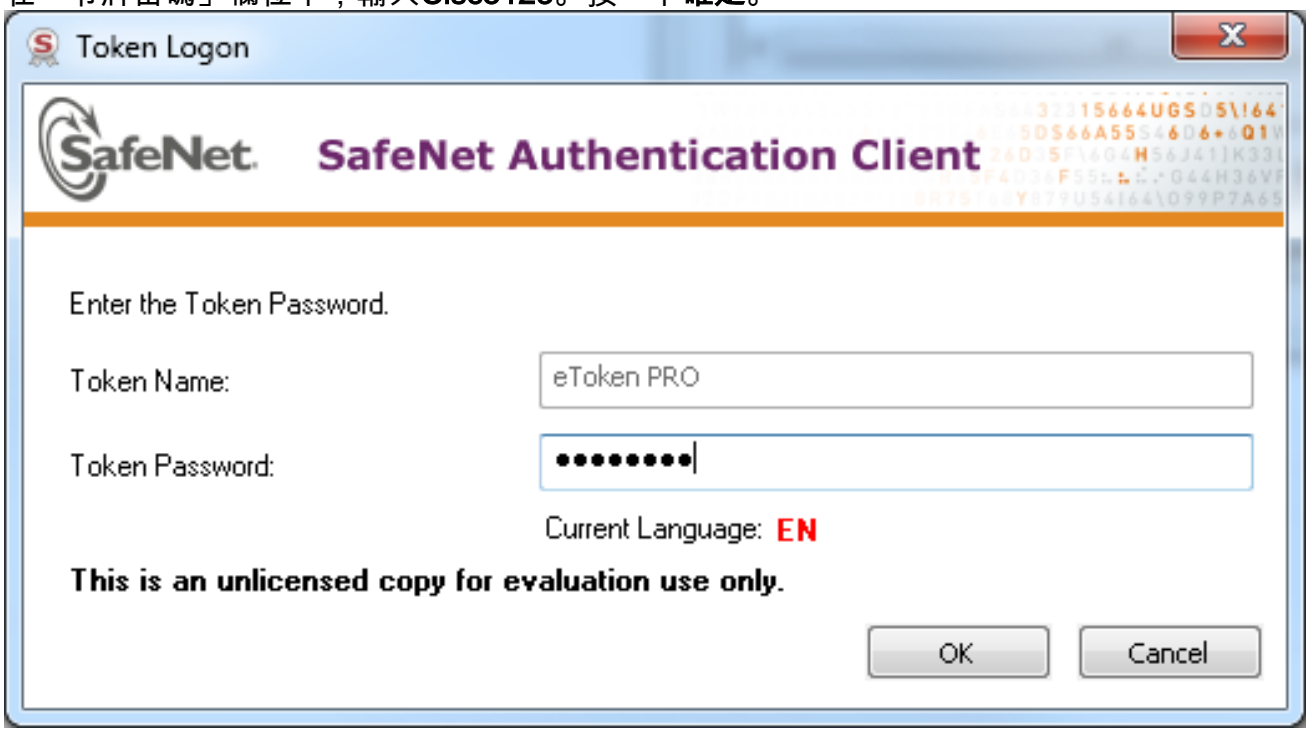
8. 此時將顯示一個螢幕，其中顯示新令牌的詳細資訊。按一下**Add**以確認和新增此權杖。



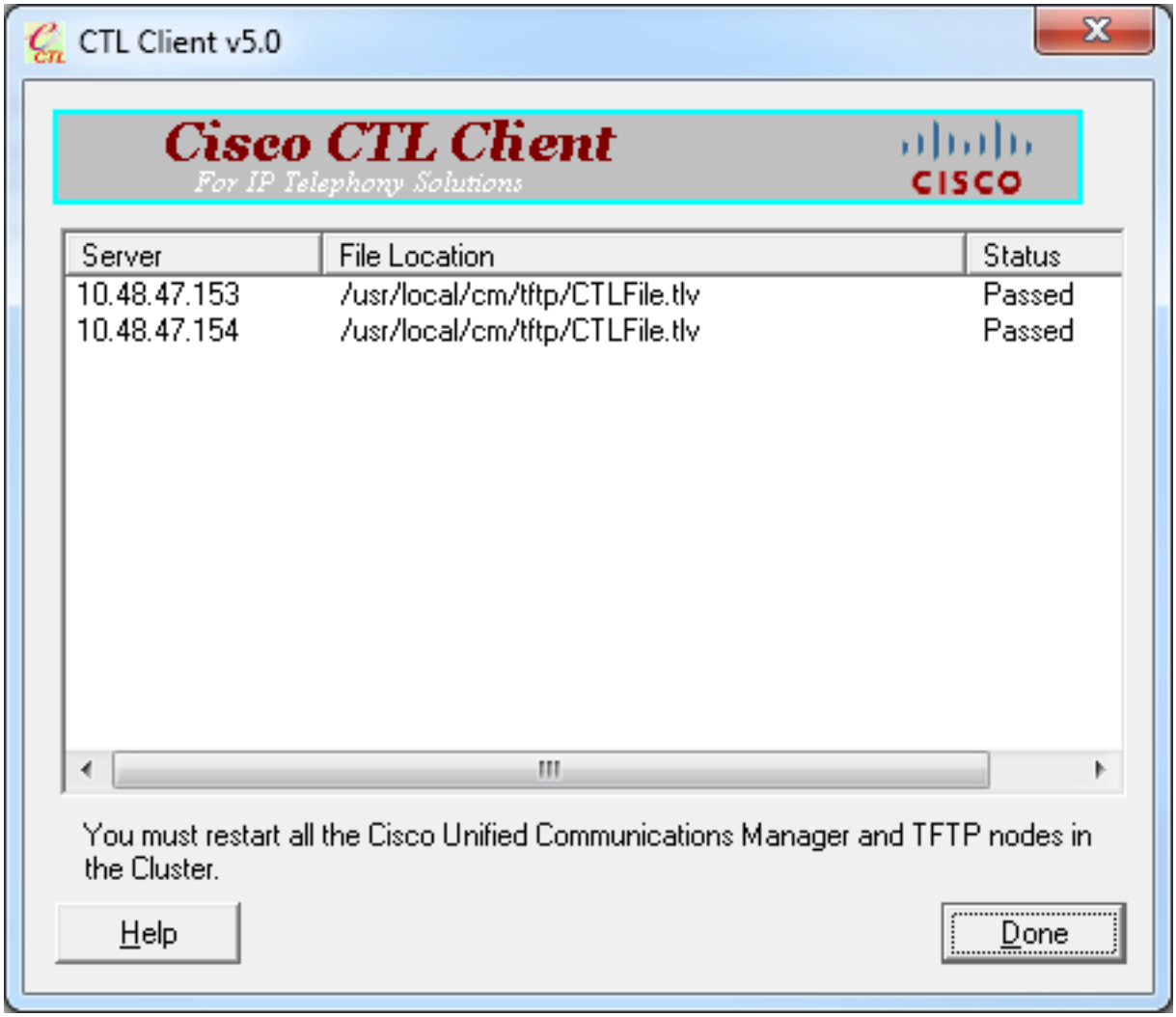
9. 您將看到顯示兩個已新增令牌的新CTL條目清單。按一下**完成**以生成新的CTL檔案。



10. 在「令牌密碼」欄位中，輸入**Cisco123**。按一下**確定**。



11. 您將看到流程已成功的確認。按一下「**Done**」以確認並退出CTL使用者端。



12. 重新啟動Cisco TFTP，然後啟動CallManager服務(Cisco Unified Serviceability > Tools > Control Center - Feature Services)。 應生成新的CTL檔案。輸入**show ctl**命令進行驗證。

```
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. 從群集中的每台電話上刪除CTL檔案(此過程可能因電話型別而異 — 請參閱文檔瞭解詳細資訊，例如Cisco Unified IP Phone 8961、9951和9971管理指南)。**附註**：電話可能仍可以註冊（取決於電話上的安全設定）並工作，而無需繼續執行步驟13。但是，電話將安裝舊的CTL檔案。如果重新生成證書、將其他伺服器新增到群集或更換伺服器硬體，則可能導致問題。建議不要將群集保持此狀態。
14. 將群集移至非安全。有關詳細資訊，請參閱使用CTL客戶端將CUCM群集安全從混合模式更改為非安全模式部分。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。