CUCM集群从混合模式更改为非安全模式配置示例

目录

简介

本文档介绍将Cisco Unified Communications Manager(CUCM)安全模式从混合模式更改为非安全模式所需的步骤。它还显示完成此移动后如何更改证书信任列表(CTL)文件的内容。

更改CUCM安全模式需要三个主要部分：

1a。运行CTL客户端并选择所需的安全模式变体。
1b。输入CLI命令以选择所需的安全模式变体。
2.在运行这些服务的所有CUCM服务器上重新启动Cisco CallManager和Cisco TFTP服务。
3.重新启动所有IP电话，以便它们可以下载CTL文件的更新版本。

> **注意：**如果集群安全模式从混合模式更改为非安全模式，则服务器和电话上仍存在CTL文件，但CTL文件不包含任何CCM+TFTP（服务器）证书。由于CTL文件中不存在CCM+TFTP（服务器）证书，因此这会强制电话在CUCM中注册为非安全。

先决条件

要求

思科建议您了解 CUCM 版本 10.0(1) 或更高版本的知识。此外，请确保：

- CTL提供程序服务已启动并在集群中的所有活动TFTP服务器上运行。默认情况下，服务在TCP端口2444上运行，但可以在CUCM服务参数配置中修改该服务。
- 证书颁发机构代理功能(CAPF)服务已启用并在发布器节点上运行。
- 群集中的数据库(DB)复制工作正常，服务器实时复制数据。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CUCM版本10.0.1.11900-2集群两个节点
- Cisco 7975 IP电话(使用瘦呼叫控制协议(SCCP)注册，固件版本SCCP75.9-3-1SR3-1S)
- 要将集群设置为混合模式，需要两个思科安全令牌
- 要将集群设置为非安全模式，需要使用之前列出的安全令牌之一

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

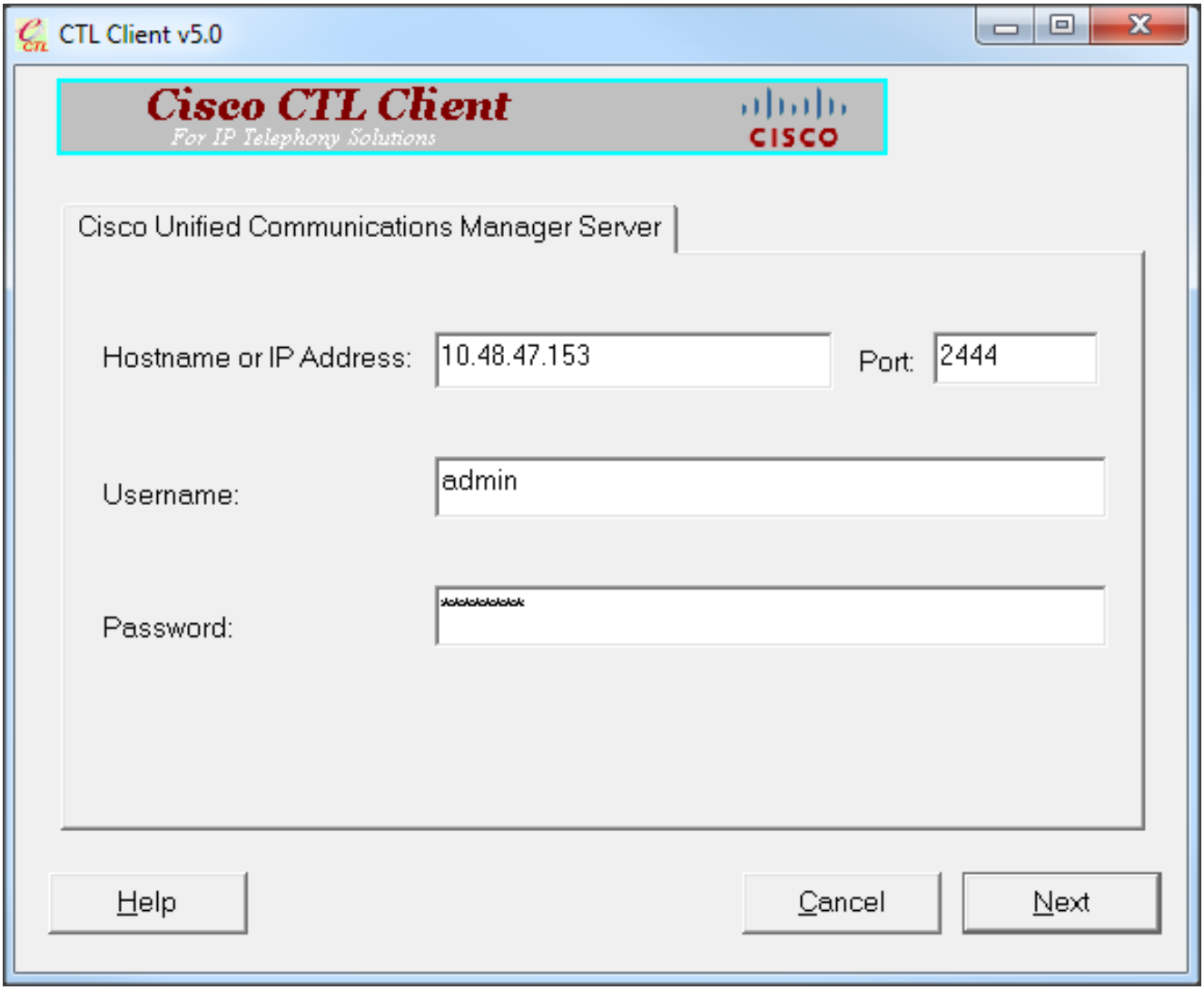
要运行CTL客户端插件，需要具有对至少一个安全令牌的访问权限，该安全令牌是为了创建或更新CUCM发布服务器上存在的最新CTL文件而插入的。换句话说，CUCM上当前CTL文件中至少有一个电子令牌证书必须位于用于更改安全模式的安全令牌上。

配置

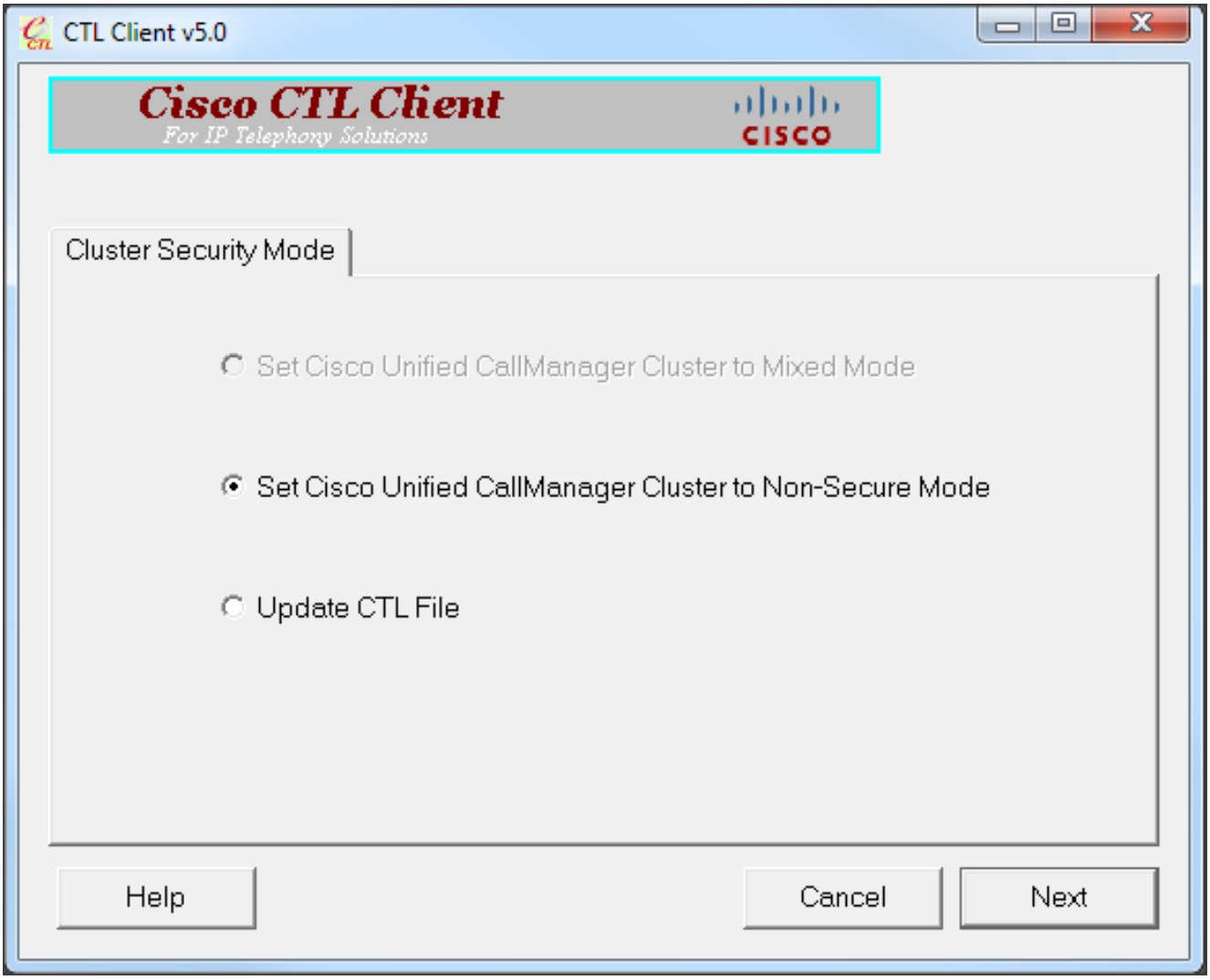
使用CTL客户端将CUCM集群安全从混合模式更改为非安全模式

要使用CTL客户端将CUCM集群安全性从混合模式更改为非安全模式，请完成以下步骤：

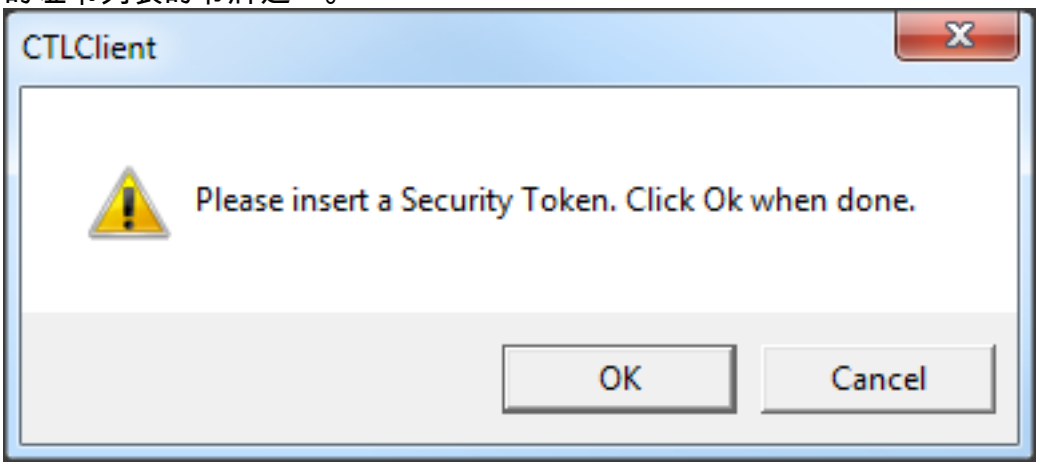
1. 获取一个您插入的安全令牌，以配置最新的CTL文件。
2. 运行CTL客户端。提供CUCM Pub的IP主机名/地址和CCM管理员凭证。单击 **Next**。



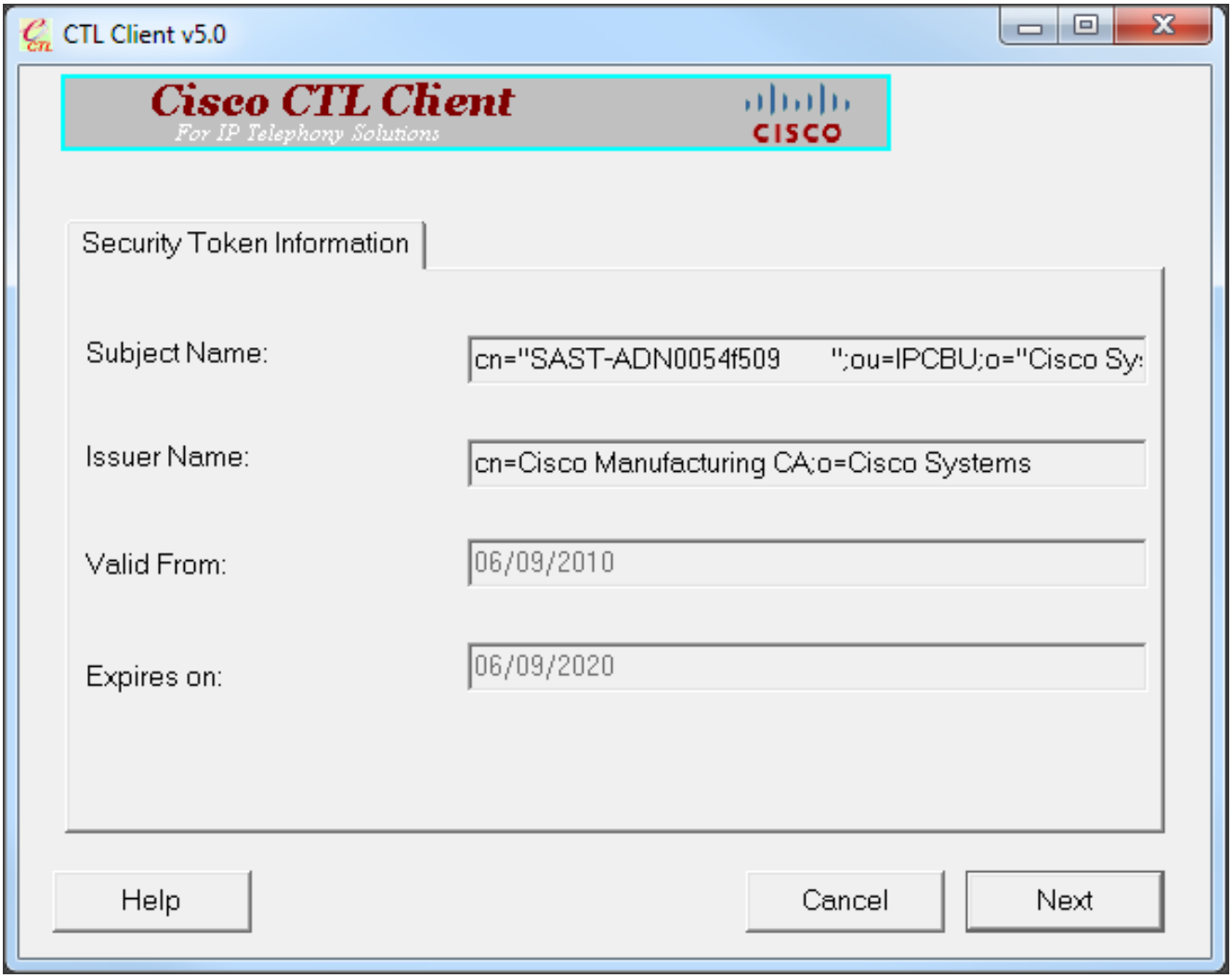
3. 单击Set Cisco Unified CallManager Cluster to Non-Secure Mode单选按钮。单击 Next。



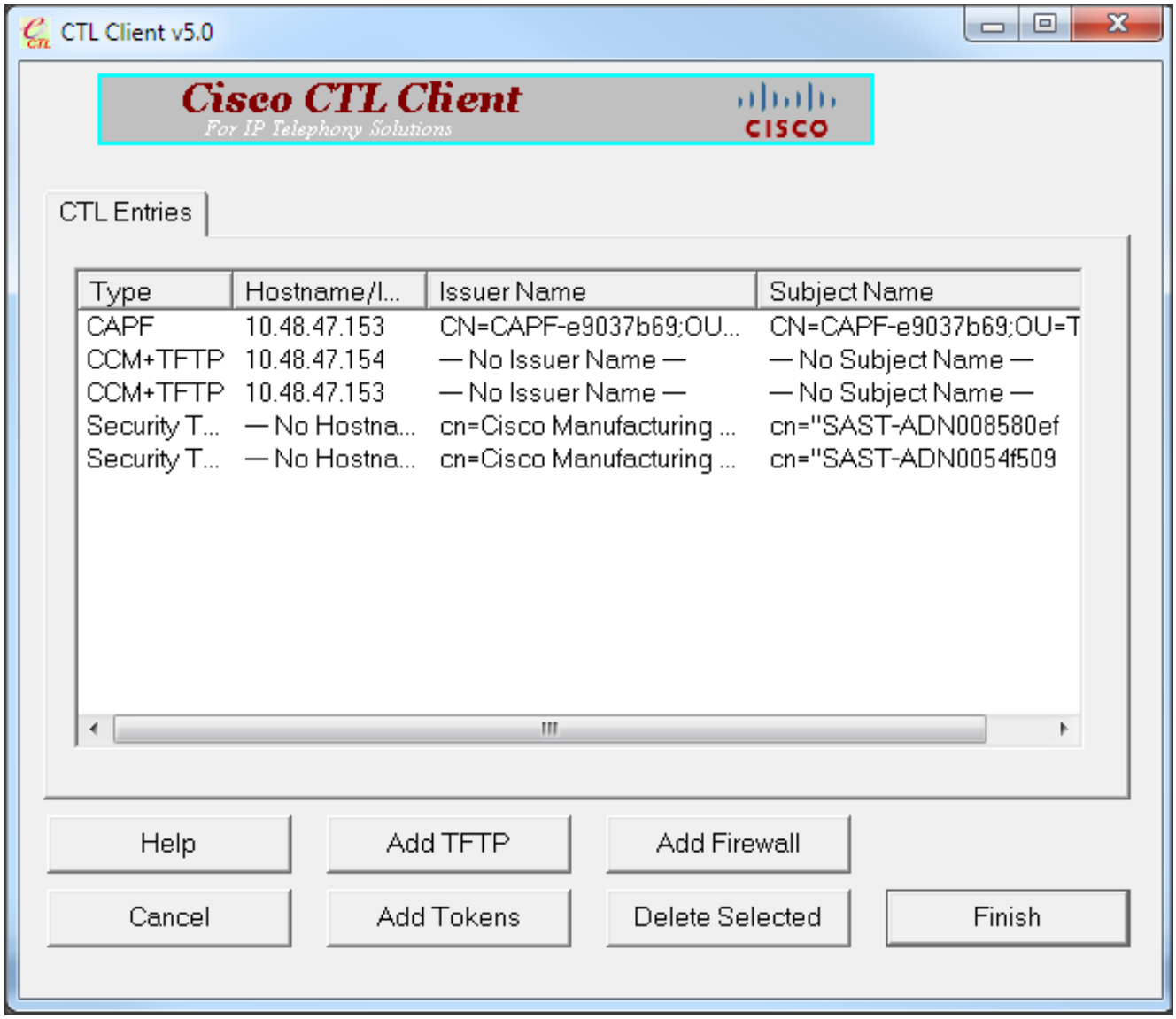
4. 插入一个插入的安全标记，以配置最新的CTL文件，然后单击**OK**。这是用于填充CTLFile.tlv中的证书列表的令牌之一。



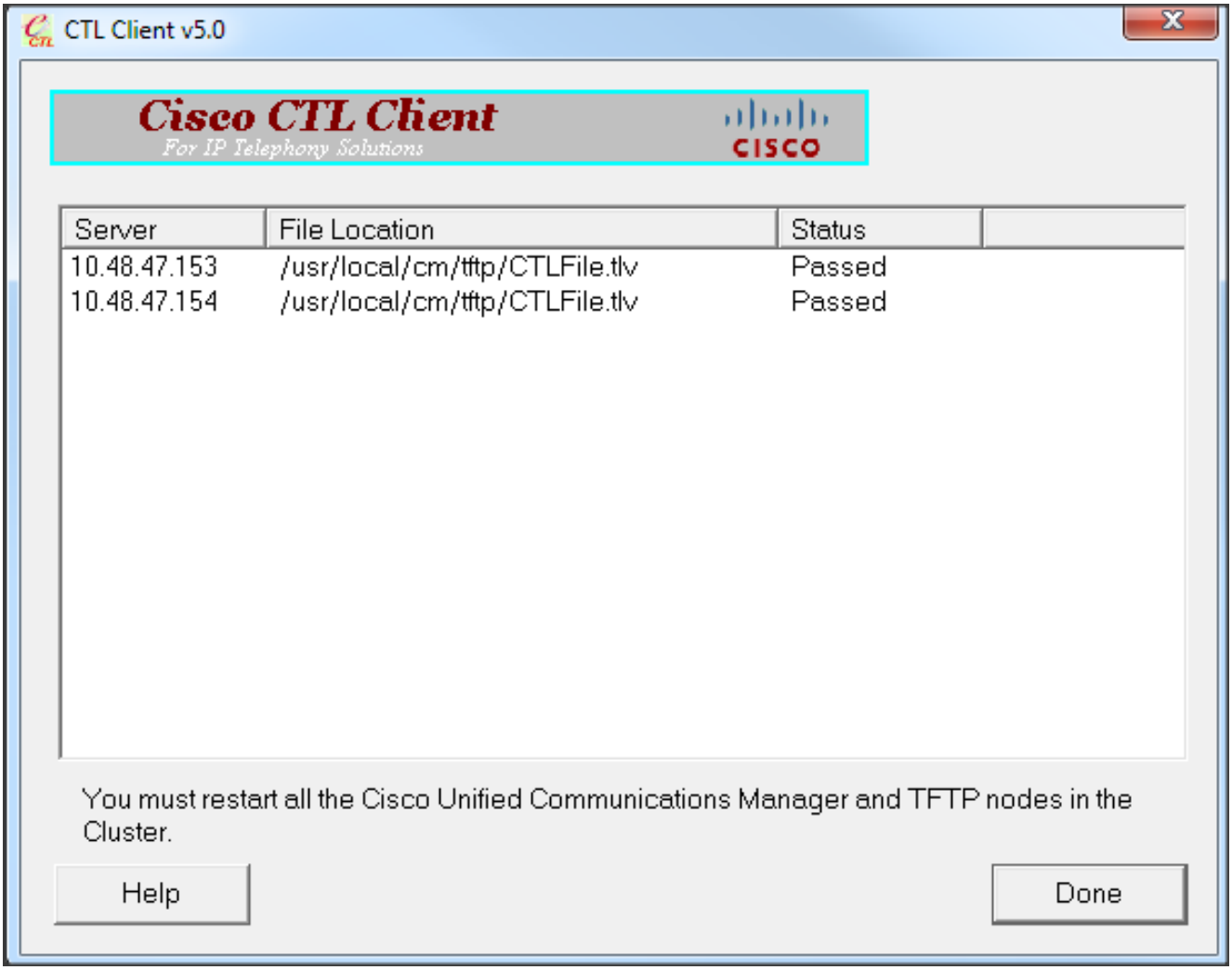
5. 系统将显示安全令牌详细信息。单击 **Next**。



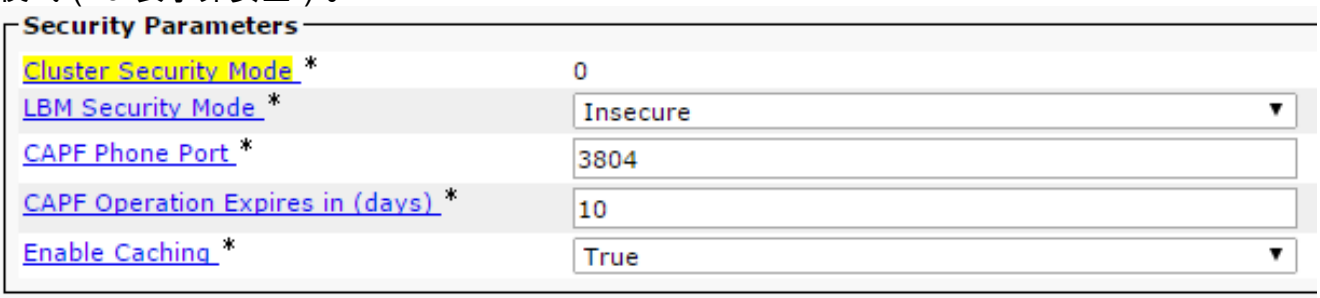
6. 显示CTL文件的内容。单击 **完成**。当提示输入口令时，输入**Cisco123**。



7. 显示CTL文件所在的CUCM服务器列表。单击**Done**。



8. 选择**CUCM Admin Page > System > Enterprise Parameters**，并验证集群是否设置为非安全模式（“0”表示非安全）。



9. 在运行这些服务的集群中的所有节点上重新启动TFTP和Cisco CallManager服务。
10. 重新启动所有IP电话，以便它们可以从CUCM TFTP获取新版本的CTL文件。

使用CLI将CUCM集群安全从混合模式更改为非安全模式

此配置仅适用于CUCM版本10.X及更高版本。要将CUCM集群安全模式设置为非安全，请在发布方CLI上输入**utils ctl set-cluster non-secure-mode**命令。完成后，在运行这些服务的集群中的所有节点上重新启动TFTP和Cisco CallManager服务。

以下是显示该命令的CLI输出示例。

```
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:
```

验证

使用本部分可确认配置能否正常运行。

为了验证CTLFIle.tlv，您可以使用以下两种方法之一：

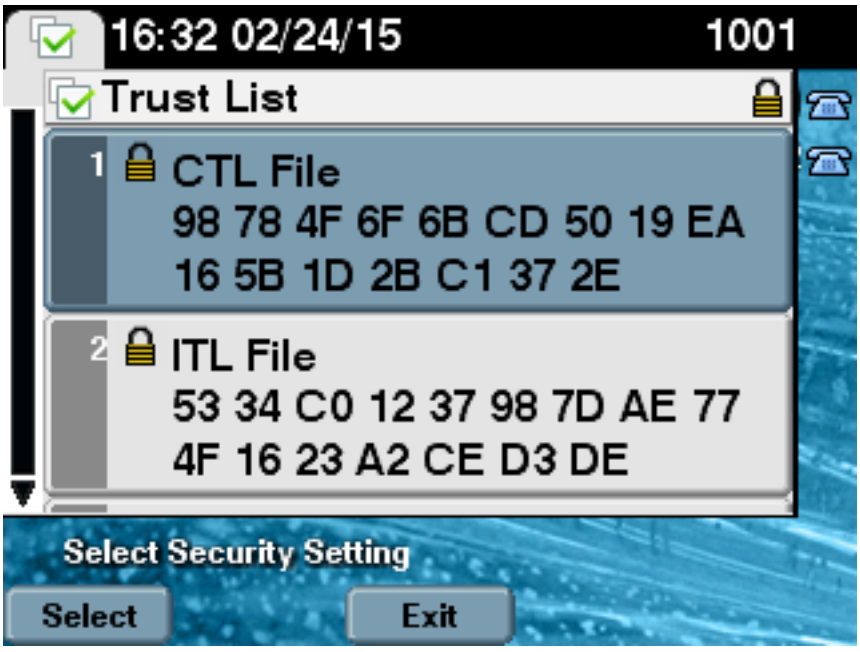
- 要验证CUCM TFTP端上存在的CTLFIle.tlv的内容和MD5校验和，请在CUCM CLI上输入**show ctl**命令。所有CUCM节点上的CTLFIle.tlv文件应该相同。
- 要验证7975 IP电话上的MD5校验和，请选择**设置>安全配置>信任列表> CTL文件**。

  注意：当您检查电话上的校验和时，您会看到MD5或SHA1，具体取决于电话类型。

CUCM集群设置为安全模式 — CTL文件校验和

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

在IP电话端，您可以看到安装了相同的CTL文件（与CUCM的输出相比，MD5校验和匹配）。



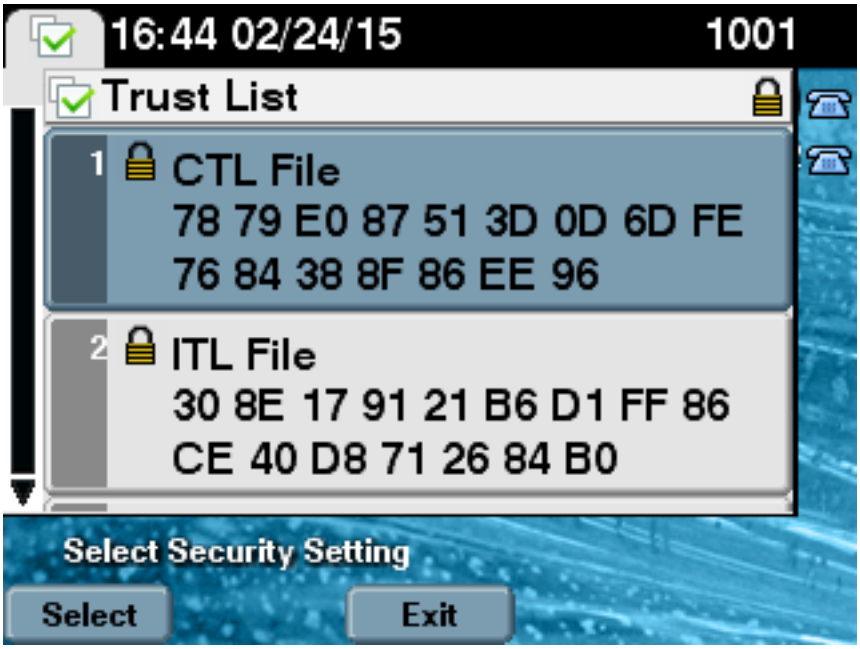
CUCM群集设置为非安全模式 — CTL文件内容

以下是CUCM集群中设置为非安全模式的CTL文件的示例。您可以看到CCM+TFTP证书为空，不包含任何内容。CTL文件中的其余证书没有更改，并且与CUCM设置为混合模式时完全相同。

```
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电话端，在重新启动并下载更新的CTL文件版本后，您可以看到，与CUCM的输出相比，MD5校验和匹配。



当USB标记丢失时，将CUCM集群安全从混合模式置于非安全模式

安全集群的安全令牌可能丢失。在这种情况下，您需要考虑以下两种情况：

- 集群运行版本10.0.1或更高版本
- 集群运行早于10.x的版本

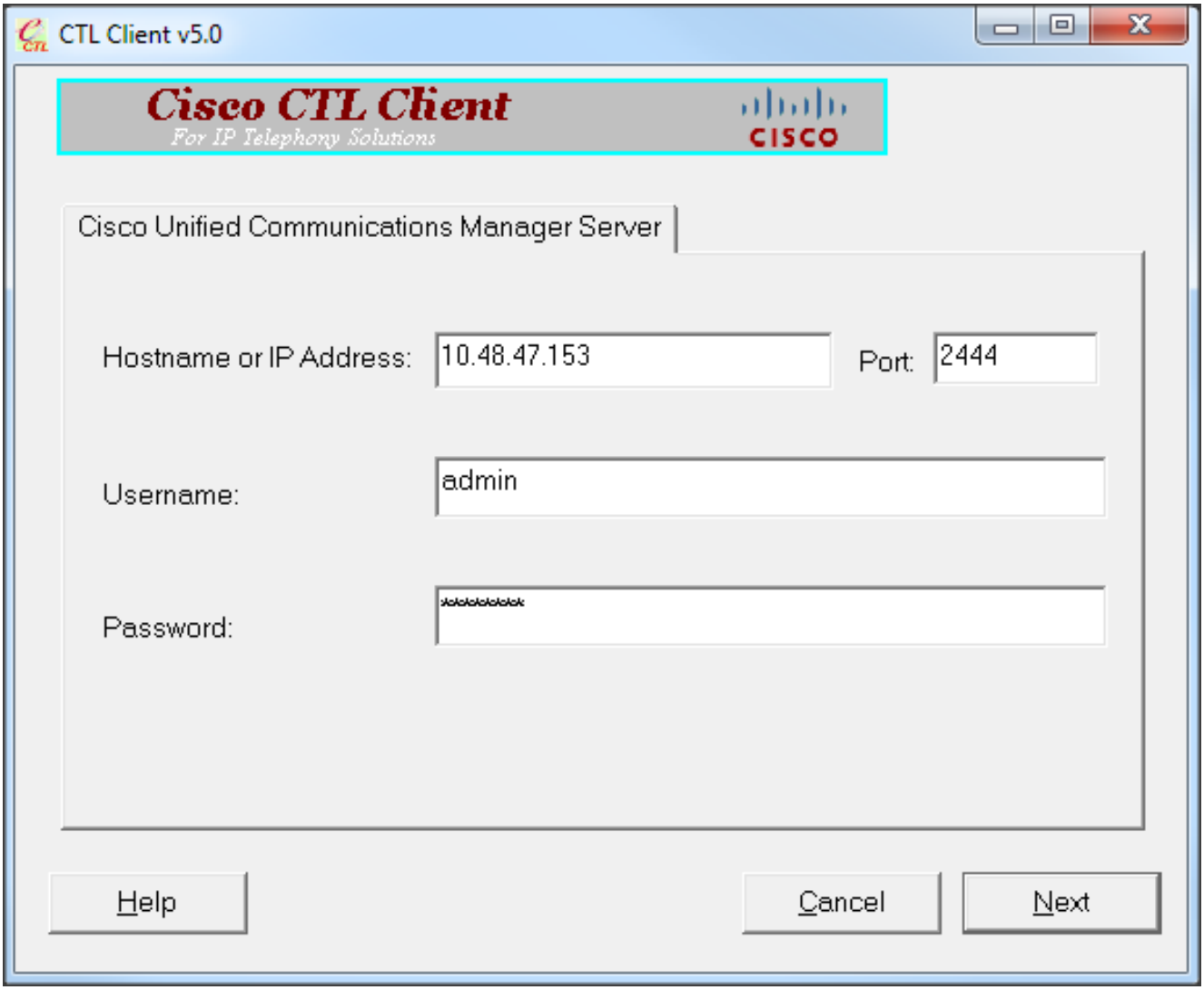
在第一个场景中，请使用CLI完成将CUCM集群安全性从混合模式更改为非安全模式部分中所述的过程，以便从问题中恢复。由于CLI命令不需要CTL令牌，因此即使集群与CTL客户端处于混合模式，也可使用它。

当使用早于10.x的CUCM版本时，情况会变得更加复杂。如果丢失或忘记其中一个令牌的密码，您仍然可以使用另一个令牌运行具有当前CTL文件的CTL客户端。强烈建议获取另一个eToken并尽快将其添加到CTL文件，以实现冗余。如果您丢失或忘记了CTL文件中列出的所有eTokens的密码，您需要获得新的一对eTokens并运行一个手动过程，如这里所述。

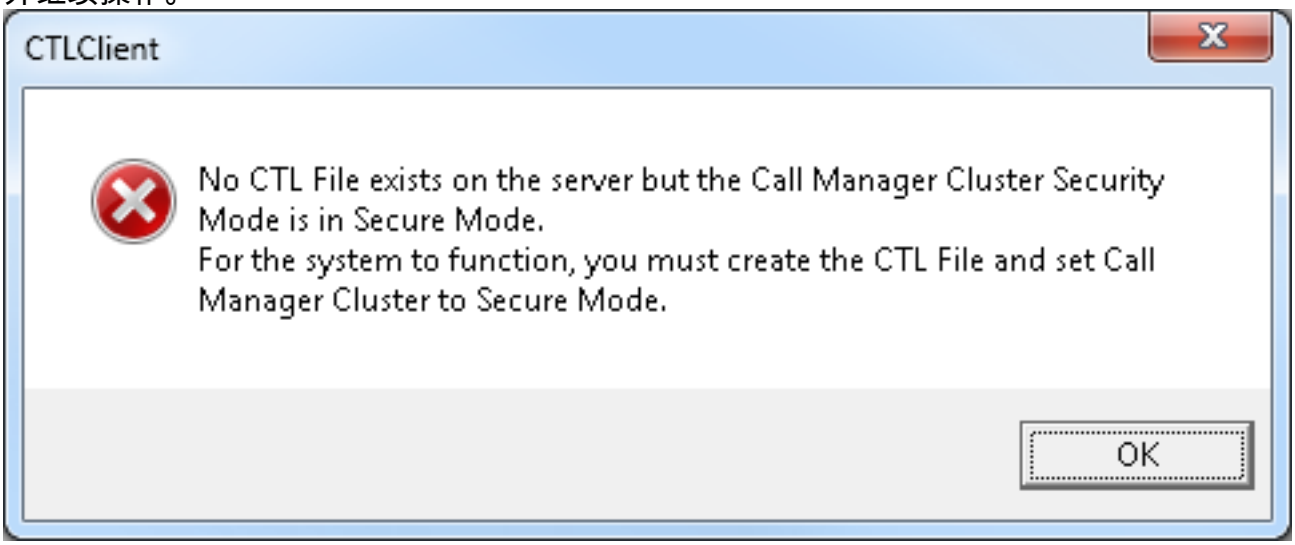
1. 输入**file delete tftp CTLFile.tlv**命令以从所有TFTP服务器中删除CTL文件。

```
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.
```

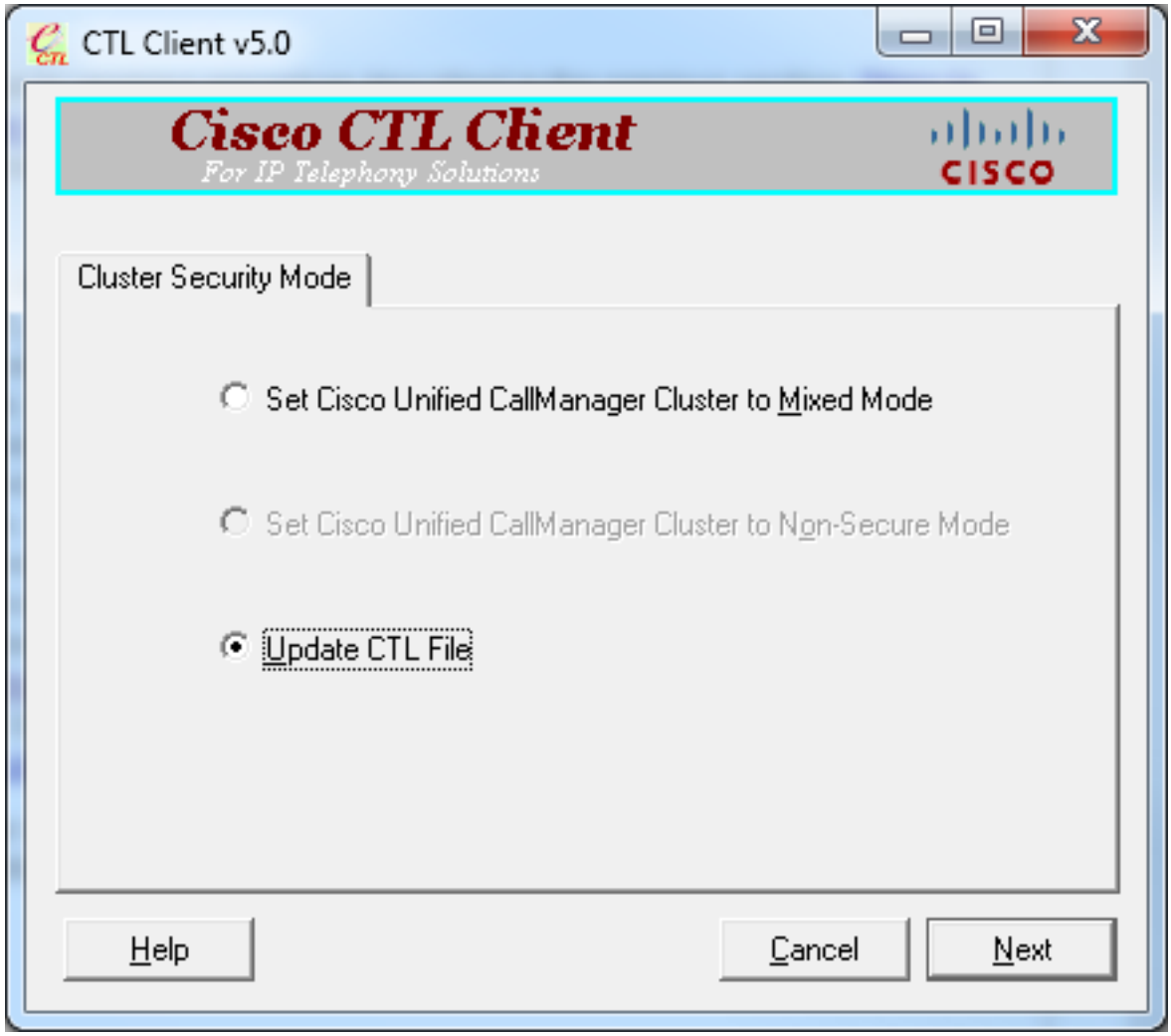
2. 运行CTL客户端。输入CUCM Pub的IP主机名/地址和CCM管理员凭证。单击 **Next**。



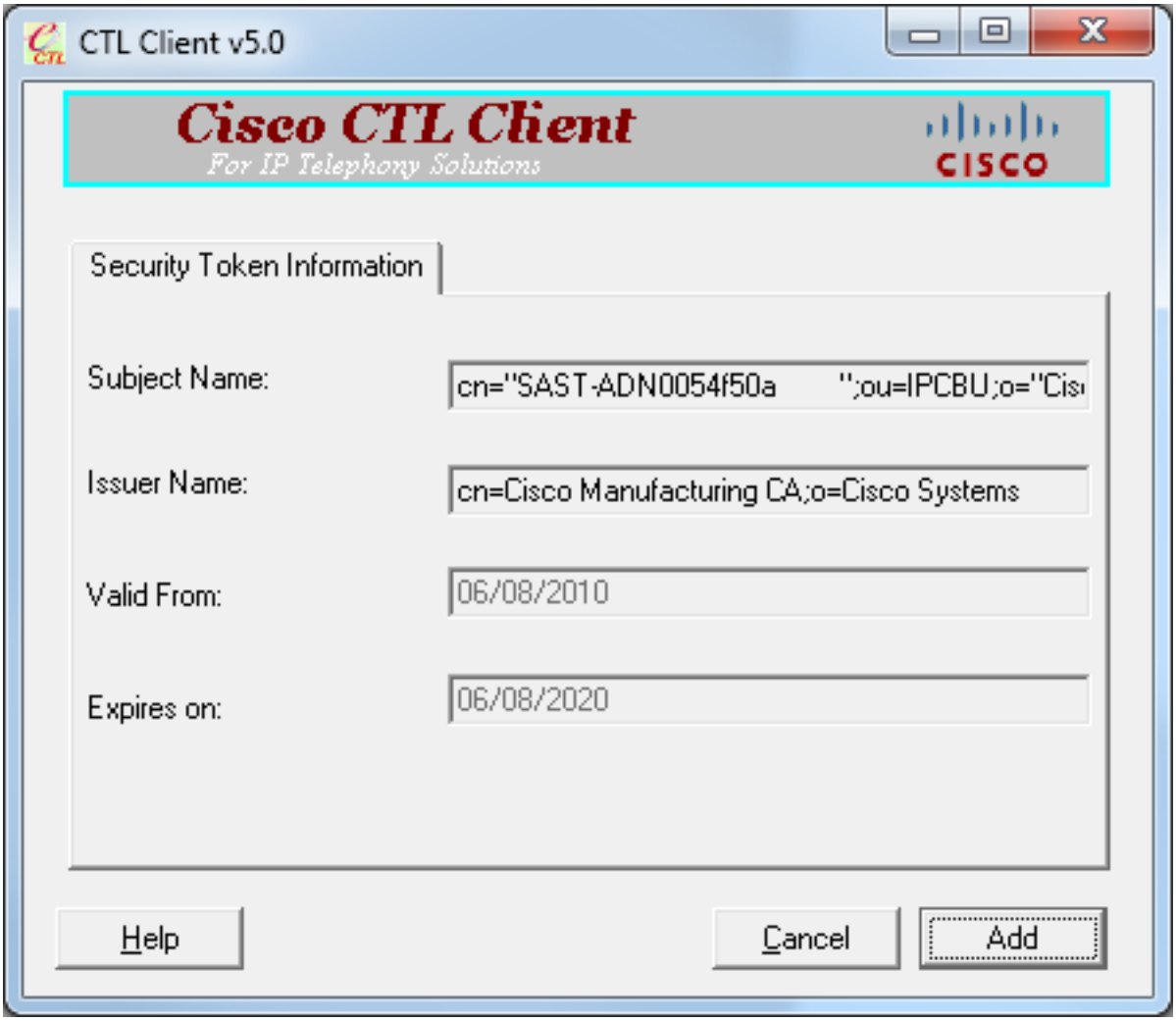
3. 由于集群处于混合模式，但Publisher上不存在CTL文件，因此显示此警告。单击**OK**以忽略它并继续操作。



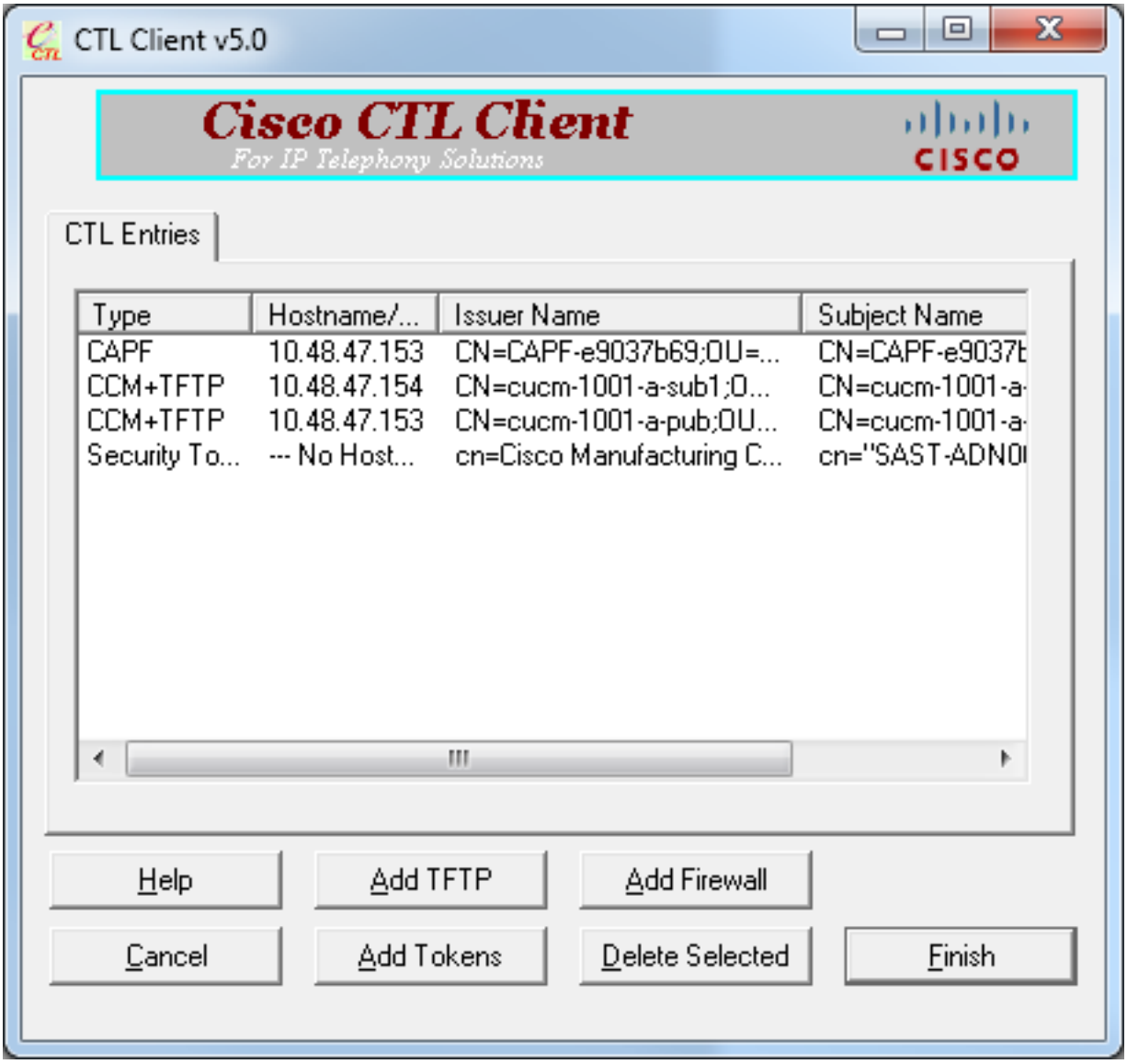
4. 单击**Update CTL File**单选按钮。单击 **Next**。



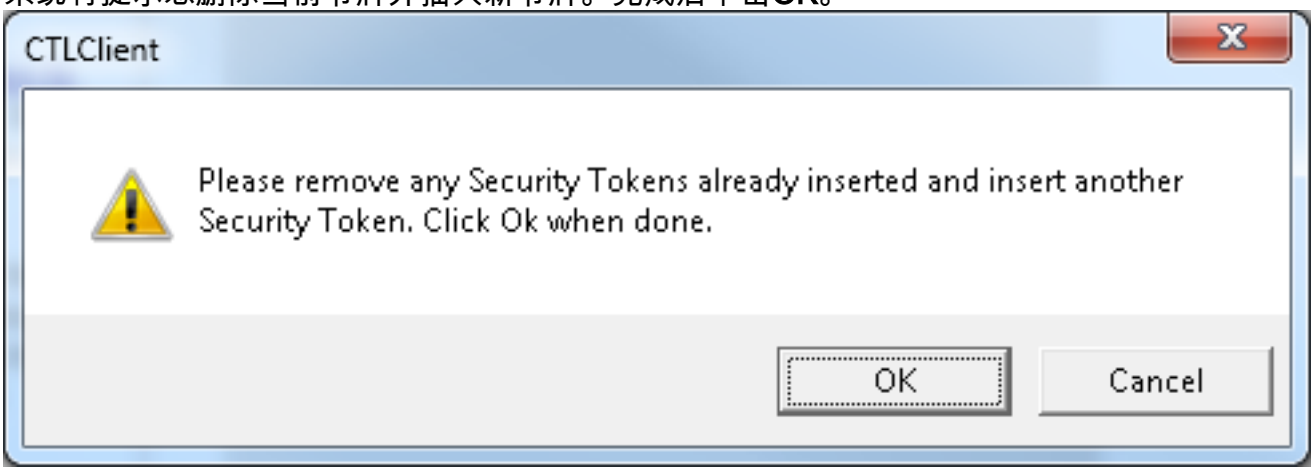
5. CTL客户端要求添加安全令牌。单击Add以继续。



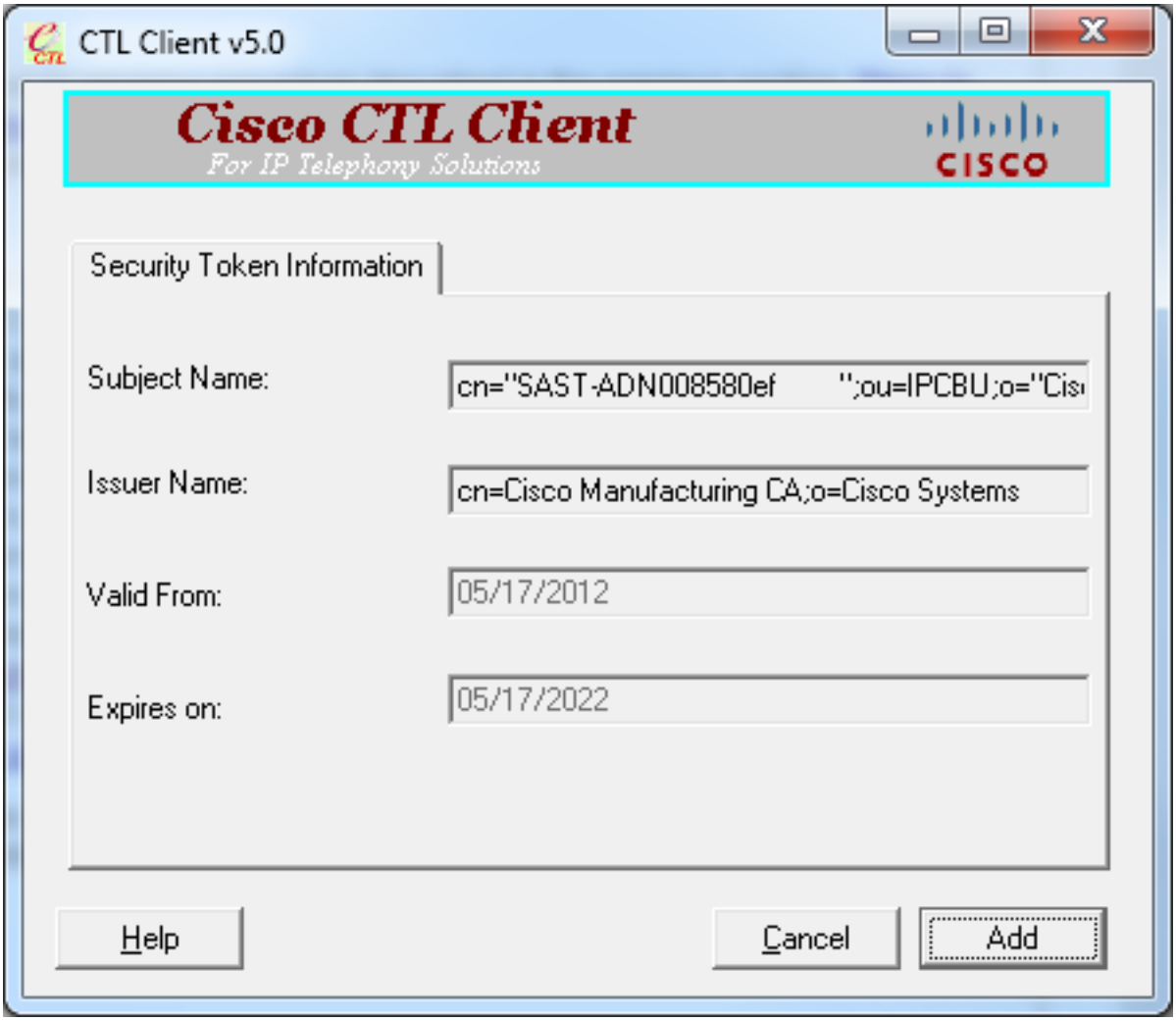
6. 屏幕将显示新CTL中的所有条目。单击**Add Tokens**以添加新对中的第二个令牌。



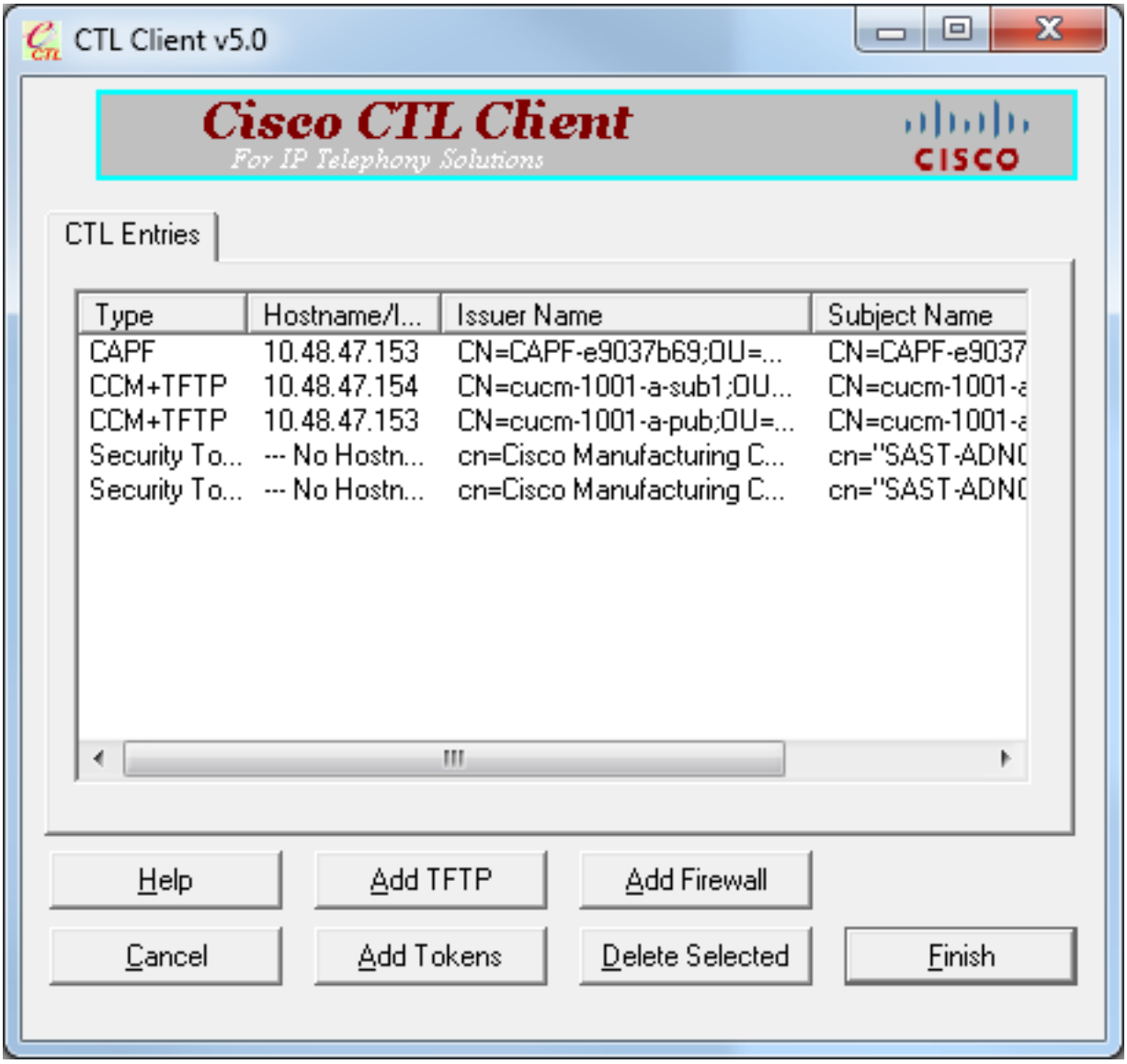
7. 系统将提示您删除当前令牌并插入新令牌。完成后单击**OK**。



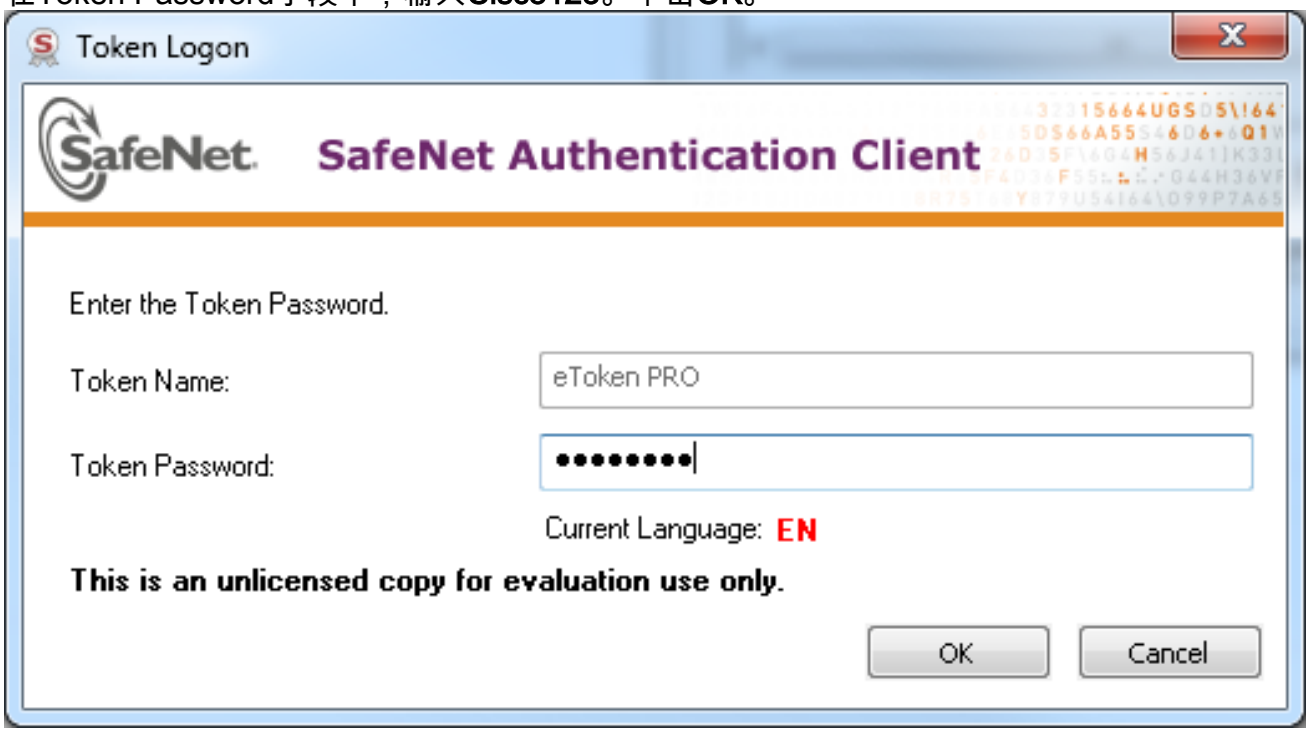
8. 系统将显示一个屏幕，其中显示新令牌的详细信息。单击**Add**以确认它们并添加此令牌。



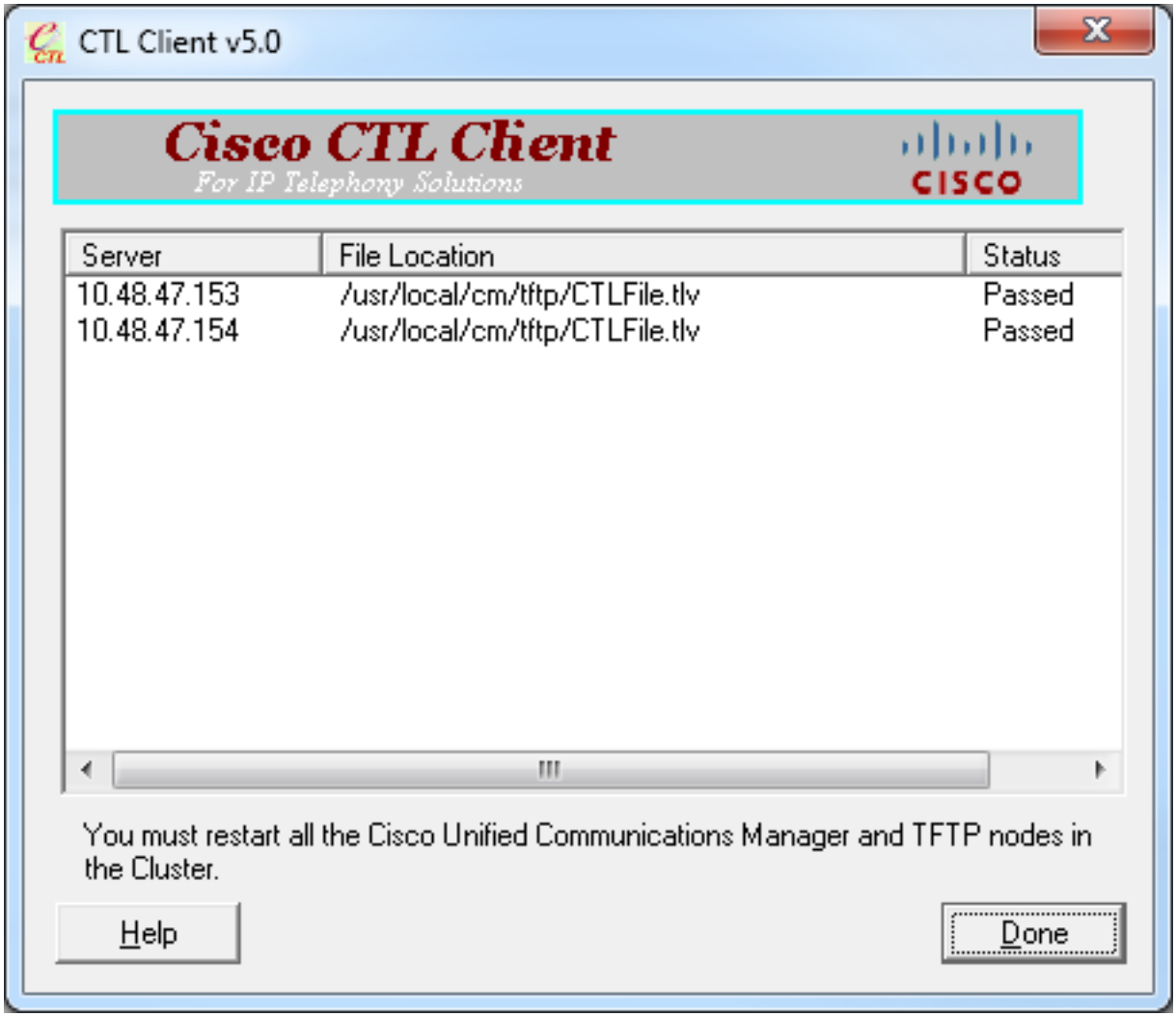
9. 您将看到显示两个已添加令牌的新CTL条目列表。单击**完成**以生成新的CTL文件。



10. 在Token Password字段中，输入**Cisco123**。单击**OK**。



11. 您将看到流程已成功的确认。单击**Done**以确认并退出CTL客户端。



12. 重新启动Cisco TFTP，然后重新启动CallManager服务(Cisco Unified Serviceability > Tools > Control Center - Feature Services)。 应生成新的CTL文件。输入**show ctl**命令进行验证。

```
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. 从集群中的每台电话上删除CTL文件(此过程可能因电话类型而异 — 有关详细信息，请参阅文档，例如Cisco Unified IP Phone 8961、9951和9971 Administration Guide)。**注意**：电话可能仍可以注册（取决于电话的安全设置）并且无需执行步骤13即可工作。但是，电话将安装旧的CTL文件。如果重新生成证书、向集群添加其他服务器或更换服务器硬件，则可能导致问题。建议不要将群集保持此状态。
14. 将集群移至Non-Secure。有关详细信息，请参阅使用CTL客户端将CUCM集群安全性从混合模式更改为非安全模式部分。

故障排除

目前没有针对此配置的故障排除信息。